TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA

RESOLUÇÃO N. 377/2022/TCE-RO

Dispõe sobre a Política Corporativa de Segurança da Informação e sobre o Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados do Tribunal de Contas do Estado de Rondônia.

O PRESIDENTE DO TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA, no uso das atribuições legais que lhe conferem os artigos 3º e 66, inciso I, da Lei Complementar n. 154, de 26 de julho de 1996, c/c o artigo 173, II, "b", do Regimento Interno do Tribunal de Contas do Estado de Rondônia;

CONSIDERANDO a importância de aprimorar e sistematizar em política as práticas institucionais relacionadas à segurança da informação e privacidade, que contribuem para assegurar o suporte necessário ao pleno exercício das funções do Tribunal de Contas do Estado de Rondônia;

CONSIDERANDO a hierarquia das políticas indicadas no Anexo A da NBR ISO/IEC 27003:2020, que prevê uma política de segurança da informação apoiada por políticas de tópicos específicos relacionados aos aspectos de segurança da informação e privacidade;

CONSIDERANDO a coleta, recepção, produção, utilização, arquivamento, armazenamento, transferência e a veiculação de informações essenciais ao exercício de 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 Tribunal de Contas do Estado de Rondônia 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 n. 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

CONSIDERANDO o advento da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), que 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;

CONSIDERANDO a Lei n. 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 n. 269/2018/TCERO que aprovou o Código de Ética dos Servidores do Tribunal de Contas do Estado de Rondônia;

CONSIDERANDO os termos da Resolução n. 287/2019/TCERO, que Instituiu o Comitê de Segurança da Informação e Comunicação 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 n. 123, de 30 de março de 2021, que aprovou a implantação do Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados, 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 Tribunal de Contas do Estado de Rondônia, além de adequar-se à Lei n. 13.709, de 14 de agosto de 2018, 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 Tribunal de Contas do Estado de Rondônia, 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 n. 355/2021/TCERO 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 do Estado de Rondônia e 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 na Corte;

CONSIDERANDO a necessidade de aprimorar os mecanismos de proteção e de segurança das informações, ativos e serviços de tecnologia da informação do Tribunal de Contas do Estado de Rondônia, 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, registrada no item 9.1.3 do Acórdão n. 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 a 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,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A Política Corporativa de Segurança da Informação do Tribunal de Contas do Estado de Rondônia (PCSI/TCERO) observa os princípios, objetivos e diretrizes estabelecidos nesta Resolução, orientando e apoiando a segurança da informação e privacidade no âmbito do Tribunal de Contas do Estado de Rondônia, em consonância com as disposições constitucionais, legais e regimentais vigentes.

§ 1º A alta administração do Tribunal de Contas do Estado de Rondônia está comprometida em estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação e privacidade no âmbito do Tribunal, apoiar o desenvolvimento de políticas de segurança da informação e privacidade, e o acréscimo de políticas específicas que auxiliem a PCSI/TCERO com a estruturação de controles de segurança para alcançar compliance com as regulamentações e legislações de proteção de dados.

§ 2º A PCSI/TCERO e as políticas específicas que auxiliam na execução do Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados (PCGSIPD/TCERO) serão submetidas à aprovação do Conselho Superior de Administração do Tribunal.

§ 3º A alta administração, servidores, colaboradores e quaisquer pessoas, inclusive advogados, que tenham acesso a informações do Tribunal de Contas do Estado de Rondônia sujeitam-se às diretrizes, normas e procedimentos de segurança da informação e privacidade da Política de que trata esta Resolução, sendo responsáveis por garantir a segurança das informações a que tenham acesso.

§ 4º A PCSI/TCERO compreende o conjunto de normas a serem seguidas em todas as atividades ligadas à Segurança da Informação e Privacidade.

§ 5º Integram, também, a PCSI/TCERO as medidas, os procedimentos e os controles destinados à proteção da informação e à disciplina de sua utilização.

§ 6º A PCSI/TCERO observa o respeito e promoção dos direitos e garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação.

§ 7º A alta administração do Tribunal de Contas do Estado de Rondônia está comprometida em garantir os recursos necessários para a execução desta Política Corporativa de Segurança da Informação e do Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados da Corte.

Art. 2º A segurança da informação, privacidade e proteção de dados pessoais no Tribunal de Contas do Estado de Rondônia se alinha com estratégias organizacionais e aos princípios da segurança institucional e tem como princípios:

I - garantia da integridade, da autenticidade e da privacidade das informações produzidas;

II - preservação da integridade, da autenticidade e da privacidade das informações recebidas;

III - transparência das informações públicas;

IV - proteção adequada às informações com necessidade de restrição de acesso;

V - planejamento das ações de segurança da informação e privacidade por meio de uma abordagem baseada em riscos; e

VI - garantia da disponibilidade e privacidade das informações custodiadas.

Parágrafo único. A segurança da informação, privacidade e proteção de dados pessoais no Tribunal de Contas do Estado de Rondônia abrange aspectos físicos, tecnológicos e humanos.

CAPÍTULO II

DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Art. 3º A Política Corporativa de Segurança da Informação (PCSI/TCERO), especificada em normativo do Colegiado do Tribunal, integra o Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados do Tribunal de Contas do Estado de Rondônia (PCGSIPD/TCERO) aprovado pela Portaria- TCERO n. 123, de 05 de abril de 2021, composto pelos seguintes eixos:

I - organização da segurança da informação e privacidade;

II - classificação da informação;

III - proteção de dados pessoais;

IV - controle de acesso à informação;

V - gestão de riscos de segurança da informação e privacidade;

VI - gestão de incidentes em segurança da informação e privacidade;

VII - segurança da informação em recursos humanos;

VIII - segurança em tecnologia da informação e comunicações;

IX - aquisição, desenvolvimento e manutenção de sistemas; e

X - segurança física e do ambiente.

§ 1º Os eixos do PCGSIPD/TCERO são interdependentes e devem ser estruturados e monitorados de forma a permitir sua melhoria contínua.

§ 2º A Gestão de Continuidade de Negócios (GCN), a ser disposta em política específica, harmoniza-se com os eixos do PCGSIPD/TCERO e tem por objetivo, em relação à segurança da informação e privacidade, garantir níveis adequados de disponibilidade, integridade, confidencialidade, autenticidade e privacidade das informações essenciais ao funcionamento dos processos críticos de negócio do Tribunal de Contas do Estado de Rondônia.

Art. 4º A organização da segurança da informação e privacidade, abordada na seção 6 da ABNT NBR ISO/IEC 27002:2013, tem por objetivo estabelecer uma estrutura organizacional de gerenciamento de processos para controlar a implementação, operação, revisão e melhoramento da segurança da informação e privacidade.

Parágrafo único. O Tribunal de Contas do Estado de Rondônia promoverá, com prioridade, estrutura administrativa com vistas a atender a efetiva concretização das políticas de segurança cibernética e segurança da informação, privacidade e proteção de dados pessoais, podendo, mediante legislação própria, criar ou reestruturar unidades internas.

Art. 5º A classificação da informação tem por objetivo assegurar que a informação receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a organização.

§ 1º A informação deve ser classificada para indicar a necessidade, prioridades e o nível esperado de proteção quanto ao tratamento da informação durante todo o seu ciclo de vida.

§ 2º O acesso às informações produzidas ou custodiadas pelo Tribunal de Contas do Estado de Rondônia, que não sejam públicas, deve permanecer restrito às pessoas que tenham necessidade de conhecê-las.

§ 3º O acesso a informações não públicas por quaisquer colaboradores deve estar condicionado ao aceite de termo confidencialidade.

§ 4º Serão objeto de normativo, diretrizes sobre acesso à informação e classificação da informação, bem como procedimentos de segurança e controles administrativos e tecnológicos afetos à classificação da informação de informações produzidas ou custodiadas pelo Tribunal de Contas do Estado de Rondônia.

Art. 6º A proteção de dados pessoais tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

§ 1º As diretrizes sobre a proteção de dados pessoais serão objeto de ato normativo específico.

§ 2º A proteção de dados pessoais deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular, harmonizados pela transparência.

Art. 7º O controle de acesso à informação, a ser disposto em norma regulamentar específica, tem por objetivo garantir que o acesso físico e lógico à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação e privacidade.

Art. 8º A gestão de riscos de segurança da informação e privacidade, a ser disposta em política específica, tem por objetivo identificar os riscos que possam comprometer a confidencialidade, a integridade, a disponibilidade a autenticidade ou a privacidade da informação, priorizando seu tratamento com base em critérios para aceitação de riscos compatíveis com os objetivos institucionais.

§ 1º Os controles de segurança da informação e privacidade devem ser planejados, aplicados, implementados e, periodicamente, testados e avaliados de acordo com os objetivos institucionais e os riscos para o Tribunal de Contas do Estado de Rondônia.

§ 2º O processo de gestão de riscos de segurança da informação e privacidade deve consistir na definição do contexto externo e interno, processo de avaliação de riscos, tratamento do risco, aceitação do risco, comunicação e consulta do risco, e ainda, monitoramento e análise crítica de riscos.

§ 3º O processo de gestão de risco de privacidade deve compreender os riscos relativos ao tratamento de dados pessoais (DP), identificando e avaliando os riscos para os titulares de DP, determinando os requisitos de salvaguarda de privacidade, identificando e implementando controles de privacidade para evitar ou reduzir os riscos para os titulares de DP, e, ainda, o monitoramento e análise crítica, acompanhamento dos riscos e controles, e o melhoramento do processo.

Art. 9º A gestão de incidentes de segurança da informação e privacidade, a ser disposta em política específica, tem por objetivo assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação e de privacidade, incluindo a comunicação sobre fragilidades e eventos de segurança da informação, a violação envolvendo dados pessoais, e ainda, a identificação e registro de incidentes para permitir tomada de decisão e ação de resposta em tempo hábil.

§ 1º O Tribunal de Contas do Estado de Rondônia deverá instituir uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), bem como, estabelecer as responsabilidades para receber, analisar e responder às notificações e atividades relacionadas

aos incidentes cibernéticos em sistemas computacionais e redes de dados no âmbito do Tribunal, para assegurar respostas rápidas, efetivas e ordenadas aos incidentes.

§ 2º A ETIR deverá ser composta por administradores de segurança, administradores de sistema, administradores de banco de dados, administradores de rede e analistas de suporte, todos integrantes do quadro de pessoal da Secretaria de Tecnologia da Informação e Comunicação, e, ainda, pelo encarregado de proteção de dados pessoais (DPO). A composição da equipe poderá ser estendida com a inclusão de representantes de áreas específicas, com conhecimento, habilidades e experiência técnica compatíveis com a missão da Equipe ou outros que o Tribunal de Contas do Estado de Rondônia entenda ser adequado.

§ 3° Os integrantes da ETIR serão indicados pelo Secretário de Tecnologia da Informação e Comunicação, e designados por ato da presidência do Tribunal de Contas do Estado de Rondônia.

§ 4º Os membros da ETIR, além das suas funções regulares, desempenharão as atividades relacionadas ao tratamento e respostas aos incidentes cibernéticos no Tribunal, a serem dispostas em norma específica.

§ 5º A ETIR deverá reportar, formalmente e imediatamente à unidade de segurança da informação, privacidade e proteção de dados pessoais, a ocorrência de todo o incidente que coloque em risco a segurança da informação e a privacidade, conforme normativo a ser definido pelo Tribunal de Contas do Estado de Rondônia, com vistas a permitir que sejam adotadas soluções integradas, objetivando minimizar vulnerabilidades e ameaças que possam comprometer a missão do Tribunal.

§ 6º As Autoridades, servidores e quaisquer colaboradores do Tribunal são responsáveis por:

I – informar imediatamente à unidade responsável pela segurança da informação, privacidade e proteção de dados pessoais, à unidade especializada em segurança cibernética e ao encarregado de proteção de dados pessoais (DPO) os incidentes em segurança da informação de que tenham ciência ou suspeita, conforme normativo a ser definido pelo Tribunal de Contas do Estado de Rondônia; e

II - colaborar, na respectiva área de competência, na identificação e no tratamento de incidentes em segurança da informação e privacidade.

Art. 10. A segurança da informação em recursos humanos, a ser disposta em política específica, tem por objetivo garantir que quaisquer pessoas que tenham vínculo estatutário, funcional, contratual ou processual com o Tribunal de Contas do Estado de Rondônia entendam suas responsabilidades e atuem em consonância com os preceitos da PCSI/TCERO, para que o risco de furto, vazamento, fraude ou mau uso de informações seja reduzido.

§ 1º A conscientização em segurança da informação e privacidade tem por objetivo internalizar conceitos e boas práticas de segurança da informação e privacidade na cultura organizacional do Tribunal de Contas do Estado de Rondônia, por meio de ações permanentes de divulgação, treinamento e educação, para minimizar riscos de segurança da informação.

§ 2º A segurança da informação em recursos humanos e a conscientização em segurança da informação e privacidade se alinham, no que couber, ao disposto na Política de Gestão de Pessoas do Tribunal definida pela Resolução n. 307/2019/TCERO, às diretrizes contidas no Plano de Segurança Institucional disposto na Resolução n. 197/2015/TCERO, e, ainda, aos termos da Resolução n. 333/2020/TCERO, que dispõe sobre ações educacionais no âmbito da Escola Superior de Contas.

Art. 11. A segurança em tecnologia da informação e comunicações tem por objetivo adotar medidas e controles tecnológicos para proteger as informações em meio eletrônico, e, ainda, assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam, mantendo a segurança da informação transferida dentro do Tribunal e com quaisquer entidades externas.

§ 1º As diretrizes e os procedimentos para o uso de recursos de tecnologia, tais como sistemas de informação, computadores, dispositivos móveis e pessoais, teletrabalho e mídias sociais, computação em nuvem (cloud computing), sujeitam-se, no que couber, aos comandos da PCSI/TCERO e serão objeto de políticas específicas no âmbito do TCE-RO.

§ 2º Os recursos de tecnologia da informação de propriedade do Tribunal de Contas do Estado de Rondônia são fornecidos para uso corporativo, para os fins a que se destinam e no interesse da administração, estando sujeito o seu uso a monitoramento e auditoria, e que os registros assim obtidos poderão ser utilizados para detecção de violações desta PCSI/TCERO e demais regulamentações em vigor.

§ 3º O acesso às informações produzidas ou custodiadas pelo Tribunal de Contas do Estado de Rondônia se submete a controles administrativos e tecnológicos definidos de acordo com a respectiva classificação.

§ 4º A utilização dos recursos de Tecnologia da Informação e Comunicação da rede do Tribunal de Contas do Estado de Rondônia é monitorada e controlada pela Secretaria de Tecnologia da Informação e Comunicação, responsável pela infraestrutura de TIC, com vistas a identificar inobservâncias à PCSI/TCERO e a fornecer evidências, no caso de incidentes de segurança da informação e privacidade, respeitados os direitos e as garantias individuais previstos em lei.

Art. 12. A aquisição, desenvolvimento e manutenção de sistemas, a ser disposta em política específica, tem por objetivo garantir que a segurança da informação e privacidade sejam parte integrante de todo o ciclo de vida dos sistemas de informação, e que as exigências relacionadas à segurança da informação e privacidade sejam incluídas nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.

§ 1º Na aquisição de novos sistemas deverá ser seguido um processo formal de aquisição e teste, objetivando avaliar as funcionalidades da segurança no produto proposto, identificando os requisitos e o risco associado antes da sua compra.

§ 2º Durante todo o ciclo de vida de desenvolvimento e manutenção de sistemas de informação deverá se aplicar os conceitos de Privacy by Design e Privacy by Default, objetivando assegurar que os processos e sistemas incorporem a privacidade e a proteção de dados

pessoais desde a sua concepção, e que sejam projetados de tal forma que a coleta e o tratamento (incluindo o uso, divulgação, retenção, transmissão e descarte) de dados pessoais estejam limitados a um mínimo que seja adequado, relevante, proporcional e necessário para os propósitos identificados.

§ 3º Durante todo o ciclo de vida de desenvolvimento e manutenção de sistemas de informação deverá se aplicar os conceitos de Security by Design, objetivando incorporar boas práticas de segurança da informação para diminuir as vulnerabilidades desde o início do desenvolvimento de software, e para que haja uma relação de trabalho positiva entre os desenvolvedores e a equipe de segurança, com requisitos claros e apropriados, além da possibilidade de testar a segurança do código-fonte buscando uma adequação incorporada ao desenvolvimento do software desde seu planejamento inicial e concepção.

§ 4º A identificação e a gestão dos requisitos de segurança da informação e privacidade e os processos associados devem ser integrados aos estágios iniciais dos projetos de sistemas de informação.

§ 5º Os requisitos de segurança da informação e privacidade dos sistemas de informação devem ser identificados usando vários métodos, como requisitos de conformidade oriundos de política e regulamentações, modelos de ameaças, análises críticas de incidentes ou o uso de limiares de vulnerabilidade.

Art. 13. A segurança física e patrimonial, a ser disposta em política específica, harmoniza-se com os processos do PCGSIPD/TCERO e tem por objetivo, em relação à segurança da informação e privacidade, controlar e prevenir acesso físico não autorizado, danos e interferências nas instalações do Tribunal de Contas do Estado de Rondônia que possam causar perda, roubo ou comprometimento das informações.

Parágrafo único. O controle de acesso físico à informação se alinha, no que couber, às diretrizes contidas no Plano de Segurança Institucional disposto na Resolução n. 197/2015/TCERO.

CAPÍTULO III

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 14. O Comitê de Segurança da Informação e Comunicação (COSIC) é órgão colegiado de natureza consultiva e de caráter permanente, instituído pela Resolução n. 287/2019/TCE-RO, ao qual compete, entre outras atribuições:

I - formular, conduzir diretrizes e propor modelo de governança corporativa de segurança da informação e privacidade, e, ainda, promover a implementação e monitoramento do Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados (PCGSIPD/TCERO), da Política Corporativa de Segurança da Informação (PCSI/TCERO) e da Lei Geral de Proteção de Dados Pessoais (LGPD), bem como analisar periodicamente sua efetividade;

II – manifestar-se sobre propostas de alteração ou de revisão da PCSI/TCERO, bem como sobre minutas de normativo e iniciativas de natureza estratégica ou que necessitem de cooperação entre unidades, que versem sobre segurança da informação ou proteção de dados pessoais;

III – manifestar-se sobre matérias atinentes à segurança da informação e privacidade que lhe sejam submetidas;

IV - supervisionar periodicamente as ações e resultados de auditorias de conformidade de segurança da informação e privacidade, a partir de aspectos legais relacionados à proteção das informações adotadas pelo Tribunal de Contas do Estado de Rondônia;

V - avaliar informações recebidas a partir do monitoramento e da análise crítica de incidentes de segurança da informação e recomendar ações apropriadas como resposta;

VI - acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de segurança da informação que gerem quebra de segurança; e

VII – requerer às unidades do Tribunal as informações que considerar necessárias ao acompanhamento das ações de gestão de segurança da informação, privacidade, proteção de dados pessoais e segurança cibernética.

Art. 15. Compete à Secretaria de Gestão de Pessoas (SEGESP), em relação à segurança da informação em recursos humanos, elaborar as proposições de normas e políticas acessórias aos procedimentos de segurança referentes aos dados pessoais e informações sobre recursos humanos e a vida funcional dos servidores com vínculo estatutário, funcional, contratual ou processual integrantes deste Tribunal, em observância, no que couber, às diretrizes e princípios definidos na Política de Gestão de Pessoas do Tribunal de Contas do Estado de Rondônia.

Art. 16. Compete à Escola Superior de Contas Conselheiro José Renato da Frota Uchôa (ESCon), relativamente à segurança da informação em recursos humanos, contemplar a promoção continuada de cursos e eventos de formação, capacitação, aperfeiçoamento e especialização sobre a Lei Geral de Proteção de Dados Pessoais e sobre Segurança da Informação e Privacidade aos servidores, estagiários e terceirizados deste Tribunal, nos termos da Resolução nº 333/2020/TCERO que dispõe sobre ações educacionais no âmbito da ESCon.

Art. 17. Compete à Assessoria de Comunicação Social (ASCOM), quanto à segurança da informação em recursos humanos, promover, de forma continuada e sistematizada, por meio de Plano de Comunicação, ações de elaboração e divulgação de conteúdo (cartilhas, banners, matérias, vídeos, entre outros) informativo sobre o Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados (PCGSIPD/TCERO), sobre a Lei Geral de Proteção de Dados Pessoais (LGPD) e sobre Segurança da Informação e Privacidade, objetivando fortalecer a cultura de segurança da informação e a conscientização dos servidores, estagiários e terceirizados sobre suas responsabilidades e da importância da temática no âmbito do Tribunal de Contas do Estado de Rondônia.

Art. 18. Compete à Secretaria de Tecnologia da Informação e Comunicação (SETIC), no que concerne à segurança em tecnologia da informação e comunicações:

I - a gestão dos ativos de tecnologia da informação e comunicação, a ser disposta em política específica, com vistas a priorizar investimentos e concentrar esforços nos ativos críticos que sustentam os processos do Tribunal, onde as informações são criadas, processadas, armazenadas e compartilhadas;

II - adotar medidas técnicas e controles tecnológicos para assegurar a privacidade e proteção das informações em redes e dos recursos de processamento da informação que as apoiam;

III - garantir que as redes sejam gerenciadas, monitoradas e controladas para proteger as informações nos bancos de dados, sistemas e aplicações, e, ainda, manter a segurança da informação transferida na rede interna do Tribunal de Contas do Estado de Rondônia e com quaisquer entidades externas;

IV - coordenar a aquisição, desenvolvimento e manutenção de sistemas, garantindo que os requisitos de segurança da informação e privacidade sejam parte integrante de todo o ciclo de vida dos sistemas de informação, e que as exigências relacionadas à segurança da informação e privacidade sejam incluídas nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes;

V - estabelecer controles adicionais para sistemas que processem informações sensíveis, valiosas ou críticas, ou que exerçam algum impacto, devendo ser determinados com base em requisitos de segurança e análise/avaliação de riscos;

VI - estabelecer e implementar tipos de proteção e controles de acesso aos sistemas de informação e redes de dados, que venham a minimizar riscos e impactos na garantia de execução das atividades e continuidade do negócio do Tribunal;

VII - estabelecer as formas de gerenciamento, controle, concessão e revogação de privilégios de acesso aos bancos de dados do Tribunal, garantindo que apenas usuários autorizados executem operações sobre as bases de dados, com vistas a proteger as informações de qualquer ação, intencional ou acidental, que resulte em perdas ou degradação de parte ou da totalidade da integridade, confidencialidade, disponibilidade e privacidade dos dados, observadas, no que couber, as regras a serem dispostas em política específica;

VIII - aplicar e controlar as credenciais e níveis de acesso de servidores, estagiários, prestadores de serviços e jurisdicionados, aos sistemas, equipamentos, dispositivos e atividades vinculadas aos sistemas de informação e redes de dados do Tribunal de Contas do Estado de Rondônia, observadas as regras a serem dispostas em política específica;

IX - criar e manter registros e procedimentos, como trilhas de auditoria que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos, à internet e à rede interna de comunicação de dados do Tribunal;

X - avaliar periodicamente as práticas de segurança em tecnologia da informação e comunicações adotadas para garantir a confidencialidade, integridade, disponibilidade, autenticidade e auditabilidade das redes e sistemas de informação do Tribunal;

XI - garantir a continuidade do uso da informação, com pelo menos uma cópia de segurança atualizada e guardada em local seguro, com o nível de proteção equivalente ao nível de proteção da informação original, observadas as regras dispostas em política específica;

XII - elaborar e executar um plano de resposta a incidentes de segurança em tecnologia da informação e comunicações, bem como, a notificação e detecção de incidentes, relatórios, triagem, análise, resposta, contenção, erradicação, recuperação e conclusão, com vistas a identificar as causas, extensão e impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção ou para seu encaminhamento;

XIII - elaborar as proposições de normas e políticas acessórias aos procedimentos de segurança de tecnologia da informação, no que couber, em harmonia com os processos previstos no PCGSIPD/TCERO;

XIV - planejar e executar atividades pedagógicas e instrutivas voltadas às áreas e unidades do Tribunal de Contas do Estado de Rondônia, referentes aos procedimentos e boas práticas de segurança de tecnologia da informação a serem observados em relação às suas respectivas esferas de competência e responsabilidades, bem como, sobre os procedimentos de notificações de incidentes de segurança da informação em operações de TIC;

XV - colaborar para a implementação e o funcionamento do Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados (PCGSIPD/TCERO) e da Política Corporativa de Segurança da Informação (PCSI/TCERO); e

XVI - coordenar a unidade especializada de segurança cibernética, promovendo ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético que possam comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

Art. 19. Compete à Assessoria de Segurança Institucional (ASI), no que concerne à segurança física e patrimonial, elaborar as proposições de normas e políticas acessórias aos procedimentos de segurança física e patrimonial para controlar e prevenir acesso físico não autorizado, danos e interferências nas instalações do Tribunal de Contas do Estado de Rondônia, alinhando-se, no que couber, ao disposto no Plano de Segurança Institucional disposto na Resolução n. 90/2012/TCERO e alterado pela Resolução n. 197/2015/TCERO.

Art. 20. Compete à Ouvidoria, no que concerne à Lei Geral de Proteção de Dados Pessoais – LGPD no âmbito do Tribunal de Contas do Estado de Rondônia:

I – atuar como canal de comunicação oficial entre o encarregado de proteção de dados pessoais (DPO) do Tribunal de Contas do Estado de Rondônia, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD); e

II – receber e controlar as requisições dos titulares de dados pessoais, solicitações da ANPD ou quaisquer outros expedientes que lhe sejam encaminhados acerca da LGPD e adotar providências para encaminhamento imediato ao encarregado de proteção de dados pessoais do Tribunal de Contas do Estado de Rondônia.

Art. 21. Os Gestores de Segurança da Informação e Privacidade têm atuação regulada pela Resolução n. 330/2020/TCERO, são coordenados pelo encarregado de proteção de dados pessoais (DPO) com supervisão do Comitê de Segurança da Informação e Comunicação (COSIC), competindo-lhes:

I – disseminar, no âmbito do Tribunal, em especial na secretaria, gabinete ou setor em que estiver lotado, as boas práticas sobre segurança da informação e privacidade de dados;

II - levar ao conhecimento da chefia e dos demais integrantes da secretaria, gabinete ou setor em que estiver lotado, as orientações institucionais relacionadas à segurança da informação e privacidade de dados; e

III - apoiar o encarregado de proteção de dados pessoais (DPO) e o COSIC no desempenho de suas funções.

Art. 22. Compete ao Encarregado de Proteção de Dados Pessoais (DPO):

I – recepcionar as reclamações e comunicações dos titulares de dados pessoais por intermédio do canal da Ouvidoria do Tribunal de Contas do Estado de Rondônia, bem como, prestar esclarecimentos e adotar providências necessárias à resolução da demanda;

II - receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD), por meio da Ouvidoria do Tribunal de Contas do Estado de Rondônia, e adotar as providências cabíveis;

III – encaminhar à Ouvidoria, respostas às requisições dos titulares de dados pessoais e solicitações da ANPD, nos prazos e nos termos previstos na LGPD;

IV - orientar os servidores, estagiários e terceirizados do Tribunal a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

V - executar as demais atribuições determinadas ou estabelecidas em normas complementares peloTribunal de Contas do Estado de Rondônia.

§ 1º O encarregado de proteção de dados pessoais, quando da execução de suas atribuições, deverá:

I - possuir independência e reportar diretamente à alta administração do Tribunal de Contas do Estado de Rondônia as intercorrências ou fatos relevantes, que entender necessários, ocorridas durante a execução da Política Corporativa de Segurança da Informação, para assegurar uma efetiva gestão de riscos de privacidade (NBR 27701:2019 - 6.3.1.1);

II - ser envolvido na gestão de questões que estejam relacionadas ao tratamento de dados pessoais;

III - ser especialista na legislação, na regulamentação e na prática de proteção de dados;

IV - fornecer orientações em relação às avaliações de impacto de privacidade conduzidas pelo Tribunal de Contas do Estado de Rondônia;

V - ser envolvido para acompanhar e apoiar os procedimentos para a identificação e registro de violações de dados pessoais, bem como, para notificação das partes envolvidas nas violações de dados pessoais e à divulgação para as autoridades, observando a regulamentação e/ou legislação aplicadas; e

VI - ser envolvido e acompanhar o processo de gestão e resposta a incidentes de segurança da informação global no Tribunal de Contas do Estado de Rondônia;

§ 2º O encarregado, durante o exercício da função de encarregado e outras funções relacionadas ao tema, deverá, obrigatoriamente, participar de cursos periódicos de capacitação que contemplem conteúdo de caráter multidisciplinar tais como:

I - aspectos jurídicos da proteção de dados pessoais;

II - gestão e governança de dados pessoais; e

III - tecnologias da informação e comunicação e segurança da informação.

Art. 23. Compete aos responsáveis por informações produzidas ou custodiadas pelo Tribunal de Contas do Estado de Rondônia:

I – assegurar a segurança e privacidade das informações;

II - classificar as informações e definir procedimentos e critérios de acesso, observados os dispositivos legais e normativos relativos à confidencialidade e a outros critérios de classificação pertinentes, devendo observar, no que couber, as disposições da Política de Gestão de Documentos Arquivísticos do Tribunal de Contas do Estado de Rondônia;

III - propor regras específicas para o uso das informações; e

IV- definir os requisitos de segurança da informação necessários ao negócio, com base em critérios de aceitação e tratamento de riscos inerentes aos processos de trabalho.

§ 1º O Presidente, Conselheiros, Conselheiros-Substitutos e Procuradores do Ministério Público de Contas podem, dentro de suas atribuições funcionais, indicar, orientar e autorizar, a qualquer tempo, procedimentos que visem a garantir a segurança da informação e privacidade nos processos e documentos de sua competência, a serem seguidos pelos responsáveis.

§ 2º Em caso de dúvida na identificação do responsável pela informação, compete ao comitê responsável pela segurança da informação defini-lo.

Art. 24. São responsabilidades do custodiante da informação:

I – assegurar a privacidade e segurança da informação sob sua posse, conforme os critérios definidos pelo respectivo responsável pela informação;

II - comunicar tempestivamente ao responsável pela informação sobre eventos que comprometam a privacidade e segurança das informações sob custódia; e

III - comunicar ao responsável pela informação eventuais limitações para o cumprimento dos critérios por ele definidos, com vistas à privacidade e proteção da informação.

Art. 25. São responsabilidades dos dirigentes das unidades e demais gestores do Tribunal de Contas do Estado de Rondônia, no que se refere à segurança da informação e privacidade:

I - apoiar o gestor de segurança da informação e privacidade representante da sua área quando da execução de atividades relacionadas ao Programa Corporativo de Gestão de Segurança da Informação e Privacidade de Dados (PCGSIPD/TCE-RO);

II - conscientizar servidores e quaisquer colaboradores sob sua supervisão em relação aos conceitos e às práticas de segurança da informação e privacidade;

III - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação e privacidade; e

IV - tomar as medidas administrativas necessárias para que sejam adotadas ações corretivas em tempo hábil em caso de comprometimento da segurança da informação e privacidade.

Art. 26. A estrutura e competências da unidade de segurança da informação, privacidade e proteção de dados pessoais, bem como, da unidade de segurança cibernética serão definidas mediante ato normativo da presidência do Tribunal de Contas do Estado de Rondônia.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 27. Os atos normativos e administrativos decorrentes da Política Corporativa de Segurança da Informação utilizarão o Glossário de Termos da PCSI/TCERO, constante no Anexo I, para promover compreensão comum e consistente de conceitos em função da natureza específica do tema.

Art. 28. As informações produzidas por qualquer pessoa com vínculo permanente ou transitório com o Tribunal que tenha acesso, de forma autorizada, às informações ou às dependências do Tribunal de Contas do Estado de Rondônia, no exercício de suas atribuições, são patrimônio intelectual do Tribunal e não cabe a seus criadores qualquer forma de direito autoral, ressalvado o reconhecimento da autoria, se for o caso.

§ 1º Quando as informações forem produzidas por colaboradores do Tribunal de Contas do Estado de Rondônia para uso exclusivo do Tribunal, instrumento próprio estabelecerá as obrigações dos criadores, inclusive no que se refere a eventual confidencialidade das informações, devendo observar, no que couber, as disposições da Política de Gestão de Documentos Arquivísticos do Tribunal.

§ 2º É vedada a utilização das informações a que se refere o parágrafo anterior em projetos ou atividades diversas daquelas estabelecidas pelo Tribunal de Contas do Estado de Rondônia, salvo autorização específica dos Membros do Tribunal, nos processos e documentos de sua competência, ou do Presidente, nos demais casos.

Art. 29. Não é permitido acessar, armazenar, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar, com recursos computacionais do Tribunal de Contas do Estado de Rondônia ou por qualquer meio, fotografia, vídeo ou outro registro que contenha conteúdo pornográfico, erótico, indecente, ofensivo, ou que incentive a violência ou a discriminação de raça, credo ou gênero, além da utilização desses recursos para acesso a conteúdo que não seja de utilidade do Tribunal de Contas do Estado de Rondônia.

Art. 30. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Tribunal de Contas do Estado de Rondônia devem observar, no que couber, as disposições da PCSI/TCERO, e ainda, conter cláusulas versando sobre proteção de dados pessoais e dados pessoais sensíveis, em consonância com a Lei Geral de Proteção de Dados Pessoais (LGPD).

Art. 31. A não observância dos dispositivos da PCSI/TCERO sujeita os infratores, isolada ou cumulativamente, às sanções administrativas, civis e penais, nos termos da legislação pertinente, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 32. A revisão da PCSI/TCERO 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 quatro anos, de modo a atualizá-la frente a novos requisitos corporativos e legais.

Art. 33. Compete ao Presidente do Tribunal de Contas do Estado de Rondônia, 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. 34. Revoga-se a Resolução n. 41/2006/TCERO.

Art. 35. Esta Resolução entra em vigor na data de sua publicação.

Porto Velho, 12 de dezembro de 2022.

(assinado eletronicamente)
PAULO CURI NETO
Conselheiro Presidente

ANEXO I DA RESOLUÇÃO N. 377 DE 12 DE DEZEMBRO DE 2022.

APRESENTAÇÃO

Este glossário fornece definições de termos aplicáveis à Política Corporativa de Segurança da Informação do Tribunal de Contas do Estado de Rondônia, para promover uma compreensão comum e consistente de conceitos sobre a temática.

GLOSSÁRIO

A

Autenticidade: propriedade que assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria.

Aquisição de evidência: processo de coleta e cópia das evidências relacionadas a incidente de segurança em redes computacionais.

Autoridade nacional de proteção de dados: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei 13.709, de 2018, em todo o território nacional.

C

Ciclo de vida da informação: compreende etapas e eventos de produção, recebimento, armazenamento, acesso, uso, alteração, cópia, transporte e descarte da informação.

Colaborador: prestador de serviço terceirizado, estagiário ou qualquer pessoa com vínculo transitório com o TCE-RO que tenha acesso, de forma autorizada, às informações ou às dependências do Tribunal.

Coleta de evidências de segurança em redes computacionais: processo de obtenção de itens físicos que contém uma potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Este processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente.

Confidencialidade: propriedade que garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais.

Controles de privacidade: medidas que tratam os riscos de privacidade por meio da redução de sua probabilidade ou de suas consequências.

Controles de segurança: medidas adotadas para evitar ou diminuir o risco de ocorrência de um incidente de segurança da informação.

Custodiante da informação: 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 Tribunal de Contas do Estado de Rondônia.

D

Dado pessoal: informação relacionada à pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Disponibilidade: propriedade que garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido.

Dispositivos móveis: equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: notebooks, netbooks, smartphones, tablets, pen drives, USB drives, HD externo e cartões de memória.

E

Encarregado de proteção de dados pessoais - data protection officer (DPO): pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

ETIR - Equipe de tratamento e resposta a incidentes em redes computacionais: grupo de pessoas com responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes cibernéticos.

G

Gestão de riscos em segurança da informação e privacidade: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

Gestão de vulnerabilidades: conjunto de atividades coordenadas que tem por objetivo a redução, a níveis aceitáveis, das vulnerabilidades de segurança encontradas durante o processo de "Análise de Segurança" ou "Análise de Vulnerabilidades" em um determinado ativo ou conjunto de ativos de Tecnologia da Informação e Comunicação - TIC.

I

Incidente: interrupção não planejada ou redução na qualidade de um serviço.

Incidente de segurança da informação: evento adverso, confirmado ou sob suspeita, que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema.

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.

Integridade: propriedade que garante a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital.

Invasão: incidente de segurança no qual o ataque foi bem-sucedido, resultando no acesso, na manipulação ou na destruição de informações em um computador ou em um sistema da organização.

L

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

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 quanto de cada recurso ou sistema o usuário pode utilizar.

Notificação de incidente: ato de informar eventos ou incidentes para uma equipe de tratamento de incidentes de rede ou grupo de segurança.

O

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

P

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

Plano de continuidade de negócio: documentação dos procedimentos e informações necessárias para que o Tribunal de Contas do Estado de Rondônia mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes.

Plano de resposta a incidentes: plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.

Privacy by default: conceito de garantir que o uso e o tratamento de dados pessoais sejam minimizados ao máximo. Somente as informações estritamente necessárias para a proposta do produto, serviço ou software devem ser coletadas, utilizadas, armazenadas e difundidas.

Privacy by design: conceito de utilizar a privacidade de dados desde a concepção de um determinado projeto, produto ou serviço, integrando-a desde a criação, desenvolvimento e planejamento.

Programa corporativo de gestão da segurança da informação e privacidade de dados: programa de governança em privacidade com base nas normas ISO da família 27000, que objetiva aumentar o nível de confidencialidade, integridade e disponibilidade das informações e processos críticos de informação do Tribunal de Contas do Estado de Rondônia, além de adequar-se à Lei n. 13.709, de 2018, delineando ações para a aplicação de diretrizes visando a maximizar o desempenho do Tribunal nos aspectos de segurança da informação e privacidade.

Programa de gestão da continuidade de negócios: processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção.

R

Responsável pela informação: órgão colegiado do Tribunal de Contas do Estado de Rondônia, autoridade do Tribunal ou dirigente de área ou unidade responsável por informação em matéria de sua competência ou inerente a sua área de atuação.

S

Security by design: conceito de incorporar boas práticas de segurança da informação desde a concepção de um determinado projeto, produto ou serviço, integrando-a desde a criação, desenvolvimento e planejamento.

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 Tribunal de Contas do Estado de Rondônia.

T

Termo de responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade, a autenticidade e a privacidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

Time de resposta a incidentes de segurança: time responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

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 externo: qualquer pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal e que não seja usuário interno ou usuário colaborador.

Usuário interno: qualquer servidor ou unidade do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo próprio Tribunal.

V

Vazamento de dados: transmissão não autorizada de dados de dentro de uma organização para um destino ou recipiente externo. O termo pode ser usado para descrever dados que são transferidos eletronicamente ou fisicamente. Pode ocorrer de forma acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso).

Violação de privacidade: situação onde os dados pessoais são tratados em violação de um ou mais requisitos pertinentes de salvaguarda da privacidade.