RESOLUÇÃO Nº TC-0179/2021

Estabelece a Política de Segurança da Informação, Comunicação, Privacidade e Proteção de Dados (POSICPD) no âmbito do Tribunal de Contas de Santa Catarina.

O TRIBUNAL DE CONTAS DO ESTADO DE SANTA CATARINA TCE/SC), no uso das atribuições que lhe são conferidas pelos arts. 4º da Lei Complementar (estadual) n. 202, de 15 de dezembro de 2000, e 2º, da Resolução n. TC-06/2001, de 03 de dezembro de 2001 (Regimento Interno);

considerando que a Constituição da República Federativa do Brasil de 1988 (CRFB/88) garante o acesso à informação e a proteção aos dados pessoais, no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216;

considerando que a Lei de Acesso à Informação (LAI), Lei n. 12.527, de 18 de novembro de 2011, determina, como dever do Estado, a proteção das informações pessoais dos cidadãos e a Lei Geral de Proteção de Dados (LGPD), Lei n. 13.709, de 14 de agosto de 2018, determina que as instituições adotem mecanismos de tratamento e proteção de dados pessoais; dentre outros diplomas legais que tratam do tema da segurança da informação, comunicação, privacidade e proteção de dados;

considerando que a criação da política de segurança da Informação foi inserida no Plano de Ação do TCE/SC 2019-2020 (Portarias ns. TC-0895/2019, TC-153/2020 e TC-176/2020), o que denota o reconhecimento da necessidade de se instituir e manter uma política sobre a segurança no tratamento de dados e informações no âmbito da TCE/SC;

considerando a necessidade de incrementar a segurança das redes e dos bancos de dados governamentais;

considerando a necessidade de manter as informações íntegras, autênticas, disponíveis e, quando for o caso, sigilosas ou de acesso restrito;

considerando a necessidade de estabelecer princípios, objetivos, diretrizes e requisitos gerais que promovam a gestão integrada e coerente de processos voltados à segurança da informação, privacidade e proteção de dados, que sejam periodicamente revistos;

considerando que a informação, em todo o seu ciclo de vida, constitui bem estratégico e ativo fundamental para o desempenho das atribuições constitucionais e para as atividades do TCE/SC;

considerando que as informações geradas, recebidas, mantidas, transmitidas e tratadas pelo TCE/SC estão em diferentes suportes, e que é necessário prevenir incidentes que comprometam a segurança desses dados e informações;

considerando as competências e a finalidade da Assessoria de Governança Estratégica de Tecnologia da Informação (AGET), estabelecidas nos arts. 14 e 15 da Resolução n. TC-149/2019 e do Comitê Gestor de Segurança da Informação, Privacidade e Proteção de Dados (CGSIPD), instituído pela Portaria n. TC-149/2020;

RESOLVE:

CAPÍTULO I
DOS OBJETIVOS

Art. 1º A Política de Segurança da Informação, Comunicação, Privacidade e Proteção de Dados (POSICPD) tem como objetivo assegurar, por meio de princípios, diretrizes, normas e procedimentos, que toda a informação coletada, gerada, adquirida, utilizada, em trânsito e armazenada, própria ou custodiada, por meio de tecnologias, procedimentos, pessoas e ambientes do Tribunal de Contas de Santa Catarina (TCE/SC), seja tratada como parte do seu patrimônio e protegida quanto aos aspectos de autenticidade, confidencialidade, integridade e disponibilidade, bem como de proteção de dados pessoais, privacidade e conformidade legal.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para fins de aplicação da POSICPD no âmbito do TCE/SC, serão adotadas as definições constantes do anexo I desta Resolução.

CAPÍTULO III
DO PÚBLICO DE INTERESSE

Art. 3º Estão sujeitos à POSICPD do TCE/SC:

I – Conselheiros, conselheiros-substitutos, servidores, colaboradores, estagiários e prestadores de serviços do Tribunal de Contas;

II – procuradores, servidores, colaboradores, estagiários e prestadores de serviço do Ministério Público de Contas;

III – qualquer pessoa física ou jurídica, pública ou privada, que venha a ter acesso a dados, informações e ativos de informação do Tribunal de Contas.

Art. 4º Todos deverão observar as diretrizes, normas e procedimentos de segurança da informação, privacidade e proteção de dados concernentes à política de que trata esta Resolução, e serão responsáveis por garantir a segurança dos dados e informações a que tenham acesso.

CAPÍTULO IV
DOS PRINCÍPIOS DA POSICPD

Art. 5º A POSICPD rege-se pelos seguintes princípios, além daqueles previstos no art. 6º da Lei n. 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais:

I – aprendizado permanente: desenvolvimento individual e profissional de conhecimentos, habilidades e atitudes para a análise, gestão e comunicação de dados, incentivado por programa de formação, aperfeiçoamento e capacitação permanente;

II – celeridade: as ações de segurança da informação, comunicação, privacidade e proteção de dados devem oferecer respostas tempestivas a incidentes e falhas;

III – ciência: todos os usuários devem ter conhecimento sobre as normas, os procedimentos, as orientações e demais informações que permitam a execução de suas atribuições sem comprometimento da segurança de dados, informações e ativos de informação do Tribunal de Contas;

IV – clareza: as regras sobre a segurança da informação, da comunicação, e da privacidade e proteção de dados devem adotar linguagem simples, precisa, concisa, acessível e de fácil entendimento;

V – criticidade: princípio de segurança que define a importância da informação para a continuidade das atividades da instituição;

VI – dignidade da pessoa humana: devem ser respeitados todos os direitos e interesses legítimos dos usuários;

VII – impessoalidade: a POSICPD não será utilizada para finalidades particulares ou para a obtenção de benefícios ou promoção pessoais;

VIII – legalidade: a POSICPD observará a política institucional, os atos normativos, os procedimentos e as instruções formalmente estabelecidos pelo Tribunal de Contas;

IX – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

X – moralidade: a POSICPD deverá observar os preceitos da boa-fé, da boa administração pública e estar pautada pela atuação ética e nos ideais de honestidade, probidade e justiça;

XI – não discriminação: o tratamento de dados não deve ser realizado com fins discriminatórios ilícitos ou abusivos;

XII – não repúdio: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo sua identificação;

XIII – necessidade: terão acesso às informações todos que tenham necessidade de conhecê-las para o bom desempenho de suas atribuições profissionais;

XIV – privacidade: informações relativas à intimidade, à integridade e à honra dos cidadãos devem ser resguardadas, de acordo com a legislação vigente;

XV – proporcionalidade: o custo das ações de segurança da informação, comunicação, privacidade e proteção de dados não deve ser maior do que o valor do ativo da informação a ser protegido, salvo os casos formalmente analisados e justificados durante o processo de Gestão de Riscos;

XVI – transparência: as diretrizes, as normas e os procedimentos da POSICPD, além de publicados, devem ser amplamente divulgados aos usuários a fim de orientarem o desempenho de suas atribuições.

CAPÍTULO V
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6º Na gestão da segurança da informação, das comunicações, da privacidade e proteção de dados deverão ser observadas as seguintes normas e referências legais:

I - Lei n. 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

II - Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet Brasileira), que estabeleceu princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

III - Lei n. 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências;

IV - Lei n. 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso à informação;

V - Resolução n. TC-101/2014, de 8 de dezembro de 2014, que dispõe sobre o Código de Ética dos Membros do Tribunal de Contas de Santa Catarina;

VI - Resolução n. TC-087/2013, de 27 de novembro de 2013, que dispõe sobre o Código de Ética dos Servidores Públicos do Tribunal de Contas de Santa Catarina;

VII – Resolução n TC-071/2012, de 31 de outubro de 2012, que estabelece procedimentos para a divulgação e o acesso à informação produzida ou custodiada pelo Tribunal de Contas de Santa Catarina;

VIII - Portaria n. TC-0149/2020, de 24 de julho de 2020, que institui o Comitê Gestor de Segurança da Informação, Privacidade e Proteção de Dados (CGSIPD) no âmbito do Tribunal de Contas do Estado de Santa Catarina (TCE/SC);

IX - Portaria n. TC-0537/2019, de 02 de agosto de 2019, que institui o Comitê de Governança da Tecnologia da Informação e Comunicação (CGTIC) no âmbito do Tribunal de Contas do Estado de Santa Catarina;

X - ABNT NBR ISO/IEC 27001:2013 – sistemas de gestão da segurança da informação – requisitos;

XI - ABNT NBR ISO/IEC 27002:2013 – código de prática para controles de segurança da informação;

XII - ABNT NBR ISO/IEC 27003:2020 – sistemas de gestão da segurança da informação – orientações;

XIII - ABNT NBR ISO/IEC 27004:2017 – sistemas de gestão da segurança da informação – monitoramento, medição, análise e avaliação;

XIV - ABNT NBR ISO/IEC 27005:2019 – gestão de riscos de segurança da informação;

XV - ABNT NBR ISO 27799:2019 – gestão de segurança da informação em saúde utilizando a ISO/IEC 27002;

XVI - ABNT NBR ISO/IEC 27007:2018 – técnicas de segurança – diretrizes para auditoria de sistemas de gestão da segurança da informação;

XVII - ABNT NBR ISO/IEC 27017:2016 – técnicas de segurança – código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem;

XVIII - ABNT NBR ISO/IEC 27014:2013 – governança de segurança da informação;

XIX - ABNT NBR 16167:2013 – diretrizes para classificação, rotulação e tratamento da informação;

XX - ABNT NBR ISO/IEC 29100:2020 – estrutura de privacidade;

XXI - ABNT NBR ISO/IEC 27701:2019 (versão corrigida: 2020) – técnicas de segurança – extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – requisitos e diretrizes;

XXII - ABNT NBR ISO/IEC 27018:2018 – código de prática para Proteção de Informações de Identificação Pessoal (PII) em nuvens públicas que atuam como processadores de PII;

XXIII - ABNT ISO/TS 21547:2016 – requisitos de segurança para arquivamento de registros eletrônicos de saúde – princípios;

XXIV - ABNT NBR 16386:2015 – diretrizes para o processamento de interceptação telemática judicial;

XXV - ABNT NBR ISO/IEC 27032:2015 – diretrizes para segurança cibernética;

XXVI - ABNT NBR ISO/IEC 27037:2013 – diretrizes para identificação, coleta, aquisição e preservação de evidência digital;

XXVII - ABNT NBR ISO/IEC 27038:2014 – especificação para redação digital;

XXVIII - ABNT NBR ISO 31000:2018 – gestão de riscos – diretrizes.

CAPÍTULO VI
DAS INSTÂNCIAS ADMINISTRATIVAS

Art. 7º São instâncias administrativas envolvidas na gestão da segurança da informação, das comunicações, da privacidade e proteção de dados:

I - Presidente do Tribunal de Contas do Estado de Santa Catarina;

II - Comitê de Governança da Tecnologia da Informação e Comunicação (CGTIC) no âmbito do Tribunal de Contas do Estado de Santa Catarina;

III - Comitê Gestor de Segurança da Informação e Comunicação, Privacidade e Proteção de Dados (CGSIPD) Tribunal de Contas do Estado de Santa Catarina;

IV - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);

V - Equipe de Tratamento e Resposta a Incidentes de Violação de Dados Pessoais (ETIPD);

VI - Encarregado de dados (Lei n. 13.709, de 14 de agosto de 2018).

Parágrafo único. Sem prejuízo do disposto na POSICPD, a composição e as atribuições das instâncias administrativas serão estabelecidas por meio de portaria do Presidente do Tribunal de Contas.

CAPÍTULO VII
DA ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO, DAS COMUNICAÇÕES, DA PRIVACIDADE E PROTEÇÃO DE DADOS

Art. 8º A estrutura normativa da segurança da informação, das comunicações, da privacidade e proteção de dados é composta por três níveis de governança, a saber:

I – POSICPD: instituída por meio desta Resolução e detalhada por um conjunto de normas, procedimentos e orientações específicas nos termos de Portaria a ser editada pelo do Presidente;

II – Normas de Segurança da Informação, Comunicação, Privacidade e Proteção de Dados (NSIPD): estabelecem as obrigações e os procedimentos, definidos a partir dos princípios e das diretrizes previstos na POSICPD, e devem ser observadas nas diversas instâncias em que a informação seja tratada. A cada norma será associado um conjunto de procedimentos destinados a orientar sua implementação.

a) o CGSIPD deverá elaborar e manter atualizadas as seguintes NSIPD sobre:

1. acesso à internet;
2. uso de correio eletrônico;
3. cópias de segurança (backup e recuperação de dados);
4. uso de ativos de informação;
5. proteção de códigos maliciosos;
6. segurança física e do ambiente;
7. controle de acesso lógico;
8. uso de criptografia;
9. uso de dispositivos móveis;
10. classificação de informações;
11. tratamento de mídias;
12. aquisição, desenvolvimento e manutenção de aplicações;
13. gestão de incidentes de segurança da informação, privacidade e proteção de dados;
14. plano de continuidade de negócios;
15. intercâmbio de informações;
16. privacidade e proteção de Dados Pessoais;
17. segurança da informação, privacidade e proteção de dados em Terceirização e Prestação de Serviços;
18. segurança e proteção de dados no trabalho remoto.

b) o CGSIPD poderá elaborar outras NSIPD a qualquer tempo.

III – procedimentos: instrumentalizam as NSIPD permitindo sua aplicação às atividades do Tribunal de Contas, podendo ser detalhados em instruções, são de uso de interno e classificam-se em:

a) Procedimentos de Segurança da Informação e da Comunicação (PSIC): são estabelecidos pelos gestores dos Sistemas de Informação e de Comunicação;

b) Procedimentos de Privacidade e Proteção de Dados (PPPD): são estabelecidos pelos operadores de dados (LGPD).

Art. 9º A POSICPD será complementada por normas, procedimentos e outros documentos pertinentes, a serem elaborados pelo CGSIPD, os quais integrarão a presente política sob a forma de anexos.

Art. 10. As diretrizes da POSICPD serão elaboradas pelo CGSIPD, e encaminhadas para a aprovação do CGTIC e do Presidente do TCE/SC, que encaminhará para deliberação pelo Pleno do TCE/SC.

Art. 11. As normas de segurança da informação, privacidade, e proteção de dados serão elaboradas pelo CGSIPD e submetidas para a aprovação do CGTIC e do Presidente.

Art. 12. Os procedimentos de segurança da informação serão elaborados pela ETIR.

Art. 13. Os procedimentos de privacidade e proteção de dados serão elaborados pela ETIPD.

Art. 14. Os servidores do TCE/SC poderão encaminhar para o CGSIPD, propostas de alteração ou criação de normas internas sobre segurança da informação, comunicação, privacidade e proteção de dados.

CAPÍTULO VIII
DAS DIRETRIZES

Seção I
Da Revisão e atualização da POSICPD

Art. 15. A POSICPD deverá ser revisada e atualizada a cada período de 2 (dois) anos, ou a qualquer tempo em resposta às mudanças do ambiente organizacional, às circunstâncias, às condições legais, ou ao ambiente de tecnologia, e deverá ser amplamente divulgada para o público de interesse descrito no art. 3° desta resolução.

Seção II
Do uso de dispositivos móveis

Art. 16. Deverão ser estabelecidas normas e procedimentos sobre segurança da informação, comunicação, privacidade e proteção dados, para gerenciar os riscos decorrentes do uso de dispositivos móveis.

Seção III
Do trabalho remoto

Art. 17. Deverão ser estabelecidas normas e procedimentos que assegurem a segurança da informação, comunicação, privacidade e proteção de dados, quando os dados e informações forem acessadas, processadas ou armazenadas em locais de trabalho remoto.

Seção IV
Da Segurança em Recursos Humanos

Subseção I
Antes da Contratação de Recursos Humanos

Art. 18. Quando do recrutamento de estagiários e colaboradores, deverá ser verificado o histórico desses, por meio de certidões negativas de registros civis e criminais, o que deverá ser realizado de acordo com a ética, as regulamentações internas e a legislação pertinente, e deve ser proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a que terão acesso.

Art. 19. Os estagiários, colaboradores, e prestadores de serviços sob contrato com o TCE/SC serão obrigados a assinar um Termo de condições de contratação, com cláusulas de confidencialidade e sigilo, em obediência ao estabelecido na POSICPD.

Subseção II
Durante a Contratação de Recursos Humanos

Art. 20. Deverão ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização, visando criar uma cultura de segurança da informação e comunicação, privacidade e proteção de dados, para que alcancem o público de interesse previsto nesta resolução, incluindo a conscientização sobre notificação de incidentes.

Art. 21. As Chefias deverão requerer aos seus servidores, estagiários, colaboradores, prestadores de serviço para que pratiquem a segurança da informação e proteção de dados, conforme estabelecido na POSICPD.

Art. 22. O descumprimento às disposições da POSICPD, bem como às suas normas complementares e violações aos controles de segurança por ela estabelecidos, caracterizam infração funcional a ser devidamente apurada no âmbito administrativo, sem prejuízo das sanções cíveis e penais cabíveis.

Subseção III
Encerramento ou mudança da Contratação de Recursos Humanos

Art. 23. As responsabilidades e obrigações pela segurança da informação e proteção de dados que permaneçam válidas após um encerramento ou mudança da contratação devem ser definidas, comunicadas aos servidores, estagiários, colaboradores, e prestadores de serviços, e cumpridas.

Seção V
Da Segregação de Funções

Art. 24. Deverá ser realizada a segregação de funções de áreas de responsabilidade, com o fim de reduzir as oportunidades de modificar ou usar ativos sem a devida autorização ou detecção autorizada ou não intencional, ou uso indevido dos ativos da organização.

Seção VI
Da Gestão de Ativos

Art. 25. Deverão ser estabelecidas normas e procedimentos para identificar os ativos de informação do TCE/SC, e definir as responsabilidades apropriadas para a proteção dos ativos relevantes no ciclo de vida da informação e documentar a sua importância.

Seção VII
Da Classificação da Informação

Art. 26. Deverão ser estabelecidas normas e procedimentos de classificação de dados e informações, com o fim de assegurar que recebam um nível adequado de proteção, de acordo com a sua importância para o TCE/SC.

Seção VIII
Do Tratamento de Mídias

Art. 27. Deverão ser estabelecidas normas e procedimentos de gerenciamento para prevenir o acesso, a divulgação, modificação, transferência, remoção ou o descarte não autorizado dos dados e informações armazenados nas mídias.

Seção IX
Do Controle de Acesso

Art. 28. As instalações, os equipamentos, as redes e os sistemas de computadores, exceto os sistemas destinados a atendimento ao público, deverão possuir mecanismos adequados de liberação, controle, e remoção de acesso físico e/ou lógico, que possibilitem a identificação das pessoas.

Art. 29. A concessão de privilégios de acesso deverá ser realizada em conformidade com o princípio do privilégio mínimo, ou seja, cada usuário deve possuir apenas o conjunto de privilégios estritamente necessários ao desempenho das suas atribuições profissionais.

Art. 30. A utilização de privilégios administrativos deverá ser realizada com a observância de rigorosos preceitos éticos, e somente quando indispensável para a execução de atividade necessária à sustentação de ativos de tecnologia da informação, ou para o cumprimento de tarefa específica formalmente atribuída.

Art. 31. O TCE/SC deverá possuir um registro preciso e atualizado dos perfis dos usuários criados, para os usuários que tenham sido autorizados a acessar o sistema de informação e os dados pessoais (DP) nele contidos. Esse perfil deverá compreender um conjunto de dados sobre aquele usuário, incluindo a identificação

do usuário (ID), necessário para implementar os controles técnicos identificados que fornecem acesso autorizado.

Art. 32. O TCE/SC deverá identificar adequadamente quem e quando acessou sistemas de informação e os dados pessoais nele contidos, e quais acréscimos, exclusões ou mudanças eles fizeram. Em sistemas específicos, deverá ser registrado o motivo do acesso.

Art. 33. Ressalvada a certificação digital, regida por norma específica, o CGSIPD, de forma complementar, estabelecerá as regras sobre uso de senhas, em especial os tamanhos mínimo e máximo, formatação e periodicidade de troca.

Seção X
Da Criptografia

Art. 34. Deverão ser estabelecidas normas e procedimentos, com o fim de assegurar o uso efetivo e adequado da criptografia, para proteger a confidencialidade, autenticidade e a integridade da informação.

Seção XI
Da Segurança física e do ambiente

Art. 35. Deverão ser estabelecidos normativos, procedimentos e mecanismos, com o fim de proteger os ativos sensíveis (dados e informações de propriedade ou custodiados pelo TCE/SC) contra o acesso não autorizado, a modificação ou destruição, assim como a proteção do próprio sistema de tecnologia da informação contra acesso indevido ou danos físicos decorrentes de ação criminosa ou incidentes naturais.

Art. 36. A segurança física e patrimonial no TCE/SC alinha-se às estratégias organizacionais, aos princípios de segurança institucional e, ainda, aos seguintes princípios:

I – adequação: a medida restritiva utilizada deve ser apropriada à consecução dos fins pretendidos;

II – necessidade: a medida restritiva utilizada deve ser a menos gravosa dentre aquelas que sejam adequadas para atingir determinado fim;

III – proporcionalidade: as desvantagens dos meios utilizados e as vantagens dos fins almejados devem ser ponderadas antes da adoção de qualquer medida restritiva.

Seção XII
Das cópias de segurança (backup)

Art. 37. Deverão ser estabelecidos normativos, procedimentos e mecanismos, visando garantir a operação segura e correta dos recursos de processamento dos dados e informações.

Art. 38. Quando da elaboração de um plano de backup, os seguintes itens devem ser levados em consideração:

I – assegurar que os procedimentos de operação sejam documentados e preparados para as atividades operacionais associadas a recursos de processamento de comunicação e informações, como procedimentos de inicialização e desligamento de computadores, geração de cópias de segurança (*backup* e *restore*), manutenção de equipamentos, tratamento de mídias, segurança e gestão do tratamento das correspondências e das salas de computadores, bem como a disponibilização para todos os usuários que necessitem deles;

II – assegurar que as cópias de segurança dos dados e informações, dos softwares e das imagens do sistema sejam efetuadas e testadas regularmente, conforme a política de geração de cópias de segurança;

III – definir os requisitos para proteção e retenção dos backups de dados;

IV – fazer registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação;

V – definir a abrangência (por exemplo, completa ou diferencial) e a frequência da geração das cópias de segurança, a fim de que representem os requisitos de negócio do TCE/SC, da POSICPD e a criticidade da informação para a continuidade da operação do Tribunal;

VI – as cópias de segurança deverão ser realizadas em mídias diferentes (exemplo: fita e disco) e ser armazenadas com várias cópias locais e também em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;

VII – dar um nível apropriado de proteção física e ambiental das informações das cópias de segurança, consistentes com as normas aplicadas na instalação principal;

VIII – assegurar que as mídias de backup sejam regularmente testadas para garantir que elas sejam confiáveis no caso do uso emergencial, combinando-se, preferencialmente, com a realização de um teste de restauração e checado contra o tempo de restauração requerido. Convém que os testes da capacidade para restaurar os dados copiados sejam realizados em uma mídia de teste dedicada, não sobrepondo a mídia original, no caso em que o processo de restauração ou backup falhe e cause irreparável dano ou perda dos dados;

IX – em situações onde a confidencialidade é importante, as cópias de segurança devem protegidas por meio de encriptação;

X – estabelecer procedimentos operacionais que monitorem a execução dos backups (programados ou não), bem como apontem suas falhas de restauração, visando garantir sua integralidade (cópias de segurança), de acordo com a política a eles estabelecida;

XI – os backups devem ser realizados com diversos tipos diferentes de pontos de restauração (intradiário, diário, mensal, anual).

Seção XIII
Gestão de capacidade

Art. 39. A utilização dos recursos deverá ser monitorada e ajustada, e as projeções devem ser feitas para necessidades de capacidade futura de garantir o desempenho requerido do sistema.

Seção XIV
Da Proteção contra *Malwares*

Art. 40. Deverão ser implementados controles de detecção, prevenção e recuperação, para proteger contra *malwares*, combinados com um adequado programa de conscientização dos usuários.

Seção XV
Do registro de eventos (*logs*)

Art. 41. Deverão ser assegurados os registros (*log*) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares, bem como que sejam protegidos contra acesso não autorizado e adulteração.

Seção XVI
Da Segurança nas Comunicações

Art. 42. Deverão ser estabelecidos normativos, procedimentos e controles de transferências formais para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação, visando assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam.

Art. 43. Deverá ser mantida a segurança da informação transferida dentro da organização e com quaisquer entidades externas.

Art. 44. Deverão ser estabelecidos normativos e procedimentos para que as mensagens eletrônicas utilizadas pelo TCE/SC sejam adequadamente protegidas.

Art. 45. O acesso a dados e informações deverá ser realizado mediante termos de confidencialidade ou acordos de não divulgação, e de proteção de dados, os quais deverão ser analisados criticamente e documentados.

Seção XVII
Da Segregação de Ambientes

Art. 46. Deverão ser elaboradas normas, procedimentos e responsabilidades operacionais, incluindo gestão de mudanças, segregação de funções e separação dos ambientes de produção, desenvolvimento e teste.

Seção XVIII
Da Aquisição, do Desenvolvimento e da Manutenção de Sistemas de Informação

Art. 47. Deve-se assegurar que processos e soluções de tecnologia da informação e comunicação sejam adotados por padrão, considerando questões de segurança da informação, Privacidade e Proteção de Dados, desde a sua concepção (*Privacy by Design*), sendo que a coleta e o tratamento de dados pessoais (incluindo o uso, a divulgação, retenção, transmissão e o descarte) estejam limitados ao que é necessário para o propósito identificado.

Seção XIX
Do relacionamento com fornecedores

Art. 48. Todos os contratos, convênios, acordos e instrumentos congêneres firmados pelo Tribunal de Contas deverão conter cláusulas exigindo a observância desta Resolução e de atos normativos e orientações dela decorrentes, bem como estabelecer como obrigação da parte a divulgação da POSICPD aos seus empregados e propostos prepostos envolvidos nas atividades que envolvam a utilização de dados ou informações do Tribunal.

Seção XX
Da gestão de incidentes

Art. 49. Deverá ser normatizada e instituída a ETIR por portaria do Presidente do TCE/SC, com a responsabilidade de receber, analisar, responder notificações e executar atividades que envolvem implementação de controles de segurança da informação, bem como atuar em respostas a incidentes dessa natureza.

Art. 50. Deverá ser normatizada e instituída a ETIPD, por portaria do Presidente do TCE/SC, com a responsabilidade de receber, analisar, responder notificações e executar atividades que envolvem implementação de controles de privacidade e proteção de dados, bem como atuar em respostas a incidentes dessa natureza.

Art. 51. Deverão ser implementados procedimentos que especifiquem quando e quais autoridades (por exemplo, encarregado de dados, corpo de bombeiros, autoridades fiscalizadoras, entidades regulatórias) serão contatadas e como os incidentes de segurança da informação identificados serão reportados em tempo hábil (por exemplo, no caso de suspeita de que a lei foi violada).

Seção XXI
Da Gestão de Continuidade do Negócio

Art. 52. A Gestão de Continuidade de Negócios deverá compreender um conjunto de normas e procedimentos que visem assegurar a disponibilidade, o uso, o acesso e a proteção dos ativos que suportam os serviços e processos críticos de trabalho do TCE/SC, por intermédio de ações de gestão de crise, prevenção e recuperação, estabelecendo uma estratégia de continuidade de negócio para reduzir a um nível aceitável a possibilidade de interrupção causada por desastres ou falhas.

Seção XXII
Da Auditoria e Conformidade

Art. 53. O TCE/SC manterá registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos aos seus ativos de informação, considerando sua criticidade.

Art. 54. Os processos de negócio envolvendo segurança da informação, privacidade e proteção de dados deverão ser auditados em conformidade com as normas de segurança da informação, comunicação, privacidade e proteção de dados e a pertinente legislação em vigor.

Seção XXIII
Da Gestão de Risco

Art. 55. A gestão de risco deverá ser um processo contínuo de planejamento, execução, verificação e revisão das ações, que vise manter em níveis aceitáveis os riscos de segurança da informação, comunicação, privacidade e proteção de dados, estabelecendo ações pelo valor dos ativos de informação, dados e informações e em função dos riscos de impacto nos negócios, atividades e objetivos institucionais do TCE/SC, considerando o balanceamento de aspectos como tecnologias, austeridade nos gastos, qualidade e velocidade.

Seção XXIV

Da proteção de dados e a privacidade

Art. 56. O TCE/SC deverá proteger os dados pessoais coletados ou que estejam sob sua custódia de acessos não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito que possa afetar a privacidade do titular em consonância com a LGPD e normativos expedidos pela Autoridade Nacional de Proteção de Dados (ANPD).

Seção XXV

Das Diretrizes Gerais

Art. 57. O custo dos controles não deve exceder os benefícios esperados.

Art. 58. Os controles devem ser apropriados e proporcionais.

Art. 59. Esta Resolução entra em vigor na data de sua publicação.

Florianópolis, 25 de outubro de 2021.

_____ PRESIDENTE
Adircélio de Moraes Ferreira Júnior

_____ RELATOR
Luiz Eduardo Cherem

_____
Herneus De Nadal

_____

José Nei Alberton Ascari

_____

Wilson Rogério Wan-Dall

_____

Luiz Roberto Herbst

_____

Cesar Filomeno Fontes

FUI PRESENTE

_____ PROCURADOR-GERAL ADJUNTO DO MPC

Aderson Flores