POLÍTICA DE ARMAZENAMENTO DE DADOS, DOCUMENTOS E ARQUIVOS – PADDA

Conselho Regional de Contabilidade do Estado de São Paulo

Conselho Diretor

José Aparecido Maion - **Presidente**

João Carlos Castilho Garcia - **Vice-presidente de Administração e Finanças**

Marcelo Roberto Monello - **Vice-presidente de Fiscalização, Ética e Disciplina**

Flávia Augusto - **Vice-presidente de Desenvolvimento Profissional**

Daisy Christine Hette Eastwood - **Vice-presidente de Registro**

Comissão de Implantação da Lei Geral de Proteção de Dados – LGPD do CRCSP

Domingos Sávio Mota - **Coordenador**
Cláudio Rafael Bifi – ***Vice Coordenador***

Membros

Ronaldo Cesar da Silva
Fernando Eugênio do Santos
Gilmar Pires de Simões
Valeria Vanessa de Campos Pinezi
Reginaldo Gomes Ferreira
Clarindo Bibiano de Araújo
Luiz Fernando Lopes
Luciana de Souza Ramos
Elaine Constantino Santos
Guilherme Andreas Campos Del Guerra
Andrea Fernandes dos Santos Guenka

Política de Armazenamento de Dados, Documentos e Arquivos - PADDA

(Versão 1.0)

Histórico de Alterações

Data	Versão	Descrição	Autor

Sumário

1. Introdução

As normas desta política aplicam-se aos conselheiros, empregados, colaboradores, bem como a quaisquer pessoas que tenham acesso a dados, arquivos e documentos do CRCSP.

A Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) tem por objeto: garantir condições para que os conselheiros, empregados, colaboradores e, quando aplicável, terceiros e quaisquer outras pessoas que prestem serviços ao CFC sejam orientados sobre a existência e a utilização dos instrumentos normativos, procedimentos e controles de uso e armazenamento adotados pelo CFC.

As diretrizes desta política visam assegurar que dados, documentos e arquivos digitais e não digitais de uso sensível e/ou sigiloso sejam removidos do espaço de trabalho do usuário e guardados quando não estiverem em uso ou em períodos de ausência do usuário.

As diretrizes desta política visam assegurar que dados, documentos e arquivos de uso sensível e/ou sigiloso digitais sejam armazenados de modo a garantir a sua recuperação, integridade e autenticidade, para que possam servir de fonte de prova e informação.

2. Objetivos

Esta política tem o objetivo estabelecer as melhores práticas para o manuseio e o armazenamento de documentos não digitais e arquivos digitais do CRCSP.

A PADDA está alinhada às estratégias institucionais, com a política de governança, com a gestão de riscos e com os normativos que regem a matéria.

A PADDA trata do uso e do armazenamento de dados, arquivos e documentos no âmbito do CRCSP, em todo o seu ciclo de vida, objetivando à continuidade de seus processos, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação armazenadas no âmbito do CRCSP.

Para a segurança do uso e do armazenamento da informação no CRCSP, serão rigorosamente observados o compromisso institucional com a proteção das informações de sua propriedade e/ou sob sua guarda, a participação e o cumprimento por todos os funcionários em todo o processo e o disposto neste normativo, nas disposições constitucionais, legais e regimentais vigentes.

3. Princípios Básicos

A PADDA do CRCSP orienta-se pelos seguintes princípios básicos:

I - O CRCSP deve desempenhar o papel de um custodiador de confiança;

II – O Conselho Regional de Contabilidade do Estado de São Paulo é responsável pela custódia física e legal dos documentos digitais e não digitais a ele recolhidos e inseridos nos repositórios do CRCSP como um custodiador de confiança, a PADDA deve possibilitar que o CRCSP possa:

a) atuar com neutralidade, ou seja, demonstrar que não tem razões para alterar os documentos sob sua custódia e que não permitirá que outros alterem esses documentos, acidental ou propositalmente;

b) implantar um sistema de uso, armazenamento e preservação confiável, capaz de garantir autenticidade dos documentos.

III – garantir a preservação de todos os componentes digitais e não digitais dos documentos produzidos, recebidos e armazenados de modo a permitir a apresentação desses documentos no futuro;

IV – o grau de sigilo e a restrição de acesso à informação sensível relacionados aos documentos produzidos, recebidos e armazenados têm que ser identificados explicitamente e garantidos pelo CRCSP;

V – gerenciar no repositório, a permissão de acesso de documentos com grau de sigilo e/ou que registrem informação sensível, de acordo com legislação vigente e as normas de controle de acesso definidas no âmbito do CRCSP. Essas restrições devem ser registradas em metadados e procedimentos de acesso às áreas de armazenamento de dados, documentos e arquivos do CRCSP.

4. Abrangência

O disposto neste instrumento aplicar-se-á a todos os conselheiros, funcionários e colaboradores que prestem serviços ao CRCSP e que tenham acesso a qualquer informação ou comunicação, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação.

5. Conceitos das Informações

Para os efeitos desta Política de Armazenamento de Dados, Documentos e Arquivos entende-se por:

I – Acessibilidade: facilidade no acesso ao conteúdo e ao significado de um objeto digital;

II – Armazenamento digital: guarda de documentos digitais em dispositivos de memória não volátil;

III – Armazenamento: guarda de documentos em local apropriado;

IV – Arquivamento: sequência de operações intelectuais e físicas que visam à guarda ordenada de documentos;

V – Arquivo Digital: conjunto de *bits* que formam uma unidade lógica interpretável por um programa de computador e armazenada em suporte apropriado;

VI – Ativo de informação: qualquer dispositivo de software ou hardware que agrega valor ao negócio e compõe a infraestrutura de rede de dados do CRCSP, assim como também os locais onde se encontram estes dispositivos, gestão do pessoal que a eles possuem acesso, além dos processos envolvidos na gestão e operacionalização dos ativos de informação;

VII – Banco de Dados: um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;

VIII – Computação em nuvem: modelo computacional que permite acesso, por demanda e independentemente da localização, a conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

IX – Confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

X – Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso do usuário;

XI – Cópia de Segurança: guarda de dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade;

XII – Custódia: responsabilidade jurídica de guarda e proteção de arquivos, independentemente de vínculo de propriedade;

XIII – Custodiante da informação: usuário que atua em uma ou mais fases do tratamento da informação, recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, incluindo a sigilosa;

XIV – Disponibilidade: propriedade de estar acessível e utilizável sob demanda por um usuário autorizado;

XV – Dispositivos móveis: equipamentos portáteis, dotados de capacidade computacional e

dispositivos removíveis de memória para armazenamento, entre eles, *notebooks, netbooks, smartphones, tablets, pen drives, USB drives*, HD externos e cartões de memória;

XVI – Documento arquivístico: documento produzido ou recebido no curso de uma atividade prática como instrumento ou resultado dessa atividade, retido para ação ou referência;

XVII – Documento digital: informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional;

XVIII – Documento não Digital: documento que se apresenta em suporte, formato e codificação diferente dos digitais, tais como: documentos em papel, documentos em películas e documentos eletrônicos analógicos;

XIX – Fidedignidade: credibilidade de um documento arquivístico como uma afirmação do fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no processo de sua produção;

XX – Gestão de Segurança da Informação: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação;

XXI – Incidente de segurança: evento ou conjunto de eventos de segurança da informação, indesejados ou inesperados, confirmados ou sob suspeita, que tenham grande probabilidade de comprometer as operações e ameaçar a segurança da informação;

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

XXIII – Integridade: propriedade de salvaguarda da exatidão e completeza da informação contra alterações, intencionais ou acidentais, em seu estado e atividades;

XXIV – Metadados: dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo;

XXV – Política de Segurança da Informação: documento aprovado pela autoridade responsável pelo

órgão, com objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

XXVI – Preservação: prevenção da deterioração e danos em documentos, documentos por meio de adequado controle ambiental e/ou tratamento físico e/ou químico;

XXVII – Preservação digital: conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação de documentos digitais pelo tempo que for necessário;

XXXVIII – Público-Alvo: conjunto de usuários internos e externos atendidos pela Equipe de Tratamento e Resposta a Incidentes;

XXIX – Recurso Criptográfico: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXX – Repositório arquivístico digital: repositório digital que armazena e gerencia documentos arquivísticos, seja nas idades corrente e intermediária, seja na idade permanente;

XXXI – Repositório arquivístico digital confiável: é o repositório que deve ser capaz de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável;

XXXII – Repositório digital: complexo que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de hardware, software e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos;

XXXIII – Repositório digital confiável: é um repositório digital que é capaz de manter autênticos os materiais digitais, de preservá-los e prover acesso a eles pelo tempo necessário;

XXXIV – Risco: possibilidade potencial de uma ameaça comprometer a informação ou o sistema de informação pela exploração da vulnerabilidade;

XXXV – Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;

XXXVI – Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XXXVII – Unidade Gestora de Segurança da Informação: é a unidade responsável pela gestão de segurança da informação no CFC;

XXXVIII – Unidade Organizacional: unidade em que está lotado o empregado, assessor, terceirizado, estagiário ou aprendiz;

XXXIX – Usuários: pessoa física ou jurídica que opera algum sistema informatizado do Conselho Regional de Contabilidade do Estado de São Paulo;

XL – Vulnerabilidade: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorada negativamente por uma ou mais ameaças;

6. Classificação das Informações

A classificação e o tratamento da informação, realizados por meio de procedimento definido, abrange informações provenientes dos serviços essenciais de Tecnologia da Informação do CRCSP.

As informações devem ser classificadas de forma a permitir tratamento diferenciado de acordo com o seu grau de importância, criticidade, sensibilidade e em conformidade com requisitos legais.

As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

I – **Pública**: são informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico, editais de licitação, agendas e rotinas;

II – **Interna**: são informações disponíveis aos funcionários do CRCSP para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo, em especial, memorandos, portarias, procedimentos internos, avisos e campanhas internas;

III – **Sigiloso**: são informações de acesso restrito a um funcionário ou grupo de funcionários. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros, em especial, processos judiciais e dados cadastrais de funcionários;

IV – **Sigiloso/Restrito:** são informações de acesso restrito a um funcionário ou grupo de funcionários que, obrigatoriamente, são destinatários. Em geral, informações associadas ao interesse estratégico do CRCSP estão restritas ao presidente, à diretoria, aos gerentes, chefes, supervisores e funcionários, cujas funções requeiram conhecê-las.

7. Competências

Ao Departamento de Informática compete:

I – promover e estruturar a preservação e o armazenamento dos documentos arquivísticos digitais, nas fases corrente, intermediária e permanente, que devem estar associadas a um repositório digital confiável. Os arquivos devem dispor de repositórios digitais confiáveis para a gestão, a preservação e o acesso de documentos digitais;

II – elaborar plano de ação para disponibilizar os repositórios digitais confiáveis para a gestão, a preservação e o acesso de documentos digitais, de acordo com as diretrizes previstas na Resolução nº. 39, de 29 de abril de 2014 do Conselho Nacional de Arquivos (Conarq);

III – implantar os parâmetros para repositórios arquivísticos digitais confiáveis, de forma a garantir a autenticidade, identidade, integridade, confidencialidade, disponibilidade, o acesso e a preservação, tendo em vista a perspectiva da necessidade de manutenção dos acervos documentais por longos períodos de tempo ou, até mesmo, permanentemente.

8. Responsabilidades

8.1 Usuários

Os usuários e quaisquer outras pessoas que prestem serviços ao CRCSP e tenham acesso ao ambiente de uso e armazenamento de dados, documentos e arquivos digitais e não digitais do Conselho, têm as seguintes responsabilidades:

I – ter pleno conhecimento e cumprir fielmente esta política, as normas e os procedimentos de uso e armazenamento do CRCSP;

II – solicitar esclarecimentos à Comissão de Implantação da LGPD, em caso de dúvidas relacionadas à esta Política;

III – gerenciar os dados, documentos e arquivos digitais e não digitais sob sua responsabilidade e garantir que os dados, documentos e arquivos não digitais ou digitais, equipamentos e recursos tecnológicos à sua disposição permaneça seguro;

IV – armazenar documentos não digitais em ambientes seguros, não devendo permanecer sobre a mesa de trabalho do usuário quando não estiver em uso, ou em locais onde pessoas, não autorizadas tenham acesso ao seu conteúdo;

V – remover do espaço de trabalho dados, informações, documentos e arquivos sensíveis e/ou sigilosas quando ausente e ao final do dia de trabalho;

VI – manter trancados armários com documentos sensíveis e/ou sigilosos quando não estiverem em uso;

VII – manter em sigilo as chaves/senhas/credenciais usadas para acesso a informações, documentos e arquivos sensíveis.

VIII – evitar a impressão de documentos que contenham informações sensíveis e/ou sigilosas. Em caso de impressão, remover imediatamente da impressora;

IX – restituir prontamente os documentos recebidos por empréstimo de outros departamentos, quando não forem mais necessários;

X – utilizar recursos de criptografia e guardar em locais seguros de armazenamento documentos que contenham informações sensíveis e/ou sigilosas;

XI – salvar e armazenar dentro da pasta ou unidade lógica específicas, documentos que contenham dados pessoais.

XII – zelar pela custódia de dados e informações institucionais e evitar o salvamento de conteúdos e informações pessoais em máquinas e espaço físico do Conselho;

XIII – tratar terminais particulares como se institucionais fossem;

XIV – garantir que todas as informações não digitais e digitais, sejam mantidas e armazenadas em local seguro quando não estiverem em uso;

XV – armazenar os documentos que contenham dados pessoais somente pelo período necessário ao seu uso ou cumprimento do seu dever legal e prazos de guarda e locais indicados na Tabela de Temporalidade de Documentos utilizada no CFC;

XVI – seguir os procedimentos e a legislação vigente para a eliminação de documentos digitais e não-digitais do CRCSP;

XVII – estar ciente de que toda informação digital ou não digital armazenada, processada e transmitida no ambiente computacional ou físico do CRCSP pode ser auditada.

8.2 Custodiante

Ao Custodiante da Informação cabem as seguintes responsabilidades:

I – cumprir e zelar pela observância integral das diretrizes desta política e demais normas e procedimentos decorrentes;

II – zelar pela disponibilidade, integridade e confidencialidade das informações e recursos em qualquer suporte sob sua custódia, conforme condições estabelecidas nesta política e demais normas e procedimentos referentes ao uso e armazenamento de dados, documentos e arquivos;

III – participar de capacitação e treinamento em procedimentos de uso e armazenamento de dados, documentos e arquivos, quando convocado;

IV – proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;

V – comunicar prontamente ao seu gestor imediato e ao Comitê de Segurança da Informação qualquer incidente de que tenha conhecimento ou situações que comprometam a disponibilidade, integridade e confidencialidade das informações armazenadas.

8.3 Gestores dos Departamentos

Os Gestores dos Departamentos são responsáveis por:

I – ter postura exemplar em relação ao uso e armazenamento de dados, documentos e arquivos para servir como modelo de conduta para os funcionários sob sua gestão;

II – cumprir e fazer cumprir esta política;

III – adotar os procedimentos necessários sempre que identificar descumprimentos da política.

9. Divulgação e atualização

Esta política e suas atualizações, após publicação, deverão ser amplamente divulgadas aos usuários e disponibilizadas no portal do CRCSP e em sua intranet (*Flow*), sendo consideradas um documento de relevante interesse público.

Esta Política de Armazenamento de Dados, Documentos e Arquivos deverá ser revisada sempre que se fizer necessário.

Os casos omissos desta política serão resolvidos pela Comissão da LGPD do CRCSP.