RESOLUÇÃO CRCPR Nº 846/2022, DE 28 DE OUTUBRO DE 2022.

Institui a Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do Conselho Regional de Contabilidade do Paraná - CRCPR.

O **Plenário do CONSELHO REGIONAL DE CONTABILIDADE DO PARANÁ - CRCPR**, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir ambientes digitais e não digitais controlados, eficientes e seguros, de forma a oferecer todas as informações necessárias à classe contábil e à sociedade com integridade, confidencialidade e disponibilidade,

CONSIDERANDO que o Conselho Regional de Contabilidade do Paraná recebe e produz informações de caráter e procedência diversos, as quais devem permanecer íntegras, disponíveis e, nas situações em que a observância for obrigatória, com o sigilo resguardado;

CONSIDERANDO que no CRCPR as informações são armazenadas de diferentes formas, veiculadas em diferentes meios físicos e eletrônicos e são, portanto, vulneráveis a incidentes como casos fortuitos e de força maior, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

CONSIDERANDO o número progressivo de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança da informação;

CONSIDERANDO a Lei Federal n.º 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD), de 14 de agosto de 2018, 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 Decreto n.º 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação, em especial o inciso II do Art. 15;

CONSIDERANDO o Decreto n.º 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

CONSIDERANDO a Instrução Normativa n.º 1 (GSI), de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

CONSIDERANDO a Resolução Conarq n.º 43, de 04 de setembro de 2015, que estabelece diretrizes para a implementação de repositórios arquivísticos digitais confiáveis para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente, dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (Sinar);

CONSIDERANDO a Resolução Conarq n.º 38, de 9 de julho de 2013, que dispõe sobre a adoção das "Diretrizes do Produtor – A Elaboração e a Manutenção de Materiais Digitais: Diretrizes Para

Indivíduos" e das "Diretrizes do Preservador – A Preservação de Documentos Arquivísticos digitais: Diretrizes para Organizações";

CONSIDERANDO a Recomendação Técnica do Arquivo Nacional n.º 2, de junho de 2019, que dispõe sobre as Recomendações para Elaboração de Política de Preservação Digital;

CONSIDERANDO a necessidade de estabelecer responsabilidade internas quanto ao armazenamento de dados, documentos e arquivos,

RESOLVE:

Art. 1° Fica instituída a Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do Conselho Regional de Contabilidade do Paraná – CRCPR, nos termos do Anexo I desta Resolução.

Parágrafo único. Todos os instrumentos normativos gerados a partir da Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do Conselho Regional de Contabilidade do Paraná são partes integrantes desta e emanam dos princípios e diretrizes nela estabelecidos.

Art. 2° A Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do CRCPR se aplica a todos os conselheiros, empregados, estagiários, prestadores de serviços e, quando aplicável, a terceiros e a quaisquer outras pessoas que prestem serviços ao CRCPR e que tenham acesso a qualquer documento, arquivo e meio de informação e 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 ou por meio de outros recursos.

Art. 3° A íntegra da Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do Conselho de Contabilidade do Paraná será disponibilizada em seu Portal e em sua intranet.

Art. 4° Esta Resolução entrará em vigor na data de sua publicação no Diário Oficial do Estado do Paraná (DOE-PR), cujo inteiro teor estará disponível no portal da Transparência do CRCPR (https://www3.crcpr.org.br/transparencia/portal/), revogando-se as disposições em contrário.

ORIGINAL ASSINADO
Contador **LAUDELINO JOCHEM**
Presidente
CO – CRCPR Nº 44.143/O

ORIGINAL ASSINADO

ALBERTO BARBOSA
CO – CRCPR Nº 31.006/O

ORIGINAL ASSINADO

ANSELMO LUIZ PEDRANGELO
CO - CRCPR Nº 71.010/O

ORIGINAL ASSINADO

ARIANE YUMI DE ALMEIDA ROCHA
CO - CRCPR Nº 40.667/O

ORIGINAL ASSINADO

CARLOS AUGUSTO BITTENCOURT GOMES
TC – CRCPR Nº 45.041/O

ORIGINAL ASSINADO

CESAR ALBERTO PONTE DURA
CO - CRCPR Nº 30.816/O

ORIGINAL ASSINADO

CLAUDEMIR APARECIDO MATIUSSO
CO – CRCPR Nº 42.270/O

ORIGINAL ASSINADO

CLAUDIO LUIZ BRUNETTO
CO - CRCPR Nº 40.176/O

ORIGINAL ASSINADO

DANIELLA NOVAK
CO – CRCPR Nº 72.852/O

ORIGINAL ASSINADO

DANILO ALVES GRANI
CO – CRCPR Nº 56.387/O

ORIGINAL ASSINADO

EUNICE MARIA CAVALI DUARTE
CO – CRCPR Nº 34.322/O

ORIGINAL ASSINADO

EVA SCHRAN DE LIMA
CO - CRCPR Nº 30.116/O

ORIGINAL ASSINADO

EVERSON LUIZ BREDA CARLIN
CO – CRCPR Nº 29.607/O

ORIGINAL ASSINADO

FERNANDO ANTONIO BORAZO RIBEIRO
CO - CRCPR Nº 32.263/O

ORIGINAL ASSINADO

FRANCISCO SAVI
CO - CRCPR Nº 31.030/O

ORIGINAL ASSINADO

JEFFERSON PAULO MARTINS
CO - CRCPR Nº 35.401/O

ORIGINAL ASSINADO

JOÃO GELASIO WEBER
TC – CRCSC Nº 10.131/O-T

ORIGINAL ASSINADO

LAURI HELFENSTEIN
CO - CRCPR Nº 19.967/O

ORIGINAL ASSINADO

LUIZ FERNANDO FERRAZ
CO - CRCPR Nº 13.542/O

ORIGINAL ASSINADO

MARCIA OGIDO HOKAMA
CO - CRCPR Nº 34.399/O

ORIGINAL ASSINADO

MICHEL GULIN MELHEM
CO – CRCPR Nº 64.351/O

ORIGINAL ASSINADO

NARCISO DÓRO JUNIOR
CO - CRCPR Nº 33.171/O

ORIGINAL ASSINADO

RAFAEL BENJAMIM CARGNIN FILHO
CO - CRCPR Nº 21.538/O

ORIGINAL ASSINADO

RODINEI BONFADINI
CO - CRCPR Nº 42.621/O

ORIGINAL ASSINADO

ROSEMERE KIYOMI HAYASHI
CO – CRCPR Nº 35.176/

Aprovada na 1.380ª Reunião Plenária, realizada em 28 de outubro de 2022.

ANEXO I

POLÍTICA DE ARMAZENAMENTO DE DADOS, DOCUMENTOS E ARQUIVOS (PADDA) DO CRCPR

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Seção I
DAS PREMISSAS

Art. 1° As normas desta política aplicam-se aos conselheiros, empregados, colaboradores, delegados, bem como a quaisquer pessoas que tenham acesso a dados, arquivos e documentos do CRCPR.

Art. 2° A Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) tem por objeto:

I – garantir condições para que os conselheiros, empregados, colaboradores, delegados e, quando aplicável, terceiros e quaisquer outras pessoas que prestem serviços ao CRCPR sejam orientados sobre a existência e a utilização dos instrumentos normativos, procedimentos e controles de uso e armazenamento adotados pelo CRCPR.

Art. 3° 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 em local apropriado,-em períodos de ausência do usuário ou quando não estiverem em uso.

Art. 4° As diretrizes desta política visam assegurar que dados, documentos e arquivos digitais de uso sensível e/ou sigiloso sejam armazenados de modo a garantir a sua recuperação, integridade e autenticidade, para que possam servir como fonte de prova e informação.

Seção II
DOS OBJETIVOS

Art. 5° Esta política tem o objetivo de estabelecer as melhores práticas para o manuseio e o armazenamento de documentos não digitais e arquivos digitais do CRCPR.

Parágrafo único. 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.

Art. 6° A PADDA trata do uso e do armazenamento de dados, arquivos e documentos no âmbito do CRCPR, 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 CRCPR.

Art. 7° Para a segurança do uso e do armazenamento da informação no CRCPR, 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 colaboradores, em todo o processo e o disposto neste normativo, nas disposições constitucionais, legais e regimentais vigentes.

Seção III
DOS PRINCÍPIOS BÁSICOS

Art. 8° A PADDA do CRCPR orienta-se pelos seguintes princípios básicos:

I. o CRCPR deve desempenhar o papel de um custodiador de confiança;
II. o Conselho Regional de Contabilidade do Paraná é responsável pela custódia física e legal dos documentos digitais e não digitais a ele recolhidos e inseridos em seus repositórios. A PADDA possibilita que o CRCPR possa:

a) atuar com neutralidade, demonstrando não ter 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 CRCPR;
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 CRCPR. Essas restrições devem ser registradas em metadados e em procedimentos de acesso às áreas de armazenamento de dados, documentos e arquivos do CRCPR.

Seção IV
DA ABRANGÊNCIA

Art. 9° O disposto neste instrumento aplicar-se-á a todos os conselheiros, empregados, delegados e colaboradores que prestem serviços ao CRCPR 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.

CAPÍTULO II

DOS CONCEITOS E DA CLASSIFICAÇÃO DAS INFORMAÇÕES

Seção I

DOS CONCEITOS E DAS DEFINIÇÕES

Art. 10. 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 de *hardware* que agrega valor ao negócio e compõe a infraestrutura de rede de dados do CRCPR, assim como os locais onde se encontram esses dispositivos e 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 mínimos esforços 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 de informação, recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação ou controle, incluindo-se, aqui, a informação considerada sigilosa.
XIV. Disponibilidade: propriedade de estar acessível e utilizável, sob demanda, por 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, cartões de memória e afins.

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 e 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;

XXVIII. 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 utilize 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 por procedimentos normativos e técnicos;

XXXIII. Repositório digital confiável: é um repositório digital que é capaz de manter autênticos os materiais digitais, preservando-os e provendo-lhes acesso 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 consideradas sigilosas;

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

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 Paraná;

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

Seção II
DA CLASSIFICAÇÃO DAS INFORMAÇÕES

Art. 11. A classificação e o tratamento da informação, realizados por meio de procedimento definido, abrangem informações provenientes dos serviços essenciais de Tecnologia da Informação do CRCPR.

Parágrafo único. 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.

Art. 12. As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis, conforme estabelecido na Política de Classificação da Informação do CRCPR:

I. Pública – a informação cujo acesso pode ser franqueado a qualquer pessoa. Com menor nível de controle, pode ser divulgada a todos sem prejuízo, sendo permitida a veiculação a funcionários, fornecedores, terceirizados, clientes e ao público em geral.

II. Interna – a informação que somente os funcionários e prestadores de serviços do CRCPR podem ter acesso. O vazamento ocasional pode gerar prejuízo ao negócio. Contudo, seu grau de sigilo ainda é baixo.

III. Secreta – a informação que somente pode ser acessada pelas pessoas da área envolvida (Ex. Comercial, Financeiro etc.). Seu vazamento pode causar prejuízo significativo, como perdas financeiras, competitividade ou de imagem no mercado. Necessária a implantação de controle de acesso e integridade. Quando descartada não pode ser possível recuperá-la.

IV. Sigilosa – a informação enquadrada nas hipóteses de sigilo previstas em legislação específica, tal como a de natureza fiscal, a bancária, a relacionada a operações e serviços no mercado de capitais, a protegida por sigilo comercial, profissional, industrial ou por segredo de justiça e aquela relativa a denúncias. Acesso apenas à Diretoria da empresa, que será responsável por liberar os acessos apenas a profissionais específicos.

CAPÍTULO III
DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I
DAS COMPETÊNCIAS

Art. 13. À Comissão Permanente de Avaliação de Documentos (CPAD) sob a supervisão da Gerência Operacional 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 n.º 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.

Seção II
DAS RESPONSABILIDADES

Subseção I
DOS USUÁRIOS

Art. 14. Os usuários e quaisquer outras pessoas que prestem serviços ao CRCPR 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 CRCPR.
II. Em caso de dúvidas relacionadas a esta política, solicitar esclarecimentos à Comissão de Governança, Riscos, Compliance e LGPD.
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 permaneçam seguros.

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 sigilosos 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 outras unidades, 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 de pasta ou unidade lógica específica, documentos que contenham dados pessoais.

XII. Zelar pela custódia de dados e de informações institucionais e evitar o salvamento de conteúdos e de 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 de seu dever legal e prazos de guarda e locais indicados na Tabela de Temporalidade de Documentos utilizada no CRCPR.

XVI. Seguir os procedimentos e a legislação vigente para a eliminação de documentos digitais e não-digitais do CRCPR.

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

Subseção II
DO CUSTODIANTE

Art. 15. Ao Custodiante da Informação, cabem as seguintes responsabilidades:

I. Cumprir e zelar pela observância integral das diretrizes desta política e das demais normas e procedimentos decorrentes.

II. Zelar pela disponibilidade, integridade e confidencialidade das informações e de recursos, em qualquer suporte, sob sua custódia, conforme condições estabelecidas nesta política e em 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 autorizados.

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

Subseção III

DOS GESTORES DAS UNIDADES ORGANIZACIONAIS

Art. 16. Os Gestores das Unidades Organizacionais são responsáveis por:

I. Ter postura exemplar em relação ao uso e ao armazenamento de dados, documentos e arquivos, para servir como modelo de conduta para os colaboradores sob sua gestão.

II. Cumprir e fazer cumprir esta política.

III. Adotar os procedimentos necessários sempre que identificar descumprimentos da política.

CAPÍTULO IV
DA DIVULGAÇÃO E ATUALIZAÇÃO

Art. 17. Esta política e suas atualizações, após publicação, deverão ser amplamente divulgadas aos usuários e disponibilizadas no portal do CRCPR e em sua intranet, sendo consideradas um documento de relevante interesse público.

Art. 18. Esta Política de Armazenamento de Dados, Documentos e Arquivos deverá ser revisada sempre que se fizer necessário.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 19. Os casos omissos desta política serão resolvidos pelo Comitê Gestor de Privacidade e Proteção de Dados do CRCPR.

Art. 20. Esta política entra em vigor na data de sua publicação.