Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Política de Retenção de Dados

Objetivo

Estabelecer os períodos de retenção de todas as informações e dados da Instituição, definindo os padrões mínimos a serem aplicados na eliminação de dados e informações da Instituição.

Visão Geral

Esta política aplica-se a todas as informações usadas na Instituição, incluindo endereços de e-mail, documentos impressos, documentos digitais, gravações de vídeo, gravações de áudio e dados gerados por sistemas de controle de ponto.

1. Programa Geral de Retenção de Dados e Informações

O período de retenção de Dados Pessoais exigido para os fins desta Política será definido de acordo com a base legal de tratamento de cada um dos Dados Pessoais da Instituição, e após a utilização estes dados deverão ser devidamente eliminados, segundo os preceitos desta política, ou anonimizados, segundo os preceitos da Política de Anonimização e Pseudonimização.

Para tanto, o cronograma de retenção de dados pessoais deve ser concebido da seguinte maneira:

EMBRASI

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

- Os Dados Pessoais tratados de acordo com as bases legais contidas no art. 7º da LGPD serão retidos pelo período máximo de 10 anos após o tratamento;

- Os dados pessoais sensíveis tratados de acordo com as bases legais contidas no art. 11 da LGPD serão retidos pelo período máximo de 10 anos após o tratamento;

- Os Dados Pessoais de Crianças e Adolescentes tratados de acordo com as bases legais contidas no art. 14 da LGPD serão retidos pelo período máximo de 10 anos após o tratamento.

Os demais documentos e registros da Instituição que não contenham Dados Pessoais, mas que contenham quaisquer informações relevantes serão retidos pelo período máximo de 10 anos.

Poderão existir exceções aos períodos de retenção nos seguintes casos:

- Investigações em andamento por autoridades brasileiras, havendo necessidade de manutenção de dados para que a Instituição comprove o eventual cumprimento legislações e regulações aplicáveis; ou

- Na existência de litígios e processos judiciais ou administrativos envolvendo a Instituição.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

2. Backup dos Dados Pessoais

Durante o período de retenção, deve-se realizar periodicamente o backup dos dados de acordo com a Política de *Backup* da Instituição.

3. Eliminação dos Dados Pessoais

A Instituição deve rever periodicamente a finalidade de tratamento e a relevância de todos os dados que retiver, sejam estes dados mantidos em meio eletrônico ou em meio físico. Os dados irrelevantes, ou cuja finalidade de tratamento cessou, devem ser excluídos, triturados ou destruídos, dependendo da sua forma de armazenamento e atentando-se ao seu nível de confidencialidade.

O método de destruição é determinado pelo Responsável pela Segurança da Informação junto com as partes interessadas e depende da natureza do documento. Quaisquer documentos que contenham informações sensíveis ou confidenciais (incluindo dados pessoais sensíveis ou referentes a crianças e adolescentes) devem ser destruídos como lixo confidencial (meio físico) ou estarem sujeitos à eliminação eletrônica segura (meio eletrônico).

Os integrantes da Instituição devem executar a destruição de dados de maneira adequada, com especial atenção àquelas diretrizes dispostas na Política de Segurança da Informação e na Política de Privacidade e Proteção de Dados Pessoais da Instituição.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Devem existir controles apropriados que garantam a integridade e a disponibilidade das informações essenciais aos negócios da Instituição. Para tal, o Responsável pela Segurança da Informação deve documentar e aprovar qualquer processo de destruição de informações dentro da Instituição.

4. Métodos de Eliminação de Dados Pessoais

O descarte de informações dentro da Instituição será realizado pela caracterização dos documentos em três níveis distintos.

Os **documentos de Nível I** são aqueles que contêm informações de mais alta segurança e confidencialidade e aqueles que incluem Dados Pessoais Sensíveis, inclusive Dados Pessoais de crianças e adolescentes. Estes documentos devem ser eliminados como lixo confidencial (triturado transversalmente e incinerados) ou estarão sujeitos a uma eliminação eletrônica segura. A destruição dos documentos deve incluir a prova da destruição.

Os **documentos de Nível II** são documentos proprietários que contêm informações confidenciais, como nomes, assinaturas e endereços de terceiros, ou que podem ser usados por terceiros para cometer fraudes, mas que não contêm dados pessoais. Os documentos devem ser cortados transversalmente e depois colocados em lixeiras trancadas para recolha por uma Instituição de eliminação aprovada. Se forem documentos eletrônicos, estarão sujeitos à eliminação eletrônica segura. A destruição dos documentos deve incluir a prova da destruição

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Os **documentos de Nível III** são aqueles que não contêm informações confidenciais ou dados pessoais e são documentos da Instituição publicados. Estes devem ser triturados ou descartados através de uma Instituição de reciclagem e incluir, entre outras coisas, anúncios, catálogos panfletos e boletins informativos. A destruição dos documentos não necessita incluir prova de destruição.

5. Rotinas de Eliminação de Informações Não-Confidenciais

Os registros que não contenham quaisquer dados ou informações confidenciais da Instituição, a menos que sujeitos a uma investigação legal ou regulatória em andamento, serão considerados de **Nível III** e serão eliminados em períodos não superiores a 01 ano, tais como:

- Anúncios e avisos de reuniões diárias e outros eventos, incluindo aceitações e pedidos de desculpas;
- Solicitações de informações comuns, como rotas de viagens;
- Reservas para reuniões internas sem cobranças ou custos externos;
- Transmissão de documentos, tais como cartas, folhas de ponto, mensagens de e-mail ou postal, folhetos e itens semelhantes que acompanham documentos, mas não adicionam qualquer valor;

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

- Lista de endereços substituídas, listas de distribuição, dentre outros documentos desatualizados;
- Duplicação de documentos como cópias de documentação de identificação pessoal, rascunho inalterados, impressões de *screenshots* ou extratos de bancos de dados e arquivos diários;
- Publicações internas de estoque obsoletas; e
- Revistas comerciais, catálogos de fornecedores, folhetos e boletins informativos de fornecedores ou outras organizações externas.