LGPD
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Relacionamento entre Ciclo de Vida do Tratamento de Dados Pessoais e Ativos Organizacionais

Saudações, colegas e colaboradores! Vimos nas últimas publicações explicações sobre as fases do ciclo de tratamento de dados e posteriormente os ativos organizacionais relevantes. Pois bem, para cada fase do ciclo de tratamento de dados é importante identificar os ativos organizacionais que estarão envolvidos.

Na fase de **Coleta** deve-se identificar os ativos envolvidos no processo de obtenção de dados pessoais. Eles podem entrar na organização por um **documento**, **sistema** hospedado em **equipamento** instalado em **local físico** do órgão público, como por exemplo um Data Center. Podem ser coletados pela prestação de algum serviço externo ou serviço prestado pelo próprio órgão público por meio de alguma de suas **unidades organizacionais**.

Na fase de **Retenção**, deve-se avaliar os ativos utilizados para armazenar os dados pessoais. Esses dados podem estar armazenados em bases de dados, documentos, equipamentos ou sistemas. É preciso considerar também as **unidades organizacionais** responsáveis pelo armazenamento e guarda dos dados, bem como os **locais físicos** onde estão localizados os ativos que armazenam esses dados. Se o armazenamento for em "nuvem", por exemplo, é necessário considerar o serviço de armazenamento contratado e/ou utilizado.

A fase de **Processamento** segue a mesma linha de raciocínio das anteriores. Identifica-se os ativos onde são realizados os tratamentos dos dados. O tratamento pode ser realizado em **documento**, pode ser feito por um **sistema** interno ou contratado pelo órgão. É preciso identificar as pessoas (papeis organizacionais), **unidade organizacionais e equipamentos** envolvidos nesse tratamento. Onde estão **localizadas fisicamente** essas unidades organizacionais e os equipamentos envolvidos nesse tratamento também são importantes.

Na fase de **Compartilhamento** é preciso mapear os ativos envolvidos na distribuição ou divulgação dos dados pessoais para dentro e para fora do órgão público. Quais **sistemas** são usados para transmitir, exibir ou divulgar dados pessoais? Quais **pessoas** são destinatárias dessas informações? Quais **unidades organizacionais**, quais **equipamentos** são usados para tal?

No que se refere à fase de **Eliminação**, deve-se avaliar os ativos que armazenam os dados pessoais que possam ser objeto de solicitação de eliminação a pedido do titular dos dados pessoais; ou descarte nos casos necessários ao negócio da instituição. Os dados pessoais a serem eliminados podem estar armazenados em ativos relacionados com **bases de dados, documentos, equipamentos ou sistemas**. É necessário considerar também as **unidades organizacionais** responsáveis pelo armazenamento e guarda dos dados que possam ser objeto de eliminação ou descarte, bem como os **locais físicos** onde estão localizados os ativos que contenham dados a serem eliminados ou descartados. Se a eliminação do dado pessoal ou descarte do ativo tiver relação com solução em "nuvem", por exemplo, é preciso considerar o serviço de armazenamento contratado ou utilizado.

Fique atento à próxima publicação, quando continuaremos a abordar a relação entre as fases do tratamento de dados pessoais e os ativos organizacionais!

LGPD
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

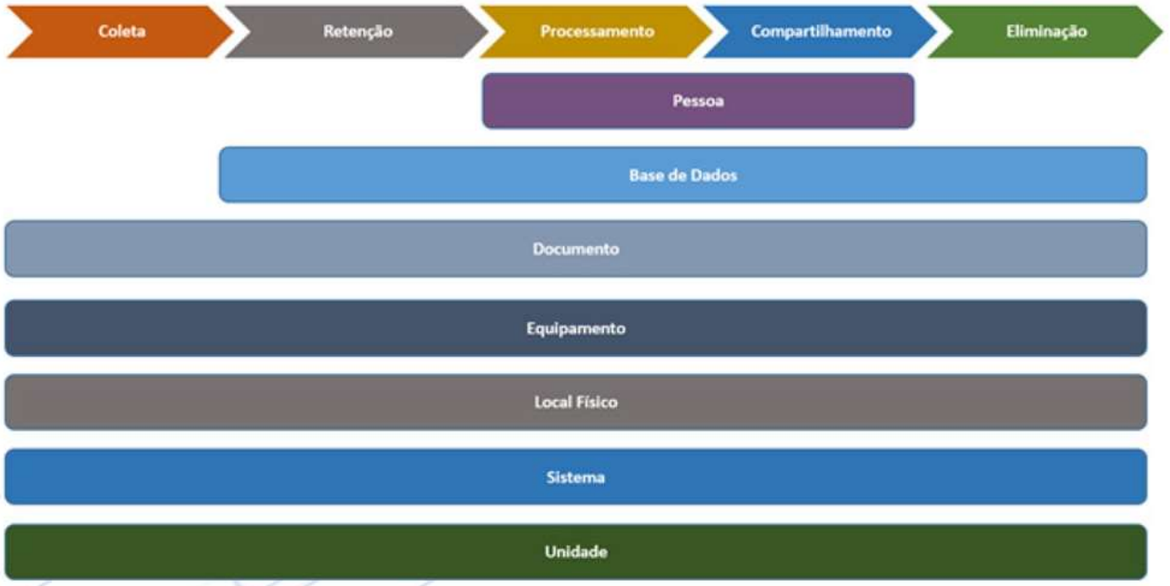
Relacionamento entre Ciclo de Vida do Tratamento de Dados Pessoais e Ativos Organizacionais

Olá! Hoje daremos continuidade à análise do relacionamento entre as fases do tratamento de dados pessoais e os ativos organizacionais envolvidos.

Quando os dados pessoais estiverem contidos em documentos arquivísticos, qualquer que seja o suporte ou formato, esses dados poderão ser tratados no contexto da LGPD, mas os documentos arquivísticos propriamente ditos, deverão seguir os procedimentos definidos pela gestão de documentos.

Esse processo demanda esforço considerável, principalmente para grandes organizações. O ideal é que se estabeleçam ações de mapeamento e análise dos processos organizacionais, tendo em vista que, desta forma, o órgão conseguirá identificar de maneira mais eficaz os ativos descritos anteriormente.

Por exemplo, a figura abaixo apresenta o relacionamento entre as fases do ciclo de tratamento de dados pessoais e os ativos que podem ser utilizados em cada etapa. É importante registrar, assim, que existem ativos presentes em todas as fases do ciclo (ex: Documento) e outros que estarão em apenas algumas delas (ex: Pessoa).



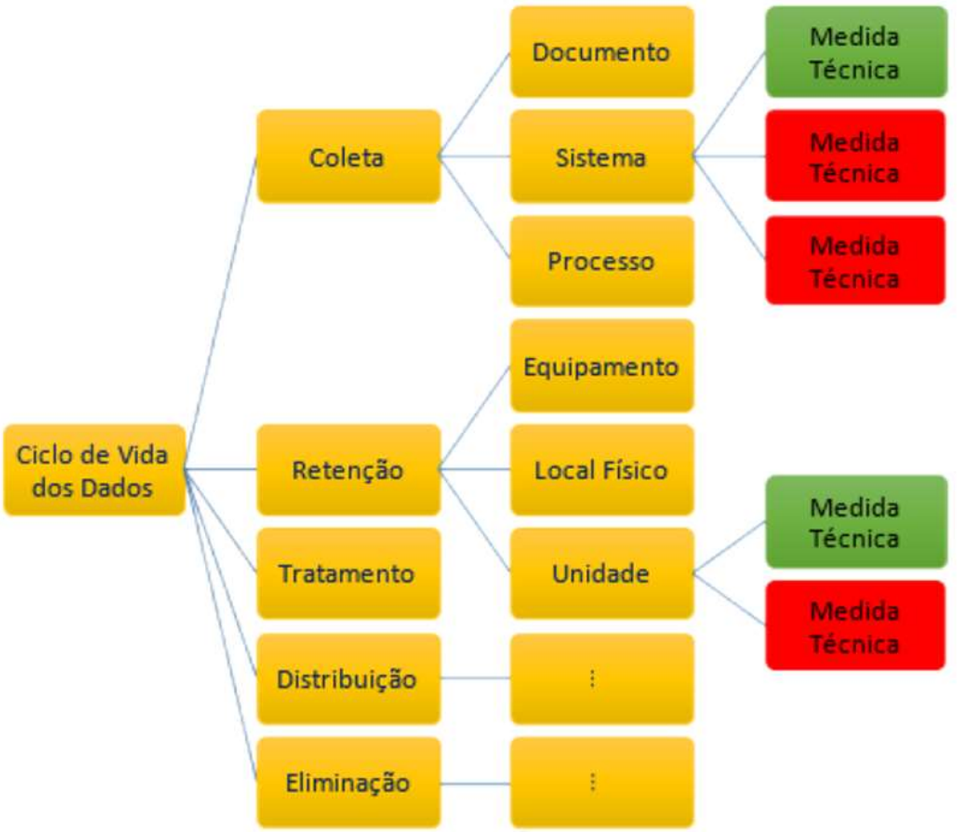
Uma vez identificados os ativos, é necessário analisá-los para verificar quais medidas técnicas de segurança estão efetivamente implementadas nesses ativos, com vistas a prover a adequada proteção aos dados pessoais de que trata a LGPD.

Recomenda-se a utilização de algum framework, boa prática ou norma técnica aplicável como a ABNT NBR ISO/IEC 27001 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos; ABNT NBR ISO/IEC 27002 – Código de Prática para controles de segurança da informação; ABNT NBR ISO/IEC 27701 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; ISO/IEC 29151 – Code of practice for personally identifiable information protection; CIS® (Center for Internet Security, Inc.®) Controls™ e ISO/IEC 29134 - Guidelines for privacy impact assessment.

LGPD
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Relacionamento entre Ciclo de Vida do Tratamento de Dados Pessoais e Ativos Organizacionais

O resultado dessa análise vai determinar quais medidas de segurança devem ser implementadas em cada ativo e quais devem ser ajustadas para que o órgão público possua o adequado grau de proteção de dados exigido pela LGPD. A figura abaixo apresenta esquema de mapeamento dos ativos e suas respectivas medidas de segurança implementadas (destacadas em verde) e não implementadas (destacadas em vermelho).



Até a próxima publicação!

LGPD
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

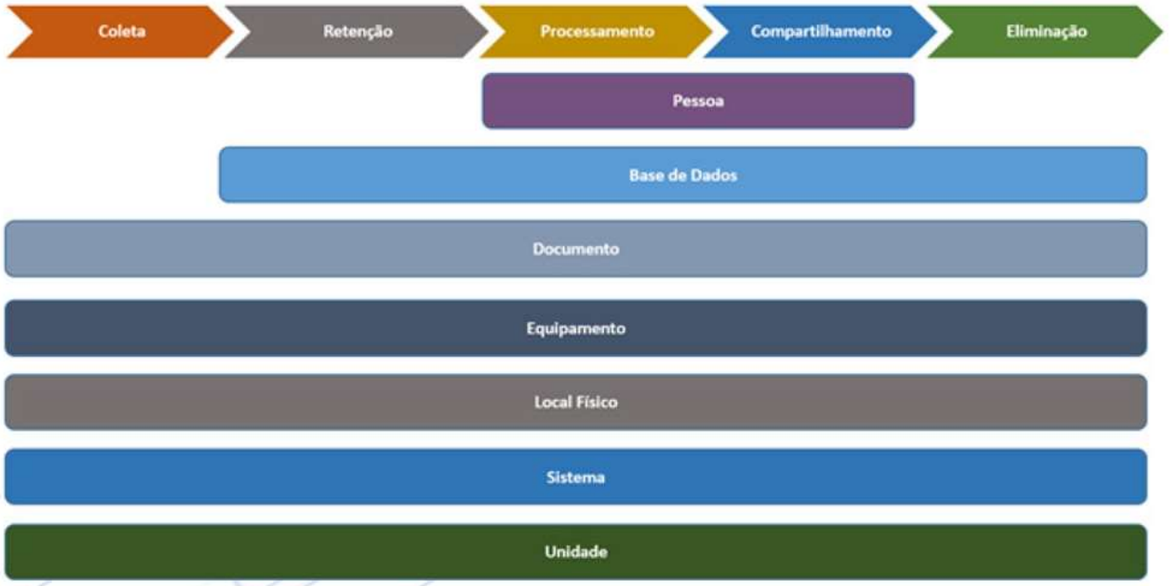
Relacionamento entre Ciclo de Vida do Tratamento de Dados Pessoais e Ativos Organizacionais

Olá! Hoje daremos continuidade à análise do relacionamento entre as fases do tratamento de dados pessoais e os ativos organizacionais envolvidos.

Quando os dados pessoais estiverem contidos em documentos arquivísticos, qualquer que seja o suporte ou formato, esses dados poderão ser tratados no contexto da LGPD, mas os documentos arquivísticos propriamente ditos, deverão seguir os procedimentos definidos pela gestão de documentos.

Esse processo demanda esforço considerável, principalmente para grandes organizações. O ideal é que se estabeleçam ações de mapeamento e análise dos processos organizacionais, tendo em vista que, desta forma, o órgão conseguirá identificar de maneira mais eficaz os ativos descritos anteriormente.

Por exemplo, a figura abaixo apresenta o relacionamento entre as fases do ciclo de tratamento de dados pessoais e os ativos que podem ser utilizados em cada etapa. É importante registrar, assim, que existem ativos presentes em todas as fases do ciclo (ex: Documento) e outros que estarão em apenas algumas delas (ex: Pessoa).



Uma vez identificados os ativos, é necessário analisá-los para verificar quais medidas técnicas de segurança estão efetivamente implementadas nesses ativos, com vistas a prover a adequada proteção aos dados pessoais de que trata a LGPD.

Recomenda-se a utilização de algum framework, boa prática ou norma técnica aplicável como a ABNT NBR ISO/IEC 27001 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos; ABNT NBR ISO/IEC 27002 – Código de Prática para controles de segurança da informação; ABNT NBR ISO/IEC 27701 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; ISO/IEC 29151 – Code of practice for personally identifiable information protection; CIS® (Center for Internet Security, Inc.®) Controls™ e ISO/IEC 29134 - Guidelines for privacy impact assessment.