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 Anonimização e Pseudoanonimização.

Objetivo

Estabelecer as diretrizes de gerenciamento da confidencialidade das informações mantidas pela Instituição, através da realização de procedimentos diretos ou indiretos que impeçam a revelação destas informações.

Visão Geral

A escolha dos procedimentos de anonimização e pseudonimização observará a natureza e o volume dos Dados Pessoais mantidos pela Instituição. Quanto maior o volume ou mais sensível a natureza dos Dados Pessoais, maior deve ser o grau de anonimização.

1. Técnicas de anonimização de Informações e Dados

Consideram-se procedimentos de anonimização:

a) Supressão de seção

Definição: procedimento que visa a retirada integral de determinada seção ou coluna da base de dados.

EMBRASI

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

Quando aplicar: ocasiões em que a seção não for necessária ao conjunto de dados anonimizados, ou quando a seção não puder ser anonimizada de forma segura por outras técnicas.

Como aplicar: deve-se proceder com a eliminação permanente da seção que contenha os dados.

Observação: considera-se essa técnica uma das mais segura, pois não há forma de recuperar a informação apagada.

b) Supressão de registro

Definição: procedimento que visa a retirada integral de determinado registro ou linha da base de dados.

Quando aplicar: ocasiões em que o registro não puder ser seguramente protegido por outras técnicas.

Como aplicar: deve-se proceder com a eliminação permanente do registro que contenha os dados.

Observação: considera-se essa técnica a mais segura, pois não há forma de recuperar a informação apagada. Ressalte-se que esta técnica pode interferir na aferição de termos estatísticos, como médias ou medianas.

c) Supressão de valores

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

Definição: procedimento que visa a retirada parcial ou integral de determinados valores dentro de uma célula contida nas bases de dados da Instituição.

Quando aplicar: ocasiões em que a mera supressão de caracteres forneça o grau de anonimização necessário.

Como aplicar: deve-se proceder com a eliminação parcial ou integral de alguns caracteres da célula (substituindo-os pelos caracteres "*" ou "x").

Observação: deve-se atentar a aplicação desta técnica principalmente àqueles dados que permitam diferenciar pessoas homônimas, como por exemplo o nº de CPF, do RG, da CNH, da CTPS ou do cartão de crédito do titular.

d) Generalização

Definição: procedimento que visa a redução deliberada da precisão das informações contidas nas bases de dados da Instituição.

Quando aplicar: em ocasiões em que, mesmo após generalizados, os dados ainda sejam úteis para a finalidade pretendida.

Como aplicar: deve-se proceder com a concepção de categorias de dados com as dimensões apropriadas à necessidade de tratamento.

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

Observação: deve-se atentar para a utilização de informação derivada da informação principal, como por exemplo, substituição da data de nascimento pela faixa etária ou do endereço pela área de residência.

e) Pseudoanonimização

Definição: procedimento que visa atrelar determinados valores da base de dados da Instituição a um pseudônimo inventado. Pode ser irreversível, com a eliminação dos valores originais nas bases de dados da Instituição, ou reversível, com a manutenção dos valores originais nas bases de dados da Instituição de maneira segura e criptografada.

Quando aplicar: em ocasiões que os valores dos dados necessariamente devam ser distinguidos e individualizados uns dos outros.

Como aplicar: deve-se proceder com a substituição dos valores originais por aleatórios, que devem ser únicos e não devem ter relação com os valores originais.

Observações: para pseudônimos reversíveis, a base de dados com os valores originais não pode ser compartilhada, devendo ser mantida pela Instituição apenas para resolver questões específicas. Caso seja utilizada encriptação, os métodos de encriptação não devem ser compartilhados e devem ser revistos periodicamente, seguindo-se o disposto na Política de Criptografia.

f) Agregação

Definição: procedimento que visa somar os valores da base de dados da Instituição, mostrando apenas os resultados totais do tratamento.

Quando aplicar: ocasiões em que os registros individuais não sejam necessários e os dados agregados sejam suficientes para o objetivo pretendido.

Como aplicar: deve-se proceder com a utilização de medições totais e médias para a base de dados, bem como a aplicação de outras medidas estatísticas.

Observação: deve-se atentar para a omissão ou ofuscamento dos valores individuais de cada célula, sendo aplicada em conjunto com a supressão.

2. Diretrizes de anonimização

Tendo em vista que nenhum dos procedimentos acima é capaz de, por si só, garantir a anonimização dos Dados Pessoais contidos nas bases de dados da Instituição, deve-se observar as seguintes diretrizes:

- Limitação do número de pessoas e fornecedores com acesso às bases de dados da Instituição que contenham Dados Pessoais, de acordo com os níveis de confidencialidade da informação previstos na Política de Segurança da Informação e com as disposições do art. 13 do Regulamento do Marco Civil da Internet (Decreto nº 8.771/16);

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

- Controle restrito do acesso às informações capazes de reverter os processos de anonimização e pseudonimização da base de dados da Instituição, de acordo com os níveis de confidencialidade da informação previstos na Política de Segurança da Informação e com as disposições do art. 13 do Regulamento do Marco Civil da Internet (Decreto nº 8.771/16);

- Segregação das bases de dados da Instituição, limitando os riscos internos de reversão do processo de anonimização;

- Previsão contratual de proibição de reversão do processo de anonimização, de delimitação de papeis de acordo com o objeto da atividade de tratamento e de eliminação dos dados tão logo concluído o tratamento ou condição resolutiva;

- A revisão e atualização periódicas dos procedimentos de anonimização e pseudonimização, com o fito de garantir a melhoria contínua destes procedimentos.