1 OBJETIVO

Este documento tem por objetivo estabelecer as orientações sobre quando e como anonimizar ou pseudonimizar dados pessoais, bem como sobre o nível desejado de identificabilidade de dados nos ambientes de desenvolvimento, integração, qualidade e produção da Fundação Carlos Alberto Vanzolini (FCAV).

2 ABRANGÊNCIA

Este é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir de sua publicação, aos colaboradores e terceiros da FCAV, responsáveis pelos processos de anonimização e pseudonimização.

3 REFERÊNCIAS

- Política de Segurança da Informação.
- Norma de Controles Criptográficos.

4 DEFINIÇÕES

✓ **Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

✓ **Dado anonimizado:** dado que não identifica de forma direta ou indireta um titular dos dados pessoais, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

✓ **Dado auxiliar:** identificador adicional empregado para vincular um dado pessoal, que passou por um processo de pseudonimização, e que é capaz de permitir a reidentificação da pessoa natural.

✓ **Dado pessoal:** informação relacionada à pessoa física identificada ou identificável.

✓ **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

✓ **Dado pseudonimizado:** dado que perde a possibilidade de associação direta ou indireta a um indivíduo, exceto mediante o uso de informações adicionais que são mantidas separadamente pelo controlador em um ambiente controlado e seguro.

✓ **Operador:** pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de

dados em nome do controlador.

✓ **Prevenção:** aplicação de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

✓ **Pseudonimização:** tratamento por meio do qual um dado pessoal perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

✓ **Reidentificação:** processo de tentar discernir os identificadores que foram removidos dos dados desidentificados, inclusive, a partir de técnicas de anonimização de dados.

✓ **Tentativa de burla:** tentativa de burlar as diretrizes e os controles estabelecidos. Quando constatada, deve ser tratada como uma violação.

✓ **Terceiro:** pessoa física ou jurídica, de direito público ou privado, que mantém relação contratual direta ou indireta com a FCAV, por meio da qual trata dados pessoais de propriedade ou que estejam sob a responsabilidade desta.

✓ **Titular dos dados pessoais:** pessoa física a quem se referem os dados pessoais que são objeto de tratamento.

✓ **Tratamento de dados pessoais:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

✓ **Violação:** qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos.

5 DIRETRIZES GERAIS

Anonimização e pseudonimização são duas técnicas distintas que permitem o uso de dados não identificados. A diferença entre as duas técnicas reside em se os dados podem ser reidentificados ou não.

✓ **Anonimização:** é um processo de transformação de dados pessoais que visa remover ou alterar informações que possam identificar uma pessoa, tornando impossível a identificação de um indivíduo específico, mesmo com o uso de dados adicionais, o qual, após realizado, torna-se irreversível, consistindo em uma medida mais extrema e permanente de proteção de dados. Entretanto, não é infalível e não é totalmente segura em todos os contextos, o que requer ser continuamente avaliada pelo agente de tratamento de dados pessoais.

✓ **Pseudonimização:** é um processo de proteção de dados em que informações identificáveis de uma pessoa são substituídas por identificadores artificiais, ou pseudônimos. Com isso, os dados perdem a possibilidade de serem diretamente associados a um indivíduo específico, a menos que informações adicionais sejam usadas para reestabelecer essa associação. Essas informações adicionais são mantidas separadamente e protegidas, em ambiente seguro e controlado, de

forma a garantir que a reidentificação seja difícil ou impossível sem autorização.

A definição sobre o uso de técnicas de anonimização e pseudonimização deve considerar a governança da informação:

- ✓ objetivo da proteção de dados;
- ✓ natureza dos dados;
- ✓ reversibilidade;
- ✓ conformidade regulamentar;
- ✓ finalidade do uso dos dados;
- ✓ riscos de reidentificação;
- ✓ custo e complexidade.

A FCAV pode optar por empregar técnicas de anonimização ou pseudonimização com as seguintes finalidades:

- ✓ como parte de uma estratégia de "privacidade desde a concepção" (*privacy by design*) destinada a oferecer uma proteção adicional aos titulares dos dados;
- ✓ como parte de uma estratégia de minimização de riscos ao compartilhar dados com operadores ou outros controladores de dados;
- ✓ para evitar violações acidentais quando a equipe tem acesso a informações pessoais;
- ✓ como parte de uma estratégia de "minimização de dados" voltada a reduzir os riscos de violações de dados para os titulares deles.

O processo de anonimização é irreversível e, portanto, deve ser usado apenas para fins que não exijam a identificação exclusiva do titular dos dados pessoais, como para dados estatísticos em pesquisas eleitorais.

Na FCAV, o uso do processo de anonimização deve ser aplicado para o tratamento de dados convergentes com as finalidades originárias da coleta, com informação clara ao titular dos dados, inclusive sob a condição de anonimização futura deles. Após o tratamento dos dados, a retenção para uso da FCAV é possível, dada a necessidade, com anonimização dos dados pessoais.
O tipo de tecnologia a ser usada para a anonimização e/ou pseudonimização deverá considerar:

✓ **objetivo:** Qual será o objetivo da utilização dos dados? Quais são os requisitos de qualidade de dados?;

✓ **tipos de dados:** Que tipo de dados devem se tornar anônimos? São dados estruturados, semiestruturados ou não estruturados? Onde os dados são armazenados?;

✓ **processos/ocorrência:** Com que frequência os dados precisam ser anonimizados? É um projeto único ou será necessário fazer isso constantemente?

Os princípios da proteção de dados pessoais não se aplicam a dados anônimos, ou seja, dados pessoais que não se relacionam a uma pessoa física identificada ou identificável, isso significa que:✓ não há a necessidade de armazená-los com o mesmo rigor aplicado a dados pessoais (a menos que sejam

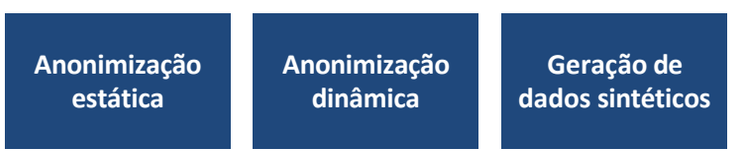
sensíveis ou valiosos por outros motivos);

- ✓ os titulares de dados pessoais não podem mais exercer seus direitos de dados sobre eles (portanto, não será necessário fornecer acesso, excluí-los ou retificá-los mediante solicitação);

- ✓ se forem comprometidos por uma violação de dados, não será necessário notificar as autoridades ou os indivíduos afetados.As diretrizes e os princípios de proteção de dados pessoais aplicam-se aos dados coletados e a todo processo de tratamento que antecede a anonimização. O processo de anonimização também é considerado uma operação de tratamento de dados pessoais, com isto, requer que seja informado ao titular e deve estar alinhado à finalidade original do tratamento de dados.

6 MÉTODOS DE ANONIMIZAÇÃO

Os métodos de anonimização mais populares atualmente podem ser classificados em três categorias diferentes:



- ✓ **Anonimização estática:** o editor torna o banco de dados anônimo em sua totalidade. Terceiros podem então acessar os dados anônimos sem serem considerados dados pessoais. O anonimato estático pode ser alcançado manualmente ou por meio de ferramentas disponíveis.

  - Com o anonimato estático, é possível atingir um bom nível de anonimato, mas sempre que houver alterações nos dados, o processo precisará ser realizado novamente, havendo o risco de reidentificação. Mesmo ao usar uma ferramenta, o anonimato estático requer um analista qualificado para ser capaz de avaliar se os dados resultantes são utilizáveis e anônimos.

  - Exemplos de aplicação: monetização de dados, relatórios para terceiros, retenção de dados.

- ✓ **Anonimização dinâmica:** o anonimato é aplicado dinamicamente à medida em que os dados são consultados. Após a leitura, são aplicados ruídos e outras técnicas de mascaramento aos resultados.

  - Exemplos de aplicação: monetização de dados, parceria, dados abertos/dados governamentais abertos, painéis de relatórios.

- ✓ **Dados sintéticos**: dados gerados artificialmente e que têm aproximadamente as mesmas propriedades (ou seja, valores) dos dados brutos, mas isso não permite que conclusões sejam tiradas sobre os indivíduos no conjunto de dados original. Dados sintéticos podem ser criados para parecerem sensíveis aos humanos, para servir como teste ou para fins de *machine learning*. Criar dados para fins de teste requer níveis de conhecimento significativos e esforço manual.

- Exemplos de aplicação: *machine learning* com preservação de privacidade e criação de conjuntos de dados de testes.

7 TÉCNICAS DE ANONIMIZAÇÃO

São as técnicas de anonimização:

✓ **Aleatorização:** essa técnica altera a veracidade dos dados, visando eliminar sua ligação com o titular de dados pessoais. Quanto mais imprecisos forem, melhor sua desconexão com o dado pessoal. Essa técnica, sozinha, não reduzirá a possibilidade de individualização de um registro, mas pode proteger contra ataques maliciosos e riscos de inferência, podendo, ainda, ser combinada com técnicas de generalização ou outras para garantir a impossibilidade de identificação de um titular de dados pessoais.

✓ **Supressão:** é a técnica mais básica e envolve a remoção de alguns dados de identificação do registro de dados para reduzir sua identificabilidade, sem necessariamente eliminá-lo permanentemente, portanto, permanecendo armazenados, porém inacessíveis ou invisíveis para os usuários, podendo ser restaurados, caso necessário.

✓ **Generalização:** envolve a transformação de valores específicos em uma faixa mais ampla de valores, por exemplo, transformar a idade específica de um indivíduo, como 18 anos, em uma faixa etária, como 18-24 anos. Ela não permite, no entanto, a anonimização de forma efetiva, devendo-se utilizar de outras técnicas para que a anonimização seja apropriada.

✓ **Adição de ruído:** envolve alternar os valores de identificação exclusiva de um indivíduo em um conjunto de dados pelos valores de identificação exclusiva de outro indivíduo no conjunto de dados, por exemplo, alterar a data de nascimento real (17/06/1988) pela data de nascimento de outro indivíduo a partir desse conjunto de dados (22/04/1990). Na avaliação sobre eventual utilização da adição de ruído, deve ser considerado o impacto na qualidade dos dados em relação ao resultado da estatística.

✓ **Permutação:** essa técnica mistura, de forma aleatória, os valores de atributos existentes em tabela, fazendo com que esses dados sejam ligados artificialmente a titulares de dados pessoais diferentes. É considerada uma forma especial de adição de ruído, que, assim como aquela, pode não oferecer sozinha as salvaguardas necessárias para que a anonimização seja adequada, devendo ser combinada com a remoção de outros atributos identificadores.

A aplicação dos métodos descritos nesta norma não fornecerá uma garantia absoluta de que os dados não serão mais identificáveis de maneira única quando usados incorretamente.

✓ De preferência, essas técnicas deverão ser aplicadas com a ajuda de cientistas de dados experientes.

Ao avaliar se as informações foram anonimizadas de forma eficaz, é necessário considerar se outras informações estão disponíveis e se elas, combinadas com as informações anônimas, resultariam na divulgação de dados pessoais.

A avaliação da possibilidade de reidentificação de dados e a reversão do processo de anonimização devem ter em consideração não apenas o uso de meios próprios, mas também a atuação de outras pessoas ou entidades que, com meios e esforços razoáveis, podem reidentificar um conjunto de dados anonimizados.

As informações anonimizadas usando as técnicas acima devem permanecer tão protegidas quanto qualquer outro dado da FCAV.

8 PSEUDONIMIZAÇÃO

A pseudonimização é uma técnica de segurança que reduz a identificação direta dos dados, tornando-os irreconhecíveis sem o uso de informações adicionais. Como é um processo reversível, os dados pessoais podem ser recuperados a qualquer momento, caso seja necessário.

A pseudonimização de dados pessoais significa substituir quaisquer características identificáveis dos dados por um pseudônimo, ou seja, um valor que não permite a identificação direta do titular dos dados.

✓ Os dados pseudonimizados não são anônimos, pois ainda existe a possibilidade de identificar o titular de dados pessoais, sendo considerados dados pessoais pela Lei Geral de Proteção de Dados.

São as técnicas de pseudonimização:

✓ **Criptografia (simétrica ou assimétrica):** é uma técnica em que um algoritmo de criptografia é usado para transformar dados pessoalmente identificáveis em texto cifrado (ou seja, dados pseudonimizados).

- Se e quando necessário, a FCAV pode usar uma chave de criptografia armazenada em local seguro para descriptografar o texto cifrado e, assim, recuperar os dados pessoais identificáveis originais.

- A FCAV deve dispor de medidas técnicas e organizacionais apropriadas para gerenciar e proteger a chave de criptografia armazenada em particular contra o acesso não concedido e, como tal, somente usuários autorizados podem descriptografar os dados pseudonimizados.

✓ ***Hashing*:** processo unidirecional, em que cadeias de entrada (ou seja, os campos de dados que contêm dados pessoais que devem ser pseudonimizados) de comprimento variável são transformadas em cadeias de saída de comprimento fixo de caracteres aleatórios.

- O algoritmo de *hash* é geralmente projetado de tal maneira que uma pequena variação nas sequências de entrada resulta em diferenças muito grandes nas sequências de saída correspondentes.

- No entanto, é de importância crucial o uso de algoritmos de *hash* modernos e complexos

para impedir que usuários mal-intencionados cancelem o anonimato das sequências de saída geradas.

✓ ***Tokens*:** processo no qual o identificador de dados pessoais do titular de dados pessoais é trocado por números gerados aleatoriamente, sem qualquer relação com dados que possam identificar o titular de dados pessoais.

- Essa é uma técnica utilizada, em sua maioria, no setor financeiro e substitui o número de identificação de cartões por valores que têm uma utilidade reduzida no caso de incidentes.

- Utiliza-se de mecanismos de criptografia ou função de indexação, de um número sequencial ou gerado aleatoriamente que não derive matematicamente dos dados originais.

9 RISCOS DE DIVULGAÇÃO

Antes de realizar a divulgação, o compartilhamento ou qualquer outra forma de divulgação de dados pseudonimizados ou anonimizados, o encarregado pelo tratamento de dados pessoais deverá ser consultado pelos gestores responsáveis da FCAV.

✓ O encarregado pelo tratamento de dados pessoais fará uma análise dos riscos envolvidos e tomará a decisão sobre aprovar ou não a divulgação de tais dados.

Os dados nunca devem estar descritos de forma minuciosa ao ponto de permitir que as informações concatenadas possam ser vinculadas a um titular de dados pessoais específico.

Os riscos podem ser divididos em:

✓ **individualização de um resultado:** ocorre quando um atributo da base de dados pertence a um titular de dados pessoais específico, mesmo que os dados daquele indivíduo não tenham sido divulgados.

- Exemplo: determinada empresa divulga em uma pesquisa interna que 100% dos colaboradores do gênero feminino da área X possuem interesse em algum assunto específico. Se a área tiver apenas uma mulher, o resultado será individualizado.

✓ **correlação com outro dado:** ocorre quando houver a utilização do dado para identificar um titular de dados pessoais com base naquele registro.

- Pode ocorrer quando houver reidentificação ao se conectar o referido dado com outro, quando se reverter o processo de pseudonimização, ou quando o processo de anonimização não for suficientemente seguro ou apropriado.

✓ **inferência:** ocorre quando houver inferência sobre um titular de dados pessoais, mesmo que ele não esteja na base de dados apresentada.

- Exemplo: pesquisa revela que 95% dos clientes de determinada empresa, que têm plano de saúde da mais alta categoria, possuem renda acima de R$ 10 mil. Logo, se você possui esse plano, é possível que alguém faça a inferência e presuma sua renda mensal.

10 TABELA DE RISCOS

Com base nas técnicas que podem ser utilizadas e nas práticas mais recentes de mercado, a Tecnologia da Informação deverá utilizar a técnica mais apropriada, mitigando o risco com base no motivo pelo qual o dado será tratado de forma anonimizada.

✓ A tabela de riscos deverá estar em constante atualização para que sejam inseridos os tipos de tecnologias utilizados nos procedimentos de pseudonimização, utilizando a seguinte tabela como exemplo:

TÉCNICA	RISCO DE INDIVIDUALIZAÇÃO	RISCO DE CORRELAÇÃO	RISCO DE INFERÊNCIA
Adição de ruído	Sim	Não	Não
Permutação	Sim	Sim	Não
Pseudonimização	Sim	Sim	Não

11 DAS RESPONSABILIDADES ESPECÍFICAS

11.1. Diretoria Executiva

Assegurar que os recursos sejam alocados à execução da aplicação das técnicas de anonimização ou pseudonimização, quando necessário.

11.2. Encarregado pelo tratamento de dados pessoais

Apoiar na tomada de decisão sobre o uso de técnicas de anonimização e/ou pseudonimização em projetos ou serviços, sempre que for aplicável.

Avaliar os riscos de divulgação e/ou compartilhamento de dados que passam pelo processo de pseudonimização ou anonimização.

Comunicar à área de Tecnologia da Informação quais dados pessoais ou sensíveis tratados em projetos ou processos são elegíveis para a aplicação de anonimização ou pseudonimização, quando aplicável.

Monitorar a aplicação dos procedimentos de anonimização e pseudonimização.

11.3. Comitê de Privacidade e Proteção de Dados Pessoais

Aprovar a avaliação dos dados elegíveis à anonimização ou pseudonimização, sempre que cabível.

11.4. Tecnologia da Informação

Viabilizar os recursos técnicos necessários para anonimizar e pseudonimizar os dados na FCAV.

Aplicar a anonimização ou pseudonimização nos dados indicados pelo encarregado de dados pessoais. Quando não for viável, informar ao encarregado pelo tratamento de dados pessoais as razões da impossibilidade, bem como sugerir possíveis alternativas técnicas para anonimização ou pseudonimização.

Viabilizar para que as técnicas de anonimização/pseudonimização utilizadas estejam em conformidade com as melhores práticas do setor e sejam suficientes para assegurar a proteção dos dados pessoais tratados pela FCAV.

Apoiar na avaliação de riscos de reversão do processo de anonimização, com o encarregado pelo tratamento de dados pessoais.

11.5. Gestores

Solicitar apoio ao encarregado pelo tratamento de dados pessoais quanto à necessidade de aplicação de técnicas de anonimização e pseudonimização em dados tratados em projetos ou serviços.

Consultar antecipadamente o encarregado pelo tratamento de dados pessoais quando da necessidade de divulgação ou compartilhamento de dados anonimizados ou pseudonimizados.

Avaliar, com o encarregado pelo tratamento de dados pessoais e com a área de Tecnologia da Informação, os riscos de reversão dos processos de anonimização e pseudonimização.

11.6. Colaboradores

Indicar, sempre que possível, dados tratados que não são necessários para a sua atividade.

12 PENALIDADES

Qualquer atividade que desrespeite as disposições estabelecidas nesta norma ou em quaisquer dos documentos complementares da FCAV deve ser considerada como uma violação e tratada pela mesma a fim de apurar as responsabilidades dos envolvidos de acordo com as “medidas disciplinares” da Fundação, visando a aplicação das sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

A tentativa de burlar as diretrizes e os controles estabelecidos, quando constatada, deve ser tratada como uma violação.

13 DISPOSIÇÕES FINAIS

Esta norma deve ser revisada, no mínimo, anualmente, ou sempre que existir a necessidade de alterações nos critérios definidos nas demais normas e políticas específicas da FCAV.

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as normas e procedimentos aplicáveis pela FCAV.

Esta norma, bem como os demais documentos que a complementam, encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitados ao encarregado pelo tratamento de dados pessoais da FCAV por meio do *e-mail* suportelgpd@vanzolini.org.br.

Qualquer dúvida relativa a esta norma deve ser encaminhada ao encarregado pelo tratamento de dados pessoais da FCAV por meio do *e-mail* suportelgpd@vanzolini.org.br.

Esta norma entra em vigor na data de sua publicação.

14 ANEXOS

Anexo I – Fluxos de aplicação de anonimização e pseudonimização 1.13.

15 NATUREZA DAS ALTERAÇÕES

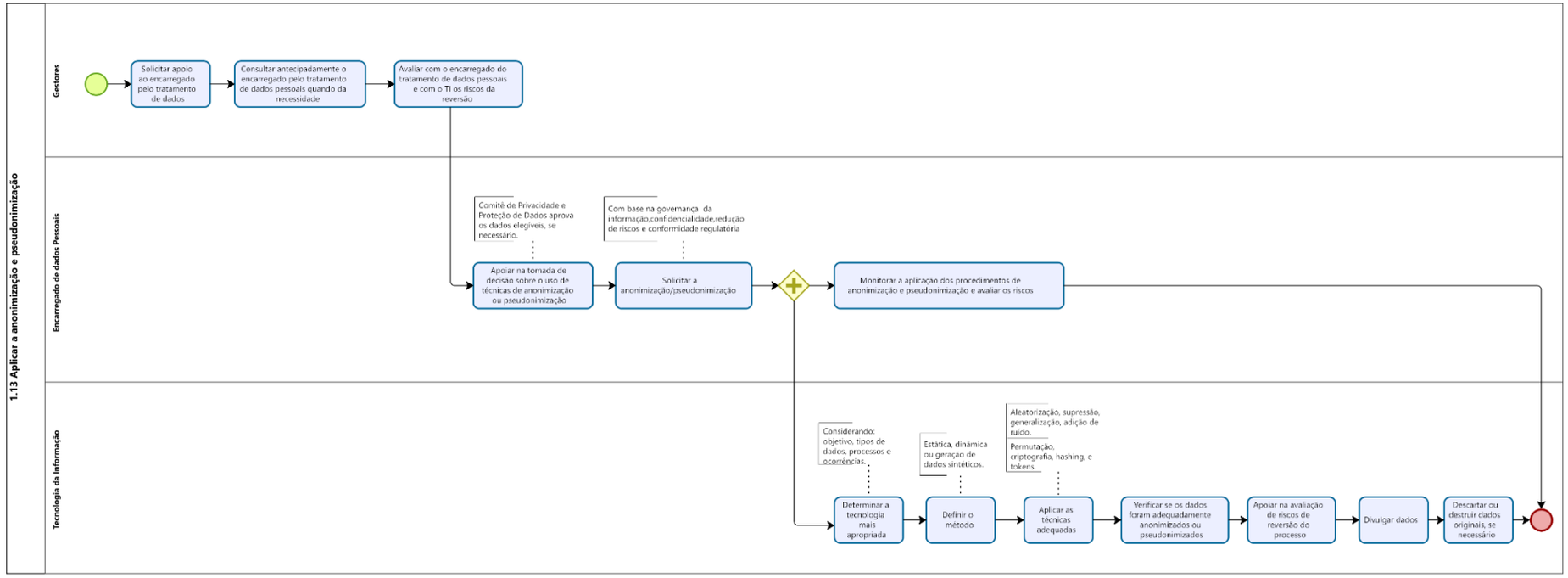
Revisão	Alterações (inclusões ou exclusões)	Data
00	Emissão inicial	20/09/2022
01	Na emissão inicial, para a numeração indicada no cabeçalho como “Revisão 01” lê-se “Revisão 00”. Esta versão de revisão mantém a numeração como “Revisão 01”. Inclusão dos fluxos de trabalho e atividades 1.13 (Anexo I) aprovados pelo Comitê de Privacidade e Proteção de Dados Pessoais. Ajustes nos textos de todos os capítulos do procedimento, conforme as necessidades identificadas durante a revisão.	07/11/2024

Revisão	Aprovação da Diretoria Executiva	Data
00	Emissão inicial	13/10/2022
01	Revisão 01	23/12/2024

16 ANEXO I

As atividades representadas nos fluxos para a execução desta norma de anonimização e pseudonimização têm por objetivo facilitar a compreensão do processo em cada etapa. Composto por um arquivo em formato PDF, denominado processo 1.13, que deve ser seguido pelos responsáveis pela execução desta norma.

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Validado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.13 Aplicar a anonimização e pseudonimização	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 17/10/2024	
	APROVADO POR: Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 07/11/2024	
OBJETIVO DO SUBPROCESSO: Implementar as técnicas de anonimização e pseudonimização levando em conta a proteção de privacidade, conformidade legal e utilidade dos dados.			



1.13 – Processo: Aplicar Anonimização e Pseudonimização