Fundação Vanzolini

PROCEDIMENTO DE RETENÇÃO E DESCARTE SEGURO

1 OBJETIVO

Este documento tem por objetivo estabelecer o procedimento de retenção e descarte seguro de informações na Fundação Carlos Alberto Vanzolini (FCAV).

2 PÚBLICO-ALVO

Este é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir de sua publicação, aos colaboradores, parceiros e fornecedores da FCAV.

3 REFERÊNCIAS

Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Política de Segurança da Informação.

Norma de Classificação da Informação.

Procedimento de Pseudonimização e Anonimização.

4 DEFINIÇÕES

- ✓ **Ativo intangível:** Qualquer ativo que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível; por exemplo: dados, reputação, imagem, marca e conhecimento.
- ✓ **Ativo tangível:** Qualquer ativo que possua corpo físico.
- ✓ **Ativo:** Qualquer elemento que tenha valor e precise ser adequadamente protegido.
- ✓ **Descarte seguro:** Forma de descarte em que as informações são inutilizadas por processos de sanitização física ou lógica, de modo a impossibilitar sua recuperação ou acesso por pessoas não autorizadas.
- ✓ **Dispositivo removível de armazenamento de informação:** Dispositivo capaz de armazenar informações que pode ser removido do equipamento, possibilitando a portabilidade dos dados; por exemplo: CD, DVD e *pen drive*.
- ✓ **Incidente de segurança da informação:** Ocorrência de evento ou série de eventos identificados em sistema, dado, informação, serviço ou rede, com probabilidade significativa de comprometer a confidencialidade, a integridade e a disponibilidade das informações e as operações da FCAV**.**
- ✓ **Informação:** Conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.
- ✓ **Informação lógica:** Informação digital armazenada em meio eletrônico, seja na nuvem, seja em dispositivo.
- ✓ **Retenção:** Armazenamento de informações em ativos de informação, em suporte físico ou

digital.

- ✓ **Registro das Atividades de Tratamento de Dados Pessoais (*Record of Processing Activities* – RoPA):** Documento em que se registram todas as atividades de tratamento de dados pessoais executadas pelo controlador e pelo operador de uma instituição, conforme determinado no artigo 37 da Lei Geral de Proteção de Dados Pessoais (LGPD).
- ✓ **Sanitização:** Processo realizado por métodos de limpeza, expurgo ou destruição e que torna inviável a recuperação dos dados.
- ✓ **Tentativa de burla:** Tentativa de violar diretrizes ou controles estabelecidos. Quando constatada, deve ser tratada como violação.
- ✓ **Operador (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 sob responsabilidade desta.
- ✓ **Violação:** Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos.

5 DIRETRIZES GERAIS

O descarte seguro é parte essencial do ciclo de vida das informações físicas e lógicas. Ele visa garantir que o conteúdo de propriedade ou sob responsabilidade da FCAV não seja recuperado nem acessado por pessoas não autorizadas. No caso de informações lógicas, trata-se de descarte de informações e sanitização de mídias por meio de eliminação completa, segura e definitiva, que torna os dados irrecuperáveis – um processo distinto da remoção lógica de dados realizada pelas áreas da FCAV mediante apagamento deles em interface de *software* ou sistema.

As informações físicas e lógicas devem ser descartadas, conforme Tabela de Temporalidade aprovada, de modo a impossibilitar sua recuperação por meio de processos de sanitização, nos termos deste procedimento.

Para o descarte seguro de informações físicas, como papéis, documentos e rascunhos, devem ser utilizadas fragmentadoras ou trituradoras disponibilizadas em cada unidade organizacional, sob responsabilidade do gestor de área. O colaborador deve estar atento ao limite de quantidade de folhas que podem ser inseridas nas fragmentadoras ou trituradoras e, em caso de dúvida, acionar a Área de Tecnologia da Informação.

Todas as áreas devem ter seus arquivos físicos catalogados, organizados e controlados, tanto aqueles alocados em seus próprios espaços quanto aqueles em terceirizados, buscando manter a integridade, a qualidade e a confidencialidade das informações e dos dados, em conformidade com a Tabela de Temporalidade e as legislações aplicáveis.

Deve-se estabelecer acordo de confidencialidade e sigilo com empresas terceirizadas contratadas para o armazenamento de arquivos físicos.

No caso de arquivos físicos digitalizados, o gestor responsável deve, com apoio da Consultoria

Jurídica, verificar se as informações físicas podem ser descartadas de forma segura e observar a Tabela de Temporalidade.

No caso de documentos com alta categorização de segurança (alto nível de sigilo e importância), devem ser utilizadas ferramentas para desintegrar totalmente o papel.

O descarte de informações lógicas, independente do meio de armazenamento (nuvem ou dispositivos móveis), deve ser previamente avaliado pela área de Tecnologia da Informação para garantir a segurança e apoiar o processo. No caso de armazenamento em meios físicos, como *smartcards*, HDs externos, *pen drives* ou outros dispositivos, a área de Tecnologia da Informação deverá analisar e considerar os seguintes aspectos:

- ✓ se as mídias serão reutilizadas internamente, doadas ou inutilizadas, de acordo com as necessidades das atividades na FCAV;
- ✓ se ocorrerá apenas sanitização lógica ou também sanitização física das mídias.

A sanitização lógica deve ser realizada pela Área de Tecnologia da Informação, por meio de processos de limpeza ou expurgação dos dados, a saber:

- ✓ limpar: reescrever dados por meio de comandos padrão do dispositivo ou redefinir o dispositivo para o estado de fábrica;
- ✓ expurgar: sobrescrever dados (processo *wipe*), desmagnetizar o dispositivo e proceder a apagamento criptográfico.

A sanitização física deve ser realizada de maneira segura por meio de processos de destruição da mídia por fragmentadora ou trituradora adequada.

Os processos de sanitização física e lógica das mídias estão descritos no Anexo I. Para decidir quanto aos processos de limpeza, expurgação ou destruição, a Área de Tecnologia da Informação deve seguir o procedimento indicado no Anexo II.

As atividades de sanitização física e lógica das mídias podem ser terceirizadas pela Área de Tecnologia da Informação, que deve garantir a formalização de acordos de confidencialidade e laudo que garanta o descarte definitivo das informações.

6 NECESSIDADE DE DESCARTE

As áreas da FCAV cujos processos envolvem tratamento de dados pessoais devem preencher e acompanhar o RoPA. Em caso de documentos físicos, devem proceder à sua eliminação após o fim do prazo de retenção legal. No caso de informações lógicas, o gestor responsável deve solicitar a avaliação prévia da Área de Tecnologia da Informação para assegurar um descarte seguro e receber o devido suporte no processo.

O prazo de retenção legal deve estar em consonância com a Tabela de Temporalidade aprovada.

Em se tratando de dados pessoais, caso um titular solicite eliminação de dados que estejam armazenados em *backup*, o Encarregado pelo Tratamento de Dados Pessoais deve avaliar, em conjunto com a Área de Tecnologia da Informação, a possibilidade, o esforço e o custo para sua realização, quando aplicável. Não sendo viável o descarte, o Encarregado deve informar a não exclusão ao titular dos dados pessoais, garantindo que eles não serão tratados.

Em não se tratando de dados pessoais, a área responsável deve avaliar, em conjunto com a Área de Tecnologia da Informação, os custos do descarte, levando em consideração recursos e tecnologia envolvidos.

Caso seja necessária a retenção das informações, o gestor deve apresentar os motivos por meio do Termo de Retenção da Informação (Anexo III) e, em conjunto com a Consultoria Jurídica, avaliar a possibilidade ou impossibilidade, bem como os possíveis impactos legais da retenção daquelas informações específicas após o prazo estabelecido na Tabela de Temporalidade. Depois dessa análise, o gestor deve solicitar à Diretoria de sua área a devida autorização.

Existindo dados ou informações que não possam ser descartados, sob risco de impacto em outras áreas organizacionais ou tecnológicas, o conjunto deles deve passar por tratamento de segurança específico.

Caso seja autorizada a retenção (não descarte) de dados ou informações, deve ser avaliada a necessidade de anonimização dos dados retidos para cada caso concreto.

7 RESPONSABILIDADES ESPECÍFICAS

7.1. Diretoria

Autorizar a retenção de informações mediante Termo de Retenção da Informação, quando solicitado.

7.2. Área de Tecnologia da Informação

Apoiar no processo de descarte seguro de informações lógicas, sempre que solicitado por gestor de área da FCAV.

Avaliar se as mídias que armazenam informações da FCAV serão doadas, reutilizadas internamente ou inutilizadas, antes de realizar descarte seguro.

Avaliar qual processo de sanitização será utilizado (limpeza, expurgação ou destruição).

Realizar sanitização física e lógica das mídias com informações da FCAV de maneira segura.

7.3. Consultoria Jurídica

Garantir a formalização de acordos de confidencialidade com empresas terceirizadas que realizam processos de sanitização física ou lógica das mídias da FCAV.

Analisar os casos em que for apontada necessidade de retenção (não descarte) de dados ou informações além do prazo determinado pela Tabela de Temporalidade.

7.4. Gestores de área

Garantir e gerenciar o cumprimento deste procedimento e documentos complementares pelos colaboradores.

Proceder à eliminação de dados ou informações após o fim do prazo de retenção legal, em caso de documentos físicos.

Solicitar à Área de Tecnologia da Informação apoio no processo de descarte seguro de informações lógicas, armazenadas na nuvem ou em dispositivos móveis.

Solicitar e justificar a retenção (não descarte) de dados ou informações além do prazo determinado pela Tabela de Temporalidade, quando necessário.

7.5. Colaboradores

Cumprir, estar ciente e manter-se atualizado em relação a este Procedimento e documentos complementares.

Utilizar fragmentadoras ou trituradoras disponíveis para o descarte seguro de informações físicas.

Contatar a Área de Tecnologia da Informação sempre que for necessário o descarte seguro de mídias ou de informações lógicas.

Cumprir a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais exercidas na FCAV.

8 PENALIDADES

Qualquer atividade que desrespeite as disposições estabelecidas neste procedimento ou em quaisquer documentos complementares deve ser considerada violação e tratada pela FCAV, a fim de apurar as responsabilidades dos envolvidos, de acordo com as medidas disciplinares internamente estabelecidas, e aplicar as sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

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

9 DISPOSIÇÕES FINAIS

Este documento deve ser revisado, no mínimo, anualmente ou sempre que existir necessidade de alterações nos critérios definidos nas demais normas e políticas específicas da FCAV.

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

Este documento e os complementares encontram-se disponíveis na intranet e, em caso de indisponibilidade desta, podem ser solicitados ao Encarregado pelo Tratamento de Dados Pessoais da FCAV pelo *e-mail* suportelgpd@vanzolini.org.br.

Qualquer dúvida relativa a este documento deve ser encaminhada ao Encarregado pelo Tratamento de Dados Pessoais da FCAV, para o *e-mail* suportelgpd@vanzolini.org.br.

Este documento entra em vigor na data de sua publicação.

10 ANEXOS

Anexo I – Tabela de descarte.
Anexo II – Fluxo para apoio na tomada de decisão.
Anexo III – Termo de Retenção da Informação.
Anexo IV – Fluxos de retenção e descarte seguro.

11 NATUREZA DAS ALTERAÇÕES

Revisão	Alterações (Inclusões ou Exclusões)	Data
00	Emissão Inicial	20/09/2022
01	Inclusão dos fluxos de retenção e descarte seguro 1.10, 1.10.1 e 1.10.2 (Anexo I) aprovados pelo Comitê de Privacidade e Proteção de Dados Pessoais. Ajustes nos textos do documento em atendimento às necessidades identificadas durante a revisão.	07/11/2024

Revisão	Aprovação da Diretoria Executiva	Data
00	Emissão Inicial	13/10/2022
01	Revisão	28/05/2025

12 ANEXO I – TABELA DE DESCARTE

INFORMAÇÕES FÍSICAS	
Forma de Descarte	**Instrução**
Destruir	Utilizar preferencialmente triturador que produza partículas de tamanho 1 mm x 5 mm ou menor. No caso de documentos com alta categorização de segurança (alto nível de sigilo e importância), utilizar ferramentas para desintegrar totalmente o papel. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.
DISPOSITIVOS DE REDE – *SWITCHES*, ROTEADORES E *MODEMS*	
Forma de Descarte	**Instrução**
Limpar	Restaurar as definições do fabricante, a fim de redefinir as configurações conforme padrão de fábrica.
Expurgar	Veja item **Destruir**. Recomenda-se consultar o fabricante a fim de verificar se o dispositivo tem capacidade de expurgar dados com uso de técnicas de sanitização.
Destruir	Utilizar triturador capaz de suportar esses dispositivos. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.
Nota	Caso os dispositivos de rede contenham mídias de armazenamento removíveis, elas devem ser removidas e sanitizadas com técnicas específicas para mídias.
DISPOSITIVOS MÓVEIS	
Forma de Descarte	**Instrução**
Limpar	Selecionar, no dispositivo, a opção de sanitização (“Apagar todo o conteúdo”, “Limpeza” ou similar) ou restaurar as definições do fabricante, a fim de redefinir as configurações conforme padrão de fábrica. Realizar *wipe*, processo em que dados aleatórios ou sequências de zeros e uns são sobrescritos por meio de comando no dispositivo.
Destruir	Utilizar triturador capaz de suportar esses dispositivos. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.

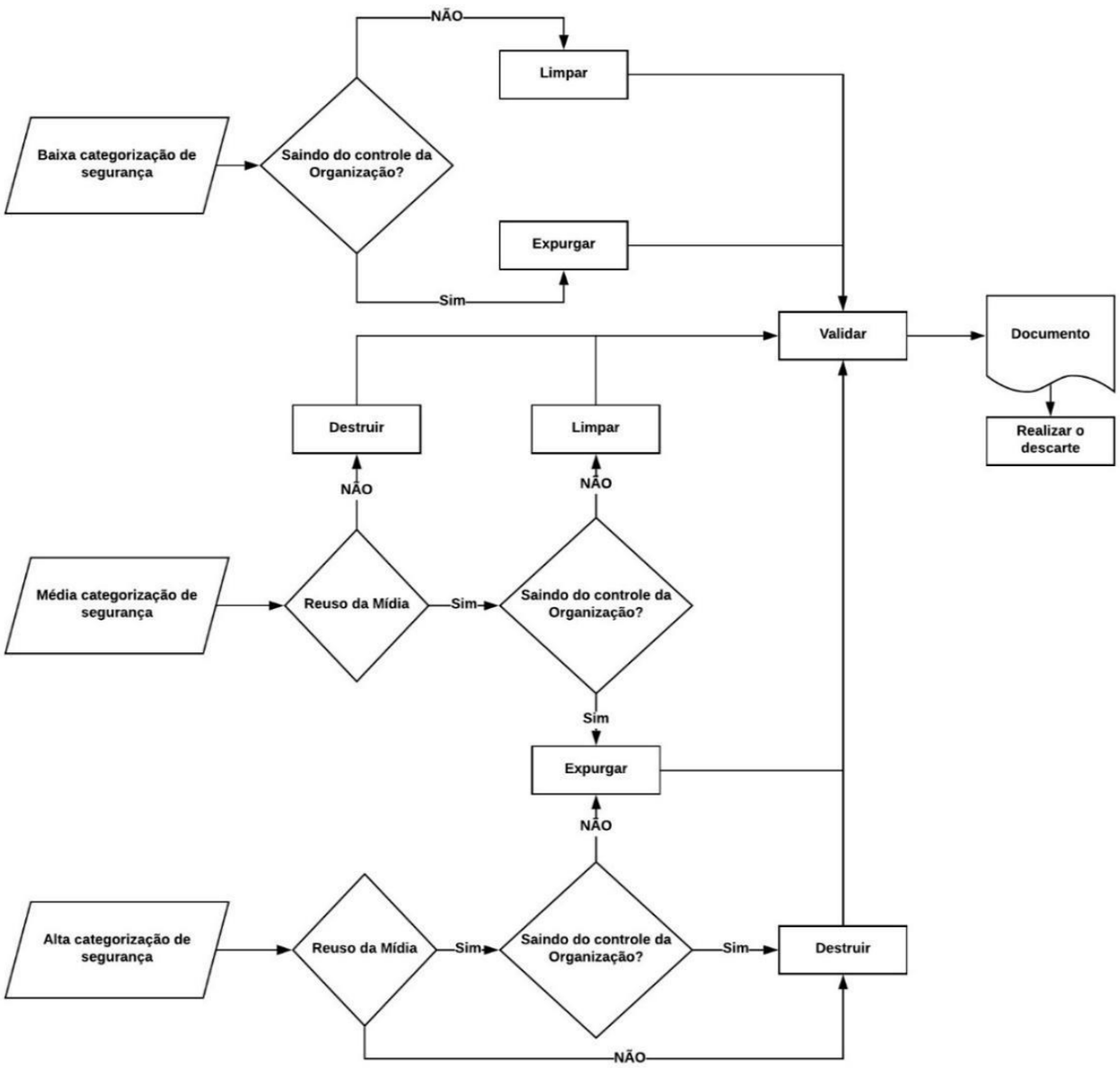
Nota	Após a operação de limpeza, navegar pelo dispositivo em áreas como histórico, fotos, *browser* e arquivos, a fim de verificar se nenhuma informação ficou retida.
EQUIPAMENTOS DE CÓPIA E/OU IMPRESSÃO E DEMAIS MÁQUINAS MULTIFUNCIONAIS	
Forma de Descarte	**Instrução**
Limpar	Restaurar as definições do fabricante, a fim de redefinir as configurações conforme padrão de fábrica.
Expurgar	Veja item **Limpar**. Recomenda-se consultar o fabricante a fim de verificar se o dispositivo tem capacidade de expurgar dados com uso de técnicas que sobrescrevam ou apaguem dados.
Destruir	Utilizar triturador capaz de suportar esses equipamentos. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.
Nota	Retirar a tinta ou o *toner* do equipamento, antes de sua destruição.
MÍDIA MAGNÉTICA – DISCOS MAGNÉTICOS	
Forma de Descarte	**Instrução**
Limpar	Realizar *wipe*, processo em que dados aleatórios ou sequências de zeros e uns são sobrescritos por meio de comando no dispositivo.
Expurgar	Desmagnetizar a mídia.
Destruir	Utilizar triturador capaz de suportar essas mídias. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.
Nota	Em geral, a desmagnetização torna o disco permanentemente inutilizável.
MÍDIA MAGNÉTICA – DISCOS RÍGIDOS	
Forma de Descarte	**Instrução**
Limpar	Realizar *wipe*, processo em que dados aleatórios ou sequências de zeros e uns são sobrescritos por meio de comando no dispositivo.
Expurgar	Utilizar o comando de sanitização, caso esteja disponível, e realizar *wipe* **sete vezes**. Realizar apagamento criptográfico e utilizar o comando de sanitização. Desmagnetizar a mídia magnética.

Destruir	Utilizar triturador capaz de suportar essas mídias. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.
Nota	Em geral, a desmagnetização torna o disco permanentemente inutilizável.
MÍDIA ÓPTICA	
Forma de Descarte	**Instrução**
Destruir	Utilizar triturador capaz de suportar essas mídias. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.
MEMÓRIA *FLASH*	
Forma de Descarte	**Instrução**
Limpar	Realizar *wipe*, processo em que dados aleatórios ou sequências de zeros e uns são sobrescritos por meio de comando no dispositivo.
Expurgar	Utilizar o comando de sanitização, caso esteja disponível, e realizar *wipe*. Realizar apagamento criptográfico e utilizar o comando de sanitização.
Destruir	Utilizar triturador capaz de suportar essas mídias. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.
MEMÓRIA *FLASH* – USB, MÍDIA REMOVÍVEL	
Forma de Descarte	**Instrução**
Limpar	Em geral, mídia removível USB não possui comando de sanitização.
Expurgar	Realizar *wipe*, processo em que dados aleatórios ou sequências de zeros e uns são sobrescritos.
Destruir	Utilizar triturador capaz de suportar essas mídias. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.
MEMÓRIA *FLASH* – CARTÃO DE MEMÓRIA	
Forma de Descarte	**Instrução**

Limpar/Expurgar	Realizar *wipe*, processo em que dados aleatórios ou sequências de zeros e uns são sobrescritos por meio de comando no dispositivo ou ferramenta específica.
Destruir	Utilizar triturador capaz de suportar essas mídias. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável
MEMÓRIA *FLASH* INCORPORADA EM DISPOSITIVOS	
Forma de Descarte	**Instrução**
Limpar	Restaurar as definições do fabricante, se opção disponível, a fim de redefinir as configurações conforme padrão de fábrica.
Expurgar	Remover do dispositivo e destruir.
Destruir	Utilizar triturador capaz de suportar essas mídias. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.
Nota	Antes do processo de sanitização, verificar se estão presentes dados sensíveis.
MEMÓRIAS *RAM* E *ROM* – MEMÓRIA *DRAM*	
Forma de Descarte	**Instrução**
Limpar	Desligar o dispositivo e remover a fonte de energia, a bateria e a memória *DRAM*.
Destruir	Utilizar triturador capaz de suportar essas mídias. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.
Nota	A memória *DRAM* deve permanecer sem energia por pelo menos cinco minutos.
MEMÓRIAS *RAM* E *ROM* – MEMÓRIA *EAPROM*	
Forma de Descarte	**Instrução**
Limpar	Realizar sanitização, conforme manual do fabricante.
Destruir	Utilizar triturador capaz de suportar essas mídias. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.

MEMÓRIAS *RAM* E *ROM* – MEMÓRIA *EEPROM*	
Forma de Descarte	**Instrução**
Limpar/Expurgar	Realizar *wipe*, processo em que dados aleatórios ou sequências de zeros e uns são sobrescritos por meio de comando no dispositivo ou ferramenta específica.
Destruir	Utilizar triturador capaz de suportar essas mídias. Utilizar desintegrador autorizado. Recomenda-se que esse processo seja feito por empresa ambientalmente responsável.

13 ANEXO II – FLUXO PARA APOIO NA TOMADA DE DECISÃO



Categorização de segurança

NÍVEL	TIPOS DE INFORMAÇÃO
Alta categorização de segurança	Documentos confidenciais, conforme Norma de Classificação da Informação. Dados pessoais. Documentos sob custódia de Diretoria.

NÍVEL	TIPOS DE INFORMAÇÃO
Média categorização e segurança	Documentos internos, conforme Norma de Classificação da Informação. Documentos sob custódia de gerentes de unidade.
Baixa categorização de segurança	Documentos públicos, conforme Norma de Classificação da Informação. Documentos sob custódia de colaboradores.

Reúso de mídia

É importante decidir e/ou verificar se a mídia será destinada a reutilização ou reciclagem. Algumas formas de mídia são frequentemente reutilizadas para conservar recursos internos.

Se não houver planos de reúso da mídia dentro ou fora da FCAV devido a danos ou outro motivo, o método de controle mais simples e mais econômico pode ser sua destruição.

14 ANEXO III – TERMO DE RETENÇÃO DA INFORMAÇÃO

Este documento deve ser utilizado pelo gestor solicitante e autorizado pela Diretoria da área, quando da necessidade de retenção ("não descarte") de informações além do prazo determinado na Tabela de Temporalidade.

1. Considerando que a lógica de uso da informação, inclusive do tratamento de dados pessoais, preconiza seu descarte após findar-se o prazo legal de retenção, mesmo que isso ocorra depois de esgotada sua finalidade inicial, serve o presente para, em atendimento, entre outros, ao Procedimento de Retenção e Descarte Seguro e à Política de Segurança da Informação da FCAV e à Lei Geral de Proteção de Dados Pessoais (LGPD), justificar a retenção das informações e dos dados pessoais abaixo especificados, com a descrição da justificativa, bem como a indicação do prazo de manutenção.
2. Nas hipóteses de retenção de dados pessoais, deve o titular dos dados pessoais ser informado da extensão da retenção, salientando-se justificativa e prazo, salvo nas situações em que ela já for de seu conhecimento.
3. Caso a retenção refira-se a informações parciais, deve-se pontuar tal condição, descrevendo-se no campo de observações os mecanismos de sanitização utilizados.
4. Caso sejam aplicados processos de anonimização e pseudonimização, eles devem ser mencionados no campo de observações.

1. INFORMAÇÕES DA ÁREA GESTORA

Área/Departamento			**Nº do Termo de Retenção da Informação**		
Gestor responsável					
Nome do projeto/processo					
Descrição	*Dados pessoais*		*Informação*		*[Informar perfil de dados e informações.]*
Justificativa	*[Informar razões para a manutenção.]*				
Prazos		**Embasamento**			
Prazo final de retenção (conforme Tabela de Temporalidade)					
Novo prazo					
Local					
Observações					

2. AVALIAÇÃO DA CONSULTORIA JURÍDICA

Processos ou projetos relacionados ao pedido de retenção de informações:	
Existem dados ou informações que não possam ser descartados, sob risco de impacto em outras áreas organizacionais ou tecnológicas?	
Se sim, existe tratamento de segurança específico para o conjunto de dados ou informações em questão?	
A retenção é possível?	
A retenção tem impactos legais?	
Existe RoPA atualizado das atividades relacionadas ao conjunto de dados ou informações em questão?	
Ações recomendadas:	
Impactos da não implementação das ações recomendadas:	
Data:	
Assinatura:	

A Diretoria da <NOME DA ÁREA DA FCAV>, na pessoa de <NOME DO DIRETOR>, <CARGO/FUNÇÃO>, ciente das políticas, das normas e dos procedimentos de segurança da informação, privacidade e proteção de dados da FCAV, bem como das ações recomendadas e dos impactos legais identificados, decide autorizar a retenção solicitada.

_____ , _____ de _____ de _____.

[Local] [Data]

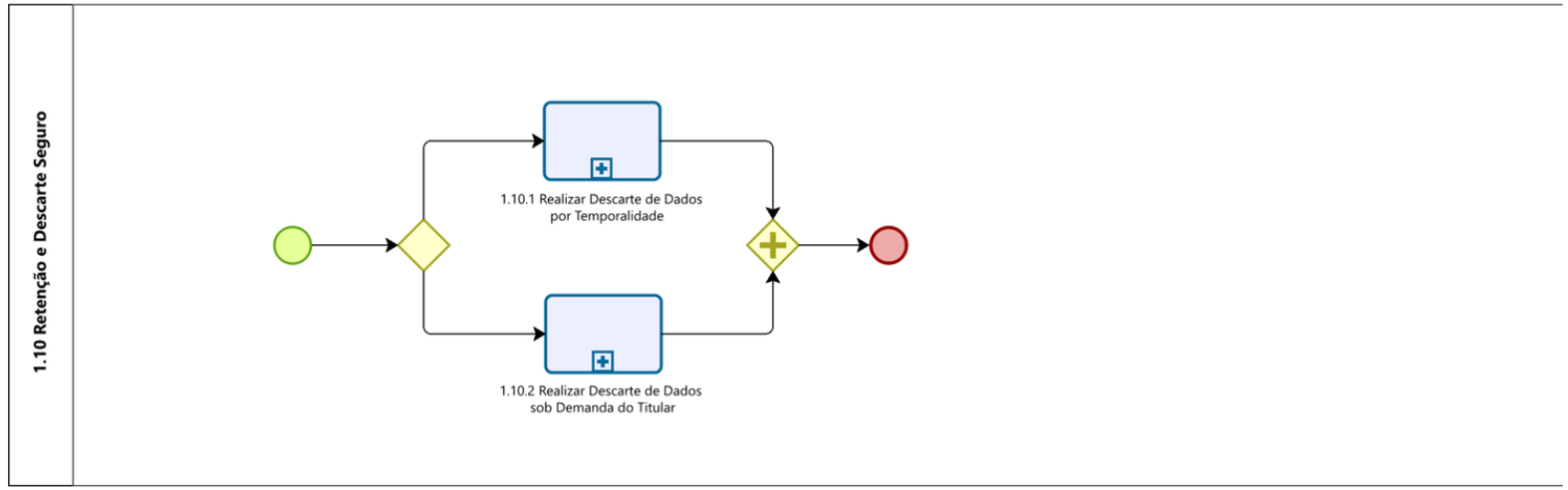
_____

Assinatura

ANEXO IV – FLUXOS DE RETENÇÃO E DESCARTE SEGURO

As atividades para execução deste procedimento estão representadas em fluxos, com objetivo de facilitar a compreensão do processo em cada etapa. Os fluxos compõem três arquivos em formato PDF, que deverão ser conhecidos de todos os envolvidos na execução deste procedimento.

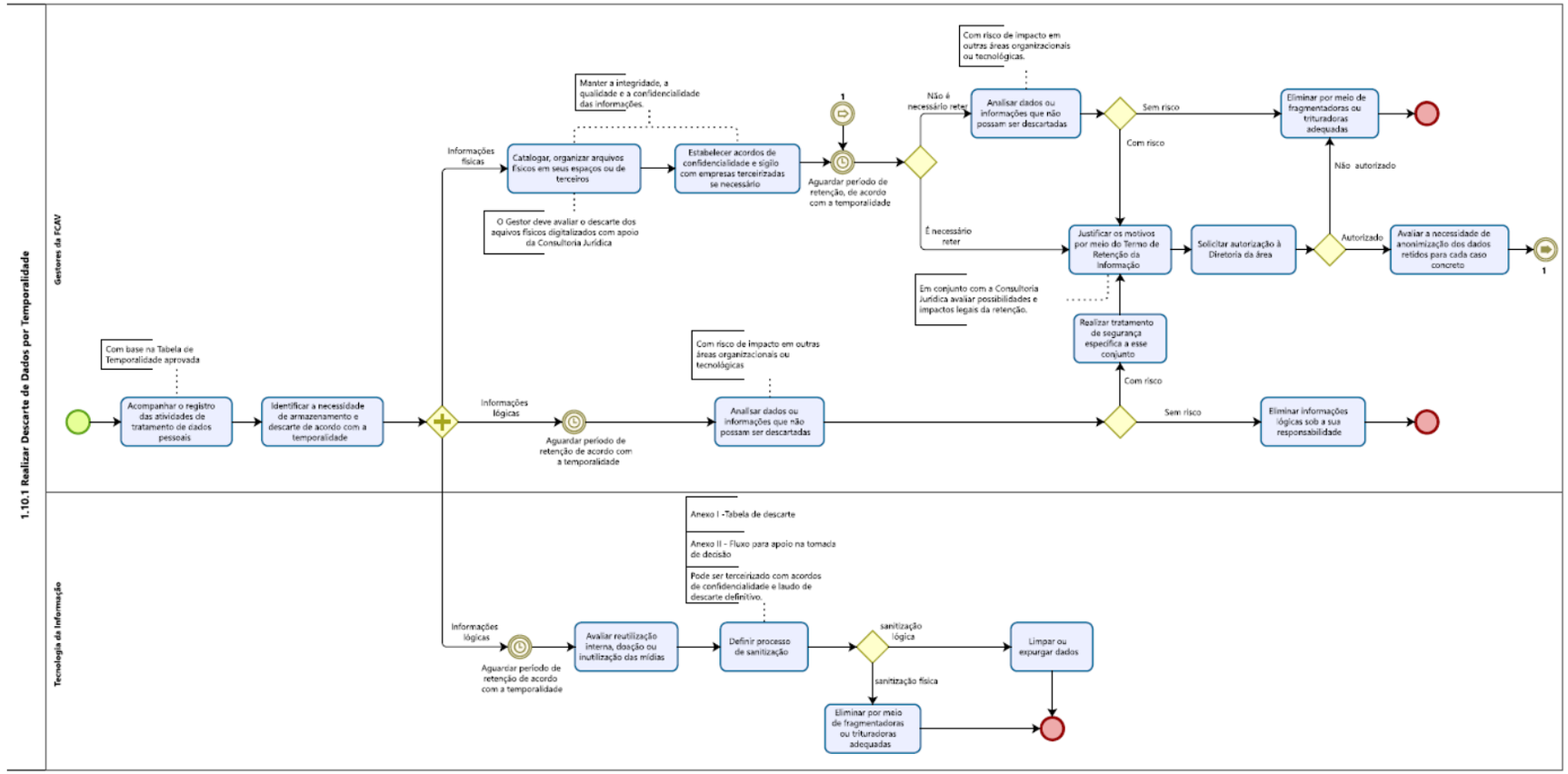
FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Validado	**VERSÃO:** 1.0	Fundação Vanzolini
	ELABORADO POR: FCAV	**DATA DA ELABORAÇÃO:** 07/2024	
PROCESSO: 1.10 Retenção e Descarte Seguro	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 07/11/2024	



Fluxo 1.10 – Processo: Retenção e descarte seguro

PROCEDIMENTO DE RETENÇÃO E DESCARTE SEGURO

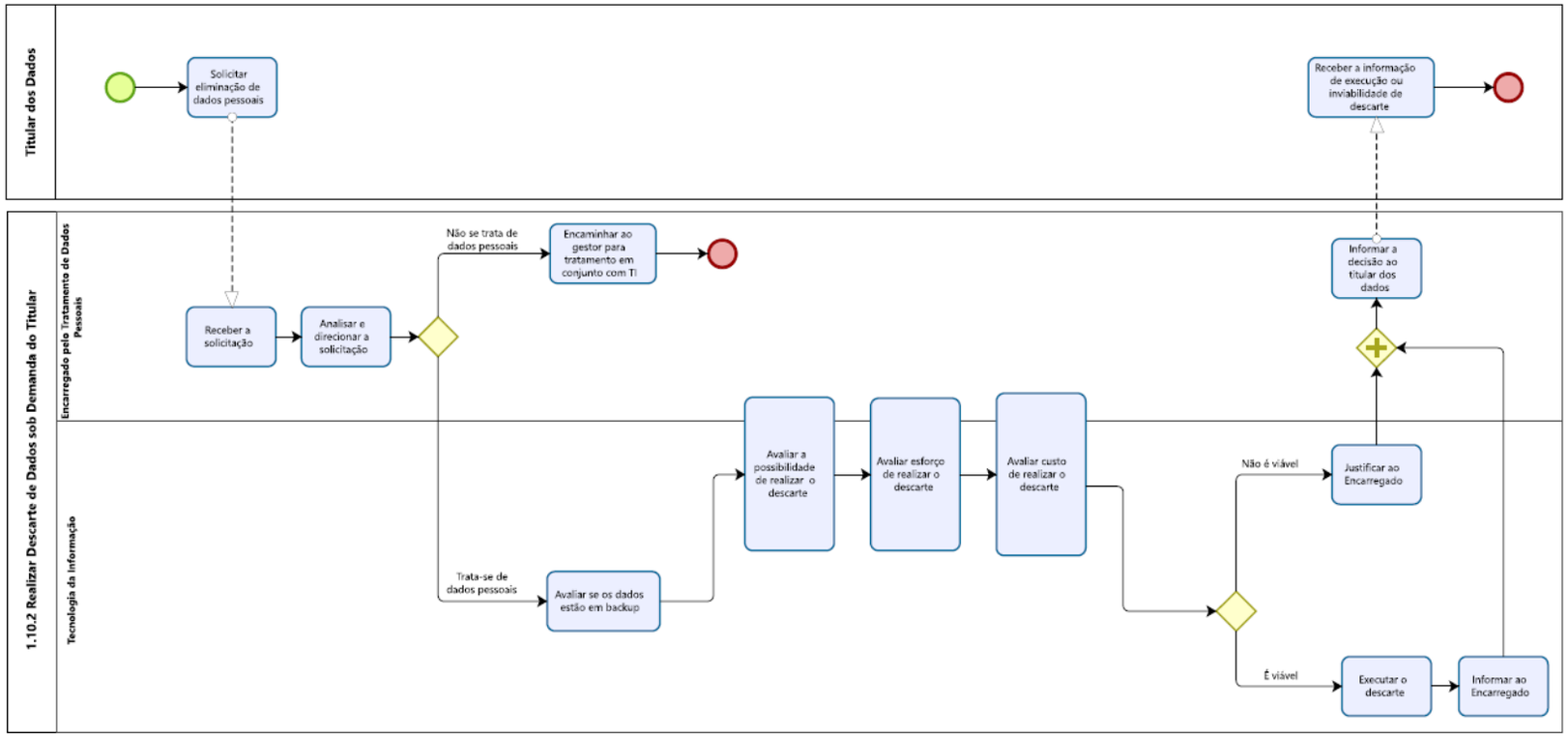
FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Validado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.10 Retenção e Descarte Seguro	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 07/2024	
SUBPROCESSO: 1.10.1 Realizar Descarte de Dados por Temporalidade	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 07/11/2024	
OBJETIVO DO SUBPROCESSO: Monitorar, identificar e descartar dados de forma apropriada, para garantir a segurança da informação.			



Fluxo 1.10.1 – Subprocesso: Realizar descarte de dados por temporalidade

PROCEDIMENTO DE RETENÇÃO E DESCARTE SEGURO

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Validado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.10 Retenção e Descarte Seguro	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 07/2024	
SUBPROCESSO: 1.10.2 Realizar Descarte de Dados sob Demanda do Titular	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 07/11/2024	
OBJETIVO DO SUBPROCESSO: Garantir os direitos dos titulares de dados em conformidade com a legislação sobre retenção e descate de dados pessoais.			



Fluxo 1.10.2 – Subprocesso: Realizar descarte de dados sob demanda do titular