1 OBJETIVO

Este documento tem por objetivo estabelecer as regras e as restrições para salvaguarda das informações e dos dados necessários para completa recuperação dos sistemas (*backup*) 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, parceiros e fornecedores da FCAV.

3 REFERÊNCIAS

Política de Segurança da Informação da FCAV.

ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.

ISO/IEC 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.

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.

4 DEFINIÇÕES

✓ ***Backup*:** Salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de recuperação em caso de incidente ou necessidade de restauração ou, ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada.

✓ **Colaborador:** Toda e qualquer pessoa física, contratada conforme a Consolidação das Leis do Trabalho (CLT) ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça atividade dentro ou fora da FCAV.

✓ **Criptografia:** Mecanismo de segurança que visa proteger as informações permitindo que somente o receptor da informação circulada leia-a com facilidade.

✓ **Descarte seguro:** Forma de descarte em que as informações são inutilizadas por processos de sanitização física ou lógica, de modo que impossibilite a sua recuperação ou o seu acesso por pessoas não autorizadas.

✓ **Incidente de segurança da informação:** Ocorrência de evento ou série de eventos identificados em sistema, dados, informações, serviços ou rede que tem probabilidade significativa de comprometer a confidencialidade, a integridade e 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.

✓ **Recurso de Tecnologia da Informação e Comunicação (TIC):** *Hardware*, *software*, serviço de conexão e comunicação ou de infraestrutura física necessário para criação, registro, armazenamento, manuseio, transporte, compartilhamento ou descarte de informações.

✓ **Restauração ou *restore*:** Processo de recuperação dos dados salvaguardados e sua colocação em produção.

✓ **Sanitização:** Processo que, por métodos de limpeza, expurgo e destruição, torna inviável a recuperação de dados.

✓ **Segurança da informação:** Preservação de confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação, com vistas a protegê-la dos diversos tipos de ameaça e, assim, garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação.

✓ **Tentativa de burla:** Tentativa de infringir diretrizes e controles estabelecidos. Quando constatada, deve ser tratada como violação.

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

5 DIRETRIZES GERAIS

A execução de *backup* deve garantir a proteção dos atributos de disponibilidade, integridade e confidencialidade das informações e dos dados necessários para completa recuperação dos sistemas da FCAV, o que pode incluir a preparação de recursos de TIC adicionais para assegurar o sucesso da restauração.

A Área de Tecnologia da Informação é responsável por garantir o *backup* e o *restore* dos dados e das informações da FCAV.

Para atender às necessidades de salvaguarda de informações e dados para completa restauração dos sistemas da FCAV, a preservação deles deve ser executada mediante emprego de ferramentas como servidores de *storage* e *softwares* de gerenciamento de rotinas de salvaguarda por cópias de segurança.

As ferramentas e as mídias utilizadas para geração de *backup* devem ser adequadas às necessidades do negócio, autorizadas e homologadas previamente pela FCAV.

Todas as atividades de *backup* e *restore* devem ser registradas e documentadas de forma exata e completa pela Área de Tecnologia da Informação.

Os *softwares* corporativos devem ser armazenados em servidores de produção apropriados, a fim de assegurar a execução adequada do *backup*.

Informações armazenadas localmente, como em recursos de TIC utilizados por colaboradores (área de trabalho/*desktop*), não serão submetidas à rotina de *backup*.

6 PROTEÇÃO DO *BACKUP*

Os *backups* devem ser protegidos de forma:

- ✓ física: em local com acesso restrito e protegido, seco, climatizado e livre de agentes prejudiciais como poeira;
- ✓ lógica: mediante uso de criptografia, nos termos da Norma de Classificação da Informação.

7 ARMAZENAMENTO DO *BACKUP*

O *backup* deve ser armazenado enquanto estiver vigente o devido período de guarda das informações pela FCAV, de acordo com:

- ✓ criticidade da disponibilidade da informação ou do sistema para a normalidade e a continuidade dos processos de negócio e operacionais, conforme Norma de Classificação da Informação da FCAV;
- ✓ requisitos legais, fiscais e de auditoria para a guarda de informações.

A contratação de terceiro para armazenamento de *backup* deve ser precedida de assinatura de contrato que contenha cláusulas relacionadas a:

- ✓ confidencialidade das informações armazenadas;
- ✓ disponibilidade e integridade do *backup*;
- ✓ armazenamento seguro e protegido do *backup*;
- ✓ formas de descarte e devolução do *backup*.

8 FORMAS DE GERAÇÃO DE *BACKUP*

A FCAV deve definir e manter, preferencialmente, as formas de geração de *backup*. Tais formas devem considerar aspectos relacionados às características dos dados e sistemas armazenados, especialmente quanto a serviços e aplicações a que se destinam e volumes de alterações e gravações realizadas.

Os *backups* devem ter uma das seguintes formas de execução:

- ✓ total ou completa (*full*): salvaguarda completa das informações;
- ✓ diferencial: salvaguarda apenas das informações modificadas ou geradas após a última salvaguarda total realizada;
- ✓ incremental: salvaguarda apenas das informações modificadas ou geradas após a última salvaguarda incremental ou total realizada.

Os *backups* devem ter as seguintes recorrências:

- ✓ diária: executado na modalidade incremental, a cada seis horas, com retenção de um mês;
- ✓ semanal: executado na modalidade total, à zero hora de domingo, com retenção de três meses;
- ✓ mensal: executado na modalidade total, à zero hora do último domingo do mês, com retenção de um ano;
- ✓ anual: executado na modalidade total, à zero hora do primeiro dia útil do ano, com retenção de cinco anos.

9 PROCEDIMENTO DE *BACKUP* E *RESTORE*

Os procedimentos de *backup* e *restore* devem considerar:

✓ as informações e os dados necessários para completa recuperação dos sistemas que serão salvaguardados;

✓ o local onde as informações e os sistemas que serão salvaguardados se encontram armazenados ou instalados;

✓ as ferramentas de *backup* que serão utilizadas, além dos tipos de mídia que serão empregados e sua vida útil;

✓ a montagem de jogos de mídias, incluindo rotulação, catalogação e método de rodízio;

✓ o nível de acesso necessário para que as ferramentas de *backup* automatizadas sejam capazes de acessar as informações e os dados dos sistemas;

✓ a descrição das atividades manuais necessárias relacionadas à execução de *backup*;

✓ as formas de execução de *backups*, sua recorrência e a estimativa de duração, considerando o período de menor carga de uso e impacto às atividades;

✓ a utilização de criptografia ou restrição de acesso ao *backup*;

✓ o transporte seguro das mídias que terão armazenamento externo, mesmo que realizado por fornecedor de serviços de nuvem;

✓ o armazenamento das mídias em instalações externas, de modo seguro e adequado;

✓ o *restore* das informações contidas nos *backups* realizados, bem como as formas de aprovação e solicitação de *restore* por colaboradores;

✓ a estimativa de prazo para a recuperação completa de *backups* ou dado específico que seja necessário, conforme SLA do fornecedor de serviços de nuvem;

✓ o teste ou a verificação de consistência, ao menos por amostragem, para validação de *backup* e *restore*;

✓ o descarte seguro dos dados pelo fornecedor de serviços de nuvem, considerando a eliminação definitiva de seu conteúdo.

10 *BACKUPS* ESPECÍFICOS

O *backup* de determinado arquivo ou recurso de TIC deve ser autorizado pela Área de Tecnologia da Informação após análise da pertinência da solicitação e de acordo com as necessidades do negócio.

11 VERIFICAÇÕES E TESTES

Todos os procedimentos de *backup* e *restore* devem ser periodicamente verificados e testados, inclusive as mídias, visando garantir a eficiência e a efetividade dessas atividades.

A Área de Segurança da Informação pode solicitar *backups* específicos e *restore* de mídias escolhidas aleatoriamente, a seu critério.

12 APAGAMENTO E/OU BLOQUEIO DE TRATAMENTO DE DADOS PESSOAIS POR REQUISIÇÃO DE TITULAR DE DADOS

O titular de dados pessoais pode solicitar a qualquer momento o apagamento e/ou o bloqueio do tratamento de seus dados pessoais armazenados em ambiente físico ou lógico pela FCAV, devendo o Encarregado pelo Tratamento de Dados Pessoais avaliar o pedido de apagamento e/ou bloqueio e deliberar sobre a possibilidade ou não, devido a eventuais obrigações legais.

o Encarregado fará o encaminhamento à Área de Tecnologia da Informação, para que sejam adotadas medidas de acordo com a solicitação do titular. Os gestores responsáveis pelo tratamento de dados também serão comunicados, para que atuem com a equipe de Tecnologia da Informação em atendimento à petição do titular.

Para apagamento de dados pessoais armazenados em *backups*, devem ser avaliados custo, recursos alocados e esforço razoável.

Na impossibilidade desse apagamento, o Encarregado pelo Tratamento de Dados Pessoais deve informar o fato ao titular, explicando os motivos pelos quais seus dados pessoais não poderão ser apagados.

A Área de Tecnologia da Informação deverá criar mecanismos para impedir que sejam restaurados ao ambiente lógico dados pessoais de titulares que tenham solicitado seu bloqueio e/ou apagamento.

13 RESPONSABILIDADES ESPECÍFICAS

13.1 Área de Tecnologia da Informação

Verificar e testar periodicamente os procedimentos de *backup* e *restore*, visando garantir a eficiência e a efetividade dessas atividades.

Garantir o *backup* e o *restore* dos dados e das informações da FCAV.

Utilizar somente ferramentas adequadas às necessidades do negócio, autorizadas e homologadas previamente pela FCAV.

Registrar e documentar de forma exata e completa todas as atividades de *backup* e *restore*.

Garantir que os *softwares* corporativos sejam armazenados em servidores de produção apropriados, a fim de assegurar a execução adequada do *backup*.

Proteger de forma física e lógica os *backups*.

Garantir que os *backups* sejam armazenados enquanto estiver vigente o devido período de guarda das informações pela FCAV, nos termos desta norma.

Garantir que a contratação de terceiro para armazenamento de *backup* da FCAV seja precedida de assinatura de contrato que contenha cláusulas específicas nos termos desta norma.

Definir os procedimentos de *backup* e *restore* específicos de acordo com esta norma.

Definir e manter as formas de geração de *backup*.

Avaliar e autorizar, se pertinente, *backup* de determinado arquivo ou recurso de TIC.

14 PENALIDADES

Qualquer atividade que desrespeite as disposições estabelecidas nesta norma 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 da FCAV, 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.

15 DISPOSIÇÕES FINAIS

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

Esta norma deve ser lida e interpretada sob a égide das leis brasileiras, no idioma português, em conjunto com as políticas e os procedimentos aplicáveis pela FCAV.

Esta norma e documentos complementares encontram-se disponíveis no ambiente de treinamento da FCAV e, em caso de indisponibilidade deste, podem ser solicitados ao Encarregado pelo Tratamento de Dados Pessoais da FCAV pelo *e-mail* suportelgpd@vanzolini.org.br.

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

Esta norma entra em vigor na data de sua publicação.

16 ANEXO

Anexo I – Fluxos de *backup* e *restore* 1.7, 1.7.1, 1.7.2, 1.7.3 e 1.7.4.

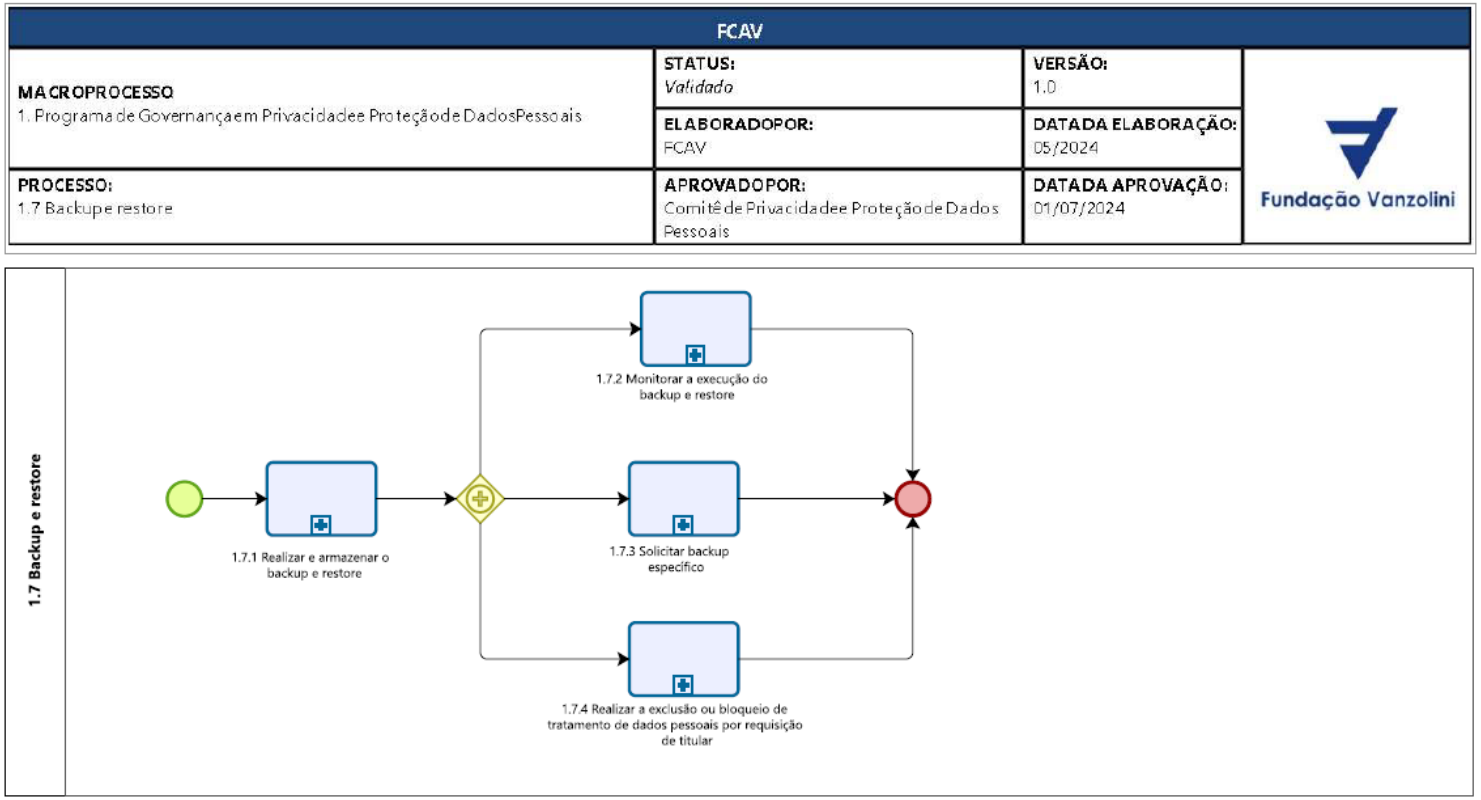
17 NATUREZA DAS ALTERAÇÕES

Revisão	Alterações (Inclusões ou Exclusões)	Data
00	Emissão Inicial	20/09/2022
01	Inclusão dos fluxos de *backup* e *restore* 1.7, 1.7.1, 1.7.2, 1.7.3 e 1.7.4 (ANEXO I) aprovados pelo Comitê de Privacidade e Proteção de Dados Pessoais; ajustes nos textos da norma em atendimento às necessidades identificadas durante a revisão.	01/07/2024

Revisão	Aprovação da Diretoria Executiva	Data
00	Emissão Inicial	13/10/2022
01	Versão 01	25/07/2024

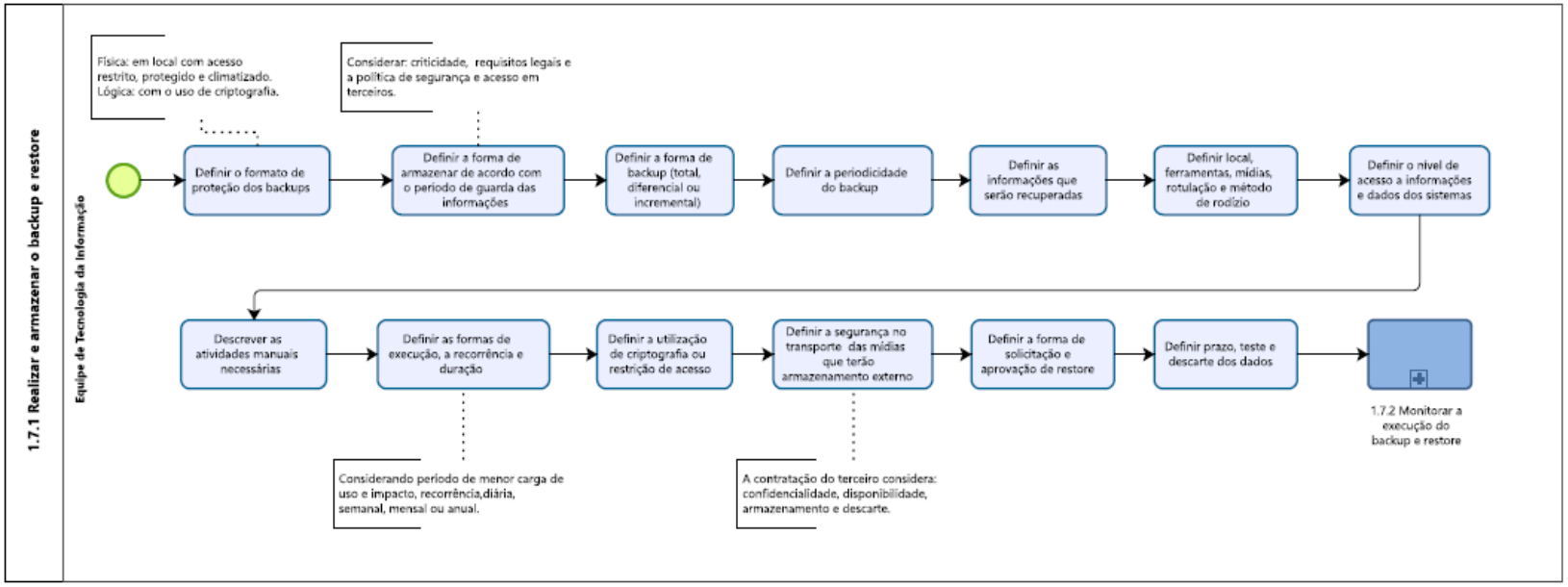
18 ANEXO I

As atividades representadas nos fluxos, para execução desta Norma de Backup e Restore, têm por objetivo de facilitar a compreensão do processo em cada etapa. Os fluxos compõem cinco arquivos em formato PDF, denominados processo e subprocessos 1.7, 1.7.1, 1.7.2, 1.7.3 e 1.7.4, respectivamente, que devem ser seguidos pelos responsáveis pela execução desta norma.



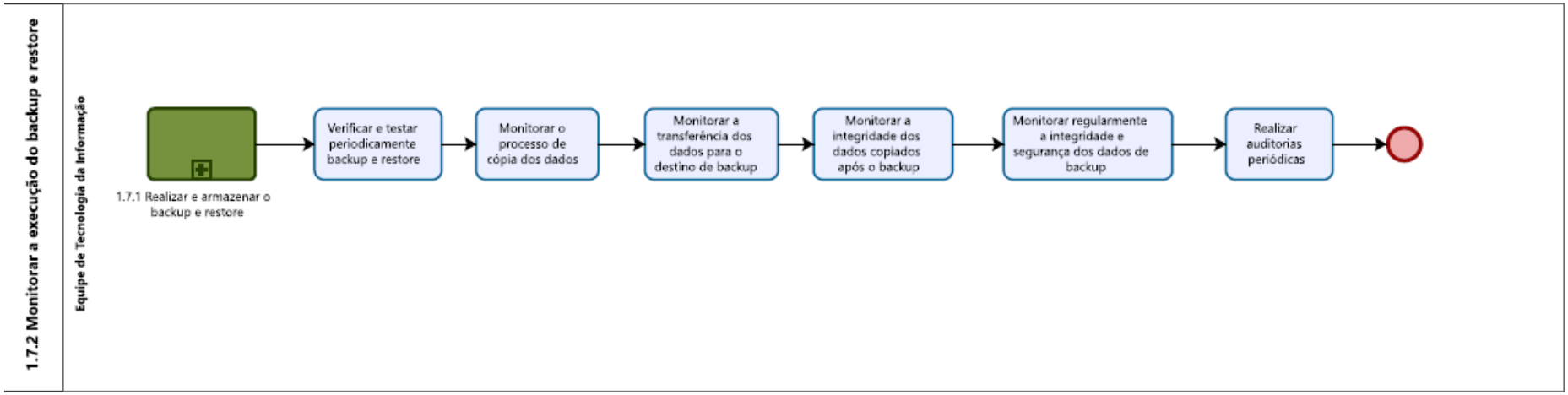
1.7 – Processo: *Backup* e *restore*

FCAV			
MACROPROCESSO 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	**STATUS:** *Validado*	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.7 Backup e restore	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 05/2024	
SUBPROCESSO: 1.7.1 Realizar e armazenar o backup e restore	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 01/07/2024	
OBJETIVO DO SUBPROCESSO: Garantir a disponibilidade e a integridade dos dados.			



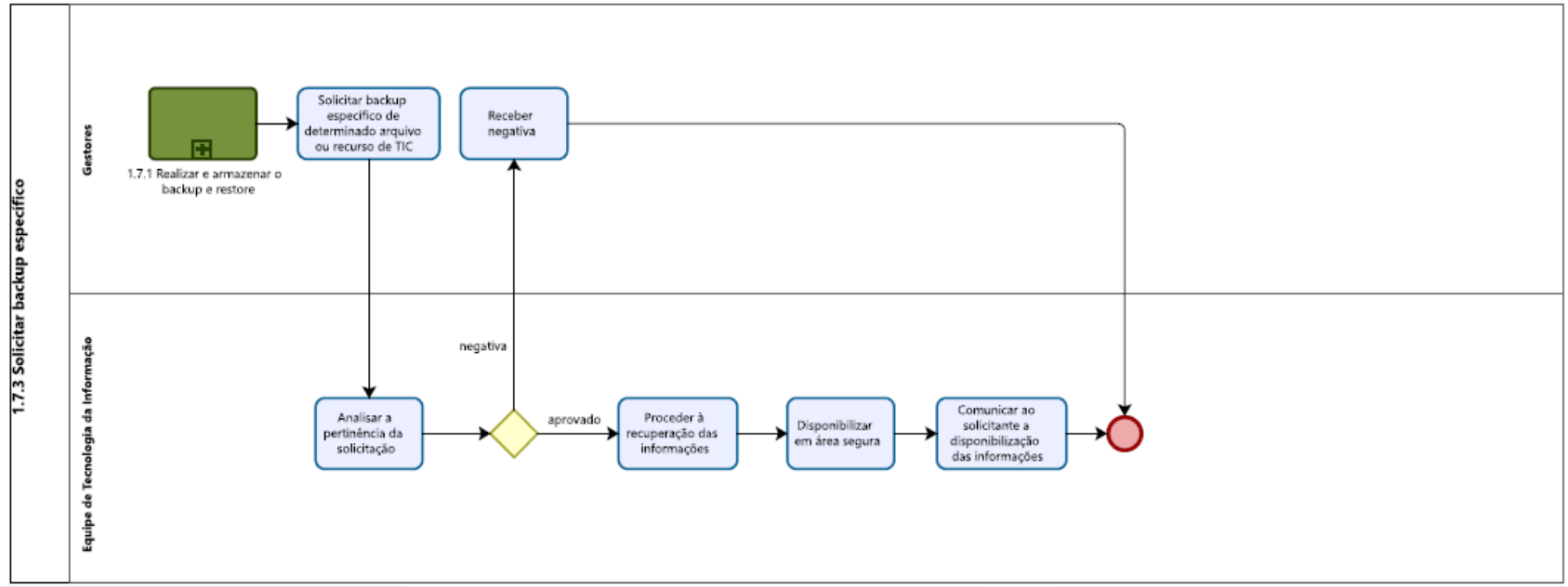
1.7.1 – Subprocesso: Realizar e armazenar *backup* e *restore*

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	**STATUS:** *Validado*	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.7 Backup e restore	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 05/2024	
SUBPROCESSO: 1.7.2 Monitorar a execução do backup e restore	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 01/07/2024	
OBJETIVO DO SUBPROCESSO: Monitorar a execução de backup garantindo a segurança da informação.			



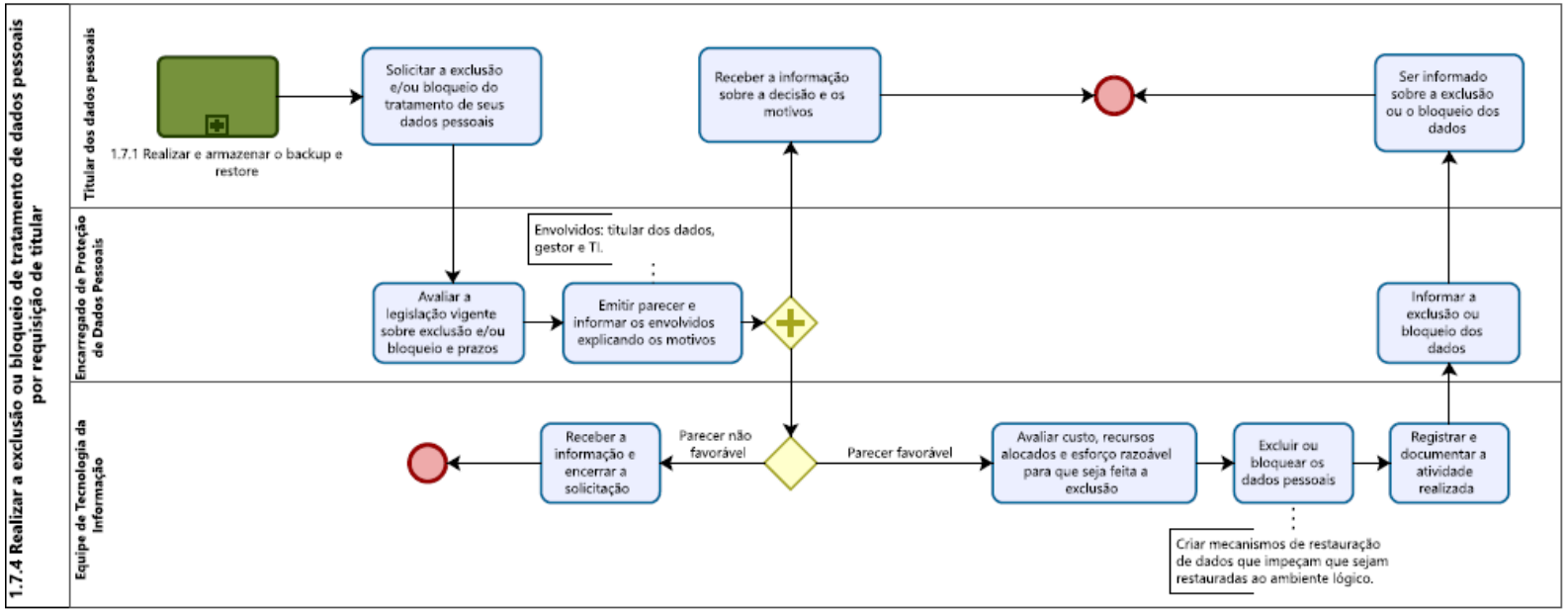
1.7.2 – Subprocesso: Monitorar execução de *backup* e *restore*

FCAV			
MACROPROCESSO 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	**STATUS:** *Validado*	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.7 Backup e restore	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 05/2024	
SUBPROCESSO: 1.7.3 Solicitar backup específico	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 01/07/2024	
OBJETIVO DO SUBPROCESSO: Avaliar e realizar o restore de dados.			



1.7.3 – Subprocesso: Solicitar *backup* específico

FCAV			
MACROPROCESSO 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	**STATUS:** *Validado*	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.7 Backup e restore	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 05/2024	
SUBPROCESSO: 1.7.4 Realizar a exclusão ou bloqueio de tratamento de dados pessoais por requisição de titular de dados	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 01/07/2024	
OBJETIVO DO SUBPROCESSO: Garantir que as solicitações de exclusão e/ou bloqueio de dados pessoais sejam tratadas de forma adequada, respeitando os direitos dos titulares.			



1.7.4 – Subprocesso: Realizar a exclusão ou bloqueio de tratamento de dados pessoais por requisição de titular de dados