1. ESCOPO

Este documento tem por objetivo estabelecer os requisitos de segurança da informação para contratação de serviços de processamento e armazenamento de dados na internet, pela 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.
- Procedimento para avaliação da proteção de dados pessoais em terceiros.

4. DEFINIÇÕES

✓ **Application Programming Interface (API)** (Interface de Programação de Aplicativos, em português): conjunto de rotinas e padrões de programação para acesso a um aplicativo de *software* ou plataforma baseado na *web*.

✓ **Colaborador:** empregado, estagiário, prestador de serviço, terceirizado, fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venha a ter relacionamento profissional, direta ou indiretamente com a organização.

✓ **Computação em nuvem:** fornecimento de serviços de computação, armazenamento de banco de dados, aplicativos e outros recursos de TI, por meio de uma plataforma de serviços pela internet (“em nuvem”), para o oferecimento de recursos flexíveis e economia de escala, conforme a necessidade da empresa, pagando apenas pelos serviços utilizados.

✓ **Controlador:** pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

✓ **Incidente de Segurança da Informação:** ocorrência de evento ou série de eventos identificados em um sistema, dados, informações, serviços ou rede que tem a probabilidade significativa de comprometer a confidencialidade, integridade e disponibilidade das informações e, além disso, comprometer as operações da FCAV.

✓ **Infrastructure as a Service (IaaS)** (Infraestrutura como Serviço, em português): modelo de fornecimento sob demanda de computação, armazenamento, rede e outros recursos pela internet.

✓ **Multi-Factor Authentication (MFA)** (Autenticação por Múltiplos Fatores, em português): método de autenticação no qual um usuário de computador obtém acesso somente após apresentar com êxito duas ou mais evidências (ou fatores) a um mecanismo de autenticação, por exemplo, conhecimento (algo que o usuário e apenas o usuário conhece) e posse (algo que o usuário e apenas o usuário tem).

✓ **Nuvem comunitária:** infraestrutura provisionada para uso exclusivo de uma comunidade específica de usuários, que têm preocupações comuns (por exemplo, considerações referentes a missão, requisitos de segurança e política). Ela pode ser controlada, gerenciada e operada por uma ou mais organizações na comunidade ou por um terceiro. Este modelo requer cuidados especiais quanto à compartimentalização e à confidencialidade dos dados utilizados na computação em nuvem.

✓ **Nuvem híbrida:** é uma composição de duas ou mais infraestruturas de nuvem distintas (privada, comunitária ou pública) que permanecem como entidades únicas, mas são unidas por tecnologia padronizada ou proprietária que permita a portabilidade de dados e aplicativos entre elas.

✓ **Nuvem privada:** infraestrutura de nuvem que é provisionada para uso exclusivo de uma única organização e é construída em um *datacenter* interno de uma organização ou em um *datacenter* de um terceiro que não é disponibilizado ao público em geral.

✓ **Nuvem pública:** modelo de implementação de computação em nuvem que consiste na oferta de serviços ao público em geral, e toda a infraestrutura física é provisionada e mantida pelo provedor de computação em nuvem.

✓ **Operador:** pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

✓ **Platform as a Service (PaaS)** (Plataforma como Serviço, em português): ambiente de desenvolvimento e implantação na computação em nuvem, com recursos que permitem fornecer desde aplicativos simples baseados em nuvem a sofisticados aplicativos empresariais habilitados para a nuvem.

✓ **Provedor de computação em nuvem:** empresa contratada que fornece plataforma, infraestrutura, aplicativo ou serviços de armazenamento baseados em computação em nuvem. Exemplos de provedores de computação em nuvem incluem, entre outros, Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform.

✓ **Risco:** combinação dos impactos advindos da ocorrência de um evento indesejado relacionado à segurança da informação e da probabilidade de sua ocorrência.

✓ **Software as a Service (SaaS)** (*Software* como Serviço, em português): modelo que permite aos

usuários se conectarem e usar aplicativos baseados em nuvem pela internet. Exemplos comuns são *e-mails*, calendário e ferramentas do Office (como Microsoft Office 365).

✓ **Segurança da informação:** é a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e de novas oportunidades de transação.

5. DIRETRIZES GERAIS

A contratação dos serviços de comunicação em nuvem para o processamento de dados da FCAV deve cumprir os requisitos de segurança quanto à confidencialidade, integridade e disponibilidade, seja para nuvem privada, nuvem pública, nuvem comunitária ou nuvem híbrida, bem como os modelos de serviços associados, tais como Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS), *Software* como Serviço (SaaS), entre outros modelos de entrega de serviços de computação em nuvem.

O acesso a esse tipo de infraestrutura deve ser rigorosamente controlado e restrito, garantindo segurança e privacidade dos dados e serviços. Essa restrição é feita por meio de diversas camadas de controle de segurança, que variam conforme o modelo do serviço contratado (IaaS, PaaS, SaaS) e o tipo de nuvem (privada, pública ou híbrida). Essas camadas de controle garantem que a FCAV tenha controle sobre quem acessa seus recursos e protejam a infraestrutura contra acessos não autorizados.

As formas de controle de acesso compreendem a autenticação e autorização, o gerenciamento de identidade e de acesso, o isolamento de dados e de recursos, o controle por meio de rede e *firewall*, a criptografia de dados em trânsito e de dados em repouso (armazenados), o monitoramento e a auditoria.

Embora o provedor de serviços em nuvem tenha acesso para gerenciar e manter a infraestrutura física, ele não têm acesso direto aos dados da FCAV, a menos que explicitamente autorizado pela Fundação ou em situações excepcionais, como cumprimento de ordens legais, fornecendo informações para auxiliar investigações e análises forenses.

Os padrões e procedimentos constituintes da Política de Segurança da Informação devem ser cumpridos para a utilização dos serviços em nuvem. A contratação de serviços em nuvem deve estar em conformidade com a presente norma e com os respectivos padrões e procedimentos integrantes da Política de Segurança da Informação.

A contratação de serviços de computação em nuvem relevantes ao processamento e armazenamento de dados deve ser previamente comunicado, por meio **da ferramenta de gestão de chamados**, à área de TI da FCAV para verificação dos requisitos desta norma. Para tanto, os seguintes itens devem ser informados previamente:

- ✓ a denominação do provedor de computação em nuvem a ser contratado;
- ✓ os serviços relevantes a serem contratados;
- ✓ a conformidade do fornecedor com a LGPD;
- ✓ a indicação dos países e regiões em cada país onde os serviços serão prestados e os dados serão armazenados, processados e gerenciados, caso a contratação do serviço em nuvem seja no exterior.

A área de TI deve avaliar, além dos itens acima, os seguintes requisitos:

- ✓ tempo de atuação no mercado;
- ✓ certificações obtidas;
- ✓ escalabilidade dos serviços prestados;
- ✓ suporte oferecido;
- ✓ plano de contingência;
- ✓ processo de monitoramento dos serviços;
- ✓ medidas de segurança implementadas;
- ✓ garantia de disponibilidade.

Os riscos concernentes à segurança da informação relativos aos serviços em nuvem são mapeados, avaliados e gerenciados pela FCAV, incluindo os riscos da infraestrutura, dos sistemas, do ambiente de rede, da legislação aplicável e das questões regulatórias.

A FCAV possui um inventário de ativos que contabiliza as informações e os ativos associados, que estão armazenados no ambiente de computação em nuvem, com a respectiva indicação de onde o ativo é mantido.

A FCAV realiza a classificação da informação e dos ativos associados mantidos em um ambiente de computação em nuvem de acordo com os procedimentos adotados pela Fundação para classificação da informação.

O provedor de computação em nuvem deve:

- ✓ fornecer as informações necessárias sobre procedimentos para que a FCAV faça a configuração do ambiente de computação e de autenticação de acessos, incluindo instruções para o armazenamento e a manutenção das informações, visando garantir que as políticas de acesso, de criptografia e de monitoramento estejam corretamente configuradas. O provedor de computação em nuvem é responsável pela segurança da infraestrutura (*datacenters*, redes, servidores e ferramentas) que ele gerencia, inclusive dos procedimentos de controle de acesso, como a autenticação forte (MFA) para acesso administrativo aos serviços em nuvem;

- ✓ manter mecanismos para garantir a confidencialidade dos dados armazenados, garantindo que eles sejam criptografados ou o permitam ser, tanto para o que concerce à sua responsabilidade quanto à da FCAV, o que inclui os dados trafegados e a utilização de APIs disponibilizadas para o exercício

de tarefas automatizadas dos seus serviços, interoperabilidade e gestão de configuração;

- ✓ manter mecanismos que permitam reduzir as vulnerabilidades a incidentes de segurança;
- ✓ possuir certificações de segurança da informação para manter-se em conformidade com os aspectos legais de confidencialidade e de privacidade dos dados e das informações;
- ✓ possuir, no mínimo, as seguintes certificações de segurança da informação ou controles equivalentes:
  - ISO 27001/27002 – padrão de segurança amplamente adotado que estabelece requisitos e práticas para uma abordagem sistemática, no gerenciamento de informações da empresa e de clientes, com base em avaliações periódicas de riscos adequadas a cenários de ameaças em constante mudança.
  - ISO 27017 – fornece orientações de implementação em controles de segurança da informação que se relacionam especificamente aos serviços em nuvem.
  - ISO 27018 – código internacional de práticas que se concentra na proteção de dados pessoais na nuvem. É baseada no padrão de segurança de informações ISO 27002 e fornece orientação para implementação sobre os controles da ISO 27002 aplicáveis às Informações Pessoais Identificáveis (PII) da nuvem pública. Também fornece um conjunto de controles adicionais e orientações associadas, destinados a atender aos requisitos de proteção PII de nuvem pública, não abordados pelo conjunto de controles existentes na ISO 27002.

A FCAV mantém uma base de dados com os certificados de segurança da informação disponibilizados pelo provedor de computação em nuvem ou controles equivalentes.

O provedor do serviço em nuvem deve fornecer à FCAV informações sobre alterações no serviço em nuvem e/ou sobre a realização de manutenção em seus equipamentos que possam afetar adversamente a prestação do serviço em nuvem, tais como:

- ✓ categoria das mudanças/manutenção;
- ✓ data e hora planejada das mudanças/manutenção;
- ✓ descrição técnica das mudanças no serviço em nuvem e nos serviços adjacentes;
- ✓ notificações de início e fim das mudanças/manutenção.

Em relação aos incidentes de segurança da informação, o provedor de computação em nuvem deve disponibilizar à FCAV uma documentação mínima abrangendo:

- ✓ procedimentos sobre a gestão de vulnerabilidades;
- ✓ o escopo dos incidentes de segurança da informação que o provedor do serviço em nuvem notificará para a FCAV;
- ✓ o nível de divulgação da detecção de incidentes de segurança da informação e as respostas

associadas;

- ✓ o período de tempo pretendido para ocorrerem as notificações de incidentes de segurança da informação;
- ✓ o procedimento para a notificação de incidentes de segurança da informação;
- ✓ informações de contato para tratar questões relacionadas a incidentes de segurança da informação;
- ✓ os planos de ação aplicáveis nos casos de ocorrência efetiva de incidentes de segurança da informação.

A FCAV deve:

- ✓ manter resgistros sobre as evidências de conformidade de como as exigências deste procedimento estão sendo cumpridas, bem como desenvolver processos para coletá-las e armazená-las, incluindo *logs* de acesso, trilhas de auditoria, relatórios de atividades e de *backups*, cópias das configurações dos sistemas, relatórios de gestão de mudanças e resultados de outros procedimentos de teste;

- ✓ compreender as políticas e os processos do provedor de computação em nuvem a respeito da retenção e destruição de dados e informações, em alinhamento com as políticas de segurança da FCAV;

- ✓ documentar a arquitetura de segurança e a configuração individual de cada componente de controle de segurança, de forma que estes possam ser utilizados para eventual conformidade, bem como para a necessidade de migração dos serviços para outro provedor de computação em nuvem.

O provedor de computação em nuvem, enquanto operador de dados pessoais da FCAV, deve possuir conformidade com a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD) do Brasil e/ou o Regulamento 2016/679 (GDPR) da União Europeia.

6. CONTRATOS COM PROVEDORES DE COMPUTAÇÃO EM NUVEM

O provedor de computação em nuvem deve garantir, em casos de encerramento de vínculo:

- ✓ a transferência dos dados para novo provedor de computação em nuvem indicado pela FCAV;
- ✓ a confirmação da integridade e da disponibilidade dos dados recebidos e armazenados, mesmo que gerenciados pela FCAV;
- ✓ uma garantia da exclusão dos dados da FCAV, quando solicitado e expressamente autorizado.

O provedor de computação em nuvem deve conceder pleno e irrestrito acesso à FCAV, aos acordos, documentações e informações referentes aos serviços prestados, dados armazenados, cópias de segurança, *logs* de acesso e, ainda:

- ✓ notificação prévia de interrupção da prestação dos serviços, com, no mínimo, trinta dias de antecedência;
- ✓ após a notificação prévia da interrupção, a empresa contratada obriga-se a aceitar eventual prazo adicional quando for de conveniência da FCAV, desde que haja solicitação expressa dentro do prazo acordado;
- ✓ a notificação prévia da interrupção deve ocorrer mesmo em situação de inadimplência.

7. DAS RESPONSABILIDADES ESPECÍFICAS

7.1. Encarregado pelo tratamento de dados pessoais

Apoiar o setor Jurídico na verificação dos contratos com provedores de serviços em nuvem quanto a questões relacionadas à segurança da informação e proteção de dados pessoais.

7.2. Área contratante do serviço em nuvem

Efetuar a solicitação de contratação de serviços em nuvem, nos termos deste procedimento, abrangendo quaisquer renovações ou extensões que possam ser necessárias durante a vigência do contrato, bem como o encerramento dos serviços quando forem de conveniência da área.

7.3. Consultoria jurídica

Apoiar a área de Tecnologia da Informação no mapeamento dos riscos concernentes à segurança da informação relativos aos serviços em nuvem e como esses riscos são gerenciados, incluindo os riscos de legislação aplicável e questões regulatórias.

Verificar os contratos com provedores de serviços em nuvem quanto às questões relacionadas à segurança da informação e à proteção de dados pessoais.

7.4. Tecnologia da Informação

Prestar o suporte necessário para que a área demandante possa realizar a contratação do serviço almejado, bem como sua rescisão em virtude da descontinuidade dos serviços.

Avaliar as informações fornecidas pelo contratante do serviço em nuvem.

Avaliar os requisitos a respeito da estrutura do provedor, tais como tempo de fundação, certificações, suporte oferecido, atendimento, garantia da disponibilidade e da confidencialidade dos dados armazenados, cumprimento das legislações aplicáveis, entre outros.

Mapear os riscos concernentes de segurança da informação relativos aos serviços em nuvem e como esses riscos são gerenciados, incluindo os riscos dos sistemas, ambiente de rede, legislação aplicável e questões regulatórias.

Manter inventários atualizados sobre os ativos em nuvem.

Realizar a classificação da informação e dos ativos associados mantidos em um ambiente de computação em nuvem, de acordo com os procedimentos adotados pela FCAV para a classificação da informação.

Verificar certificados de segurança da informação do provedor de computação em nuvem.

Solicitar tempestivamente ao provedor informações e relatórios que possam comprovar a qualidade e a segurança dos serviços contratados.

Receber os comunicados e relatórios de incidentes de segurança da informação dos provedores de serviços em nuvem e aplicar as medidas necessárias no que for cabível.

8. 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 de 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.

9. 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.

10. ANEXOS

Anexo I – Fluxos de contratação de serviços em nuvem 1.11, 1.11.1, 1.11.2 e 1.11.3.

11. NATUREZA DAS ALTERAÇÕES

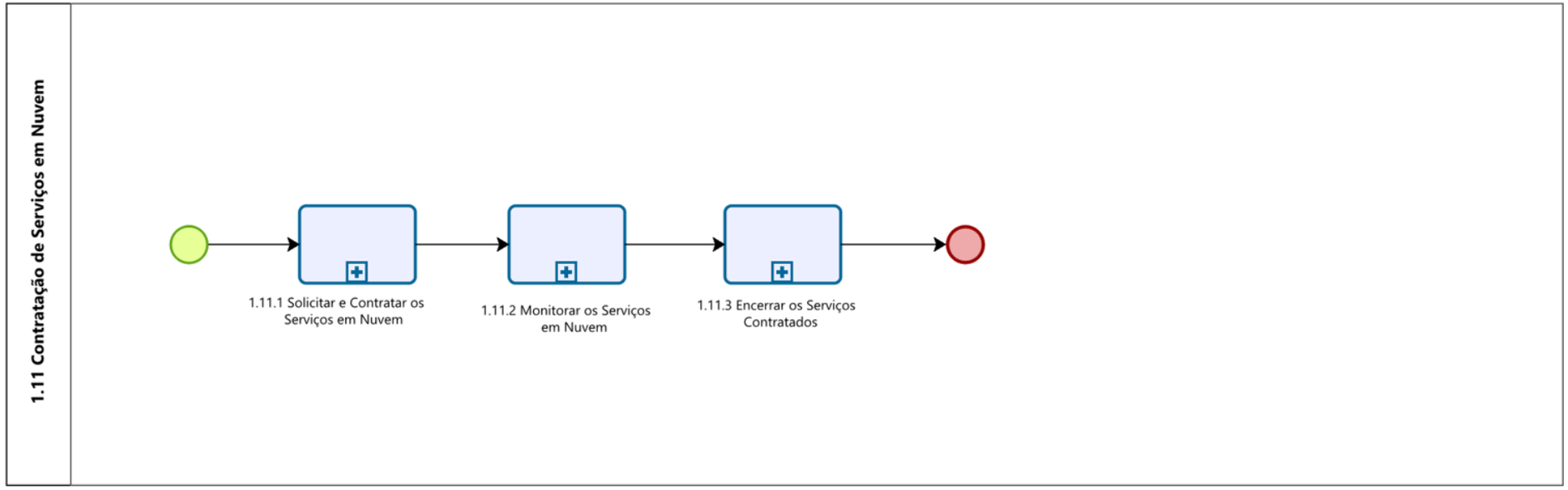
Revisão	Alterações (inclusões ou exclusões)	Data
00	Emissão inicial	20/09/2022
01	Inclusão dos fluxos de contratação de serviços em nuvem 1.11, 1.11.1, 1.11.2 e 1.11.3 (ANEXO I) aprovados pelo Comitê de Privacidade e Proteção de Dados Pessoais; ajustes nos textos da norma em atendimento às necessidades identificadas durante a revisão.	30/10/2024

Revisão	Aprovação da Diretoria Executiva	Data
00	Emissão inicial	13/10/2022
01	Revisão 01	22/11/2024

12. ANEXO I

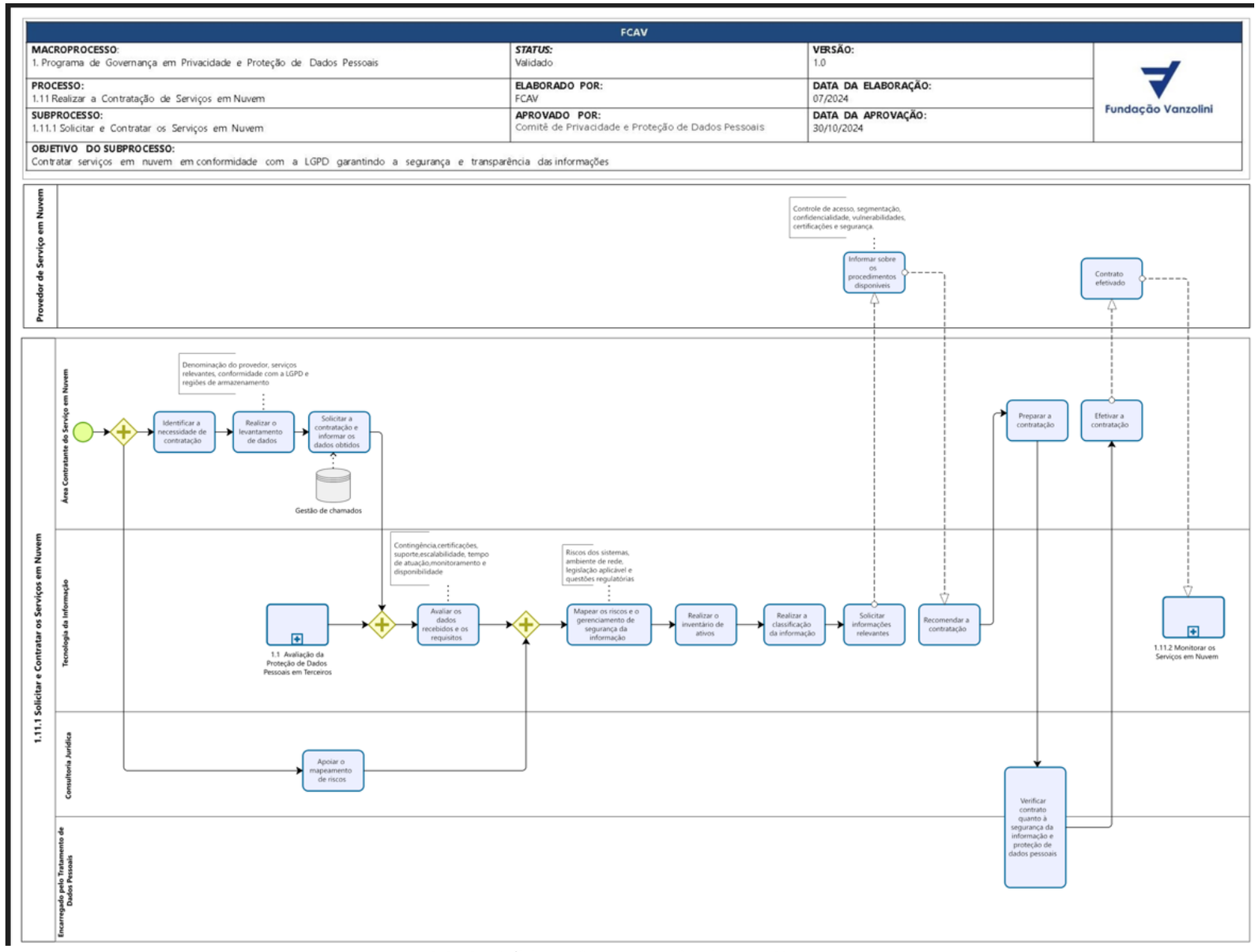
As atividades representadas nos fluxos para execução desta norma para contratação de serviços em nuvem têm por objetivo facilitar a compreensão do processo em cada etapa. Composto por quatro arquivos em formato PDF, denominados processo e subprocessos 1.11, 1.11.1, 1.11.2 e 1.11.3, respectivamente, que devem ser seguidos 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
	ELABORADO POR: FCAV	**DATA DA ELABORAÇÃO:** 07/2024	
PROCESSO: 1.11 Contratação de Serviços em Nuvem	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 30/10/24	



1.11 – Contratação de Serviços em Nuvem

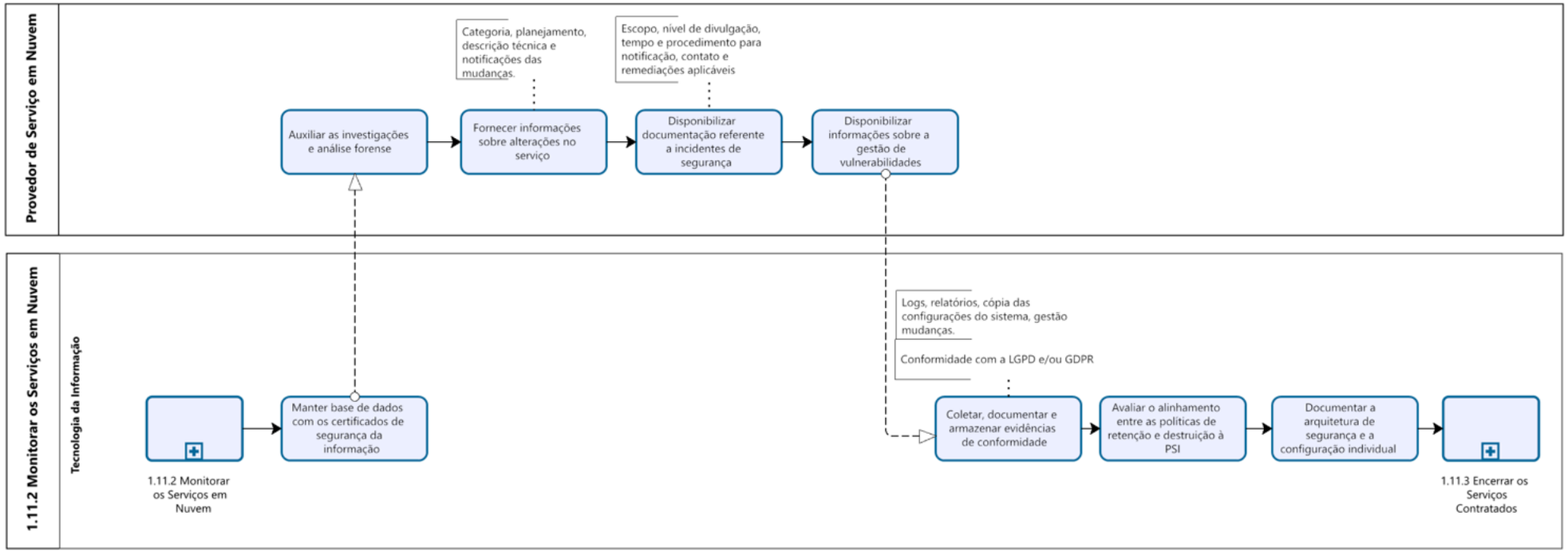
NORMA PARA CONTRATAÇÃO DE SERVIÇOS EM NUVEM



1.11.1 – Solicitar e Contratar os Serviços em Nuvem

NORMA PARA CONTRATAÇÃO DE SERVIÇOS EM NUVEM

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Validado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.11 Realizar a Contratação de Serviços em Nuvem	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 07/2024	
SUBPROCESSO: 1.11.2 Monitorar os Serviços em Nuvem	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 30/10/2024	
OBJETIVO DO SUBPROCESSO: Monitorar serviços em nuvem em conformidade com LGPD, protegendo os dados pessoais de clientes e da FCAV.			

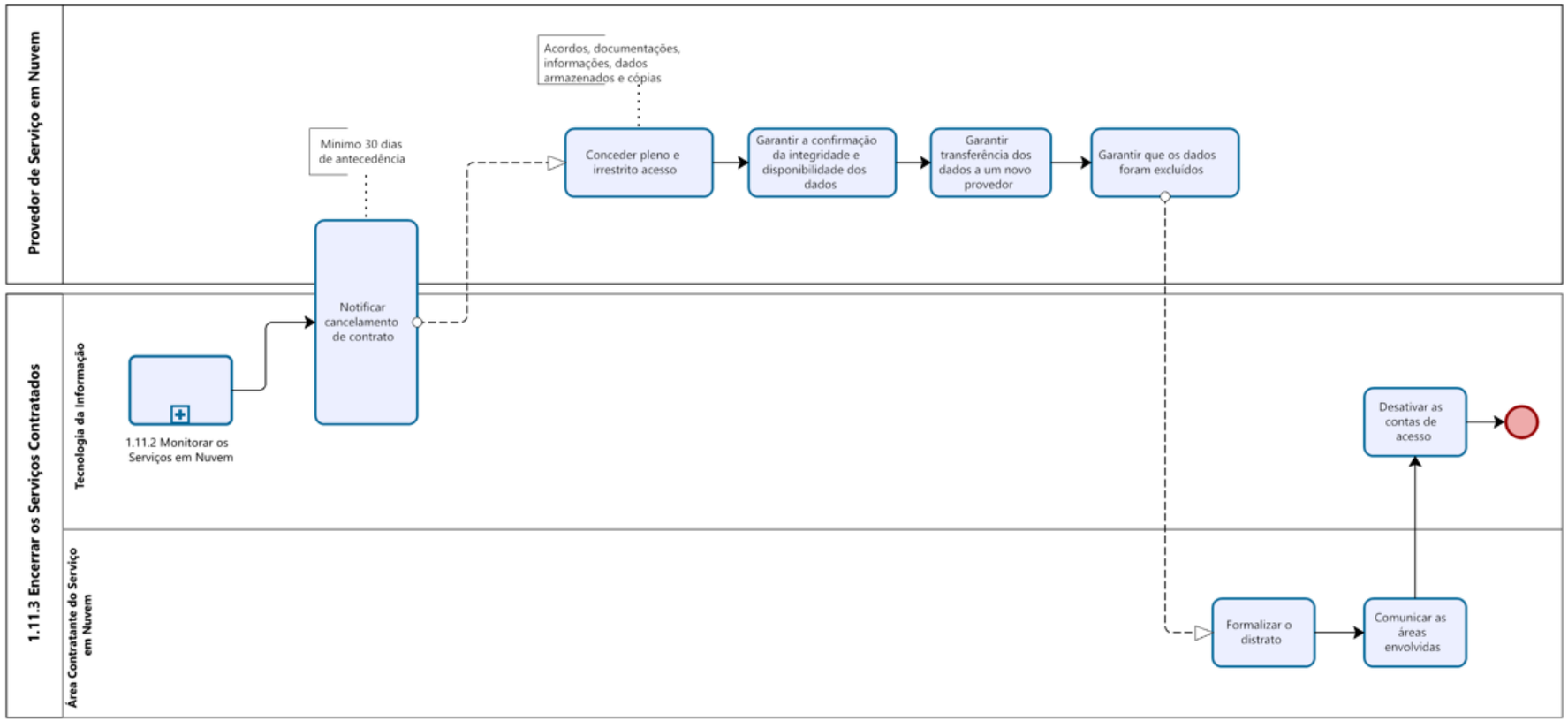


1.11.2 – Monitorar os Serviços em Nuvem

Fundação Vanzolini

NORMA PARA CONTRATAÇÃO DE SERVIÇOS EM NUVEM

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Validado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.11 Realizar a Contratação de Serviços em Nuvem	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 07/2024	
SUBPROCESSO: 1.11.3 Encerrar os Serviços Contratados	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 30/10/24	
OBJETIVO DO SUBPROCESSO: Garantir o encerramento e/ou a transição transparente e segura dos dados e serviços, garantindo a continuidade dos serviços e protegendo os interesses da FCAV			



1.11.3 – Encerrar os Serviços Contratados