1 OBJETIVO

Este documento tem por objetivo estabelecer as regras e as restrições que norteiam a gestão de identidade e o controle de acesso lógico pelos colaboradores aos recursos de Tecnologia da Informação e Comunicação (RETIC) e às informações 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.

Norma de Uso dos Recursos de Tecnologia da Informação e Comunicação (RETIC).

4 DEFINIÇÕES

✓ **Autenticação:** Etapa necessária para validar a identificação de qualquer colaborador ao acessar determinada informação ou recurso de TIC.

✓ **Conta de acesso genérica:** Conta de acesso não atrelada a identidade digital de colaborador usada para fins específicos e em recursos de Tecnologia da Informação e Comunicação (RETIC) determinados.

✓ **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.

✓ **Controle de acesso:** Conjunto de procedimentos, recursos e meios utilizados para restringir ou permitir acesso a informações e recursos de tecnologia da informação e comunicação.

✓ **Confidencialidade:** Garantia de que as informações sejam acessadas somente por pessoas

expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio.

✓ **Dispositivo móvel:** Equipamento facilmente transportado, devido a sua portabilidade, e com capacidade de registro, armazenamento ou processamento de informações, além da possibilidade de estabelecer conexões com internet, sistemas, redes e dispositivos.

✓ **Identidade digital:** Identificação do colaborador em ambientes lógicos, composta por nome de usuário (*log in*) e senha ou por outros mecanismos de identificação e autenticação, como crachá magnético, certificado digital, *token* ou biometria.

✓ **Incidente de segurança da informação e comunicação:** 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.

✓ ***Log in*:** Identificação única de colaborador para acesso a sistemas computacionais ou Recursos de Tecnologia da Informação e Comunicação.

✓ **Rastreabilidade:** Possibilidade de vincular a atividade executada ao seu executor.

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

✓ **Revogação de acesso:** Impedimento de acesso por determinada pessoa a um sistema.

✓ **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.

✓ **Senha:** Conjunto de caracteres que serve como prova de identidade digital cujo conhecimento deve ser exclusivo e único do usuário.

✓ **Movidesk:** Ferramenta de gestão de chamados que registra entrada e saída de pedidos de suporte e manutenção.

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

✓ **Trilha de auditoria:** Técnica que permite o acompanhamento de todas as atividades que afetam determinado conjunto de informações, como registro de dados, desde o momento em que ele entra no sistema até o instante em que é removido. Possibilita documentar, por exemplo, quem efetuou determinada alteração e quando isso ocorreu.

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

5 DIRETRIZES GERAIS

As diretrizes estabelecidas nesta norma aplicam-se à informação em qualquer meio ou suporte e devem ser seguidas por todos os colaboradores e prestadores de serviço.

A FCAV fornece a seus colaboradores contas de acesso à rede corporativa, para que possam executar suas atividades contratadas e/ou laborais.

Os colaboradores só podem acessar informações e recursos de TIC corporativos necessários e autorizados para o desenvolvimento de suas atividades profissionais, de acordo com as atividades exercidas para a FCAV.

Os direitos de acesso podem ser alterados ou revogados a qualquer tempo pela FCAV, sem a necessidade de aviso prévio.

6 CRIAÇÃO E CONCESSÃO DE ACESSO

O processo inicial de concessão de acesso é realizado pela Área de Recursos Humanos, no caso de contratação em regime CLT, ou pela área responsável pela contratação de terceiros, no caso de contratação de pessoa jurídica, após a efetivação legal.

A concessão de direitos de acesso aos colaboradores só é permitida após assinatura de termo de compromisso, sigilo e confidencialidade ou contrato que contenha cláusulas que assegurem a segurança das informações, bem como de ciência da Política de Segurança da Informação.

O gestor responsável pelo colaborador deverá encaminhar a solicitação de criação e concessão de acesso, inclusive para terceiro, por meio da ferramenta de gestão de chamados da FCAV.

A Área de Tecnologia da Informação será responsável pela execução de criação e concessão de acesso.

Sempre que for necessário acesso a sistema ou recurso de TIC, o gestor responsável pelo colaborador deve encaminhar solicitação que contenha:

✓ justificativa para a necessidade de acesso;
✓ função, área, cargo e modalidade de contratação do colaborador;
✓ atividades profissionais executadas pelo colaborador;
✓ tipos de informação que podem ser acessados pelo colaborador, de acordo com a necessidade

de sigilo;

✓ tipo de acesso necessário, ou seja, se compreende visualização, inclusão, modificação e/ou exclusão de informações;

✓ termo de ciência da Política de Segurança da Informação assinado pelo colaborador;

✓ aprovação do gestor.

A Área de Tecnologia da Informação deve analisar a solicitação de criação e concessão de acesso e, após a análise, deverá:

✓ criar ou liberar o acesso aos ambientes, em caso de solicitação aprovada;

✓ informar ao gestor responsável pelo colaborador os motivos pelos quais não foi possível atender à solicitação, caso ela seja reprovada.

O acesso será bloqueado somente quando a Área de Recursos Humanos e o gestor responsável solicitar tal bloqueio, por meio da ferramenta de gestão de chamados, informando o encerramento das atividades laborais ou do contrato com terceiro.

Em caso de terceiro, quando não houver renovação de contrato, a solicitação de bloqueio de acesso deverá ser encaminhada pelo gestor responsável pela contratação no prazo de até 10 dias que antecedem o encerramento do contrato.

O acesso concedido aos recursos de TIC corporativos e às informações da FCAV são para uso estritamente profissional e para execução das atividades contratadas, são intransferíveis e permitem a identificação das atividades realizadas pelo colaborador.

7 MECANISMOS DE AUTENTICAÇÃO (SENHAS)

A Área de Tecnologia da Informação deve configurar o primeiro acesso do colaborador atribuindo uma senha temporária, de modo que seja obrigatória a sua alteração em seguida da autenticação.

A senha definida pelo colaborador:

✓ deve ser tratada de forma individual, sigilosa e intransferível, não podendo ser compartilhada, divulgada ou transmitida a terceiros;

✓ não deve ser baseada em nomes, datas especiais, sequências óbvias de números e letras, palavras dicionarizadas, números de telefones, meses do ano etc.;

✓ não deve ser armazenada em computadores ou dispositivos móveis, anotada em papel ou qualquer outro suporte físico ou eletrônico;

✓ deve ser alterada periodicamente, no máximo a cada seis meses, ou em qualquer caso de suspeita de comprometimento de seu sigilo;

✓ deve conter pelo menos 7 (sete) caracteres alfanuméricos e especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúscula e minúscula), em caso de usuário sem perfil de administrador;

✓ deve conter pelo menos 10 (dez) caracteres alfanuméricos e especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúscula e minúscula), em caso de usuário com perfil de administrador ou acesso privilegiado;

✓ não deve ser igual a senhas utilizadas anteriormente, quando alterada.

8 REVOGAÇÃO, BLOQUEIO E EXCLUSÃO DO ACESSO

O acesso do colaborador deve ser revogado pela Área de Tecnologia da Informação:

✓ imediatamente, em caso de encerramento de suas atividades ou término de seu contrato com a FCAV;
✓ quando solicitado pelo gestor responsável e pela Área de Recursos Humanos;
✓ depois de 90 dias sem qualquer indicação de uso para acesso à informação ou recurso de TIC corporativo;
✓ depois de expirado o prazo estabelecido para utilização, quando não solicitada a prorrogação de acesso.

Em caso de afastamento do colaborador por prazo superior, o gestor responsável deve comunicar a Área de Tecnologia da Informação, para que não ocorra a exclusão do acesso, mantendo-se o log in bloqueado durante esse período.

Qualquer encerramento de atividades ou término de contrato de colaborador deve ser informado à Área de Tecnologia da Informação:

✓ se colaborador: a Área de Recursos Humanos ou o gestor responsável pela contratação deve solicitar a revogação de acesso por meio de chamado à Área de Tecnologia da Informação;
✓ se terceiro: o gestor responsável deve solicitar a revogação de acesso por meio de chamado à Área de Tecnologia da Informação.

O acesso deve ser bloqueado automaticamente após três tentativas malsucedidas de autenticação que denotem tentativa de quebra, de acordo com cada sistema adotado.

Em caso de encerramento de atividades ou término de contrato de colaborador, seu acesso será bloqueado e suas permissões serão removidas pela Área de Tecnologia da Informação.

9 REVISÃO DO ACESSO

Na ocorrência de alteração de função ou área do colaborador, cabe à Área de Recursos Humanos alterar no(s) sistema(s) sob sua responsabilidade e informar à Área de Tecnologia da Informação caso seja necessário algum ajuste.

Na ocorrência de alteração de atividades executadas por terceiro, cabe ao gestor responsável informar à Área de Tecnologia da Informação as alterações de acesso necessárias.

A Área de Tecnologia da Informação deve verificar, em período não superior a seis meses, se há identidade digital fora dos padrões estabelecidos e elaborar relatório interno sobre as inconformidades encontradas, com objetivo de corrigi-las e subsidiar eventuais auditorias.

10 PERMISSÕES DIFERENCIADAS

Alguns colaboradores, de acordo com a definição de alçadas, cargos ou funções, podem ter permissões diferenciadas para acesso e uso de informações ou recursos de TIC corporativos, a fim de atender aos objetivos de negócio da FCAV.

As solicitações desse tipo de permissão devem ser submetidas à análise da Área de Tecnologia da Informação de acordo com os documentos normativos da FCAV, o perfil do colaborador e a necessidade justificada e informada pelo gestor responsável.

Perfis com permissões diferenciadas devem ser criados pela Área de Tecnologia da Informação e documentados individualmente com o devido registro de responsabilidades e permissões de acesso atribuídas.

As permissões diferenciadas são concedidas a critério único e exclusivo da FCAV e apenas por prazo determinado, podendo ser revogadas a qualquer momento e sem aviso prévio.

Caso haja remanejamento, promoção ou outro evento que afaste o colaborador da atividade que exige permissões diferenciadas, o gestor responsável deve comunicar a Área de Tecnologia da Informação, para revisão das autorizações.

11 RESPONSABILIDADES ESPECÍFICAS

11.1 Área de Tecnologia da Informação

Verificar, em período não superior a 6 (seis) meses, se há identidade digital fora dos padrões estabelecidos e elaborar relatório interno sobre as inconformidades encontradas.

Autorizar a criação e o uso de contas de acesso genéricas somente em casos de exceção e nos termos desta norma.

Criar e documentar qualquer perfil que tenha permissões diferenciadas.

Analisar as solicitações de acesso, inclusive acesso remoto, enviadas por gestores de acordo com os termos desta norma.

Estabelecer mecanismos de identificação e autenticação de acordo com os critérios descritos nesta norma e de forma que possibilite a rastreabilidade dos acessos realizados.

Manter em conformidade os acessos autorizados.

Fornecer senhas provisórias de forma segura e sigilosa e de maneira que sua alteração seja exigida no primeiro acesso.

Manter, de forma segura, registro das solicitações de criação, concessão, alteração e revogação de acesso, bem como a identidade digital de colaboradores.

Revogar acessos após o encerramento das atividades ou o término do contrato de colaboradores.

Assegurar que não sejam atribuídos identificadores (ID) redundantes a nenhum colaborador.

Ajustar, bloquear ou revogar contas de acesso, quando solicitado pela Área de Recursos Humanos, pelo gestor responsável ou pela área responsável pela contratação de terceiros, bem como informar ao solicitante a efetivação de ajuste, bloqueio ou revogação.

Revisar os acessos dos colaboradores em caso de alteração das atividades ou área, conforme informação encaminhada pelo gestor responsável.

11.2 Área de Recursos Humanos

Cadastrar na ferramenta de gestão de pessoal todo novo colaborador da FCAV.

Garantir que as concessões de direitos de acesso aos colaboradores ocorram somente após assinatura de termo de compromisso, sigilo e confidencialidade e que assegurem a segurança das informações, bem como de ciência da Política de Segurança da Informação.

Ajustar nos sistemas sob sua responsabilidade quando da alteração de área, cargo ou função de colaboradores e informar à Área de Tecnologia da Informação caso seja necessário algum ajuste.

Solicitar acesso ao portal interno/intranet.

Informar e solicitar à Área de Tecnologia da Informação o bloqueio de acesso para todos os casos de encerramento de atividades de colaboradores.

11.3 Área responsável pela contratação de terceiros

Garantir que as concessões de direitos de acesso a terceiros ocorram somente após assinatura de termo de compromisso, sigilo e confidencialidade ou contrato que contenha cláusulas que assegurem a segurança das informações, bem como de ciência da Política de Segurança da Informação.

11.4 Gestores

Garantir e gerenciar o cumprimento desta norma e documentos complementares pelos seus colaboradores.

Solicitar, mediante justificativa, e autorizar a liberação e a concessão de acesso a recursos de TIC corporativos e informações da FCAV para seus colaboradores, inclusive terceiros.

Solicitar, mediante justificativa, ajustes necessários na concessão de acesso a recursos de TIC corporativos e informações da FCAV para seus colaboradores nos casos de alteração de atividades ou área.

Solicitar à Área de Tecnologia da Informação o bloqueio ou a revogação de acesso para todos os casos de encerramento de atividades ou término de contrato de terceiros e sempre que considerar necessário para a proteção da FCAV.

Informar à Área de Recursos Humanos todos os casos de encerramento de atividades e de alteração de área, cargo ou função de colaboradores.

11.5 Colaboradores em geral e em regime de exceção (temporários)

Cumprir, estar ciente e manter-se atualizado em relação a esta norma e documentos complementares.

Acessar informações ou fazer uso de recursos de TIC somente quando necessário e autorizado pela FCAV e apenas para finalidades profissionais, de acordo com sua função.

Manter a confidencialidade de sua senha, não compartilhando com terceiros.

12 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.

13 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.

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.

14 ANEXOS

Anexo I – Fluxos de gestão de acessos 1.8, 1.8.1 e 1.8.2.

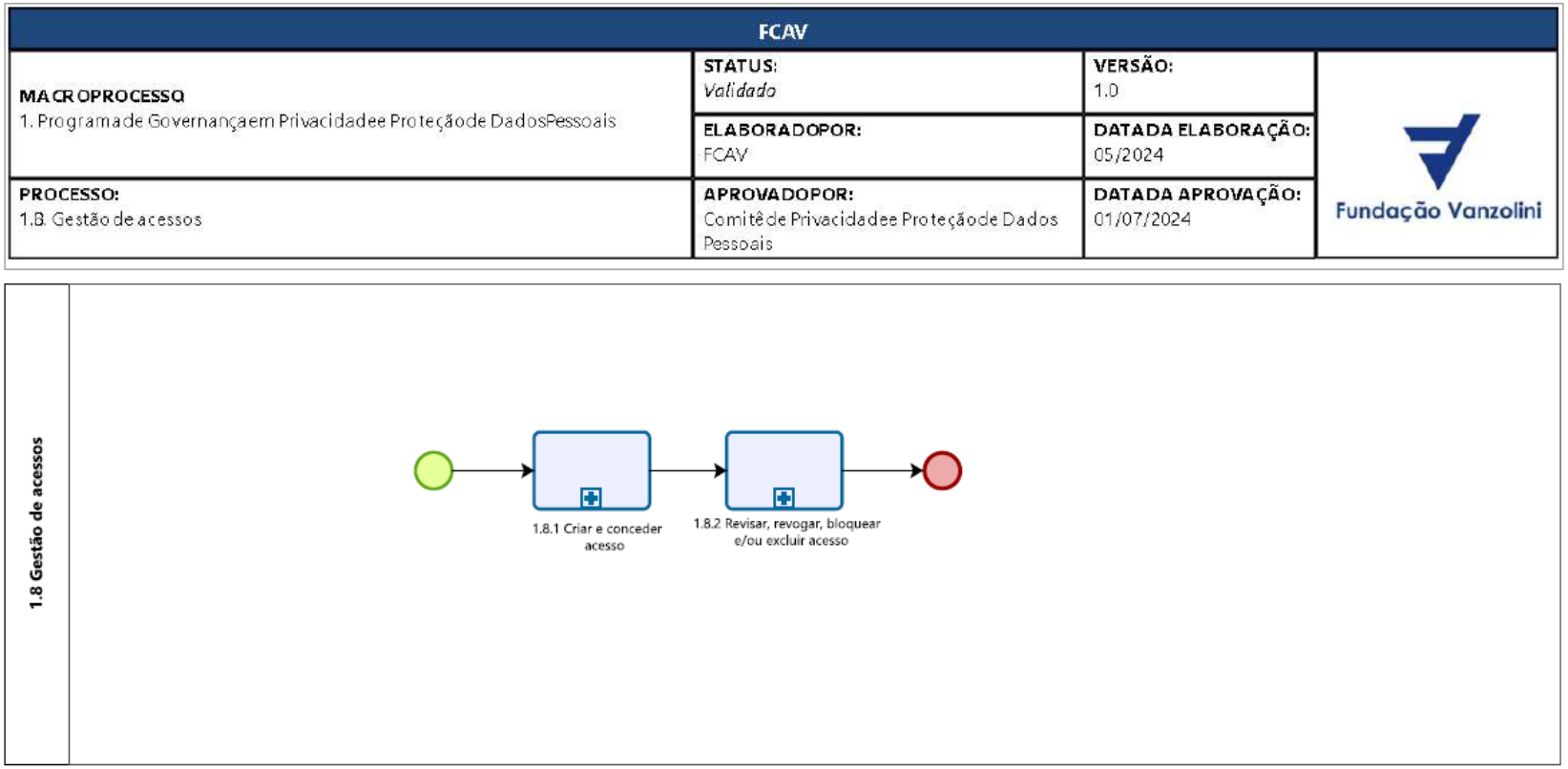
15 NATUREZA DAS ALTERAÇÕES

Revisão	Alterações (Inclusões ou Exclusões)	Data
00	Emissão Inicial	19/10/2022
01	Inclusão dos fluxos de gestão de acessos 1.8, 1.8.1 e 1.8.2 (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	09/11/2022
01	Versão 01	25/07/2024

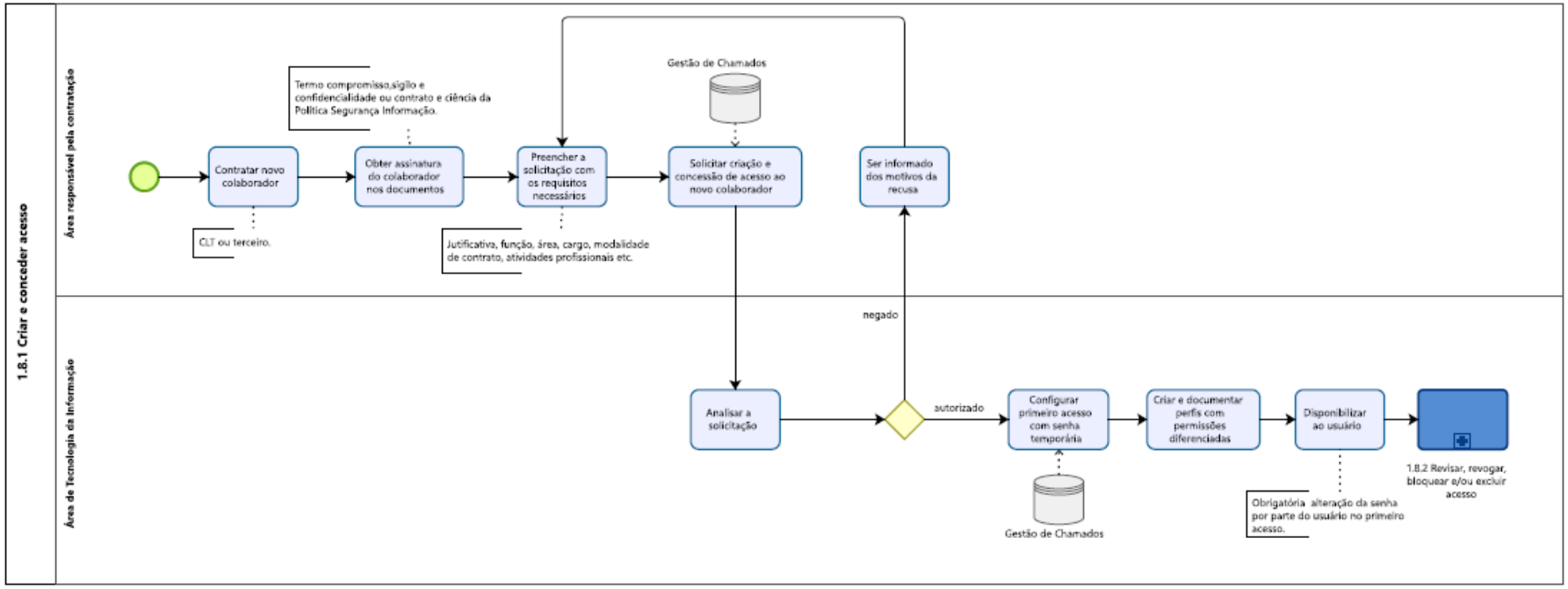
16 ANEXO I

As atividades representadas nos fluxos para execução desta norma de Gestão de Acessos, têm por objetivo de facilitar a compreensão do processo em cada etapa. Composto por três arquivos em formato PDF, denominados processo e subprocessos 1.8, 1.8.1 e 1.8.2, respectivamente, que devem ser seguidos pelos responsáveis pela execução desta norma.



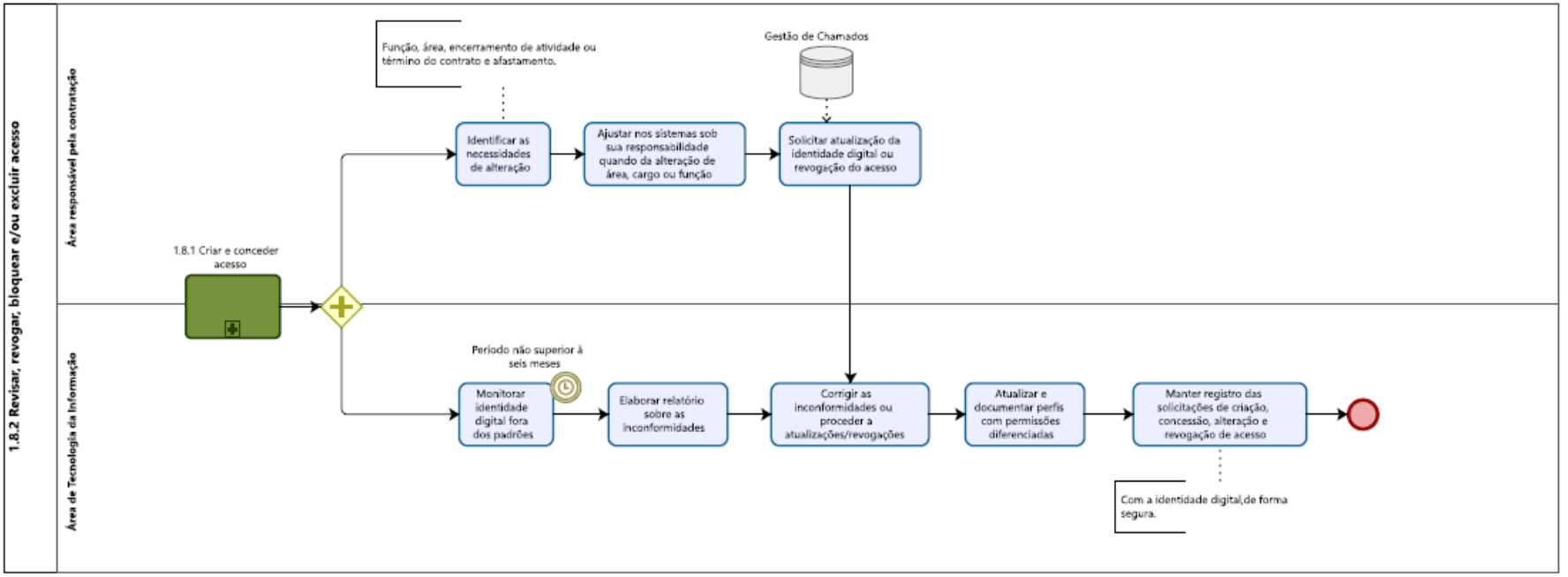
1.8 – Processo: Gestão de acessos

FCAV			
MACROPROCESSO 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	**STATUS:** *Validado*	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.8 Gestão de acesso	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 05/2024	
SUBPROCESSO: 1.8.1 Criar e conceder acesso	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 01/07/2024	
OBJETIVO DO SUBPROCESSO: Criar e conceder acesso aos novos colaboradores em conformidade com a LGPD.			



1.8.1 – Subprocesso: Criar e conceder acesso

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	**STATUS:** *Validado*	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.8 Gestão de acesso	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 05/2024	
SUBPROCESSO: 1.8.2 Revisar, revogar, bloquear e/ou excluir acesso	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 01/07/2024	
OBJETIVO DO SUBPROCESSO: Revisar, revogar, bloquear e/ou excluir acesso de colaboradores em conformidade com a LGPD.			



1.8.2 – Subprocesso: Revisar, revogar, bloquear e/ou excluir acesso