1 OBJETIVO

Este documento tem por objetivo estabelecer boas práticas, regras e restrições relativas a registro, coleta, preservação e exclusão de *logs*, trilhas de auditoria e monitoramento do ambiente lógico 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 da FCAV e terceiros responsáveis pelos processos de gestão de *logs* e trilhas de auditoria.

3 REFERÊNCIAS

Política de Segurança da Informação.

Norma de Gestão de Incidentes de Segurança da Informação.

Norma de Gestão de Incidentes de Violação de Dados Pessoais.

4 DEFINIÇÕES

- ✓ **Ambiente lógico:** Rede corporativa ou plataforma digital disponibilizada para uso interno e externo.

- ✓ **Auditoria:** Processo de exame sistemático das atividades realizadas, a fim de averiguar sua conformidade com as regras e os procedimentos prévia e expressamente estabelecidos, aferindo-lhe a implementação e a eficácia.

- ✓ **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, bem como estagiários e menores aprendizes.

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

- ✓ **Incidente de segurança com dados pessoais:** Qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação da segurança de dados pessoais, tais como acessos não autorizados, acidentais e ilícitos, que resulte em sua destruição, perda, alteração ou vazamento, ou, ainda, qualquer tratamento de dados inadequado ou ilícito que possa ocasionar risco para os direitos e as liberdades do titular dos dados pessoais.

- ✓ **Incidente de segurança da informação:** Ocorrência identificada de estado de sistema, dados, informações, serviço ou rede que indica possível violação à Política de Segurança da Informação ou a normas complementares, falha de controles ou situação previamente desconhecida que possa ser relevante à segurança da informação.

- ✓ **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*:** Registro de eventos relevantes em um recurso de Tecnologia da Informação e Comunicação (TIC) ou em ambiente lógico da FCAV.

- ✓ **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 e descarte de informações.

- ✓ **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.

- ✓ **Tratamento de incidentes de segurança da informação:** Atividade que consiste em receber, registrar, classificar e responder a solicitações e alertas sobre incidentes de segurança da informação, bem como tratá-los, a fim de extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências.

- ✓ **Trilha de auditoria:** Técnica que permite o acompanhamento de atividades que afetam determinado conjunto de informações, desde o momento em que se origina até o instante em que é finalizado, mediante identificação de autor, data e horário de cada atividade.

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

- ✓ **Violação de dados pessoais:** Destruição, perda, alteração, divulgação acidental, ilegal ou não autorizada ou acesso a dados pessoais transmitidos, armazenados ou de outra forma processados, resultante de incidente de segurança.

5 DIRETRIZES GERAIS

Os *logs* são úteis para auditorias, análises forenses, suporte a investigações internas e identificação de tendências operacionais e problemas de longo prazo. Os ambientes lógicos e recursos de TIC da FCAV devem ser configurados de forma a registrar informações de *log in* e auditoria suficientes para responder às seguintes perguntas:

- ✓ Que tipo de atividade ocorreu (tipo de evento/ação)?
- ✓ Quem ou o que realizou a atividade (sujeito)?
- ✓ Em que sistema a atividade ocorreu ou foi observada (*logger*/observador do evento)?

- ✓ Para que a atividade foi realizada (objetivo)?
- ✓ Quando a atividade foi realizada (tempo)?
- ✓ Qual foi o *status*, a resolução ou o resultado da atividade (sucesso *vs.* falha)?

Devem ser registrados em *log*, quando sua execução for requisitada pelo sistema, todos os eventos relevantes ou, no mínimo, os seguintes:

- ✓ autenticação inequívoca de usuários, tanto os bem-sucedidos quanto os malsucedidos, em ambientes lógicos e recursos de TIC;
- ✓ criação, leitura, atualização ou exclusão de informações confidenciais;
- ✓ início de conexão com internet;
- ✓ aceite de conexão com internet;
- ✓ concessão, modificação ou revogação de direitos de acesso, inclusive adição de novo usuário ou grupo, mudança em níveis de privilégio ou permissões de acesso a documentos, alterações em base de dados, regras de *firewall* ou senhas de usuários;
- ✓ mudança de configuração em sistema, rede ou serviço, inclusive instalação de *patch* e atualização de *software*;
- ✓ acesso a banco de dados da FCAV de fontes interna e externa;
- ✓ falha que resulte no fechamento anormal de aplicação, serviço de rede ou *hardware*, especialmente quando relacionada a exaustão ou atingimento de limite de recurso (como memória da Unidade Central de Processamento [*Central Processing Unit*, CPU], conexão de rede, espaço em disco etc.).
- ✓ acesso e alteração de trilhas de auditoria;
- ✓ tráfego de dados de fontes internas e externas;
- ✓ processo interno relacionado a atividades do negócio;
- ✓ data, horário e fuso horário.

Os registros dos eventos (*logs*) devem ser:

- ✓ protegidos contra acesso não autorizado e alteração, armazenados de forma segura e com acesso restrito aos colaboradores responsáveis pelo seu gerenciamento;
- ✓ gravados, acessados e analisados apenas em modo de leitura, de forma a preservar sua integridade e sua autenticidade.

A Área de Tecnologia da Informação deve se valer de ferramenta de gestão automatizada de *log* para análise dos dados gerados em toda a infraestrutura dos ambientes lógicos da FCAV.

As ameaças de segurança devem ser analisadas pela Área de Tecnologia da Informação por meio de ferramentas de correlação de dados de *logs* e eventos que viabilizem a detecção e a geração de alertas relacionados a:

- ✓ atividades que violem normas e *softwares*;
- ✓ ataques de vírus e *malwares* a rede corporativa, arquivos e *softwares*;
- ✓ ataques de intrusão;
- ✓ acessos remotos;
- ✓ vulnerabilidades previamente conhecidas e *softwares* desatualizados;
- ✓ atividades de roteadores, *firewalls* e servidores de arquivos em quarentena;

- ✓ eventos de *softwares* bem-sucedidos ou interrompidos.

A Área de Tecnologia da Informação deve emitir relatórios de correlação com periodicidade estabelecida de acordo com a criticidade do ambiente – mensal, trimestral e semestral –, para que sejam analisados criticamente.

O período de armazenamento dos registros de *log* deve atender às necessidades das áreas críticas e aos requisitos de temporalidade estipulados conjuntamente com a Consultoria Jurídica, considerando o período mínimo de um ano, caso lei específica não defina prazos inferiores ou superiores.

Em caso de ambientes que fazem parte do escopo PCI-DSS (padrão de segurança de dados da indústria de cartões de pagamento), os *logs* devem ser mantidos *on-line* por noventa dias e *off-line* por nove meses.

6 MONITORAMENTO

A FCAV realiza monitoramento lógico de seus ambientes com o objetivo de:

- ✓ identificar e registrar as atividades neles realizadas;
- ✓ garantir a segurança e a integridade dos seus ativos.

Os dados obtidos do monitoramento por meio de registro de *logs* devem ser analisados periodicamente pela Área de Tecnologia da Informação, a fim de garantir a integridade dos ativos e detectar quaisquer anormalidades ou atividades irregulares.

O monitoramento lógico deve ser realizado por meio de *softwares* estabelecidos e implementados pela Área de Tecnologia da Informação, de acordo com as necessidades da FCAV e os objetivos de negócio.

Quaisquer recursos de TIC da FCAV conectados à rede corporativa ou que utilizem suas informações para fins profissionais devem ser monitorados pela Área de Tecnologia da Informação.

A FCAV deve cientificar todos os colaboradores quanto ao monitoramento de ambientes lógicos e recursos de TIC corporativos, por meio de políticas, normas e avisos legais (*disclaimers*) disponibilizados nos próprios ambientes digitais.

Os ambientes lógicos que coletam dados e registros de *logs* advindos de fonte externa devem conter, na respectiva plataforma, termos de uso e condições de navegação e política de privacidade que:

- ✓ solicitem ao usuário consentimento para coleta de dados e registro de *logs* gerados durante a navegação;
- ✓ informem ao usuário a temporalidade do armazenamento dos dados e registros de *logs* de monitoramento;

- ✓ prevejam a exclusão de *logs* mediante solicitação do usuário.

7 TRILHAS DE AUDITORIA

Os ambientes lógicos e recursos de TIC da FCAV devem ser configurados para armazenar registros históricos de eventos em formato que permita a completa identificação dos fluxos de dados.

A geração, a análise e a forma de armazenamento de trilhas de auditoria devem ser definidas de acordo com a necessidade de cada ambiente lógico e recurso de TIC, com vistas ao planejamento de um sistema de auditoria.

O acesso adequado a uma trilha de auditoria é essencial para garantir sua auditabilidade, repetibilidade, reprodutibilidade e justificabilidade, o que contribuirá para sua admissibilidade em processos judiciais, administrativos ou disciplinares.

O acesso à trilha de auditoria deve ser confidencial e restrito aos colaboradores da Área de Tecnologia da Informação autorizados.

Para garantir a confiabilidade da trilha de auditoria, os procedimentos para sua identificação, coleta, aquisição e preservação devem contar com:

- ✓ controles de acesso, arquivamento e coleta de trilha de auditoria;
- ✓ informações sobre o ambiente lógico, o recurso de TIC ou o dado de origem;
- ✓ documentação de todas as ações realizadas;
- ✓ indicação de colaborador(es) qualificado(s), treinado(s) e autorizado(s) pela FCAV para acessar e analisar as trilhas de auditoria.

8 RESPONSABILIDADES ESPECÍFICAS

8.1. Área de Tecnologia da Informação

Estabelecer controles de acesso segredado e critérios de monitoramento e de registro de *logs* e de trilhas de auditoria dos ambientes lógicos da FCAV.

Enviar, sempre que necessário, relatórios de monitoramento para o Comitê de Privacidade e Proteção de Dados Pessoais, para eventual análise pela Equipe de Respostas a Incidentes.

Elaborar e analisar periodicamente os relatórios e registros obtidos no monitoramento, usando-os para os fins estabelecidos neste documento.

Analisar os relatórios de monitoramento.

Manter o valor probatório dos registros para fins legais, preservando a confidencialidade, a integridade, a autenticidade, a legalidade e a disponibilidade dos dados.

Estabelecer procedimentos formais para gestão de *logs* e infraestrutura adequada e segura para

seu armazenamento.

Garantir a sincronização do relógio dos ambientes lógicos e recursos de TIC da FCAV com referências de tempo confiáveis.

Configurar os ambientes lógicos e recursos de TIC da FCAV de forma a registrar todos os eventos relevantes de segurança da informação e comunicação, nos termos deste documento.

Implementar nos ambientes lógicos e nos recursos de TIC da FCAV os avisos legais de monitoramento lógico.

8.2. Consultoria Jurídica

Elaborar e implementar a tabela de temporalidade para guarda de registros obtidos por meio do monitoramento lógico dos ambientes.

9 PENALIDADES

Qualquer atividade que desrespeite as disposições estabelecidas neste documento e 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.

10 DISPOSIÇÕES FINAIS

Este documento deve ser revisado, no mínimo, anualmente ou sempre que existir necessidade de alteração 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 normas e os procedimentos aplicáveis pela FCAV.

Este documento e complementares encontram-se disponíveis na intranet e, em caso de indisponibilidade desta, podem ser solicitados ao Encarregado pelo Tratamento de Dados Pessoais da FCAV.

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.

11 ANEXOS

Anexo I – Fluxos de gestão de *logs* e trilhas de auditoria 1.9, 1.9.1 e 1.9.2.

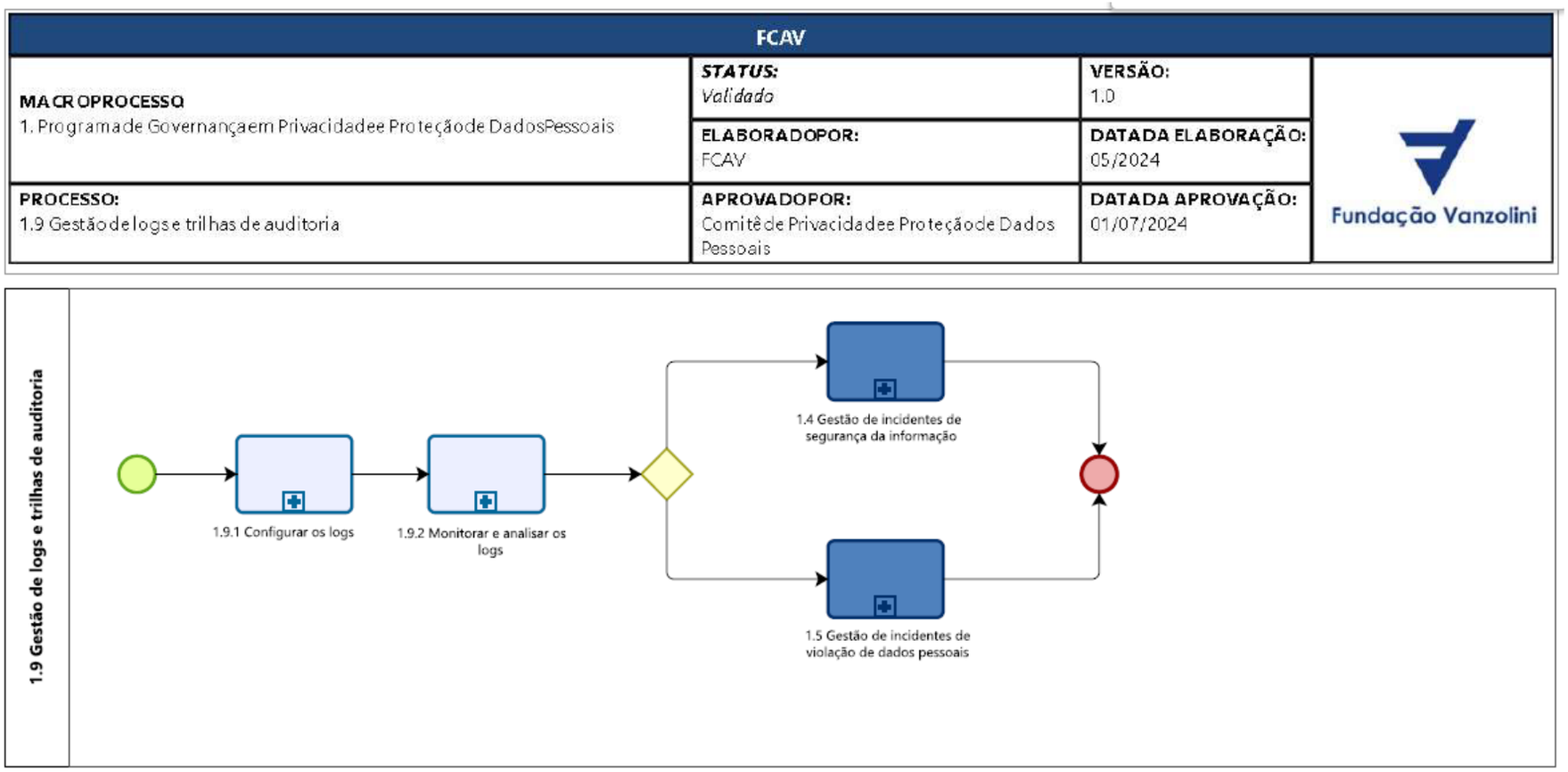
12 NATUREZA DAS ALTERAÇÕES

Revisão	Alterações (Inclusões ou Exclusões)	Data
00	Emissão	11/04/2023
01	No cabeçalho da versão inicial do documento, onde está “Revisão 01”, lê-se “Revisão 00”. A presente versão mantém a numeração “Revisão 01”. Inclusão dos fluxos de trabalho e atividades 1.9, 1.9.1 e 1.9.2 aprovados pelo Comitê de Privacidade e Proteção de Dados Pessoais. Ajustes nos textos do documento em atendimento às necessidades identificadas durante a revisão.	01/07/2024

Revisão	Aprovação da Diretoria Executiva	Data
00	Emissão	19/04/2023
01	Versão 01	25/07/2024

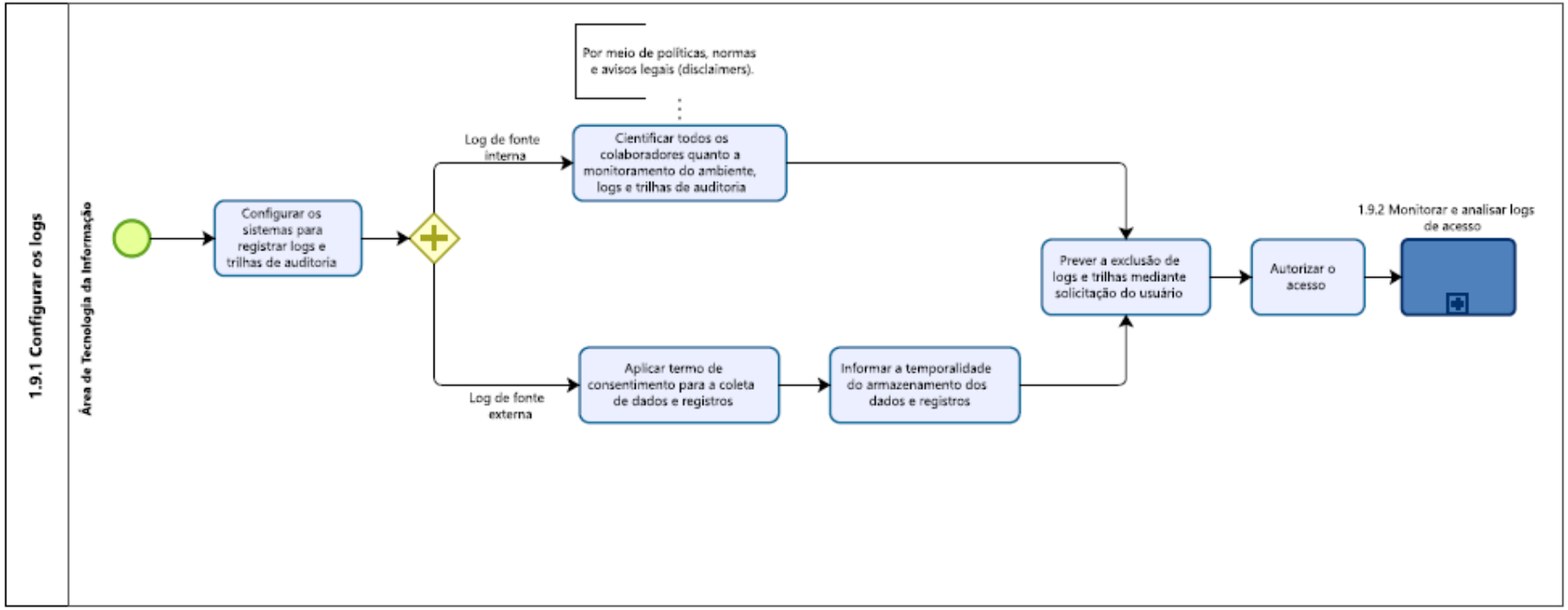
13 ANEXO I

As atividades para execução deste documento 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 documento.



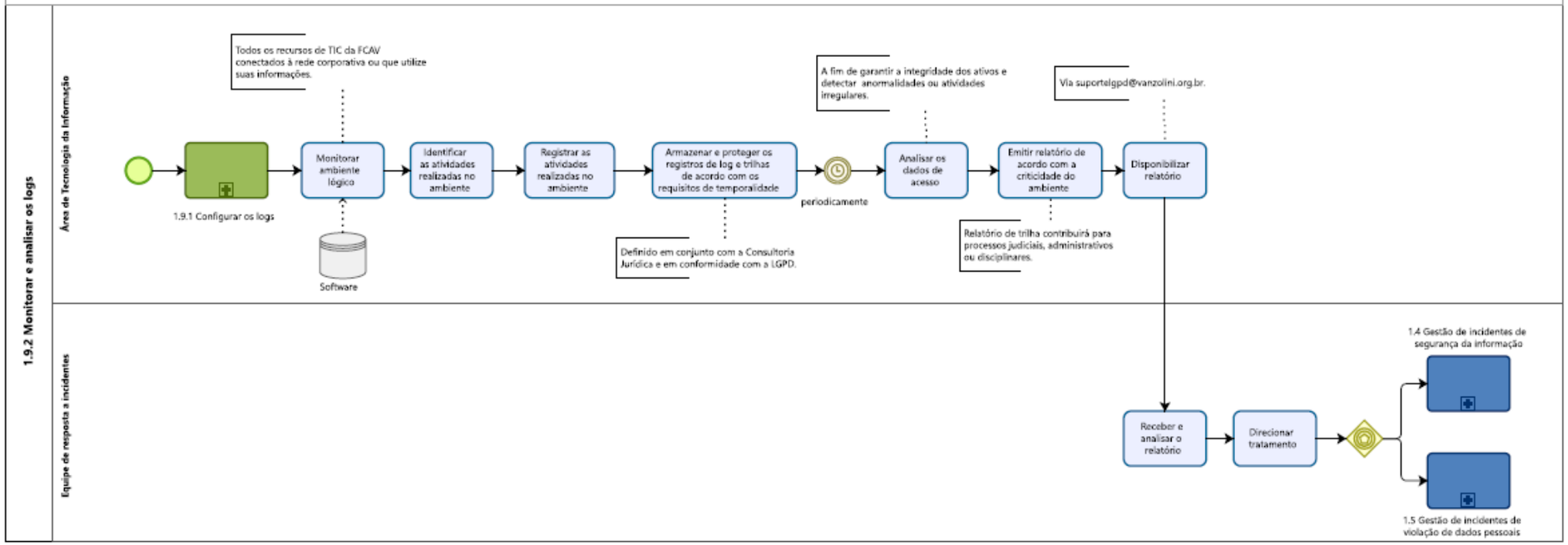
1.9 – Gestão de *logs* e trilhas de auditoria

FCAV			
MACROPROCESSO 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** *Validado*	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.9 Gestão de logs e trilhas de auditoria	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 05/2024	
SUBPROCESSO: 1.9.1 Configurar os logs	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 01/07/2024	
OBJETIVO DO SUBPROCESSO: Garantir transparência, integridade e segurança no tratamento de dados pessoais e informações.			



1.9.1 – Configurar os *logs*

FCAV		
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** *Validado*	**VERSÃO:** 1.0
PROCESSO: 1.9 Gestão de logs e trilhas de auditoria	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 05/2024
SUBPROCESSO: 1.9.2 Monitorar e analisar os logs	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 01/07/2024
OBJETIVO DO SUBPROCESSO: Identificar e registrar as atividades realizadas em seus ambientes lógicos para garantir a segurança e a integridade dos seus ativos.		



1.9.2 – Monitorar e analisar os logs