1 OBJETIVO

Este documento tem por objetivo estabelecer critérios para a implantação de ferramentas de criptografia, bem como garantir seu uso efetivo e adequado, com o intuito de proporcionar a segurança das 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

- Norma de Gestão de Incidentes de Segurança da Informação.
- Política de Segurança da Informação.

4 DEFINIÇÕES

✓ **Colaborador:** Toda e qualquer pessoa física, estagiária, 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.

✓ **Esteganografia:** Técnica utilizada para ocultar um arquivo dentro de outro, de forma criptografada. Diferentemente da criptografia, que visa deixar as mensagens codificadas, a esteganografia tem como objetivo esconder a existência de determinada mensagem, camuflando-a dentro de outros arquivos, como imagens, músicas, vídeos ou textos.

✓ **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.

5 DIRETRIZES GERAIS

O uso de ferramentas de criptografia de dados visa garantir a proteção da confidencialidade, da integridade e da autenticidade das informações da FCAV, além do não repúdio.

A Área de Tecnologia da Informação tem responsabilidade exclusiva por adquirir, implantar, administrar e fornecer aos colaboradores da FCAV quaisquer tipos de ferramenta de criptografia que se façam necessários para proteger as informações da FCAV.
As ferramentas de criptografia adquiridas pela Área de Tecnologia da Informação devem ser avaliadas criteriosamente com base em análise de riscos e seleção de controles.

6 FERRAMENTAS

Ferramentas de criptografia, simétricas ou assimétricas, devem:

- ✓ ser adquiridas de fornecedores reconhecidos no mercado por sua credibilidade e pela confiabilidade de seus produtos;
- ✓ empregar algoritmos compatíveis com os padrões internacionalmente reconhecidos;
- ✓ ser empregadas com base em consultas a especialistas que identifiquem os controles criptográficos adequados para atender aos objetivos no negócio;
- ✓ empregar tamanhos de chave (em *bits*) compatíveis com níveis aceitáveis de resistência a ataques digitais;
- ✓ empregar métodos de criptografia integral ou mediante divisão em blocos.

Tais condições aplicam-se também a:

- ✓ ferramentas de criptografia com código aberto e/ou gratuitas;
- ✓ ferramentas com funções análogas, tal como esteganografia;
- ✓ recursos de criptografia nativos de sistemas e aplicações adquiridos ou desenvolvidos (internamente ou sob encomenda) pela FCAV.

Cabe à Área de Tecnologia da Informação definir procedimentos de gerenciamento das chaves de criptografia que garantam:

- ✓ geração, armazenamento, arquivamento, recuperação, distribuição, retirada e destruição adequada das chaves;
- ✓ proteção das chaves contra modificação e perda;
- ✓ registro e auditoria das atividades relacionadas ao gerenciamento das chaves;
- ✓ definição de datas de ativação e desativação de chaves de forma que possam ser utilizadas apenas por determinado período;
- ✓ uso, quando necessário, de sistema de gerenciamento de chaves, de acordo com as necessidades do negócio.

Se empregada para autenticação de colaboradores, as ferramentas de criptografia devem utilizar obrigatoriamente chaves assimétricas (*public key infrastructure*) e ser compatíveis com o sistema de gestão de identidades e autenticação, de acordo com as definições estabelecidas pela Área de Tecnologia da Informação.

7 USO DAS FERRAMENTAS DE CRIPTOGRAFIA

Todas as funções de criptografia utilizadas para proteger informações da FCAV, inclusive dados pessoais e dados pessoais sensíveis, devem ser implantadas em sistema confiável. Para uso da criptografia em comunicação, troca ou transmissão de informações para partes externas, cabe ao Gerente da área em questão solicitar formalmente à Área de Tecnologia da Informação orientação sobre a ferramenta de criptografia mais adequada para proteção das informações da FCAV.

A transmissão de informações para partes externas deve ser realizada obrigatoriamente mediante soluções de protocolos seguros com criptografia que adotem chaves assimétricas (*public key infrastructure*).

Cabe à Área de Tecnologia da Informação definir os procedimentos relativos a:

- ✓ aquisição/emissão e uso de certificados digitais e assinatura eletrônica de documentos;
- ✓ acesso e uso de *websites* que utilizem métodos de criptografia de comunicação baseada em certificados digitais (tais como Secure Sockets Layer - SSL e/ou Transport Layer Security - TLS);
- ✓ acesso e uso de túneis criptografados de acesso remoto à rede (especialmente Virtual Private Network - VPN);
- ✓ configuração e uso de recursos de criptografia de dispositivos móveis, nativos ou instalados de forma complementar.

8 VEDAÇÕES

É vedada a aquisição de ferramentas de criptografia que utilizem algoritmos proprietários que não tenham sido testados e revisados mediante publicação e comprovação dos resultados.

É vedado ao colaborador adquirir para uso profissional ou instalar por conta própria, nos sistemas de Tecnologia da Informação da FCAV ou para cifrar informações da instituição, qualquer ferramenta de criptografia não homologada pela Área de Tecnologia da Informação.

Cabe à Área de Tecnologia da Informação inspecionar os sistemas de Tecnologia da Informação institucionais, inclusive dispositivos móveis, removendo imediatamente qualquer ferramenta ou recurso de criptografia que não tenha sido formalmente concedido ou instalado pela FCAV.

9 TRATAMENTO DE INCIDENTES

Caso seja constatado, mediante controle tecnológico de monitoramento do ambiente lógico da FCAV ou prevenção de vazamento de dados, qualquer recebimento ou envio de conteúdo criptografado em desconformidade com esta Norma, o evento será tratado como incidente de segurança da informação e se procederá ao seguinte tratamento:

- ✓ a Área de Tecnologia da Informação solicita formalmente ao Gestor do colaborador o esclarecimento do ocorrido;
- ✓ a Área de Tecnologia da Informação copia os dados criptografados, e o colaborador deve fornecer os meios necessários para descriptografar o conteúdo, se necessário, mediante fornecimento das chaves correspondentes;
- ✓ a Área de Tecnologia da Informação ou o gestor responsável reportam formalmente o caso à Equipe de Resposta a Incidentes, para que esta apure eventuais violações e correspondentes penalidades aplicáveis.

10 RESPONSABILIDADES ESPECÍFICAS

10.1 Equipe de Resposta a Incidentes

Apurar incidentes de segurança da informação reportados pela Área de Tecnologia da Informação ou gestor responsável e aplicar, quando constatada a violação pelo usuário, as penalidades previstas nas Medidas Disciplinares da FCAV e na legislação vigente.

10.2 Área de Tecnologia da Informação

Avaliar, adquirir, implementar, administrar e fornecer aos colaboradores tecnologias e ferramentas de criptografia que garantam a proteção das informações da FCAV, nos termos desta Norma.

Analisar e monitorar os incidentes de segurança da informação, além de reportá-los, sempre que necessário, à Equipe de Resposta a Incidentes.

Elaborar e definir procedimentos de criptografia e gerenciamento de chaves, conforme descrito nesta Norma.

10.3 Gestores

Garantir e gerenciar o cumprimento, pelos seus colaboradores, desta Norma e de documentos complementares.

Reportar incidentes de segurança da informação, sempre que necessário, à Equipe de Resposta a Incidentes.

10.4 Colaboradores

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

Utilizar apenas as ferramentas de criptografia homologadas e implementadas pela Área de Tecnologia da Informação.

11 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.

12 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, via *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.

13 ANEXOS

Anexo I – Fluxos de controles criptográficos 1.12, 1.12.1 e 1.12.2.

14 NATUREZA DAS ALTERAÇÕES

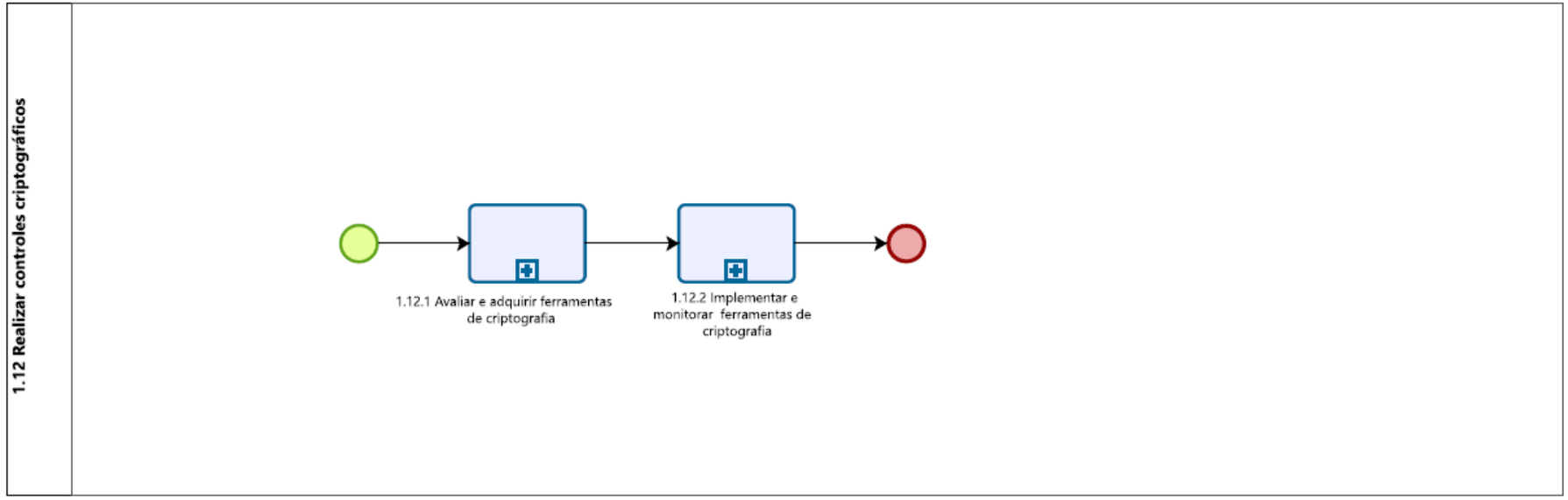
Revisão	Alterações (Inclusões ou Exclusões)	Data
00	Emissão	20/09/2022
01	No cabeçalho da versão inicial do documento, onde está “Revisão 01”, leia-se “Revisão 00”. A presente versão mantém a numeração “Revisão 01”. Inclusão dos fluxos de controles criptográficos 1.12, 1.12.1 e 1.12.2 (Anexo I) aprovados pelo Comitê de Privacidade e Proteção de Dados Pessoais. Ajustes nos textos do documento em atendimento às necessidades identificadas durante o processo de revisão.	21/08/2024

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

15 ANEXO I – FLUXOS DE CONTROLES CRIPTOGRÁFICOS

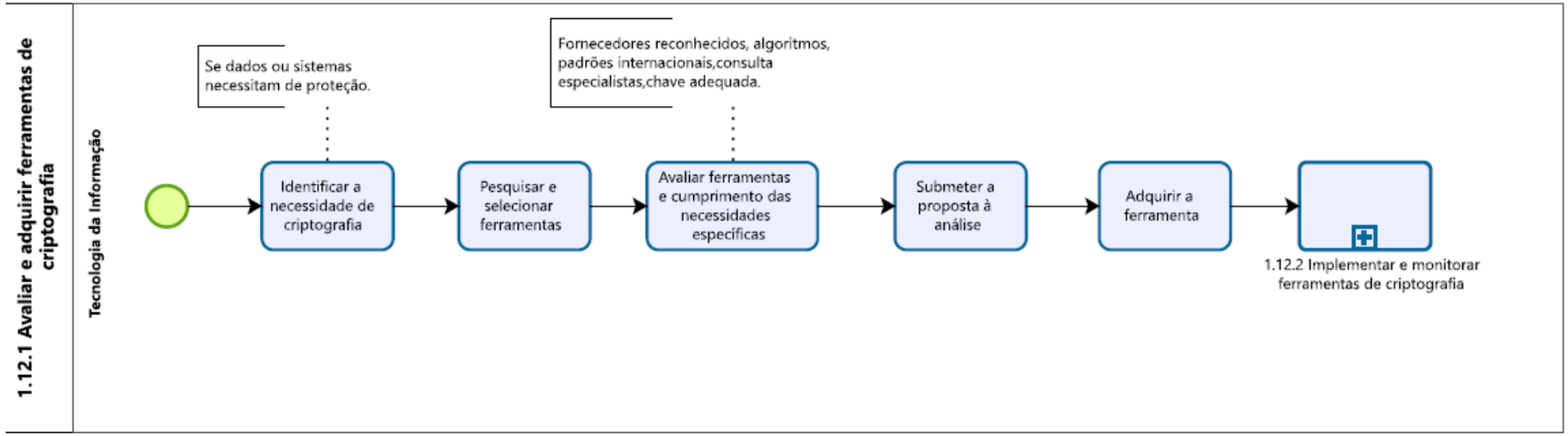
As atividades para execução deste documento estão representadas em fluxos, com objetivo de facilitar a compreensão do processo em cada etapa. Os fluxos compõem três arquivos em formato PDF, que deverão ser conhecidos de todos os envolvidos na execução deste documento.

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:** 17/07/2024	
PROCESSO: 1.12 Realizar controles criptográficos	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 21/08/2024	



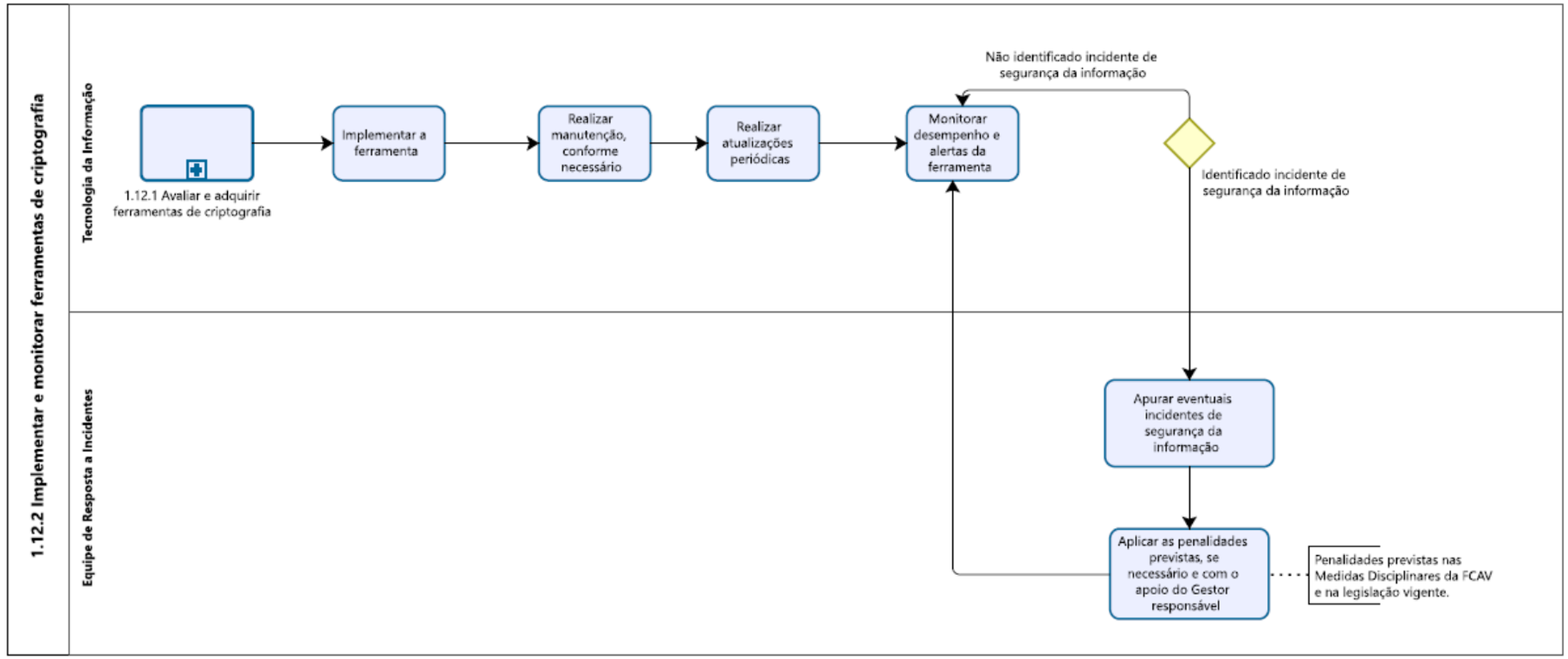
Processo 1.12 – Realizar controles criptográficos

FCAV			
MACROPROCESSO 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Validado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.12 Realizar controles criptográficos	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 17/07/2024	
SUBPROCESSO: 1.12.1 Avaliar e adquirir ferramentas de criptografia	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 21/08/2024	
OBJETIVO DO SUBPROCESSO: Avaliar e adquirir os serviços de criptografia, assegurando a conformidade legal.			



Subprocesso 1.12.1 – Avaliar e adquirir ferramentas de criptografia

FCAV			
MACROPROCESSO 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Validado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.12 Realizar controles criptográficos	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 17/07/2024	
SUBPROCESSO: 1.12.2 Implementar e monitorar ferramentas de criptografia	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 21/08/2024	
OBJETIVO DO SUBPROCESSO: Monitorar serviços de criptografia, protegendo os dados pessoais contra acessos não autorizados, a fim de garantir a integridade e segurança da informação.			



Subprocesso 1.12.2 – Implementar e monitorar ferramentas de criptografia