1 ESCOPO

Esta Norma tem por objetivo estabelecer os controles para assegurar aos incidentes de segurança de informação e potenciais incidentes sejam tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil para mitigar o impacto negativo sobre os ativos de rede e sistemas de informação (tanto físicos como lógicos) da Fundação Carlos Alberto Vanzolini (FCAV).

2 ABRANGÊNCIA

Esta Norma é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta a partir da sua publicação aos colaboradores, parceiros e fornecedores da FCAV.

3 REFERÊNCIAS

Código de Ética e Conduta;

Política de Governança de Dados Pessoais;

Política de Segurança da Informação;

Norma de Gestão de Incidentes de Violação de Dados Pessoais.

4 DEFINIÇÕES

- ✓ **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano.

- ✓ **Ativo:** qualquer coisa que tenha valor e precisa ser adequadamente protegida (material ou não).

- ✓ **Evento:** qualquer ocorrência identificada em uma rede ou sistema de informação.

  Exemplos: um usuário que vier acessar um arquivo compartilhado, um servidor que recebe uma solicitação para uma página da *Web*, um usuário que envia um e-mail ou um *firewall* que faz um bloqueio de uma tentativa de conexão, entre outros.

- ✓ **Evento adverso (ou ofensivo):** evento com consequências negativas que pode indicar uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança.

  Exemplos: falhas do sistema de informação, uso não autorizado de privilégios de sistema de informação, acesso não autorizado a dados confidenciais ou execução de *malware* que destrói dados, entre outros.

- ✓ **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.

- ✓ **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.

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

- ✓ **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, maximizar o retorno dos investimentos e de novas oportunidades de transação.

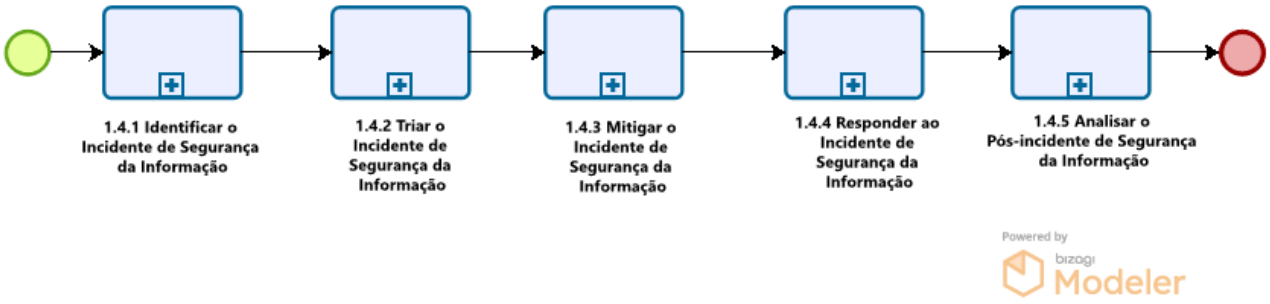
5 PREVENÇÃO

Os incidentes de segurança devem ser prevenidos pela FCAV por meio da fiscalização da conformidade frente à legislação aplicada, dos princípios éticos, bem como das regras e restrições estabelecidas pelos normativos internos.

A FCAV deve realizar o monitoramento das vulnerabilidades existentes por meio de ferramentas de supervisão de atividades, registro, monitoramento e análise de trilhas de auditoria e controle de acesso em ambientes físicos e lógicos.

6 GESTÃO DOS INCIDENTES

A gestão de incidentes de segurança da informação deve ser realizada com o auxílio do fluxo 1.4 (ANEXO I), os quais procedem com as seguintes etapas descritas nesta Norma:



Os fluxos elaborados corroboram para seguir a sequência de etapas e atividades, atores envolvidos e melhor compreensão para completar o objetivo estabelecido nesse procedimento.

7 IDENTIFICAÇÃO DO INCIDENTE

Consiste em detectar ou identificar de fato a existência de um incidente de segurança. A Equipe de resposta a incidentes baseia-se na identificação de incidentes internos ou externos, seja na detecção de alertas provenientes dos sistemas de monitoramento da rede da FCAV, denúncias ou por notificações realizadas por qualquer pessoa ou colaborador relatando ser de seu conhecimento ou mesmo se for vítima de atividade suspeita ou em desacordo com a Política de Segurança da Informação, Política de Governança de Dados Pessoais e Código de Ética e Conduta.

A FCAV deve proporcionar um Canal de Denúncia com a opção de registro anônimo para indivíduos ou colaboradores que se sintam desconfortáveis ao reportar sua denúncia de forma identificável. O responsável pelo canal de denúncia deve encaminhar, então, o registro para a Equipe de Respostas a Incidentes.

Para aqueles que optarem por se identificar, é imprescindível assegurar a confidencialidade de seus dados, abster-se de expor tais informações ou empregá-las de maneira inadequada.

As notificações internas devem ser enviadas pelos seguintes canais de comunicação:

✓ *Service Desk* por meio do e-mail suportelgpd@vanzolini.org.br;

As notificações externas devem ser enviadas pelos seguintes canais de comunicação:

✓ *Service Desk* por meio do e-mail atendimentolgpd@vanzolini.org.br;

Toda notificação ou denúncia deve ser formalmente registrada pelo *Service Desk*. Esse registro deve estar associado a alguma referência numérica (ID único) e, dessa maneira, ser gerenciado pela Equipe de Resposta a Incidentes, conforme modelo de formulário de registro de incidente de segurança da informação (ANEXO II).

8 TRIAGEM DO INCIDENTE

Etapa em que a Equipe de Resposta a Incidentes e a Área de Tecnologia da Informação deve realizar a análise inicial do evento, notificação ou denúncia visando à sua confirmação como incidente, além de classificar a sua relevância sobre as atividades da FCAV. Ainda nessa etapa deve ser identificados os sintomas do evento, suas características e os potenciais danos causados.

Confirmado que um incidente foi detectado, este deve ser analisado antes de qualquer ação ser tomada, principalmente para confirmar se é um incidente válido.

A análise realizada consiste na coleta, aquisição e análise de dados, informações e demais evidências sobre o incidente, para investigar o ativo de rede ou sistema de informação que gerou o incidente detectado ou denunciado.

Essa investigação passa pela identificação de ativos, compreendendo endereços IP, endereços MAC da interface de rede, nomes, switches e portas de acesso, bem como prédio, departamento, salas e usuários. Essas informações devem ser levantadas pelas trilhas de auditoria dos diversos sistemas e serviços disponíveis pela FCAV.

Não confirmado o incidente, a Equipe de Resposta a Incidentes deve encerrar o registro e, em seguida, informar ao responsável pela notificação.

Confirmado o incidente, a Equipe de Resposta a Incidentes deve:

- ✓ categorizar com base no impacto potencial conforme avaliação de risco em segurança da informação realizada junto à Tabela de Classificação de severidade de incidente de segurança – ANEXO III que tiver sobre a FCAV. Em casos aplicáveis, poderá ser consultado especialista externo à FCAV.

- ✓ quanto à Área de Tecnologia da Informação, em todo incidente categorizado como sendo de severidade crítica, realizar a imediata alocação dos profissionais necessários para resolução do incidente. Em casos aplicáveis, poderá ser consultado especialista externo à FCAV.

- ✓ priorizar com base no tempo e recursos necessários para recuperar ativos impactados.

Caso o incidente detectado envolva ou tenha a suspeita de envolver o tratamento não autorizado de dados pessoais, a Equipe de Resposta a Incidentes deve notificar imediatamente o Encarregado pelo Tratamento de Dados Pessoais. Este avaliará se o incidente informado trata-se de uma violação de dados pessoais.

Confirmado que o incidente é uma violação de dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais deve ser adicionado na Equipe de Resposta a Incidentes para orientar e acompanhar as medidas a serem tomadas.

Na confirmação de incidente de segurança que confirme violação de dados pessoais, deve ser acionada a Norma de Gestão de Incidentes de Violação de Dados Pessoais.

Se mais de um incidente estiver ocorrendo ao mesmo tempo, os incidentes devem ser priorizados, pois pode não haver tempo e recursos para atuar simultaneamente.

Nessa etapa, a Equipe de Resposta a Incidentes deve apresentar ainda as ações que serão priorizadas com base na categoria e no impacto do cenário encontrado, além de realizar as comunicações necessárias.

9 MITIGAÇÃO DO INCIDENTE

Essa etapa busca a solução do incidente por meio de um ciclo básico composto pelas seguintes fases:

- ✓ Análise dos dados e informações;
- ✓ Pesquisa de solução;
- ✓ Ação proposta e realizada (contenção);
- ✓ Comunicação;
- ✓ Solução efetiva ou de contorno;
- ✓ Recuperação do ambiente.

Devem ser realizados procedimentos iniciais para contenção do incidente visando a evitar a sua propagação, e posteriormente em restabelecer o ativo, mesmo que com uma solução temporária, até que a solução definitiva seja implementada.

A Equipe de Resposta a Incidentes deve assegurar às Partes Internas e às Externas Interessadas as comunicações imprescindíveis no momento oportuno. Às Partes Interessadas Internas, devem ser informadas sobre as ações que precisam ser realizadas durante o estágio de recuperação.

A Equipe de Resposta a Incidentes deve buscar a solução definitiva, ou seja, identificar a causa raiz de um incidente e eliminá-lo para garantir que o ativo esteja seguro e confiável, a fim de os procedimentos de recuperação sejam iniciados. A Equipe de Resposta a Incidentes pode solicitar o envolvimento e suporte das demais Áreas da FCAV afetadas para assegurar que os vetores do incidente sejam solucionados. Em casos aplicáveis, um especialista externo à FCAV poderá ser consultado.

A Equipe de Resposta a Incidentes deve acompanhar os processos de recuperação dos ativos até o pleno funcionamento.

Os sistemas relevantes da FCAV devem retomar a funcionalidade básica de modo prioritário. As interdependências sistêmicas também devem ser conhecidas, já que alguns sistemas apenas podem ser recuperados após outros.

Durante a recuperação, os sistemas devem ser reconstruídos, reinstalados ou restaurados pela Área de Infraestrutura de TI usando dados de *backup* e sistemas e *patches* atualizados, se necessário com apoio da Equipe de Resposta a Incidentes. Os sistemas recuperados devem ser testados e monitorados, para assegurar a não reincidência do incidente e que os ativos estejam funcionando de modo adequado.

10 RESPOSTA AO INCIDENTE

A Equipe de Resposta a Incidentes deve documentar as conclusões do tratamento do incidente, descrevendo:

- ✓ o que aconteceu;

- ✓ como o incidente foi detectado, ou seja, foi relatado por pessoal natural ou por um alerta de sistema automatizado;
- ✓ as etapas tomadas pela Equipe de Resposta a Incidentes a partir da detecção do evento até o estágio de recuperação dos ativos;
- ✓ o *status* do incidente à medida que se move ao longo do processo de solução;
- ✓ qualquer dado que seja coletado durante o processo de solução que possa ser usado como evidência;
- ✓ definir a categorização final do incidente;
- ✓ comentários e sugestões da Equipe de Resposta a Incidentes.

Essa documentação servirá como referência para pós-incidente.

A coleta e a preservação de provas, sejam digitais ou não, na etapa de solução do incidente, bem como dados e informações que possibilitaram a identificação do incidente, são muito importantes e, por isso, devem ser documentadas no registro final do incidente pela Equipe de Resposta a Incidentes, principalmente quando um incidente for categorizado como severidade crítica. Acionar a Consultoria Jurídica em caso de dúvidas quanto à sua necessidade.

A Equipe de Resposta a Incidentes deve impreterivelmente comunicar as partes interessadas sobre a conclusão do tratamento do incidente e arquivar a documentação.

11 PÓS-INCIDENTE

A etapa de pós-incidente tem o seu início após a resolução e o encerramento do incidente, e serão analisadas pela Equipe de Resposta a Incidentes as causas que motivaram a sua ocorrência, assim como identificar as medidas que podem ser tomadas com objetivo da não reincidência.

Os objetivos são melhorar os procedimentos realizados na etapa de resposta e aprimorar os ativos, com o propósito de protegê-los de futuros incidentes.

A Equipe de Resposta a Incidentes deve comunicar as partes interessadas do resultado da análise.

Os incidentes ocorridos devem ser analisados visando identificar e aprimorar os indicadores de probabilidade e a consequência dos incidentes previstos e as ocorrências reais de incidentes.

Com base no relatório e nas informações obtidas durante a solução do incidente, a Equipe de Resposta a Incidentes deve:

- ✓ elaborar um plano de ação a ser categorizado como curto, médio ou longo prazo, incluindo nomes dos responsáveis, datas de vencimento e entregas. Dessa forma, garantir a todas as partes interessadas a ciência do que se espera delas;
- ✓ monitorar a implementação de todas as ações.

Observação: o gestor da Área na qual ocorreu o incidente deverá rever a sua Planilha de Riscos e Oportunidades, conforme Procedimento de Levantamento de Riscos e Oportunidades da Fundação Vanzolini.

12 ACORDOS DE NÍVEIS DE SERVIÇOS (SLA)

De acordo com a severidade do incidente de segurança da informação, o mesmo terá um prazo para o seu tratamento.

CLASSIFICAÇÃO	PRAZO PARA TRATAMENTO
CRÍTICA	Até 8 horas
ALTA	Um dia útil
MÉDIA	Três dias úteis
BAIXA	Cinco dias úteis

13 DAS RESPONSABILIDADES ESPECÍFICAS

13.1 Diretoria Executiva

Assegurar que os recursos necessários sejam alocados à execução da gestão dos incidentes ocorridos.

13.2 Encarregado pelo Tratamento de Dados Pessoais

Analisar as notificações de incidentes de segurança da informação que possivelmente envolvam o tratamento não autorizado de dados pessoais e dados pessoais sensíveis;

Liderar as salas de crise no caso de incidentes quem envolvam o tratamento não autorizado de dados pessoais;

Iniciar processo de gestão de incidentes envolvendo a violação de dados pessoais.

13.3 Tecnologia de Informação

Monitorar continuamente o ambiente tecnológico do ponto de vista de segurança da informação, visando identificar eventos que possam causar impacto na disponibilidade, integridade e confidencialidade dos sistemas críticos e dos dados sensíveis da FCAV;

Informar a Equipe de Respostas à Incidentes assim que tiver conhecimento sobre suspeitas ou um incidente de segurança da informação constatada;

Auxiliar na análise dos incidentes de segurança por meio da apresentação das trilhas de auditoria dos sistemas sob sua gestão;

Realizar a alocação dos profissionais necessários para resolução do incidente;

Realizar as medidas de segurança e técnicas necessárias para contenção/recuperação do incidente;

Auxiliar nos processos de investigação do incidente.

13.4 Equipe de Resposta à Incidentes

Monitorar e apoiar todas as fases descritas neste documento desde a Identificação até a solução;

Auxiliar nos processos de investigação do incidente;

Apoiar com as medidas de segurança, técnicas e administrativas necessárias para contenção/recuperação do incidente;

Caso o tratamento do incidente revele impactos no ambiente de produção, a equipe de resposta a incidentes deve cuidar de notificar os gestores e usuários do recurso em questão sobre o ocorrido;

Verificar se todas as ações e notificações planejadas foram realizadas.

13.5 Consultoria Jurídica

Se o incidente tiver consequências legais, deve ser estabelecido um contato com os órgãos responsáveis pela apuração e aplicação de penalidades (Agências Reguladoras e/ou Delegacias entre outros, se for o caso), para relato dos fatos e a apresentação de indícios relativos ao incidente.

13.6 Recursos Humanos

Para os incidentes de segurança da informação que envolva desvio de conduta do colaborador ou algo em desacordo com o Código de Ética e Conduta, o caso será encaminhado para área de recursos humanos, bem como, quando for o caso, para o Gestor responsável pelas atividades desenvolvidas por terceiros e, assim, aprofundarem-se melhor na investigação.

13.7 Comunicação e Marketing

Tomar as necessárias providências, em consonância com as diretrizes da Diretoria Executiva da FCAV, no caso de incidentes que tiverem desdobramentos para fora da FCAV, e que envolvam a imprensa ou comunidade externa.

13.8 Gestores

Gerenciar, além de garantir o cumprimento desta Norma e demais documentos complementares pelos seus colaboradores;

Avaliar a necessidade de atualização da Planilha de Riscos e Oportunidades para casos de incidentes de segurança da informação ocorridos em sua área, de acordo com o Procedimento de levantamento de riscos e oportunidades.

13.9 Colaboradores

Cumprir, estar ciente e manter-se atualizado com esta Norma e os documentos complementares.

14 PENALIDADES

Qualquer atividade que desrespeite as disposições estabelecidas nesta Norma, ou ainda em quaisquer dos documentos complementares da FCAV, deve ser considerada como uma violação e tratada pela FCAV a fim de apurar as responsabilidades dos envolvidos de acordo com as “Medidas Disciplinares” da FCAV visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

A tentativa de burlar as diretrizes e os controles estabelecidos, se constatada, deve ser tratada como uma violação.

15 DAS 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 Normativo 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 e os demais documentos que a complementam encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas 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.

16 ANEXOS

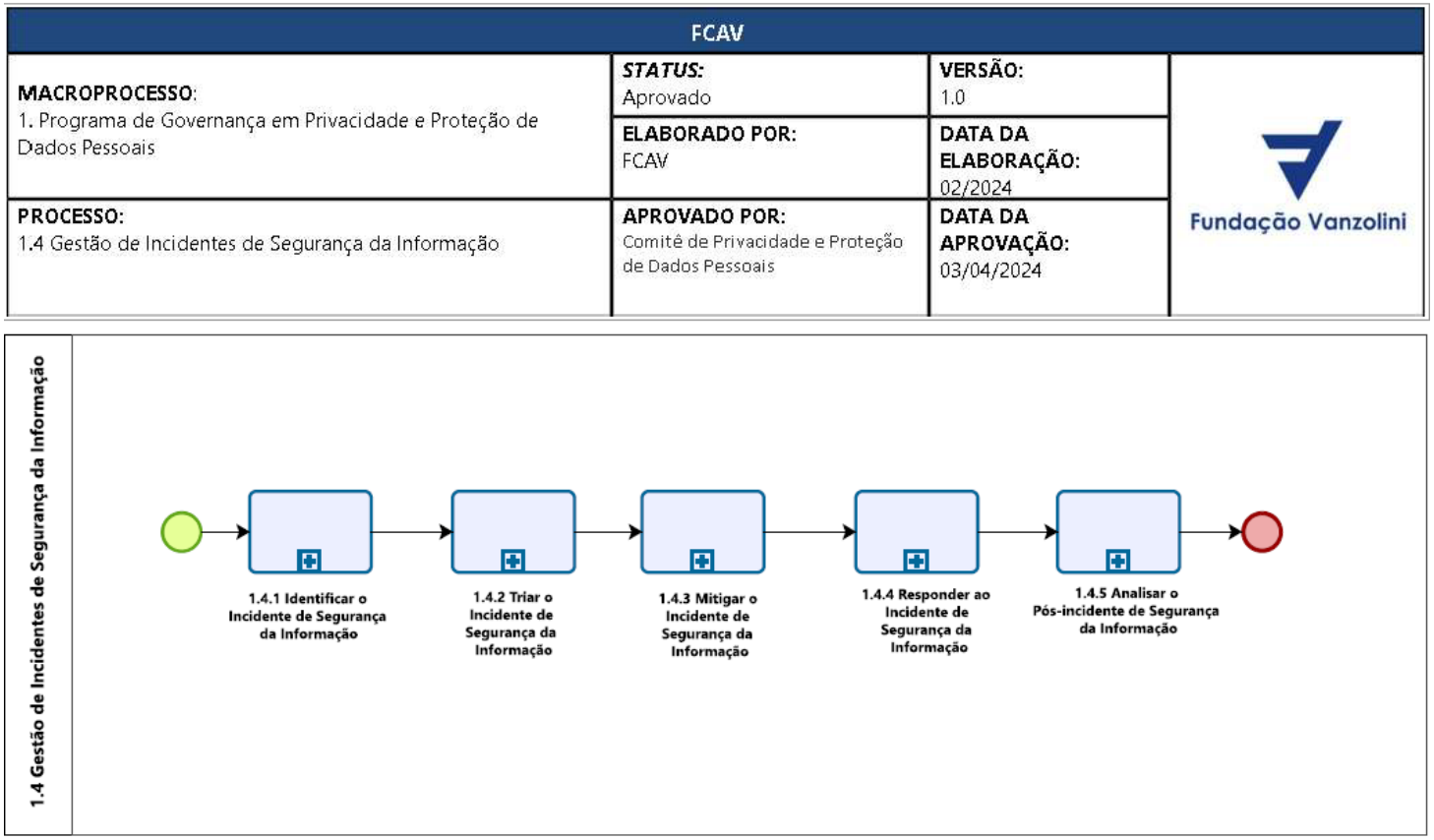
Anexo I – Fluxos Gestão de Incidentes de Segurança da Informação 1.4, 1.4.1, 1.4.2, 1.4.3, 1.4.4 e 1.4.5
Anexo II – Formulário de Registro de Incidente de Segurança da Informação
Anexo III – Tabela de Classificação de Severidade de Incidente

17 NATUREZA DAS ALTERAÇÕES

Revisão	Alterações (Inclusões ou Exclusões)	Data
00	Emissão Inicial	19/10/2022
01	Inclusão fluxos de Gestão de Incidentes de Segurança da Informação 1.4, 1.4.1, 1.4.2, 1.4.3, 1.4.4 e 1.4.5 (ANEXO I) aprovado pelo Comitê de Privacidade e Proteção de Dados Pessoais; ajustes nos textos da Norma atendendo às necessidades identificadas durante a revisão e renumeração dos anexos.	29/04/2024
Revisão	**Aprovação Diretoria Executiva**	**Data**
00	Emissão Inicial	09/11/2022
01	Versão 01	13/06/2024

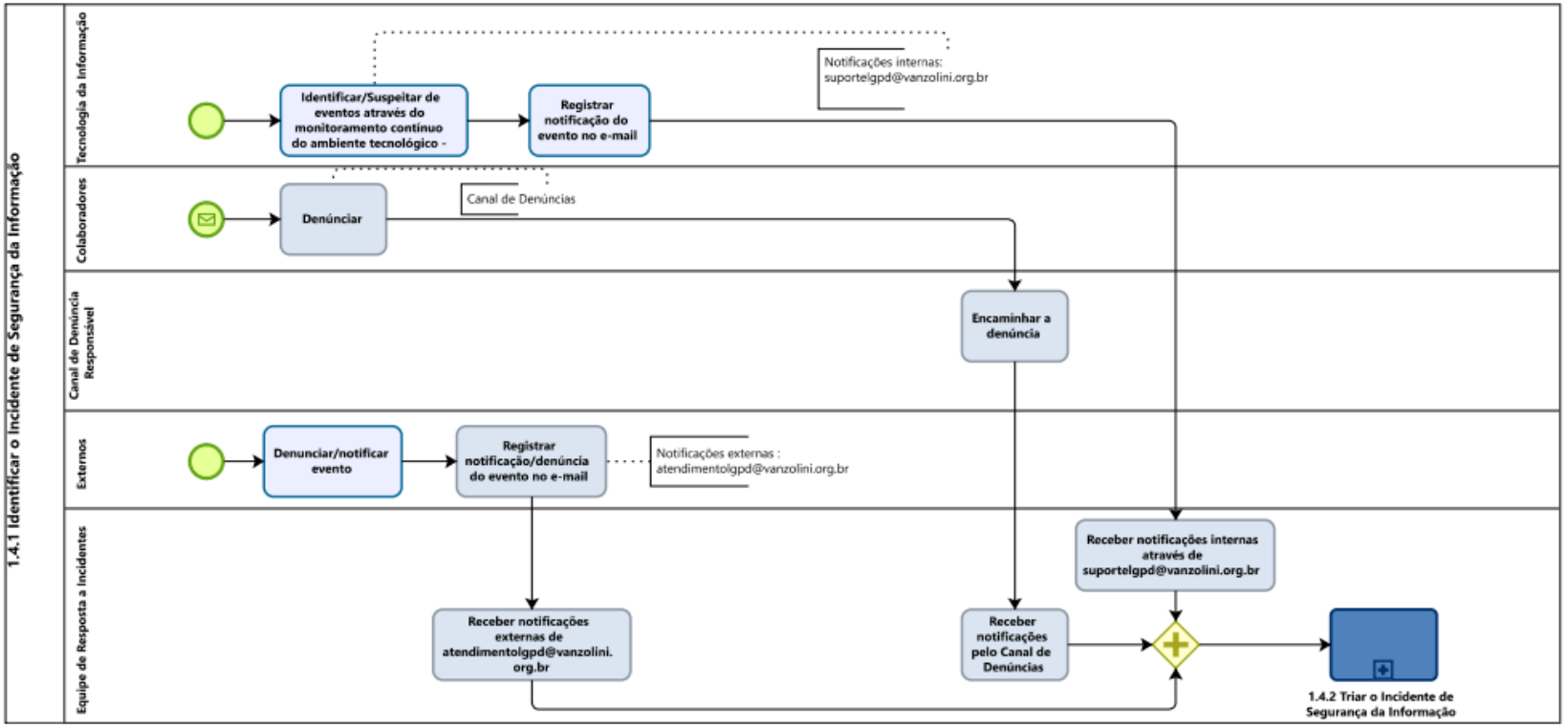
18 ANEXO I – FLUXOS GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

As atividades representadas nos fluxos, para execução desta Norma de Gestão de Incidentes de Segurança da informação, têm por objetivo facilitar a compreensão do processo em cada etapa. Composto por seis arquivos em formato PDF, denominados processo e subprocessos 1.4, 1.4.1, 1.4.2, 1.4.3, 1.1.4 e 1.4.5, respectivamente, que deverão ser seguidos pelos responsáveis pela sua execução.



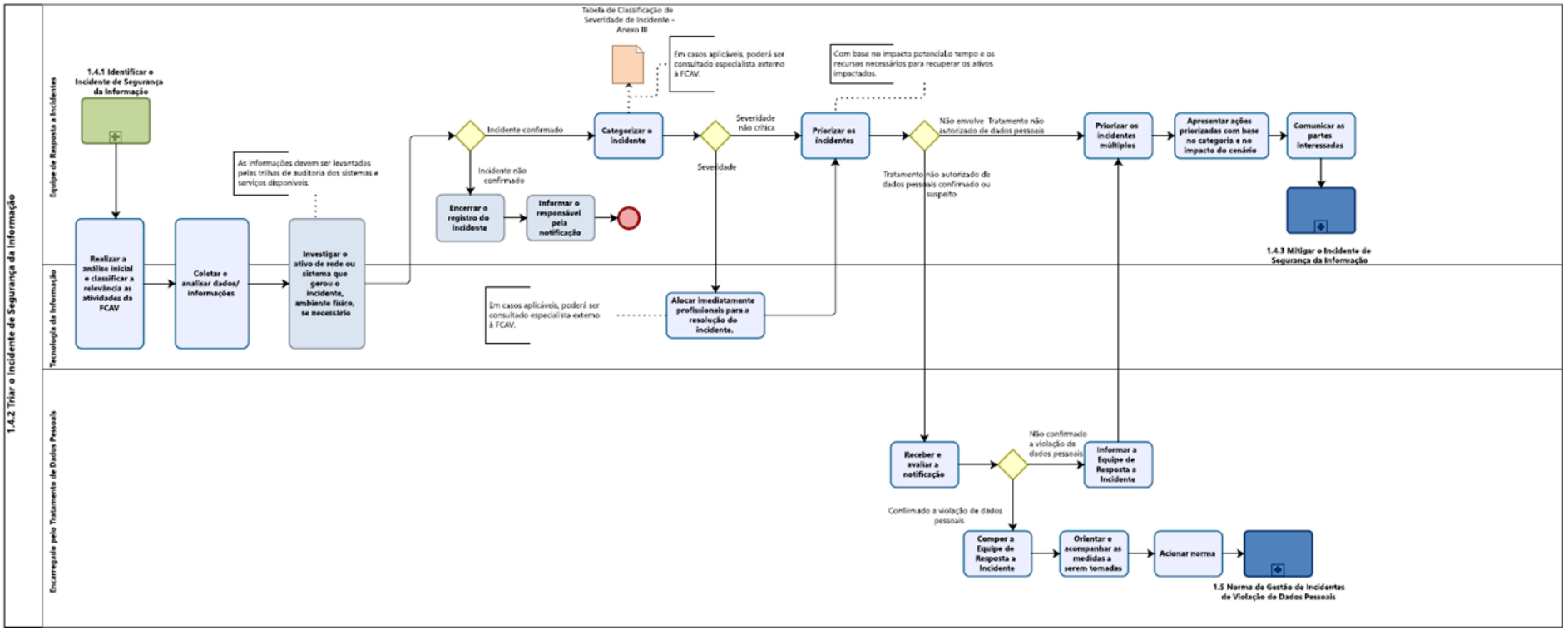
1.4 – Gestão de Incidentes de Segurança da Informação

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Aprovado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.4. Gestão de Incidentes de Segurança da Informação	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 02/2024	
SUBPROCESSO: 1.4.1 Identificar o Incidente de Segurança da Informação	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 03/04/2024	
OBJETIVO DO SUBPROCESSO: Detectar e registrar os incidentes de segurança, garantindo que todas as notificações sejam tratadas de forma apropriada e registradas para análise e resposta adequadas pela equipe responsável.			



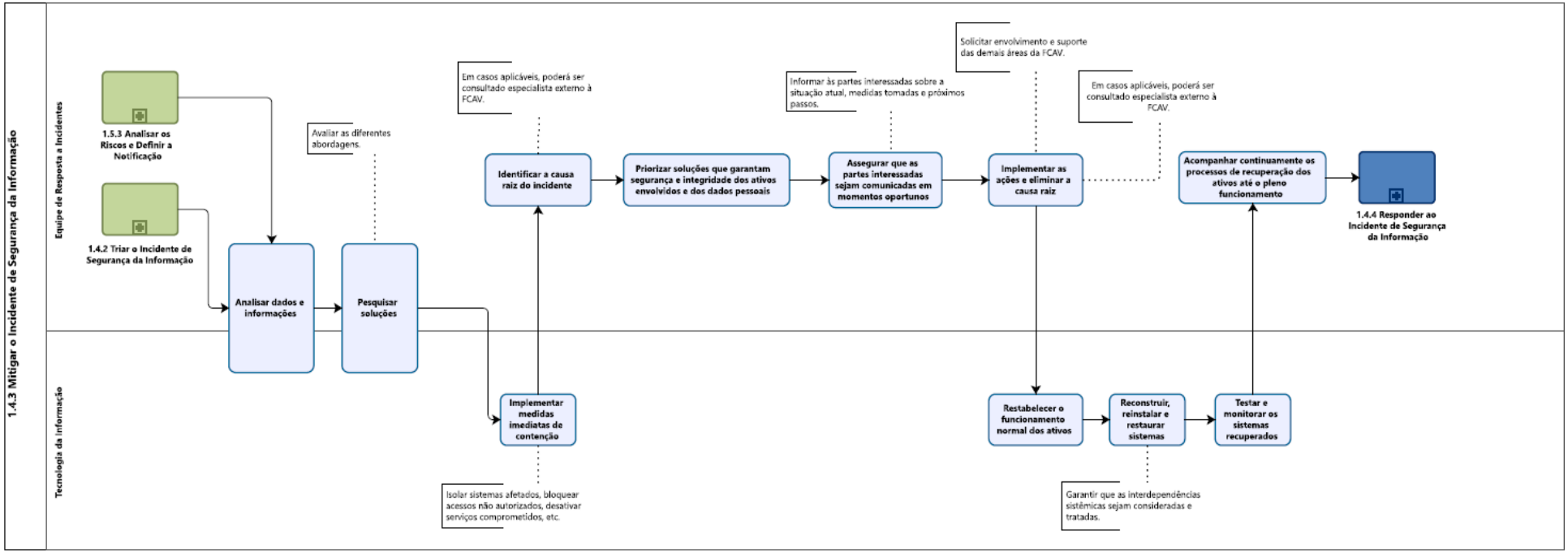
1.4.1 – Identificar o Incidente de Segurança da Informação

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Aprovado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.4 Gestão de Incidentes de Segurança da Informação	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 02/2024	
SUBPROCESSO: 1.4.2 Triar o Incidente de Segurança da Informação	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados	**DATA DA APROVAÇÃO:** 03/04/2024	
OBJETIVO DO SUBPROCESSO: Delinear o processo de resposta a incidentes de segurança da informação na FCAV, desde a detecção inicial até a comunicação das ações.			



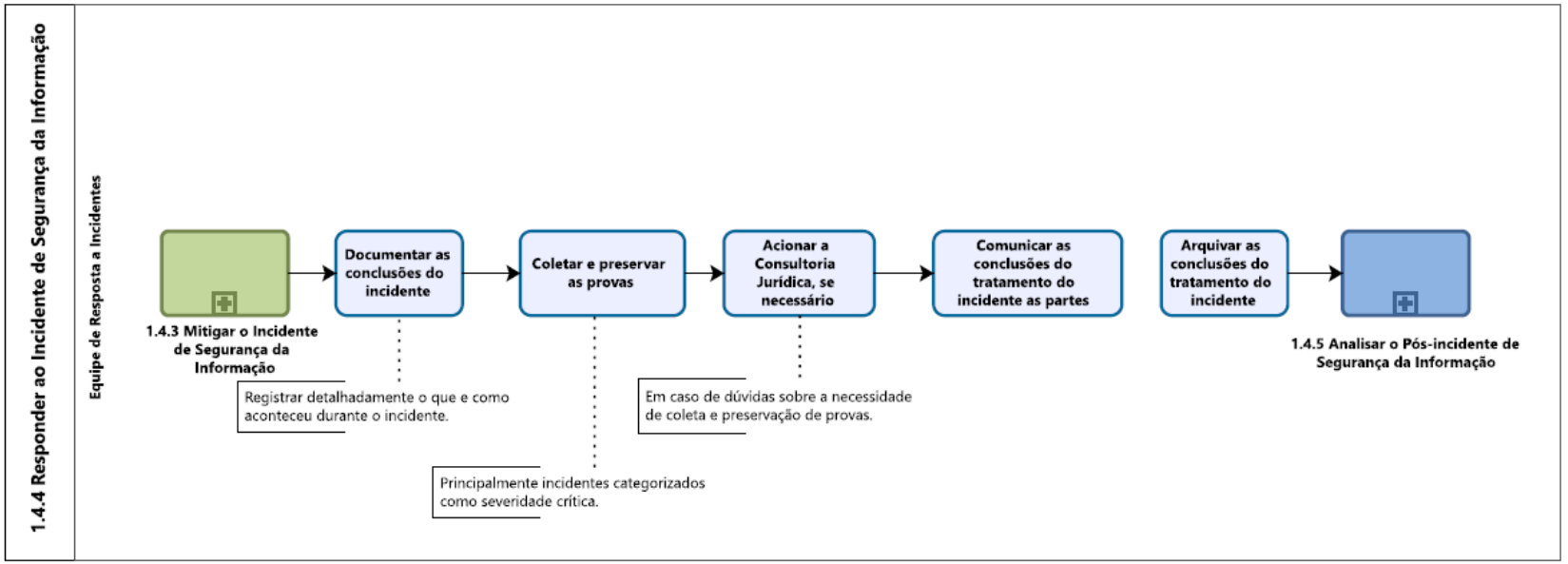
1.4.2 – Triar o Incidente de Segurança da Informação

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Aprovado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.4 Gestão de Incidentes de Segurança da Informação	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 02/2024	
SUBPROCESSO: 1.4.3 Mitigar o Incidente de Segurança da Informação	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados	**DATA DA APROVAÇÃO:** 03/04/2024	
OBJETIVO DO SUBPROCESSO: Garantir desde a análise inicial até a recuperação completa do ambiente afetado			



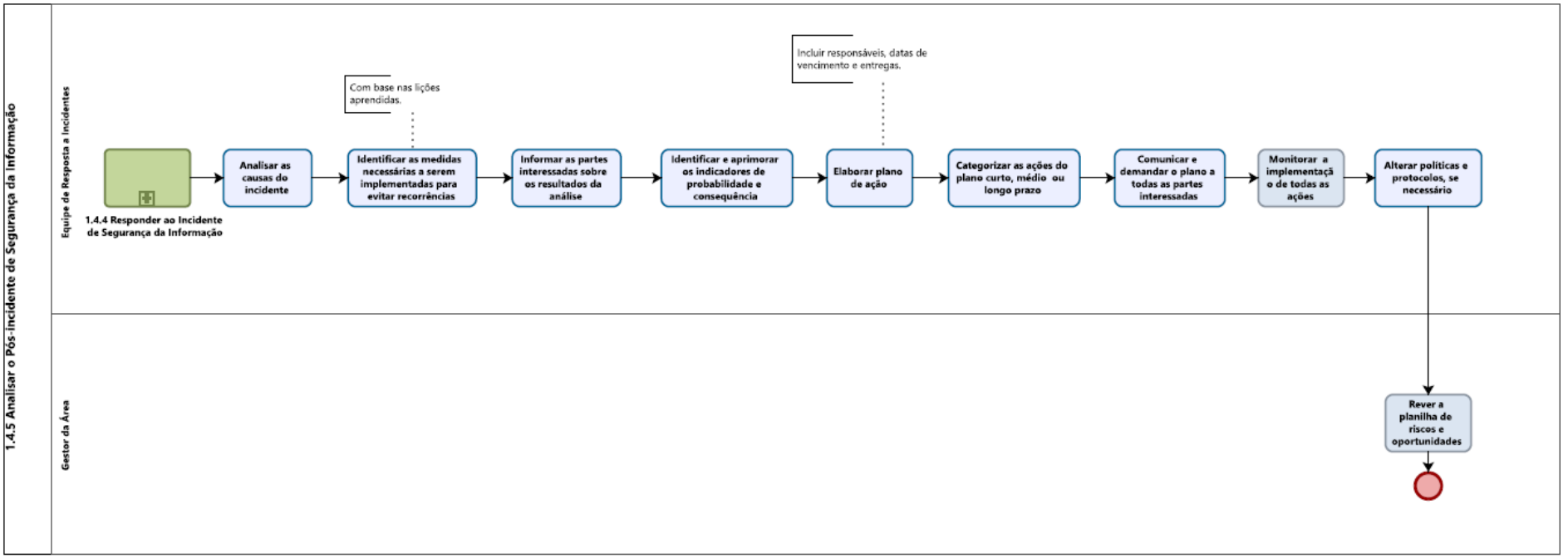
1.4.3 – Mitigar o Incidente de Segurança da Informação

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Aprovado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.4 Gestão de Incidentes de Segurança da Informação	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 02/2024	
SUBPROCESSO: 1.4.4 Responder ao Incidente de Segurança da Informação	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados	**DATA DA APROVAÇÃO:** 03/04/2024	
OBJETIVO DO SUBPROCESSO: Garantir que o tratamento de incidentes seja bem documentado, análise pós-incidente eficaz e aprimoramento contínuo do processo de resposta a incidentes.			



1.4.4 – Responder ao Incidente de Segurança da Informação

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Aprovado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.4 Gestão de Incidentes de Segurança da Informação	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 02/2024	
SUBPROCESSO: 1.4.5 Analisar o Pós-incidente de Segurança da Informação	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados	**DATA DA APROVAÇÃO:** 03/04/2024	
OBJETIVO DO SUBPROCESSO: Melhorar os procedimentos realizados na etapa de resposta e aprimorar os ativos para protegê-los de futuros incidentes.			



1.4.5 – Analisar o Pós-incidente de Segurança da Informação

19 ANEXO II – FORMULÁRIO DE REGISTRO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Formulário de Registro do Incidente de Segurança da Informação			
Código de Registro	**Data**	**Classificação da Criticidade**	**Localidade**
XXX			

Reportado por:	
Atendido por:	
Área em que ocorreu incidente:	
Telefone/*E-mail*:	

Identifique a natureza do incidente:	
☐ Perda de serviços ou de ativos	☐ Observação ou suspeitas de fragilidade em sistemas ou serviços
☐ Uso indevido de Identidade Digital	☐ Acesso ou uso indevido quanto à informação ou Recurso de TIC
☐ Violação ou tentativa de burlar aos normativos	☐ Outros (Descrever)

Tempo de Resposta:	**Esperado:**	**Real:**

1. Descrição do Incidente:
2. Como foi detectado o Incidente:
3. Dia e Hora em que o Incidente ocorreu:
4. Ativos que foram afetados (sistemas, computadores e áreas físicas):
5. Impactos do Incidente:

6. Outras informações relevantes:
7. Equipe de Resposta:
8. Providências Cabíveis para a Investigação:
9. Plano de Comunicação:
10. Áreas envolvidas na Investigação do Incidente:
11. Resultado da Investigação:
12. Deliberação do Comitê de segurança da informação para as ações de contorno e solução do Incidente:
13. Resultado:
"Este documento foi classificado pela Área de Tecnologia da Informação com o acesso restrito aos Colaboradores da Equipe de Resposta à Incidentes, à Área de Tecnologia da Informação e ao Comitê de Gestão de Segurança da Informação"

20 ANEXO III – TABELA DE CLASSIFICAÇÃO DE SEVERIDADE DE INCIDENTE

Classificação de Incidente de Segurança							
SEVERIDADE	**LEGALIDADE**	**CONFIDENCIALIDADE**	**INTEGRIDADE**	**DISPONIBILIDADE**	**REPUTACIONAL**	**FINANCEIRO**	**SLA**
CRÍTICA	Falta legal de alto impacto que pode resultar em processo e multas altas. Não atendimento a dispositivos legais. Possibilidade de litígio de grande impacto. Ocorrência de descumprimento contratual com terceiros e clientes.	Em caso de um incidente que afete sistemas ou serviços considerados como relevantes pela FCAV, há consequências para vários processos de negócios internos e/ou externos, sendo estes não previsíveis e de difícil gerenciamento. Possibilidade de exploração de vulnerabilidades (por eventuais ataques e má-fé, decorrentes do uso de informações tornadas públicas devido à incidente de segurança.	Em caso de um incidente de segurança que afete sistemas ou serviços considerados como relevantes pela FCAV, há consequências para um ou mais processos de negócios internos e/ou externos, parcialmente previsíveis e de difícil gerenciamento. Possibilidade de tomada de decisão errônea por parte da FCAV devido à falta de integridade de informações afetadas por incidente de segurança.	Em caso de um incidente de segurança que afete sistemas ou serviços considerados como relevantes pela FCAV, há consequência para um ou mais processos de negócios internos e/ou externos, parcialmente previsíveis e de difícil gerenciamento. Paralisação das atividades de uma unidade de negócio da FCAV ou de várias Áreas. Descontentamento dos colaboradores e clientes. (> 50 %).	Alta preocupação de todas as Partes interessadas e envolvidas nos processos (sistêmico). Cobertura negativa da mídia. Dano à imagem da FCAV junto ao público interno e externo.	Prejuízo financeiro acima de 50 MM.	**de 0 a 8 horas**

Classificação de Incidente de Segurança							
SEVERIDADE	**LEGALIDADE**	**CONFIDENCIALIDADE**	**INTEGRIDADE**	**DISPONIBILIDADE**	**REPUTACIONAL**	**FINANCEIRO**	**SLA**
ALTA	Falta legal de alto impacto que pode resultar em processo e multas altas. Não atendimento a dispositivos legais. Possibilidade de litígio de alto impacto. Ocorrência de descumprimento contratual com terceiros e clientes.	Em caso de um incidente de segurança que afete sistemas ou serviços pela FCAV, há consequências para vários processos de negócios internos e/ou externos, não previsíveis e de difícil gerenciamento. Possibilidade de exploração de vulnerabilidades (por eventuais ataques e má-fé) decorrentes do uso de informações tornadas públicas devido ao incidente de segurança.	Em caso de um incidente de segurança que afete sistemas ou serviços pela FCAV, há consequências para um ou mais processos de negócios internos e/ou externos, parcialmente previsíveis e de difícil gerenciamento. Possibilidade de tomada de decisão errônea por parte da FCAV devido à falta de integridade de informações afetadas por incidente de segurança.	Em caso de um incidente de segurança que afete sistemas ou serviços pela FCAV, há consequências para um ou mais processos de negócios internos e/ou externos, parcialmente previsíveis e de difícil gerenciamento. Paralisação das atividades de uma unidade de negócio da FCAV ou de várias Áreas. Descontentamento dos colaboradores e clientes (> 50 %).	Alta preocupação de todas as Partes interessadas e envolvidas nos processos (sistêmico). Cobertura negativa da mídia. Dano à imagem da FCAV junto ao público interno e externo.	Prejuízo financeiro entre 20 MM e 50 MM	Um dia útil

Classificação de Incidente de Segurança							
SEVERIDADE	**LEGALIDADE**	**CONFIDENCIALIDADE**	**INTEGRIDADE**	**DISPONIBILIDADE**	**REPUTACIONAL**	**FINANCEIRO**	**SLA**
MÉDIA	Falta legal de alto impacto que pode resultar em processo e multas altas. Falta Legal com procedimentos de investigação de incidentes e/ou ilícitos.	Em caso de um incidente de segurança que afete sistemas ou serviços pela FCAV, há consequências para um ou mais processos de negócios internos e/ou externos, parcialmente previsíveis e gerenciáveis.	Em caso de um incidente de segurança que afete sistemas ou serviços pela FCAV, há consequências para um ou mais processos de negócios internos e/ou externos, parcialmente previsíveis e gerenciáveis.	Em caso de um incidente de segurança que afete sistemas ou serviços pela FCAV, há consequências para um ou mais processos de negócio internos e/ou externos, parcialmente previsíveis e gerenciáveis. Paralisação das atividades de uma unidade de negócio da FCAV. Descontentamento dos colaboradores e clientes (> 25 %).	Preocupação de todas as Partes interessadas e envolvidas nos processos (sistêmico).	Prejuízo financeiro entre 10 MM e 20 MM	Três dias úteis

Classificação de Incidente de Segurança							
SEVERIDADE	**LEGALIDADE**	**CONFIDENCIALIDADE**	**INTEGRIDADE**	**DISPONIBILIDADE**	**REPUTACIONAL**	**FINANCEIRO**	**SLA**
BAIXA	Falta legal de baixo impacto que pode resultar em processo e multas baixas.	Em caso de um incidente de segurança que afete sistemas ou serviços pela FCAV, há consequências para um ou mais processos de negócios internos e/ou externos, previsíveis e facilmente gerenciáveis.	Em caso de um incidente de segurança que afete sistemas ou serviços pela FCAV, há consequências para um ou mais processos de negócios internos e/ou externos, previsíveis e facilmente gerenciáveis.	Em caso de um incidente de segurança que afete sistemas ou serviços pela FCAV, há consequências para um ou mais processos de negócios internos e/ou externos, previsíveis e facilmente gerenciáveis. Paralisação das atividades de um pequeno grupo de usuários. Descontentamento dos colaboradores e clientes (> 25 %).	Baixa preocupação das partes envolvidas responsáveis pelo processo.	Prejuízo financeiro entre 1 MM e 10 MM	Cinco dias úteis