1 ESCOPO

Esta Norma tem o objetivo estabelecer as regras e as restrições relativas à gestão dos Incidentes de Violação de Dados da Fundação Carlos Alberto Vanzolini (FCAV) e mitigar os riscos ao negócio e aos ativos da instituição.

2 ABRANGÊNCIA

Esta Norma é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta a partir da sua publicação a 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 Segurança da Informação;

Procedimento de Avaliação da Proteção de Dados em Terceiros.

4 DEFINIÇÕES

- ✓ **Agente de Tratamento:** controlador e operador.
- ✓ **Ameaça:** risco ou potencial perigo de um incidente, que pode resultar em danos à FCAV.
- ✓ **ANPD ou autoridade nacional de proteção de dados:** órgão da administração pública indireta responsável por implementar e fiscalizar o cumprimento da lei geral de proteção de dados pessoais aplicável, além de zelar por isso.
- ✓ **Ativo:** qualquer coisa que tenha valor e precisa ser adequadamente protegida.
- ✓ **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.
- ✓ **Controlador:** pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- ✓ **Dado pessoal:** informação relacionada à pessoa física identificada ou identificável.

- ✓ **Dado pessoal sensível:** dado pessoal sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa física.

- ✓ **Encarregado pelo tratamento de dados pessoais:** pessoa física ou jurídica indicada pela FCAV e que atua como canal de comunicação entre a FCAV com os titulares dos dados pessoais ou a ANPD.

- ✓ **Evento adverso (ou ofensivo):** evento com consequências negativas. 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.

- ✓ **Evento:** ocorrência ou mudança de um determinado conjunto de circunstâncias. Pode ser visível em uma rede ou sistema de informação. Exemplos: um usuário que acessa 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.

- ✓ **Incidente de Segurança com Dados Pessoais:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do Titular dos dados pessoais.

- ✓ **Incidente de Segurança da Informação:** ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à Política de Segurança da Informação ou 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.

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

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

- ✓ **Sistema de informação:** conjunto de aplicativos, serviços, ativos de tecnologia da informação ou outros componentes de manipulação de informações.

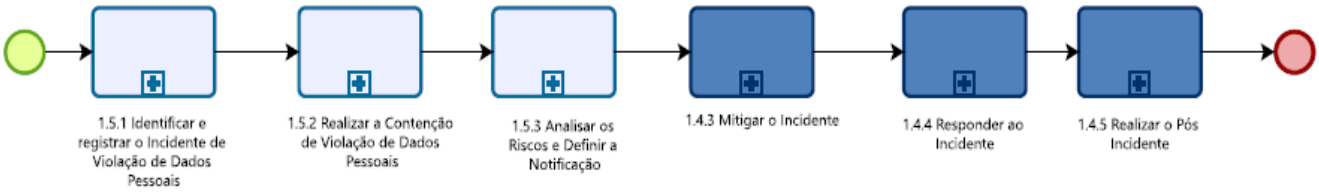
- ✓ **Tentativa de Burla:** tentativa de burlar as diretrizes e os controles estabelecidos, se constatada, deve ser tratada como uma violação.

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

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

5 GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

A gestão de incidentes de violação de dados pessoais deve ser realizada com o auxílio do fluxo 1.5 (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 nesta Norma.

6 IDENTIFICAÇÃO E REGISTRO DO INCIDENTE

Todos os colaboradores da FCAV devem se manter vigilantes diante de qualquer ocorrência que envolva uma violação de dados pessoais. Se identificada, reportá-la aos gestores imediatos.

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 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.

Incidentes ocorridos por ação ou omissão de agentes de tratamento que realizam tratamento em nome da FCAV (Instituições Terceiras/Operadores) deve ter "Formulário de Incidente de Violação de Dados" (ANEXO II) preenchido pelo próprio agente de tratamento e reportados à Equipe de Respostas a Incidentes no prazo de 24 horas por meio do *e-mail* atendimentolgpd@vanzolini.com.br.

A FCAV deve exigir a notificação imediata a ela de uma eventual violação de dados pessoais em todos os contratos com fornecedores que realizam tratamento de dados como operadores.

A Equipe de Tecnologia da Informação deve monitorar continuamente o ambiente tecnológico do ponto de vista de segurança da informação, visando identificar eventos que possam causar impactos na disponibilidade, integridade e confidencialidade de dados pessoais que sejam tratados pela FCAV. A Equipe de Resposta a Incidentes deverá receber a denúncia ou suspeita ou o "Formulário de Incidente de Violação de Dados" (ANEXO II) e enviá-la para o Encarregado pelo Tratamento de Dados Pessoais. Em conjunto, devem avaliar se a ocorrência realmente configura um incidente de violação de dados pessoais.

Caso os dados pessoais envolvidos no incidente estiverem anonimizados, deverá ser seguido o processo normal de gestão de incidentes de segurança da informação, e não mais tratado o caso em questão como 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 acompanhar as medidas a serem tomadas, dando a devida orientação.

O gestor responsável pela área/recurso do qual foi originado o incidente de violação deve ser notificado imediatamente quando identificado o incidente de violação de dados, a fim de fornecer o levantamento de informações e, ainda, preencher o "Formulário de Incidente de Violação de Dados" (ANEXO II).

A Equipe de Respostas a Incidentes deve:

- ✓ avaliar o tipo e o nível de risco criado pela violação e tomar as medidas necessárias para garantir que o incidente seja registrado pela FCAV;
- ✓ Determinar a possível existência de um risco para os direitos e liberdades dos titulares dos dados. Os riscos a direitos e liberdades incluem, entre outros, perda de controle ou confidencialidade dos Dados Pessoais, reversão não autorizada de pseudonimização, danos à reputação, discriminação, roubo ou fraude de identidade, perda financeira e outras desvantagens econômicas ou sociais;
- ✓ Avaliar se a probabilidade e a gravidade dos riscos potenciais criam um risco alto. Essa avaliação deve envolver:
    - uma análise do tipo de violação;
    - a natureza;
    - a categoria de dados pessoais;
    - a sensibilidade e volume de dados pessoais afetados;
    - a gravidade das possíveis consequências para os titulares dos dados;
    - o número e as características dos titulares de dados afetados;
    - as características do destinatário dos dados pessoais e a facilidade de identificação dos titulares dos dados.

Consideram-se riscos elevados o tratamento que se utiliza de novas tecnologias ou métodos de tratamento em que nenhuma avaliação de impacto na proteção de dados foi realizada antes da violação pelo controlador, ou quando uma avaliação de impacto nos dados se tornou necessária à luz do tempo decorrido desde o tratamento inicial aplicado.

O risco deve ser avaliado com base em critérios objetivos, entretanto o resultado será subjetivo.

A Equipe de Respostas a Incidentes informará o Comitê de Privacidade e Proteção de Dados Pessoais sobre a violação dos dados, e o Encarregado pelo Tratamento de Dados Pessoais realizará, com apoio da Consultoria Jurídica, a notificação para a ANPD e aos Titulares dos Dados Pessoais, conforme necessário, com base no nível de risco.

7 CONTENÇÃO DO INCIDENTE

A Equipe de Respostas a Incidentes deverá orientar os gestores e as áreas responsáveis e afetadas pela violação de dados quanto às medidas corretivas a serem tomadas.

O Gestor da Área originária do incidente de violação de dados deve tentar, com sua equipe, recuperar qualquer dado que tenha sido comprometido de forma a mitigar o risco ao máximo possível, com o apoio do Encarregado pelo Tratamento de Dados Pessoais, da Área de Tecnologia da Informação e Equipe de Respostas a Incidentes.

A Área de Tecnologia da Informação deverá apoiar com as medidas técnicas necessárias para contenção/recuperação do incidente, a exemplo de efetuar coleta de evidências de forma legal ou isolar recursos de tecnologia de modo a não perder informações do incidente.

A Equipe de Respostas a Incidentes deverá estabelecer quem precisa ser informado internamente acerca da violação de dados, e quais ações devem ser tomadas por quem foi informado.

8 ANÁLISE DE RISCOS

De forma a analisar os riscos envolvidos no incidente de violação de dados, deverá ser feita uma análise conduzida pelo gestor da área originária do referido incidente de violação de dados (com apoio da Equipe de Respostas a Incidentes), considerando as seguintes informações:

- ✓ Que tipo de dados pessoais estão envolvidos?
- ✓ Há dados de crianças e adolescentes nessa violação?
- ✓ Há dados pessoais sensíveis nessa violação?
- ✓ Quais medidas de segurança são aplicáveis à área ou ao recurso originário do incidente?
- ✓ Quantos indivíduos foram afetados pela violação?
- ✓ Em caso de compartilhamento indevido, quais informações um terceiro pode extrair da informação a qual teve acesso?
- ✓ Foi possível identificar todos os envolvidos na violação de dados ocorrida?
- ✓ Há informações de cadastro ou contato de todos os envolvidos na violação de dados ocorrida?
- ✓ A violação de dados ocorrida afeta algum direito do titular de dados pessoais garantido por legislação de proteção de dados nos territórios onde ocorreu a violação?

9 NOTIFICAÇÃO AO CONTROLADOR

Se os dados pessoais envolvidos no incidente estiverem sendo tratados pela FCAV, na qualidade de operador, o controlador dos dados deverá ser notificado sem demora injustificada pelo Encarregado pela Proteção de Dados da FCAV, conforme Anexo III – Notificação ao Controlador – FCAV na condição de operador, devendo a FCAV cooperar com as informações necessárias, bem como com as autoridades fiscalizadoras, para a mais breve apuração, esclarecimento e solução do caso com total transparência.

10 DECISÃO DE NÃO NOTIFICAÇÃO

A FCAV deverá avaliar internamente, com sua Equipe de Respostas a Incidentes, a relevância do risco ou dano do incidente de segurança para determinar se deverá comunicar à ANPD e ao Titular. Para tanto, é recomendável que a FCAV responda internamente às seguintes perguntas:

✓ Ocorreu um incidente de segurança relacionado a dados pessoais?

- Se a resposta for positiva, siga para a próxima pergunta;
- Se a resposta for negativa, não é necessário comunicar a ANPD se não houve incidente de segurança relacionado a dados pessoais.

✓ Existe um risco ou dano relevante aos direitos e liberdades individuais dos Titulares afetados em razão do incidente de segurança?

- Se a resposta for positiva, com o apoio da Consultoria Jurídica, a ANPD e o Titular devem ser comunicados;
- Se a resposta for negativa, a comunicação à ANPD não será necessária, caso o responsável pelo tratamento puder demonstrar, de forma irrefutável, que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e liberdades do titular dos dados.

✓ Exemplos em que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e liberdades do Titular dos dados, incluem, entre outros, violações de dados publicamente disponíveis, dados pessoais vazados, mas protegidos por uma chave que permanece confidencial, não podendo ser verificada independentemente, perdas temporárias de acesso a dados pessoais e dados pessoais enviados acidentalmente para terceiros confiáveis em virtude de seu relacionamento com a FCAV, a saber:

- Se for tomada a decisão de não se notificar a ocorrência, a justificativa para essa decisão deve ser documentada no “Formulário de Incidente de Violação de Dados” (ANEXO II);

- A FCAV deve continuar a monitorar as circunstâncias e os efeitos de uma violação e pode precisar fazer ou atualizar notificações a respeito desta junto à ANPD ou comunicações ao Titular dos dados, à medida que novas informações surgirem;

- Todas as violações e as ações tomadas para responder às violações devem ser totalmente documentadas. Mesmo que nenhuma notificação for necessária, deverá ser registrada no “Formulário de Incidente de Violação de Dados” (ANEXO II).

11 NOTIFICAÇÃO PARA A ANPD

Após a avaliação da FCAV, onde se identifica uma violação dos dados que provavelmente represente risco ou dano relevante aos direitos e liberdades das pessoas físicas, esta deve ser relatada à ANPD, sem demora injustificada dentro de **três dias úteis** depois que a FCAV tomar conhecimento da confirmação da violação. E, ainda, quaisquer possíveis motivos para demora na comunicação devem ser informados à ANPD.

A FCAV é considerada ciente de uma violação quando existe um grau razoável de certeza de que ocorreu um incidente de segurança que levou ao comprometimento dos dados pessoais.

A FCAV também é considerada ciente quando informada pelo fornecedor operador. Portanto, todos os contratos de tratamento de dados devem exigir do fornecedor a notificação imediata à FCAV de uma violação.

Uma comunicação preliminar poderá ser enviada para a ANPD no prazo de três dias úteis, caso não for possível fornecer todas as informações. Essas circunstâncias incluem violações complexas que requerem investigações detalhadas, ou quando ocorrem várias violações semelhantes em um curto período.

As informações poderão ser complementadas, de maneira fundamentada, no prazo de vinte dias úteis, a contar da data da comunicação.

O modelo de notificação à Autoridade Nacional de Proteção de Dados Pessoais apresentada (ANEXO V) consta a título de orientação quanto às informações relevantes para a comunicação do incidente.

Portanto, quando houver necessidade de comunicar um incidente de violação de dados à ANPD, deve-se seguir as orientações e as determinações vigentes expedidas pela autoridade.

A notificação para a ANPD deve ser clara, concisa e incluir:

- ✓ Data e hora da detecção;
- ✓ Data e hora do incidente, quando possível determiná-la, e sua duração;
- ✓ A descrição da natureza e da categoria dos dados pessoais afetados;
- ✓ As informações sobre os titulares envolvidos;
- ✓ o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;
- ✓ Circunstâncias em que ocorreu a violação de segurança de dados pessoais (exemplos: perda, roubo, cópia, vazamento, dentre outros);
- ✓ Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;
- ✓ A indicação das medidas de segurança, técnicas e administrativas utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- ✓ Os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

- ✓ Os motivos da demora, no caso de a comunicação não ter sido feita no prazo previsto;
- ✓ As medidas que foram ou que serão adotadas após o incidente para reverter ou mitigar os efeitos do incidente sobre os titulares;
- ✓ Identificação e pontos de contato do Controlador e do Encarregado para mais detalhes;
- ✓ A identificação do operador, quando aplicável;
- ✓ Indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar;
- ✓ Descrever possíveis consequências do incidente de violação de dados;
- ✓ Descrever medidas para endereçar o incidente de violação de dados, incluindo aquelas adotadas para mitigar possíveis efeitos adversos do incidente de violação de dados;
- ✓ O total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

12 AVISO AOS TITULARES DE DADOS PESSOAIS

Com o apoio da Consultoria Jurídica, o Encarregado pelo Tratamento de Dados Pessoais comunicará incidentes de segurança que possam acarretar riscos ou danos relevantes aos titulares de dados pessoais afetados, sem demora injustificada (Anexo IV).

Uma comunicação com o Titular dos dados pessoais, deve conter, em linguagem simples e de fácil entendimento, as seguintes informações:

- ✓ A data do conhecimento do incidente de segurança;
- ✓ A descrição da natureza e da categoria dos dados pessoais afetados;
- ✓ As informações sobre os titulares envolvidos;
- ✓ A indicação das medidas de segurança, técnicas e administrativas utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- ✓ Os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- ✓ Os motivos da demora, no caso de a comunicação não ter sido feita no prazo previsto;
- ✓ As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente;
- ✓ Identificar pontos de contato para maiores detalhes;
- ✓ Descrever possíveis consequências do incidente de violação de dados;
- ✓ Descrever medidas para endereçar o incidente de violação de dados, incluindo aquelas adotadas para mitigar possíveis efeitos adversos do incidente de violação de dados;
- ✓ Ocorrer de forma direta e individualizada, caso seja possível identificá-los.

Caso a comunicação direta e individualizada mostre-se inviável ou não seja possível identificar, parcial ou integralmente, os titulares afetados, a FCAV deve comunicar a ocorrência do incidente, no prazo e com as informações necessárias, pelos meios de divulgação disponíveis, tais como seu sítio eletrônico, aplicativos, suas mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, três meses.

A decisão de notificação pública em massa ou de forma personalizada ou individual deve levar em consideração com base em uma avaliação da quantidade de recursos necessários para notificar cada

Titular de dados individualmente, assim como sobre a capacidade da FCAV de fornecer adequadamente aos Titulares dos dados a notificação dentro do prazo especificado.

A Equipe de Resposta a Incidentes deverá monitorar e apoiar a fase de análise dos riscos e as devidas notificações.

13 MITIGAÇÃO DO INCIDENTE

Nessa etapa, é necessário seguir o fluxo estabelecido pela norma de gestão de incidentes de segurança da informação.

14 RESPOSTA AO INCIDENTE

Nessa etapa, é necessário seguir o fluxo estabelecido pela norma de gestão de incidentes de segurança da informação.

15 PÓS-INCIDENTE – PRÓXIMOS PASSOS

Nessa etapa, é necessário seguir o fluxo estabelecido pela norma de gestão de incidentes de segurança da informação.

16 DAS RESPONSABILIDADES ESPECÍFICAS

16.1 Diretoria Executiva

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

16.2 Encarregado pelo Tratamento de Dados Pessoais

Receber o “Formulário de Incidente de Violação de Dados” por parte da Equipe de Resposta a Incidentes da FCAV e prosseguir com o que for devido;

Comunicar o Comitê de Privacidade e Proteção de Dados Pessoais;

Avaliar a necessidade de comunicação do Incidente de Violação de Dados para a Autoridade Nacional de Proteção de Dados e Titulares de dados pessoais;

Notificar a Autoridade Nacional de Proteção de Dados e Titulares de dados pessoais, se necessário;

Iniciar processos de investigação do Incidente de Violação de Dados e indicar áreas envolvidas que deverão participar do processo;

Comunicar, com o apoio da Consultoria Jurídica, violações de alto risco aos titulares de dados afetados sem demora injustificada.

16.3 Equipe de Resposta a Incidentes

Reportar suspeitas e incidentes de violação de dados ao Encarregado pelo Tratamento de Dados Pessoais por meio do formulário preenchido;

Monitorar todas as fases descritas neste documento, desde a identificação até a solução do incidente, além de apoiá-las;

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

Conduzir em paralelo a este documento os procedimentos indicados na Norma de Gestão de Incidentes de Segurança da Informação;

Auxiliar nos processos de investigação do incidente;

Apoiar com medidas de segurança, técnicas e administrativas necessárias para contenção ou recuperação do incidente.

16.4 Tecnologia da Informação

Monitorar continuamente o ambiente tecnológico do ponto de vista de segurança da informação, visando a identificar eventos que possam causar impactos na disponibilidade, integridade e confidencialidade de dados pessoais que sejam tratados pela FCAV;

Propor adoção de ações ou investimentos que promovam a melhoria contínua do processo;

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

Conduzir em paralelo a este documento os procedimentos indicados na Norma de Gestão de Incidentes de Segurança da Informação;

Informar a Equipe de Respostas a Incidentes assim que tiver conhecimento sobre suspeitas ou uma violação de dados pessoais constatada;

Auxiliar nos processos de investigação do incidente;

Apoiar com medidas de segurança e técnicas necessárias para contenção ou recuperação do incidente;

Apoiar, sempre que necessário, na interação e no escalonamento com as demais áreas, a fim de prover um atendimento mais rápido ao processo.

16.5 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, se for o caso), para relato dos fatos e a apresentação de indícios relativos ao incidente;

Apoiar o Encarregado pelo Tratamento de Dados Pessoais na comunicação a violações de alto risco aos Titulares de dados afetados sem demora injustificada.

16.6 Recursos Humanos

Para os incidentes de violação de dados pessoais que envolvam desvio de conduta do colaborador ou algo em desacordo com o Código de Ética, o caso será encaminhado à área de recursos humanos, bem como, quando for o caso, ao Gestor responsável pelas atividades desenvolvidas por terceiros e, assim, aprofundarem-se na investigação.

16.7 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.

16.8 Gestores

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

Receber comunicação de incidentes de violação de dados por parte de colaboradores de sua área;

Reportar a Equipe de Respostas a Incidentes assim que tiver conhecimento sobre suspeitas ou uma violação de dados pessoais constatada;

Efetuar o preenchimento do “Formulário de Incidente de Violação de Dados” e o encaminhar a Equipe de Respostas a Incidentes;

Auxiliar nos processos de investigação do incidente;

Rever a Planilha de Riscos e Oportunidades e atualizá-la, se for o caso, de acordo com o Procedimento de Levantamento de Riscos e Oportunidades.

16.9 Colaboradores

Estar cientes e manter-se atualizados com este Documento Normativo e demais documentos complementares;

Reportar incidentes de violação de dados ao gestor de sua área;

Auxiliar no preenchimento do formulário “Formulário de Incidente de Violação de Dados”;

Auxiliar nos processos de investigação do incidente quando requerido.

17 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 como tal 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 controles estabelecidos, quando constatada, deve ser tratada como uma violação.

18 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.

19 ANEXOS

Anexo I - Fluxos Gestão de Incidentes de Violação de dados Pessoais 1.5, 1.5.1, 1.5.2 e 1.5.3
Anexo II – Formulário de Incidente de Violação de Dados Pessoais
Anexo III – Notificação ao Controlador – FCAV na condição de operador
Anexo IV – Notificação ao Titular
Anexo V – Notificação à Autoridade

20 NATUREZA DAS ALTERAÇÕES

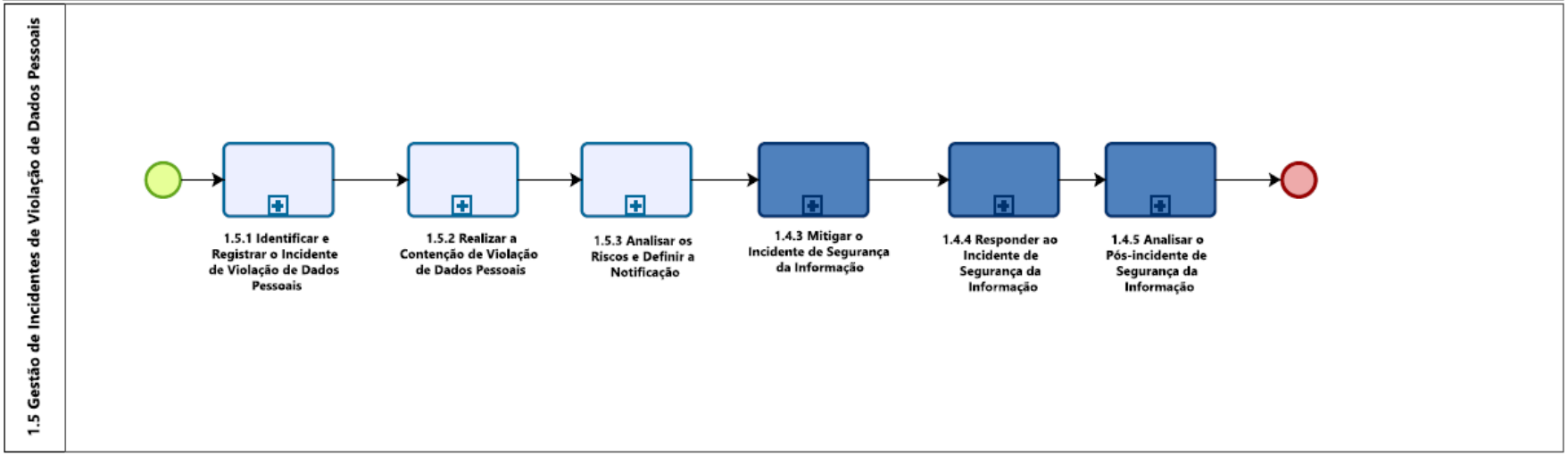
Revisão	Alterações (Inclusões ou Exclusões)	Data
00	Emissão Inicial	19/10/2022
01	Na emissão inicial, em que consta a numeração indicada no cabeçalho como “Revisão 01”, leia-se “Revisão 00”. Essa versão revisada mantém a numeração como “Revisão 01”; Inclusão fluxos gestão de incidentes de violação de dados 1.5, 1.5.1, 1.5.2 e 1.5.3(ANEXO I) aprovados pelo Comitê de Privacidade e Proteção de Dados Pessoais; Ajustes nos textos da Norma atendendo às necessidades identificadas durante o processo de revisão; Renumeração dos anexos.	29/04/2024

Revisão	Aprovação Diretoria Executiva	Data
00	Emissão Inicial	09/11/2022
01	Revisão 01	07/08/2024

21 ANEXO I – FLUXOS GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

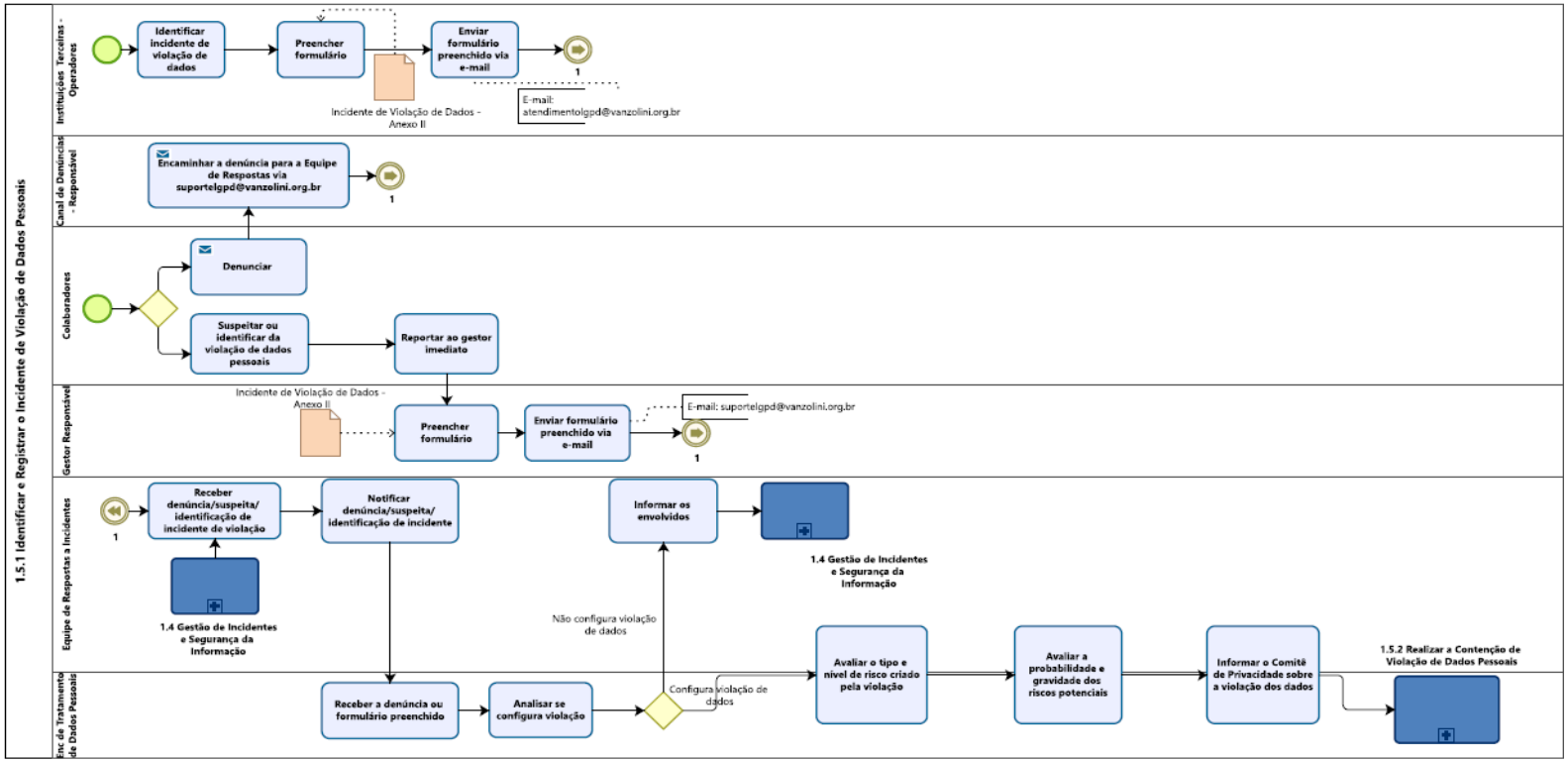
As atividades representadas nos fluxos, para execução desta Norma de Gestão de Incidentes de Violação de Dados Pessoais, têm por objetivo facilitar a compreensão do processo em cada etapa. Composto por quatro arquivos em formato PDF, denominados processo e subprocessos 1.5, 1.5.1, 1.5.2 e 1.5.3, respectivamente, que deverão ser seguidos pelos responsáveis pela execução deste Documento.

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Aprovado	**VERSÃO:** 1.0	Fundação Vanzolini
	ELABORADO POR: FCAV	**DATA DA ELABORAÇÃO:** 02/2024	
PROCESSO: 1.5 Gestão de Incidentes de Violação de Dados Pessoais	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 03/04/2024	



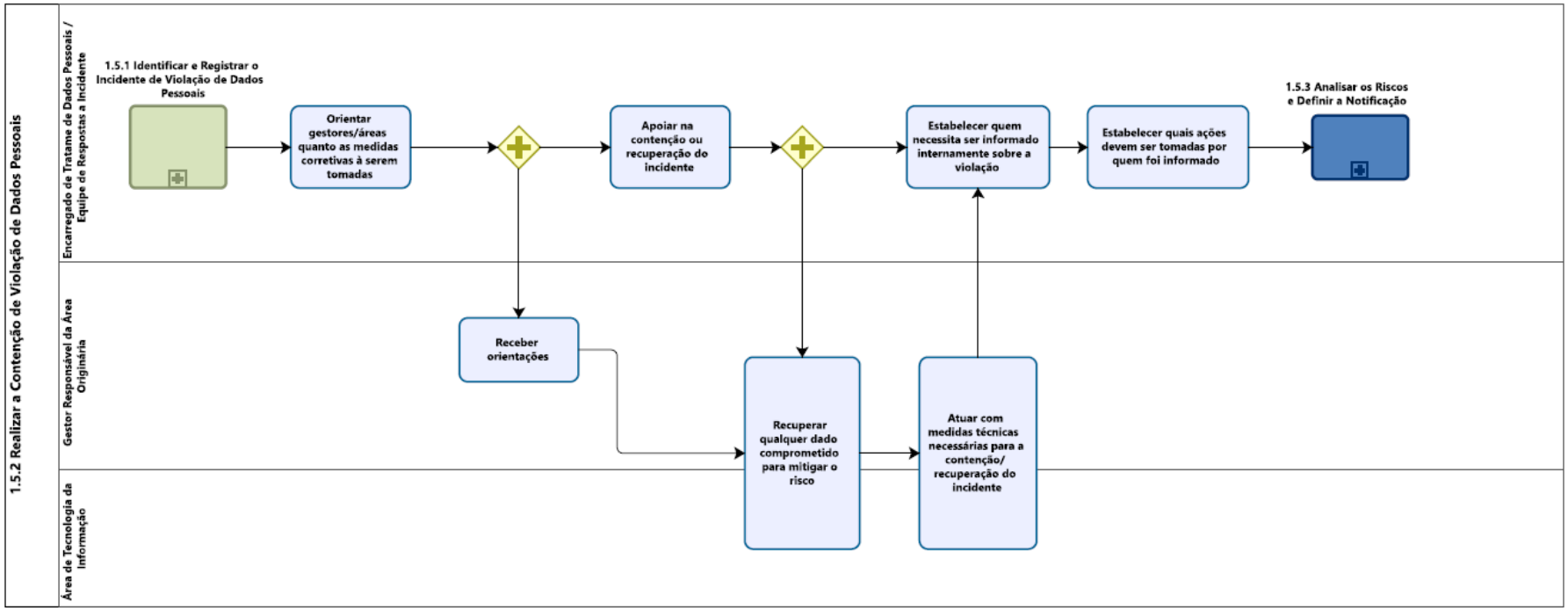
1.5 – Gestão de Incidentes de Violação de Dados Pessoais

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Aprovado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.5 Gestão de Incidentes de Violação de Dados Pessoais	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 02/2024	
SUBPROCESSO: 1.5.1 Identificar e Registrar o Incidente de Violação de Dados Pessoais	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 03/04/2024	
OBJETIVO DO SUBPROCESSO: Identificar e registrar o incidente de violação de dados pessoais, garantindo que todas as notificações sejam tratadas de forma apropriada.			



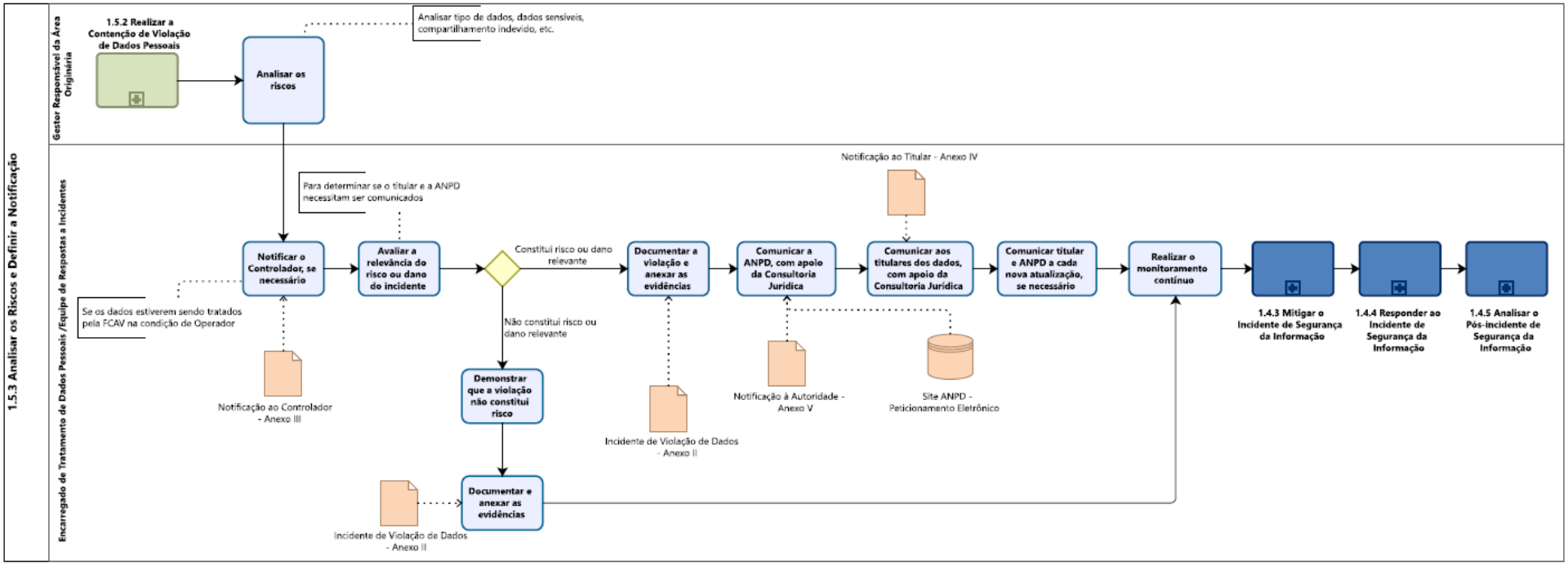
1.5.1 – Identificar e Registrar o Incidentes de Violação de Dados Pessoais

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Aprovado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.5 Gestão de Incidentes de Violação de Dados Pessoais	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 02/2024	
SUBPROCESSO: 1.5.2 Realizar a Contenção de Violação de Dados Pessoais	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 03/04/2024	
OBJETIVO DO SUBPROCESSO: Lidar eficazmente com a violação de dados pessoais minimizando danos e garantindo a conformidade com a regulamentação de proteção de dados.			



1.5.2 – Realizar a Contenção de Violação de Dados Pessoais

FCAV			
MACROPROCESSO: 1. Programa de Governança em Privacidade e Proteção de Dados Pessoais	***STATUS:*** Aprovado	**VERSÃO:** 1.0	Fundação Vanzolini
PROCESSO: 1.5 Gestão de Incidentes de Violação de Dados Pessoais	**ELABORADO POR:** FCAV	**DATA DA ELABORAÇÃO:** 02/2024	
SUBPROCESSO: 1.5.3 Analisar os Riscos e Definir a Notificação	**APROVADO POR:** Comitê de Privacidade e Proteção de Dados Pessoais	**DATA DA APROVAÇÃO:** 03/04/2024	
OBJETIVO DO SUBPROCESSO: Avaliar de forma abrangente os riscos associados à violação de dados, permitindo uma resposta adequada para mitigar esses riscos e garantir uma resposta eficiente e transparentes às partes interessadas, protegendo os direitos dos titulares dos dados e cumprindo com as obrigações legais e regulatórias.			



1.5.3 – Analisar os Riscos e Definir a Notificação

22 ANEXO II – FORMULÁRIO DE INCIDENTE DE VIOLAÇÃO DE DADOS PESSOAIS

Parte 1 – Notificação de incidente de violação de dados pessoais	
Informações	**DADOS A SEREM PREENCHIDOS PELA ÁREA**
Data e hora do incidente.	
Data e hora de descoberta do incidente.	
Local do incidente.	
Países afetados.	
Nome do colaborador responsável por identificar os incidentes.	
Detalhes de contato do colaborador responsável por suspeitar da ocorrência do incidente ou identificação deste.	
Descrição de como a instituição teve ciência do incidente.	
Breve descrição do incidente.	
Número de titulares de dados pessoais possivelmente afetados.	
Dados pessoais foram colocados em risco? Favor detalhar.	
Breve descrição das medidas adotadas após descoberta do incidente.	
Preenchimento pelo Equipe de Respostas a Incidentes e Encarregado pelo Tratamento de Dados Pessoais	
Recebido por:	
Data de recebimento:	
O Incidente configura violação de dados pessoais? Se sim, detalhar a ocorrência.	
Áreas a serem envolvidas:	

Data de notificação de envolvimento das demais áreas:	
Possíveis motivos do incidente não ter sido informado de forma imediata:	
PARTE 2 – AVALIAÇÃO DE SEVERIDADE	
Detalhes de sistemas, equipamentos, registros envolvidos no incidente:	
Detalhes de quais dados foram alvo de violação (destruição, alteração indevida, compartilhamento indevido, entre outros):	
Natureza e categoria dos dados alvo do incidente:	
Volume de dados afetado pelo incidente:	
Há salvaguarda desta informação? Caso não haja, esta violação pode ter efeitos operacionais, legais e reputacionais para a Instituição? Se sim, detalhe-as.	
Qual a quantidade de titulares afetados?	
Há dados pessoais sensíveis envolvidos?	
Há dados pessoais de crianças e adolescentes e idosos envolvidos?	
A Informação, caso acessada por terceiros, pode ser utilizada para fins ilícitos? Ex.: abertura de contas em banco.	
PARTE 3 – MEDIDAS TOMADAS	
Quais medidas de segurança, técnicas e administrativas foram tomadas após a ciência do incidente de segurança?	
Quais medidas de segurança, técnicas e administrativas foram ou serão adotadas para reverter ou mitigar os efeitos do do incidente de segurança aos titulares dos dados?	

Será necessária efetuar uma notificação para Autoridade Nacional de Proteção de Dados? Se sim, de quais países?	
Será necessária efetuar uma notificação para Titulares de Dados Pessoais?	
Será necessária efetuar uma notificação para outras partes interessadas?	
PARTE 4 – ASSINATURAS	
Gestor da Área Originária:	
Encarregado pela Proteção de Dados:	
Equipe de Respostas a Incidentes	
Diretoria Executiva	
Data:	

23 ANEXO III – NOTIFICAÇÃO AO CONTROLADOR – FCAV NA CONDIÇÃO DE OPERADORA

Prezado [NOME DO CONTROLADOR DOS DADOS],

Vimos pela presente, na qualidade de operadora dos dados e em cumprimento com as obrigações negociais firmadas, comunicar que, no dia [DD] de [MM] de [AAAA], identificamos o comprometimento de parte da nossa base de dados, que consideramos uma grave violação de segurança dos dados pessoais que tratamos conforme suas instruções.
* [No caso de a violação já ter sido investigada]

Imediatamente ao tomar ciência do incidente, abrimos uma investigação interna para apurar ocorrido e [DETALHAR COMO O INCIDENTE FOI INVESTIGADO], tendo sido apuradas as informações adiante descritas.
* [No caso de a violação estar em investigação]

Estamos investigando a violação e temos uma previsão de concluí-la até [DATA FINAL], quando forneceremos as informações adicionais necessárias. No estágio em que se encontra a investigação, podemos prestar os seguintes esclarecimentos:
* [Detalhar a violação de segurança de dados]

A informação foi [acidental ou ilegalmente destruída OU perdida OU alterada OU divulgada OU acessada sem autorização da FCAV].

A violação ocorreu nas seguintes circunstâncias e pelas seguintes razões:
• [CIRCUNSTÂNCIAS] • [RAZÕES]
* [Informar os dados pessoais colocados em risco]

A violação afeta os seguintes tipos de informações:
• [TIPOS DE INFORMAÇÃO, POR EXEMPLO, DADOS PESSOAIS OU DADOS PESSOAIS SENSÍVEIS E DETALHES DA EXTENSÃO].

É provável que a violação afete cerca de [Número estimado] titulares de dados pessoais.

Dessa forma, solicitamos ao [NOME DO CONTROLADOR] comunicar o ocorrido à ANPD (Autoridade Nacional de Proteção de Dados). Recomendamos que seja feita a notificação em até três dias úteis.
*[neste campo, listar a decisão de informar ou não informar os titulares]

[Entendemos que os titulares de dados pessoais afetados pela violação [DEVEM OU NÃO SER INFORMADOS] porque [RAZÕES DA DECISÃO].
* Contenção e recuperação

Nós [adotamos OU propomos tomar] as seguintes medidas para solucionar a violação e minimizar e mitigar seus efeitos sobre os indivíduos afetados, a saber:

• [MEDIDAS]
As informações [não] foram recuperadas [e os detalhes são os seguintes]:
• [DETALHES DE COMO E QUANDO FOI RECUPERADO]].

Também adotamos as seguintes etapas para evitar ocorrências futuras da violação:
• [AÇÃO PALIATIVA TOMADA]
• [Os fatos que cercam a violação, os efeitos dessa violação e as ações corretivas tomadas foram registrados em um formulário de violação de dados mantido pelo [nome do controlador dos dados pessoais].

Lamentamos profundamente o ocorrido, e estamos à disposição para cooperar com as informações necessárias, bem como com as autoridades fiscalizadoras, para a mais breve apuração, esclarecimento e solução do caso com total transparência.

A FCAV coloca-se inteiramente à disposição para eventuais esclarecimentos adicionais, que poderão ser obtidos por meio dos contatos abaixo indicados:

- [NOME DO CONTATO DO ENCARREGADO PELO TRATAMENTO DE DADOS]
- [ENDEREÇO]
- [NÚMERO DE TELEFONE]
- [ENDEREÇO DE *E-MAIL*]

Atenciosamente,

Fundação Carlos Alberto Vanzolini

24 ANEXO IV – NOTIFICAÇÃO AO TITULAR

[DESTINATÁRIO]
[ENDEREÇO]

Prezado(a) [Titular dos Dados Pessoais],

Lamentamos informá-lo(la) sobre uma violação da segurança que resultou na [destruição OU perda OU alteração OU divulgação acidental [ou ilegal] OU acesso não autorizado] de seus dados pessoais.

A violação foi descoberta em [DATA] e provavelmente ocorreu em [DATA].

A comunicação do incidente não foi comunicada no prazo de três dias úteis após ter tomado ciência do incidente, [JUSTIFIQUE OS MOTIVOS DA DEMORA].

Como resultado de nossa investigação, concluímos que a referida violação afeta os seguintes tipos de informações:
• [TIPOS DE INFORMAÇÃO. POR EXEMPLO, DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS].

A violação ocorreu nas seguintes circunstâncias e pelas seguintes razões:
• [CIRCUNSTÂNCIAS];
• [RAZÕES].

Tomamos as seguintes medidas para mitigar quaisquer efeitos adversos:
• [MEDIDAS].

Recomendamos para você tomar as seguintes medidas para mitigar possíveis efeitos adversos:
• [MEDIDAS].

[Informamos à Autoridade de Proteção de Dados sobre a violação em [DATA].

Eventuais esclarecimentos adicionais poderão ser obtidos por meio dos contatos abaixo indicados:
- [NOME DOS DEMAIS CONTROLADORES DE DADOS]
- [NOME DO ENCARREGADO PELO TRATAMENTO DE DADOS]
- [ENDEREÇO]
- [NÚMERO DE TELEFONE]
- [ENDEREÇO DE *E-MAIL*]
- [ENDEREÇO DO *WEBSITE*].

Atenciosamente,

Fundação Carlos Alberto Vanzolini

25 ANEXO V – NOTIFICAÇÃO À AUTORIDADE

Formulário de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD)

Comunicação

Tipo de comunicação:

☐Completa.

☐Parcial.

Para comunicação parcial:

☐Preliminar.

☐Complementar.

Critério para a comunicação:

☐O incidente de segurança pode acarretar risco ou dano relevante aos titulares.

☐Não tenho certeza sobre o nível de risco do incidente de segurança.

Agente de tratamento

O(A) notificante é:

☐Controlador(a).

☐Operador(a).

Se operador(a), informar se já houve comunicação ao(à) controlador(a): *[Resposta]*

Dados do agente de tratamento:
Número do CPF ou CNPJ: *[●]*
Nome ou Razão Social: *[●]*
Natureza da Organização *(Pública ou Privada)*: *[Resposta]*
Endereço: *[Resposta]*
Cidade: *[Resposta]*
Estado: *[Resposta]*
CEP: *[Resposta]*
Telefone: *[Resposta]*
E-mail: *[Resposta]*

Dados do(a) notificante:
Nome: *[Resposta]*
E-mail: *[Resposta]*
Telefone: *[Resposta]*

Dados do(a) encarregado(a):

☐Mesmos dados do(a) notificante.

Nome: *[Resposta]*
E-mail: *[Resposta]*
Telefone: *[Resposta]*

Incidente de segurança

Descreva, de forma resumida, como o incidente de segurança com dados pessoais ocorreu.
[Resposta]

Quando o incidente ocorreu?
[Data e hora]

☐Não tenho conhecimento. Justifique: *[Resposta]*

☐Não tenho certeza. Justifique: *[Resposta]*

Quando a organização teve ciência do incidente de segurança?
[Data e hora]

Descreva abaixo como a organização teve ciência do incidente de segurança.
[Resposta]

Se a comunicação do incidente não foi comunicada no prazo de três dias úteis após ter tomado ciência do incidente, justifique os motivos da demora.
[Resposta]

Se as informações serão complementadas, de maneira fundamentada, no prazo de vinte dias úteis, a contar da data da comunicação, justifique.
[Resposta]

Qual a natureza e categoria dos dados afetados?

☐ Origem racial ou étnica.

☐ Convicção religiosa.

☐ Opinião política.

☐ Filiação a sindicato.

☐ Filiação a organização de caráter religioso, filosófico ou político.

☐ Dado referente à saúde.

☐ Dado referente à vida sexual.

☐ Dado genético ou biométrico.

☐ Dado de comprovação de identidade oficial (Por exemplo, nº RG, CPF ou CNH).

☐ Dado financeiro.

☐ Nomes de usuário ou senhas de sistemas de informação.

☐ Dado de geolocalização.

Outros: *[Resposta]*

Qual a quantidade de titulares afetados? Discrimine, quando aplicável, o número de crianças, de adolescentes ou de idosos.
[Resposta]
Qual a categoria dos titulares afetados?

☐ Funcionários

☐ Prestadores de serviço

☐ Clientes

☐ Consumidores

☐ Usuários

☐ Pacientes de serviço de saúde

☐ Crianças ou adolescentes

Outros: *[Resposta]*

Medidas de segurança utilizadas para a proteção dos dados

Quais medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a recorrência do incidente de segurança?
[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança?
[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados?
[Resposta]

O agente de tratamento realizou relatório de impacto à proteção de dados pessoais?
[Resposta]

Riscos relacionados ao incidente de segurança
Quais as prováveis consequências do incidente de segurança para os titulares afetados?
[Resposta]

Considerando os titulares afetados, na sua avaliação, o incidente pode trazer consequências transfronteiriças?

[Resposta]

Comunicação aos titulares de dados

Os titulares foram comunicados sobre o incidente de segurança com dados pessoais?

☐ Sim.

☐ Não.

☐ Não sei.

Forneça detalhes.

[Resposta]

Caso os titulares afetados não tenham sido informados, quais são os motivos que justificam a não comunicação ou o seu retardo?

Local, data

Assinatura do Responsável