Elaboração	Tecnologia da Informação		
Aprovação	Comitê de Proteção de Dados Pessoais e Segurança da Informação	**Data**	25/11/2024

1. Resumo

Este documento traz a descrição de todo o processo a ser seguido pela Catálise Capital Partners S.A e suas controladas (em conjunto "Catálise" ou Empresa), através dos seus colaboradores designados, para o atendimento ágil a todo e qualquer Incidente de Segurança[1], de forma a:

a) mitigar ao máximo possíveis danos decorrentes do Incidente de Segurança seja aos Titulares dos dados, à Catálise ou seus Clientes;
b) garantir a comunicação tempestiva aos Clientes Catálise impactados, à ANPD[2] e aos Titulares dos dados envolvidos;
c) incrementar os processos de segurança da Catálise de forma a prevenir novos incidentes.

2. Atores

O processo de resposta a Incidente de Segurança envolverá obrigatoriamente os seguintes atores:

a) Colaborador Catálise/primeiro contato com o Incidente de Segurança (o "Identificador"), o qual poderá, em algumas situações, ser também o causador do incidente;
b) Data Protection Officer – DPO[3]; (encarregado de proteção de dados pessoais da Catálise);

[1] Incidente de Segurança: violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizado, a dados pessoais sob a tutela da Catálise.

[2] ANPD: Autoridade Nacional de Proteção de Dados.

[3] DPO: encarregado de proteção de dados pessoais da Catálise, conforme designado pelo Comitê de Segurança e Proteção de Dados da Catálise.

c) Representante(s) de Proteção de Dados Pessoais – RPDP[4] da(s) área(s)/atividade(s) envolvidas no Incidente de Segurança; e
d) Comitê de Segurança e Proteção de Dados (o ¨Comitê¨).

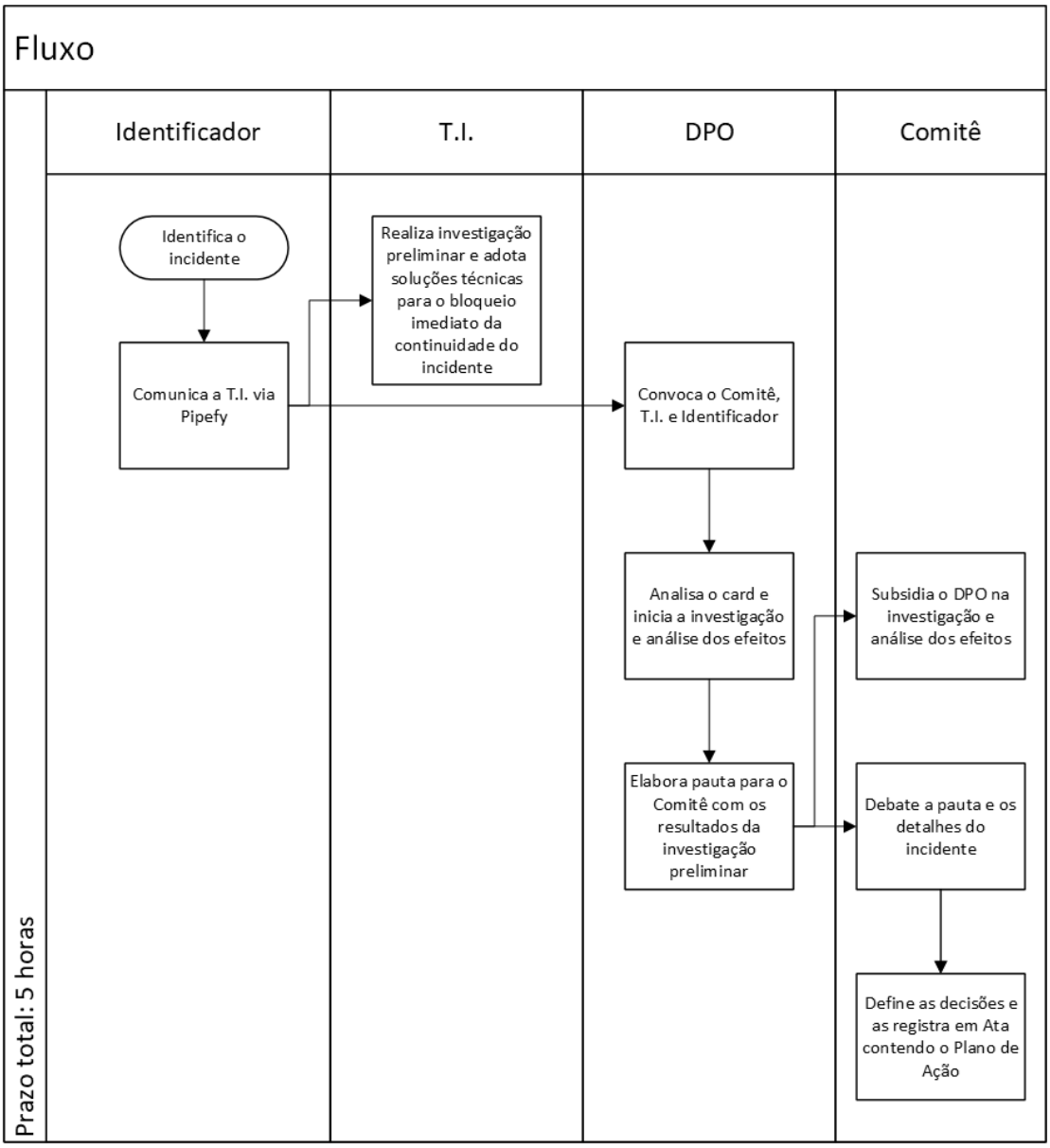
Eventualmente, a depender da gravidade do Incidente de Segurança, o Comitê poderá requisitar o suporte de serviços especializados para responder ao incidente e seus efeitos, quais sejam:

a) serviços de advocacia criminal;
b) serviços de relações públicas e comunicação com Imprensa;
c) serviços de investigação particular de práticas criminosas no âmbito digital e/ou virtual; e
d) serviços forenses (*foresinc*).

3. Fluxo – Identificação, Comunicação e Atendimento

Para o pleno e tempestivo atendimento e resposta a um Incidente de Segurança os Atores indicados deverão atuar seguindo as etapas abaixo:

[4] RPDPs: representantes de proteção de dados atuantes nas diversas áreas da Catálise (Marketing/Comunicação, Comercial, Administrativo/Financeiro, Técnica – Tecnologia da Informação, Recursos Humanos, Jurídico e Compliance) designado para o suporte e apoio às atividades do DPO.



É obrigatório e importante o preenchimento da comunicação do Incidente de Segurança no formulário disponível no Pipe "Fale com a T.I." pois através dele será aberto um card no sistema de *Pipefy* da Catálise, onde ficará registrado todo o atendimento ao Incidente.

4. Prazos de Comunicação

De acordo com a LGPD[5] a ANPD e o(s) Titular(es) dos dados deverão ser comunicados, quando ocorrer um Incidente de Segurança, se:

[5] LGPD: Lei 13.709/2018, Lei Geral de Proteção de Dados Pessoais

a) a Catálise for controladora[6] dos dados pessoais afetados; e
b) o incidente puder ocasionar risco ou dano relevante ao(s) Titular(es).

Além dessas duas condicionantes a lei ainda prevê que a comunicação deverá ocorrer em prazo razoável.

Desta forma, a Catálise adota a seguinte recomendação de prazos, quando entender que há risco o dano relevante ao(s) Titular(es), a serem observados pelo DPO e demais envolvidos no Plano de Resposta:

Dados controlados pela Catálise	72 horas* para comunicar os Titulares e a ANPD
Dados controlados por Cliente Catálise	48 horas* para comunicar o Cliente Catálise

**contados da data e horário da identificação do Incidente*

5. Documentação

Todo Incidente identificado deverá ser documentado integralmente para o fim de demonstrar aos Clientes Catálise, aos Titulares dos dados, à ANPD e demais autoridades públicas, a condução de todo o atendimento, a investigação das causas e responsáveis e as decisões tomadas para ações mitigadoras, punitivas e/ou preventivas.

O acompanhamento da consecução do Plano de Ação definido na reunião do Comitê deverá ser documentado também em Atas de reuniões periódicas do Comitê, até que seja finalizado o Plano de Resposta ao Incidente de Segurança, contendo:

a) atividades realizadas;
b) atividades não realizadas e suas causas;
c) comunicações realizadas (Clientes, Titulares e ANPD), suas datas, meios e comprovações;
d) resultado das investigações;
e) resultado das ações punitivas;
f) processos preventivos implantados; e
g) aprovação do encerramento do Plano de Resposta e seu arquivamento.

[6] Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No caso de a Catálise ser prestadora de serviços de tratamento de dados para Cliente ela é operadora de dados, enquanto o Cliente Catálise é o controlador.

6. Arquivamento

O DPO permanecerá responsável pela guarda de toda a documentação relativa ao Plano de Resposta a cada Incidente de Segurança na Catálise, especialmente aquelas que envolvam a comprovação das comunicações realizadas pela Catálise e as provas obtidas nas investigações.

A documentação deverá ser mantida pela Catálise, em meio físico e/ou digital, pelo prazo mínimo de 10 (dez) anos, contados da finalização de cada Plano de Resposta a Incidente de Segurança.