CATÁLISE	POLÍTICA INSTITUCIONAL - CCP	
Código	**Versão**	**Documento**
PIN. 01	**3ª**	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, CIBERNÉTICA E DE PROTEÇÃO DE DADOS**

Elaboração	Compliance		
Aprovação	Comitê de Proteção de Dados Pessoais e Segurança da Informação	**Data**	11/09/2024

Publicação	( ) Website Catálise Investimentos (x) Website Catálise[1] (x) ANBIMA - SSM
Público	(x) Interno (x) Externo ( )Restrito

1. OBJETIVO

Esta Política de Segurança da Informação e Cibernética é valida para a Catálise Capital Partners S.A. e suas controladas (em conjunto ¨Catálise¨ ou Empresa).

Eventualmente as controladas da Catálise Partners S.A., em razão das peculiaridades de seus objetos sociais e autoridades fiscalizadoras, poderão possuir suas próprias normas relacionadas à Segurança da Informação e Cibernética. A existência desta Política não invalida qualquer outro documento semelhante adotado pelas controladas, valendo a regra de que a norma mais restritiva vigente se sobreporá sobre as demais.

Esta Política traz as diretrizes adotadas pela Catálise para todas as questões de Segurança da Informação e de Segurança Cibernética (doravante simplesmente ¨SI¨) envolvidas em sua operação, seja em seu ambiente físico, digital (local ou em nuvem). Seu objetivo é trazer orientações para a proteção contínua às Informações tuteladas pela Empresa (próprias ou de terceiros[2]) (no plural as ¨Informações¨ ou no singular ¨Informação¨), bem como garantir a integridade, confidencialidade e disponibilidade, de forma que a operação da Catálise ocorra livre de contingências.

Desta Política derivam normas internas, regras de acessos e alçadas, bem como processos e procedimentos, inclusive aqueles que devem ser levados em consideração quando da contratação de fornecedores. Além disso, este documento deve nortear todas as ações, sejam complexas ou triviais, dos Colaboradores da Catálise.

[1] A Política disponível no website da Catálise, será uma versão resumida contendo as linhas gerais da PIN.
[2] Informações de terceiros: para fins desta Política considera-se aquelas informações de colaboradores Catálise, clientes, parceiros, investidores, fornecedores.

Documento de uso exclusivo da Catálise Capital Partners S.A.

Esta Política se embasa nos três pilares da Segurança da Informação:

- **INTEGRIDADE**: garantir que a Informação seja mantida em seu estado original, protegendo-a, tanto na sua guarda, uso ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **CONFIDENCIALIDADE**: garantir que apenas pessoas autorizadas tenham acesso à Informação.
- **DISPONIBILIDADE**: garantir que as pessoas autorizadas tenham acesso à Informação sempre que necessário.

Além dos três pilares acima detalhados esta Política e todas as ações de SI promovidas pela Catálise deverão levar em consideração os seguintes princípios:

- Autenticidade: o acesso dos usuários à Informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada Informação, tenham esse acesso.

- Irretratabilidade: a Informação não pode ser negada ou repudiada por quem a originou ou a modificou (ex: registro de *logs*).

- Privilégio Mínimo: os usuários devem ter acesso apenas às Informações que são necessárias para realizar suas tarefas.

- Proteção de Dados Pessoais: dado pessoal somente poderá ser tratado se tal tratamento estiver enquadrado em uma das hipóteses legais previstas na LGPD, resguardando integralmente a privacidade dos titulares dos dados e dos Colaboradores Catálise[3].

Esta Política tem por finalidade:

(i) orientar as ações de comportamento e segurança, minimizando riscos contra a integridade, sigilo e disponibilidade de toda Informação e dos seus elementos constituintes;

(ii) estabelecer um ideário para as práticas funcionais das rotinas e processos da Catálise, de forma que estejam de acordo com as responsabilidades da Empresa, relacionadas com as regulamentações ou leis que regem as suas atividades, tanto no que se refere à proteção ao sigilo, quanto a utilização de recursos computacionais e cibernéticos, incluindo a definição de padrões de segurança em tecnologia da informação;

(iii) conscientizar todos os Colaboradores Catálise a protegerem diligentemente as Informações, os quais terão o compromisso de observar todas as normas de SI da Catálise em especial esta Política;

[3] Colaborador Catálise: sócios, empregados, estagiários, parceiros e prestadores de serviços da Catálise.

Documento de uso exclusivo da Catálise Capital Partners S.A.

(iv) estabelecer diretrizes que possam acompanhar e responder às mudanças dos negócios, da legislação, das normas regulatórias e das soluções de tecnologia; e

(v) servir de referência para auditorias, verificações de conformidade e determinação de responsabilidades.

A Catálise baseia-se nas recomendações de práticas apresentadas pela norma ABNT NBR ISO/IEC 27002/2005 – Técnicas de Segurança – Código de prática para controles de Segurança da Informação, com o compromisso de contínuo aprimoramento e melhoria em suas ações de segurança.

A observância a todo o repertório legal e regulamentar que abranja a sua operação e de seus clientes, no que tange às questões de SI, tais como a Lei 13.708/2018 - LGPD e a Resolução CMN 4.893/2021, é também compromisso da Catálise vinculando todas as suas áreas e Colaboradores.

2. REGULAMENTAÇÃO APLICÁVEL

- Resolução CVM 21/21;
- Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros;
- Guia Anbima de Cibersegurança;
- Resolução CMN nº 4.893/2021 e Resolução BCB nº 85/3021;
- Lei nº 13.709/18 - Lei de Proteção de Dados Pessoais (LGPD) e alterações dadas pela Lei nº 13.853/19; e
- Lei nº 9.609/98 – Proteção da Propriedade Intelectual de Programa de Computador.

3. ABRANGÊNCIA

As disposições definidas nesta Política devem ser aplicadas a todos os Colaboradores da Catálise ou terceiros que tenham acesso a qualquer tipo de ativo de informação que pertença, ou que estejam sob a responsabilidade da Catálise.

4. GOVERNANAÇA DA SEGURANÇA DA INFORMAÇÃO

A Catálise adota uma estrutura de governança interna dedicada à SI, que está estruturada da seguinte forma:

4.1 Comitê de Proteção de Dados Pessoais e Segurança da Informação

O Comitê atua como órgão deliberativo colegiado, com o objetivo de definir as ações de SI bem como de proteção de dados pessoais, em todas as áreas de todas as Empresas do grupo Catálise. O Comitê foi constituído através de deliberação de

Documento de uso exclusivo da Catálise Capital Partners S.A.

sócios da Catálise em 21/08/2023, tendo o seu Regulamento aprovado em reunião de 24/08/2023. De forma resumida, a atuação do Comitê envolve, dentre outras, as seguintes matérias:

a) distribuição de responsabilidades para fins de SI e proteção de dados pessoais;
b) ações preventivas e mitigadoras de SI e proteção de dados pessoais;
c) aprovação de normas internas da Catálise relacionadas à SI e proteção de dados pessoais bem como acompanhamento das normas para fins de identificação da necessidade de atualização;
d) aprovação da implantação de ferramentas e serviços de SI;
e) definição de critérios de SI para implantação de novos produto ou serviço a ser fornecido pela Catálise;
f) regularidade de software e serviços de tecnologia utilizados/contratados pela Catálise;
g) resposta a Incidente de Segurança[4];
h) ações de comunicação interna e treinamentos; e
i) advertências e penalizações a Colaboradores que descumpram as normas de SI e proteção de dados pessoais da Catálise.

4.2 Encarregado de Dados - DPO

A Catálise possui um Encarregado de Dados – DPO, designado por deliberação em Assembleia de Sócios da Catálise. O DPO responde pelas funções conforme designado na LGPD, para todas as Empresas do grupo Catálise.

4.3 Área de Tecnologia da Informação - TI

É a área responsável por identificar as fragilidades de SI da Catálise, propor soluções ao Comitê, bem como implantar e conduzir processos voltados à melhoria contínua de SI.

A TI poderá utilizar serviços terceirizados especializados para serviços de consultoria em SI, auditorias e para implantação de ferramentas e processos de segurança.

Cada Colaborador que faça parte da equipe de TI, seja interno ou terceirizado, tem o dever de observar o compromisso:

a) em atuar na manutenção na busca da melhoria contínua em SI de todo o ambiente tecnológico da Catálise;

[4] Incidente de Segurança: violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso a Informações tuteladas pela Catálise, bem como a falha ou interrupção no funcionamento de software ou serviços de tecnologia, fornecidos ou utilizados pela Catálise (obs: esta Política de SI adota conceito mais amplo para ¨Incidente de Segurança¨ pois não se restringe apenas a incidente envolvendo dados pessoais.

b) de proteger integralmente todas as Informações de vazamentos e acessos indevidos, mesmo entre Colaboradores Catálise;
c) atuar junto à sua liderança ou ao Comitê para extinguir qualquer fragilidade de SI que identifique nos processos e ferramentas da Catálise; e
d) não copiar, replicar, ou utilizar, a seu favor ou de terceiro, qualquer Informação que tenha acesso em virtude das atividades que desempenhe para a Catálise.

Qualquer violação ao compromisso acima poderá ser objeto de responsabilização cabível, seja no âmbito trabalhista, cível e/ou criminal.

5. ATIVOS DE INFORMAÇÃO

A Catálise considera como ativos de informação todas as informações, disponíveis em qualquer meio, utilizadas ou manipuladas nas operações da empresa, bem como todos os sistemas, equipamentos e instalações onde estas informações são manuseadas ou armazenadas.

As informações podem ser apresentadas nas mais distintas formas escritas, faladas, transmitidas, digitadas, armazenadas ou processadas em qualquer equipamento, papel, telefone, programa de computador, base de dados ou outro meio existente. Seja qual for o estado ou o meio no qual a informação seja apresentada ou compartilhada, ela deverá estar sempre protegida adequadamente, de acordo com as normas definidas neste documento.

6. REGRAS GERAIS

6.1 Resultados dos Trabalhos

O produto das atividades desenvolvidas pelos Colaboradores Catálise [5], como resultado do laboro decorrente da relação contratual existente com a empresa, é considerado ativo da Catálise. Assim, a empresa envidará todos os esforços possíveis para protegê-lo de qualquer divulgação, acesso e/ou utilização indevida por terceiros não autorizados.

Nenhum Colaborador Catálise, inclusive o autor do ativo/produto, está autorizado a divulgar ou permitir a utilização do mesmo por terceiro externo à Catálise, se não houver algum acordo formal celebrado com a Catálise neste sentido.

6.2 Identidade de Usuário

Cada Colaborador Catálise terá uma única identidade de usuário, a ser aberta após a formalização de sua contratação, utilizando-se padrão de e-mail corporativo adotado pela Empresa. Este e-mail deverá ser criado no serviço em nuvem que

[5] Colaborador Catálise: pessoa física empregada da Catálise ou prestadora de serviço contratada por intermédio de pessoa jurídica que tenha acesso às ferramentas Catálise.

fornece além de e-mail outras aplicações para uso no dia a dia dos Colaboradores Catálise, por exemplo editor de texto, planilhas etc. (o "Sistema Corporativo").

Cada usuário é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. Os Colaboradores devem assinar, no momento da contratação, o Termo de Confidencialidade, Compromisso e Responsabilidade comprometendo-se a observar integralmente os termos desta Política.

6.2.1 Autenticação do Usuário

O Sistema Corporativo da Catálise deverá ser configurado para exigir a autenticação do usuário em múltiplos fatores (quando possível).

6.2.2 Senha de Acesso de Usuário

O Sistema Corporativo da Catálise exigirá que a senha adotada pelo usuário possua, no mínimo, os seguintes requisitos de complexidade:

a) no mínimo 8 caracteres;
b) ao menos 1 letra maiúscula;
c) ao menos 1 letra minúscula;
d) ao menos 1 número;
e) ao menos 1 caractere especial (ex: símbolos gráficos, sinais de pontuação etc.); e
f) não ter sido utilizada anteriormente pelo usuário.

O Sistema Corporativo deverá ser customizado para exigir a troca de senha a periodicamente.

6.2.3 Extinção de Usuário

Quando da necessidade de extinção de usuário por encerramento de sua relação contratual com a Catálise, o seu gestor imediato deverá garantir que as informações armazenadas por ele nas Ferramentas de TI da Catálise[6] sejam transferidas para o sucessor de suas atividades, antes da remoção do usuário.

A área de TI manterá em backup todas as Informações exportadas do e-mail e armazenadas em nuvem corporativa do usuário extinto.

6.2.4 E-mails para Não Usuários

A Empresa poderá conceder a abertura de e-mails para Colaboradores Catálise que não necessitem adotar uma identidade de usuário da Catálise, em razão de

[6] Ferramentas de TI: software e serviços de tecnologia, fornecidos pela Catálise ou contratados para sua operação.

Documento de uso exclusivo da Catálise Capital Partners S.A.

prestarem serviços pontuais e/ou não necessitarem utilizar as aplicações do Sistema Corporativo Catálise.

Neste caso deverá ser criado apenas um endereço de e-mail, não sendo criado um usuário no domínio interno que poderá acessar o Sistema Corporativo.

6.2.5 Usuários *Freelancers*

No caso de contratação de desenvolvedores e/ou profissionais de tecnologia para trabalhos/projetos pontuais (os *freelancers*) a Catálise poderá criar um usuário @cataliseinvestimentos.com/falcondtvm.com apenas para acesso aos sistemas que necessitarem para o projeto, mas não terão e-mail da empresa.

6.3 Liberação de Acessos às Ferramentas de TI

As Ferramentas de TI são divididas em duas modalidades de acordo com a sua finalidade e uso, bem como a responsabilidade de gestão, sendo elas:

a) Ferramentas de TI Corporativas – são ferramentas que atendem todas as áreas da Catálise e estão sob gestão da área de TI; e
b) Ferramentas de TI de Área – são ferramentas utilizadas por uma ou mais áreas da Catálise, mas não por toda empresa, estando a área para a qual a ferramenta é mais relevante responsável pela sua gestão.

Os acessos às Ferramentas de TI serão concedidos exclusivamente pela área responsável pela sua gestão considerando sempre a premissa do menor nível de acesso possível. Os acessos serão concedidos exclusivamente ao Colaborador através de sua identidade de usuário.

O acesso às Ferramentas de TI será controlado e liberado através da solicitação formal do gestor do Colaborador ou da área de Recursos Humanos. Essa autorização formal é solicitada no preenchimento da ficha de admissão ou quando for necessária a disponibilização da informação.

As Ferramentas de TI deverão ser utilizadas exclusivamente para o desenvolvimento de atividades profissionais para a Empresa.

6.3.1 Da Responsabilidade dos Acessos

Para os diretórios e serviços que possibilitem diferenciação de níveis de permissão, é de responsabilidade de cada Gestor pela validação e autorização ao acesso às informações contidas neles.

6.3.2 Revisão de Acessos

A Catálise, através da sua área de TI, adota processos para revisão/auditoria periódica a acessos concedidos, enviando trimestralmente um relatório de

permissões aos sistemas e diretórios para cada gestor, de forma a garantir a observância da premissa do menor nível de acesso às Ferramentas de TI.

6.4 Acesso Remoto

A Catálise permite o acesso remoto para todos os Colaboradores, para tanto o usuário deve ser devidamente cadastrado no grupo de segurança do firewall, ter o certificado instalado em seu equipamento e conectar-se através de uma VPN definida pela área de TI.

Ademais, os Colaboradores autorizados devem estar instruídos a: (i) manter softwares de proteção contra malware/antivírus nos dispositivos remotos; (ii) relatar à área de Tecnologia da Informação qualquer violação ou ameaça de segurança cibernética ou outro incidente que identifique em seus equipamentos que possa afetar informações da Catálise durante o trabalho remoto; e (iii) não armazenar informações confidenciais ou sensíveis da Catálise em dispositivos pessoais.

6.5 Equipamentos

A área de TI terá controle integral de todos os computadores que acessam as Ferramentas de TI, bem como terá autonomia para determinar a instalação, nos mesmos, de qualquer tipo de ferramenta de segurança e monitoramento, tais como *anti-malwares, firewalls* e ferramentas de monitoramento.

Os equipamentos fornecidos pela Catálise deverão ser utilizados exclusivamente para o desenvolvimento de atividades profissionais para a Empresa.

Poderá ser permitido, a título de exceção, que Colaborador Catálise utilize computador pessoal (BYOD) para o desenvolvimento de suas atividades para a Empresa. Tal concessão será dada pela área de TI, considerando questões como a não exclusividade do Colaborador e seu nível de maturidade/senioridade. Não obstante o computador utilizado para as atividades serem de propriedade do Colaborador, será adotado, para tais máquinas, o mesmo nível de monitoramento de segurança implantados nos equipamentos da Catálise.

Todos os equipamentos devem ser devidamente inventariados conforme suas características, de tal maneira que possam ser identificados de forma individual e única. Este processo de inventário deverá ser atualizado periodicamente, a fim de garantir a sua consistência.

A segurança das Informações contidas em qualquer equipamento portátil utilizado deverá seguir, no mínimo, os mesmos cuidados dos equipamentos equivalentes em uso exclusivo nas instalações da Empresa. A segurança física do equipamento portátil será de responsabilidade do seu usuário, e este deve respeitar totalmente as orientações fornecidas pela área de TI inclusive quanto ao bloqueio do seu dispositivo.

Ao final do expediente e sempre que necessário ausentar-se do local de trabalho todos os Colaboradores Catálise devem, obrigatoriamente, bloquear/desligar seus computadores e guardar documentos fora do alcance de pessoas não autorizadas.

Apenas a área de TI poderá encaminhar equipamento fornecido pela Catálise para manutenção, nenhum Colaborador está autorizado a fazê-lo por conta própria, mesmo que às suas expensas. A área de TI deverá garantir que qualquer equipamento que venha a ser manuseado por terceiro esteja devidamente limpo, não contendo nenhuma informação interna.

6.6 Ferramentas de TI

Nenhuma nova Ferramenta de TI poderá ser adotada pela Catálise se não houver a análise prévia da mesma pela área de TI, bem como ser seguida a Política e procedimentos de seleção, contratação e monitoramento de fornecedores adotadas pelas empresas controladas pela Catálise Capital Partners S.A..

Para a aprovação de nova Ferramenta de TI a área de TI deverá considerar os seguintes critérios:

a) reputação do fornecedor da Ferramenta de TI;
b) presença/reputação da Ferramenta TI no mercado;
c) sensibilidade da informação a transitar e/ou ser armazenada na Ferramenta de TI;
d) dependência da operação da Catálise no uso da Ferramenta de TI;
e) compatibilidade com sistema operacional, ambiente e demais ferramentas da Empresa; e
f) ROI (custo benefício).

As Ferramentas de TI deverão ser homologadas e autorizadas para uso e deverão ser de propriedade da Catálise ou ter seus direitos de uso cedidos, arrendados ou alugados (excetuando-se serviços e ferramentas gratuitos, desde que autorizados pela área de TI). Tais recursos devem, obrigatoriamente, estar em conformidade com a legislação brasileira vigente.

Toda nova Ferramenta de TI contratada será incluída em Matriz de Risco de software e serviços de TI, mantida e continuamente atualizada pela área de TI e, utilizada para respaldar ações e melhorias de segurança nas Ferramentas de TI.

Esta Matriz de Risco levará em consideração:

a) a(s) categoria(s) de risco envolvido(s) no uso de cada Ferramenta de TI, sendo eles:

(i) Estratégico: risco de impactar a capacidade da Catálise em executar sua estratégia de negócios, impedindo a Empresa de alcançar seus objetivos;

(ii) Financeiro: risco de perdas resultante de transações financeiras e investimentos realizados por agentes sem alçada, ou por terceiros não autorizados;

(iii) Operacional: risco de impedimento do funcionamento das rotinas da Catálise e atendimento a demandas de Clientes, Parceiros e Investidores, bem como risco de perdas resultantes de compromissos assumidos sem a devida alçada; e

(iv) Conformidade: risco de descumprir ou não atender à regulamentação e legislação vigentes e/ou Políticas e normas internas adotadas pela Catálise, bem como de não conseguir comprovar para autoridades públicas e fiscalizatórias que a Catálise cumpre as exigências regulamentares e legais;

b) a probabilidade de falhas, utilização não autorizada, parametrização irregular ou interrupção não programada de Ferramenta de TI; e
c) o impacto causado se um risco de segurança da informação se realizar.

6.7 Nuvem (*Cloud)*

O funcionamento e confiabilidade dos serviços de nuvem (*cloud)* é essencial para a operação da Catálise, para tanto a contratação pela Empresa de fornecedores de tais serviços deverá observar o requisito de classificação/certificação TIER IV[7].

Prestadores de Serviços contratados pela Catálise, que para consecução das suas atividades recebam Informações sensíveis, estratégicas ou que contenham dados pessoais controlados pela Empresa, deverão se comprometer a armazená-las em serviços de nuvem que possuam o mesmo nível de classificação indicado acima.

O gestor da área de TI designará, da sua equipe, no mínimo dois administradores dos sistemas que rodam em serviço de nuvem, tais administradores serão os responsáveis exclusivos por realizar a gestão de infraestrutura, plataformas e software/funções. Exceção poderá ser previamente autorizadas pela gestão da área de TI, desde que seja decorrente de férias, licenças ou outro tipo de ausência temporária de administrador designado.

A Catálise utiliza serviço de nuvem AWS para servidores e bancos de dados, com armazenamento de informações nas regiões sa-east-1, us-east-1 e us-east-2 (São Paulo, N. Virgínia e Ohio, respectivamente).

Serviços de e-mail, armazenamento de arquivos e mensageria são contratados na modalidade SaaS (Microsoft 365).

[7] TIER IV: é o nível mais alto de classificação para data centers que atendem aos padrões mais rigorosos de disponibilidade, segurança e redundância.
[8] *pentest:* teste de penetração, é uma técnica de avaliação de vulnerabilidades do ambiente cibernético.

6.7.1 Auditoria de Nuvem (*Cloud*)

A Catálise poderá se valer de serviços terceirizados de *pentest*[8] para avaliar possíveis vulnerabilidades nos ambientes em nuvem (*cloud*) utilizado pela Empresa, com o intuito de identificar melhorias a serem implantadas em seus processos.

6.8 Ambiente Físico

O ambiente físico da Catálise, para o desenvolvimento de atividades presenciais, deverá apresentar, no mínimo, os seguintes requisitos de segurança:

a) serviços de segurança predial 24 horas;
b) serviços de recepção para controle de acessos;
c) acesso ao prédio de forma eletrônica com biometria facial, mediante cadastro prévio; e
d) salas exclusivas da Catálise com acesso liberado apenas aos Colaboradores da Empresa.

Os acessos físicos devem ser controlados, de forma a garantir que apenas pessoas autorizadas possuam o efetivo acesso às instalações e equipamentos que pertençam e/ou que sejam utilizados pela Catálise. Os recursos de tecnologia da informação e comunicação que estiverem contidos e/ou que forem utilizados também devem ser abrangidos, sendo o seu acesso restrito a pessoas devidamente autorizadas.

O acesso ao prédio e determinadas salas será constantemente monitorado em função de ser realizado por meio de leitura biométrica ou leitura facial, de acordo com as responsabilidades de cada Colaborador, evitando-se acessos indevidos de Colaboradores a áreas não autorizadas.

Visitantes das instalações da Catálise Investimentos devem ser supervisionados e acompanhados. Esses indivíduos devem ter acesso apenas às áreas específicas, com propósitos autorizados e sempre acompanhados por pessoas autorizadas a acessar esses ambientes.

6.9 Ambiente de Mudanças e Ajustes

Mudanças ou ajustes em sistemas da Catálise serão sempre realizados em um ambiente de desenvolvimento/homologação e, somente após a criação e aprovação dos gestores afetados de Documento de Gestão de Mudanças (GMUD), contendo as devidas validações e aplicação de testes de segurança e vulnerabilidade que serão aplicados no ambiente de produção da Catálise.

Em situações em que a mudança ou ajuste não possam ser realizados em ambiente de desenvolvimento/homologação, a aplicação de tais procedimentos deverá ocorrer em um horário alternativo e não comercial (ex: noturno, finais de semana, feriados), com os serviços e aplicações do *host* envolvido no procedimento desligados/parados e com o monitoramento ativo sobre o *host*/rede.

7. PREVENÇÃO DE VAZAMENTO DE INFORMAÇÕES

Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuadamente.

Toda informação relevante deverá ser protegida, de acordo com seu grau de sigilo, integridade e disponibilidade, de forma a atender aos objetivos de segurança da informação.

Conforme o descrito acima, a informação alcançada em função da atividade profissional desempenhada por cada Colaborador na Catálise Investimentos não pode ser transmitida de forma alguma a terceiros não-Colaboradores ou a Colaboradores não autorizados.

8. USO DA INTERNET

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à Catálise Investimentos.

O acesso às páginas e websites é de responsabilidade de cada usuário, ficando vedado o acesso a sites com conteúdo impróprio e páginas de relacionamento.

Os acessos à internet são monitorados através de identificação e autenticação do usuário.

8.1 Recomendações sobre o uso de e-mail

É vedado o uso de sistemas webmail externo. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através do correio eletrônico da Catálise.

É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da Catálise perante seus clientes e a sociedade em geral e que possam causar prejuízo moral e financeiro. É proibido utilizar o e-mail da Catálise para assuntos pessoais.

Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, por exemplo, não reenviando e-mails do tipo corrente, com materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais.

9. METODOLOGIA DE BACKUP, FIREWALL, SOFTWARE E VARREDURAS

Todos os arquivos devem ser gravados na rede da Catálise, pois arquivos gravados no equipamento (local) não possuem cópias de segurança (backup) e podem ser perdidos.

A área de Tecnologia da Informação seguirá um protocolo definido interno de cópia de segurança (backup) conforme as melhores práticas recomendadas, neste sentido os Colaboradores não devem manter qualquer cópia de informações/arquivos mantidos na rede da Catálise (servidor de arquivos ou serviço de nuvem gerenciado).

A Catálise além de realizar as rotinas de backup em todos os sistemas e softwares e bancos de dados hospedados, também realiza o backup, cópia de segurança da máquina virtual garantindo a segurança das informações de processamento.

O processo de restauração das cópias de segurança também deve atuar em tempo hábil que possa atender a necessidade do negócio relacionado a incidentes e desastres.

Para garantir o restabelecimento dos serviços em caso de contingência, são realizados testes de restauração de cópias de segurança, detalhados no Plano de Continuidade de Negócios. Estes testes servem para familiarizar a equipe da área de Tecnologia da Informação com os processos de restauração, bem como afiançar a integridade dos dados dos backups.

Os servidores de aplicação e arquivos possuem rotinas de backup definidas em "Diário, Mensal e Anua"l, de acordo com a tabela abaixo:

Política	Frequência	Gatilho	Retenção
Servers - Anual	1/ano	04:00 UTC+00:00 01/01	10 anos
Servers - Mensal	1/mês	00:30 UTC-03:00 Primeiro domingo do mês	1 ano
Servers - Diário	1/dia	00:30 UTC-03:00	6 meses (frio) / 14 dias (quente)

Bancos de dados possuem rotinas "Anual, Mensal, Semanal e Diário" de acordo com a tabela abaixo:

Política	Frequência	Gatilho	Retenção
RDS-Snapshots-Anual	1/ano	04:00 UTC-03:00 01/01	10 anos
RDS-Snapshots-Mensal	1/mês	00:20 UTC-03:00 dia 01	1 ano (frio) / 7 dias (quente)
RDS-Snapshots-Semanal	1/semana	00:00 UTC-03:00 Sábados	6 meses (frio)
RDS-Snapshots-Diário	1/12 horas	30 minutos após hora cheia, a cada 12 horas	35 dias

Ambos os serviços são executados em nuvem AWS (AWS Backup) e armazenados na região sa-east-1 (São Paulo)

Os arquivos em armazenamento em nuvem (Onedrive), e-mails (Outlook) e mensageria (Teams) possuem backup diário com retenção de 10 anos através do serviço AnyCloud da IBM em parceria com a Vivo/Telefônica

9.1 Instalação de Software e Hardware

Toda instalação de *software* e *hardware* deve ser feita pela área de Tecnologia da Informação, sendo que todos os *softwares* e *hardwares* devem ser homologados e licenciados.

Documento de uso exclusivo da Catálise Capital Partners S.A.

Qualquer *software* que, por necessidade do serviço, precisar ser instalado deverá ser comunicado à área de Tecnologia da Informação, para que o mesmo possa ser homologado e só depois ser disponibilizado.

A Catálise respeita os direitos autorais dos *softwares* que utiliza e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores. É terminantemente proibido o uso de *softwares* ilegais (sem licenciamento).

Toda aquisição e manutenção de sistema deve zelar pela observância dos princípios de controle sobre informações processadas e armazenadas, incluindo a adequada segregação de perfis de acesso.

Os testes de homologação são aplicados pela área de TI em ambiente próprio de homologação, de forma a não gerar risco de instabilidade ou interrupção nos servidores de produção.

A área de Tecnologia da Informação, está autorizada a desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso de qualquer computador/equipamento da Catálise.

9.2 Testes e Varreduras para Detecção de Vulnerabilidades

A área de Tecnologia da Informação poderá se valer de testes de invasão periódicos em seu ambiente tecnológico para identificação de vulnerabilidades em sistemas, serviços (como site da empresa, correio interno, servidor de nomes e documentos visíveis), identificação dos *exploits*, , verificação de *firewall*, revisão das políticas de segurança, verificação de sistemas de detecção de intrusos, revisão de sistemas de telefonia.

9.3 Estabelecimento de Mecanismos de Rastreabilidade

Todo usuário é adequadamente identificado, sendo responsável pela utilização do equipamento no desempenho de suas atividades.

Os softwares, possuem trilha de auditoria para assegurar o rastreamento de eventos, possibilitando:

- Identificação do usuário;
- Data e horário de ocorrência do evento; e
- Identificação do evento (inclusão, alteração ou exclusão).

No caso da rede interna de computadores, são utilizadas trilhas de auditoria com os seguintes registros de acessos: usuário, data e horário.

9.4 Utilização da Rede Corporativa

Nenhuma Informação poderá ser armazenada em computador de trabalho de usuário, mas exclusivamente em nuvem do Sistema Corporativo da Catálise, o qual estará em compartilhamento SMB-*Server Message Block* ou outro serviço/protocolo. O compartilhamento de Informações armazenadas por uma área da Catálise para acesso a usuários de outra área deverá ser autorizado formal e previamente pelo gestor da área concedente.

Nenhum material de origem ilícita ou decorrente de crime, ou que fira os

princípios de conduta previstos no Código de Ética e Conduta da Catálise poderá ser editado, distribuído, armazenado através do uso dos recursos computacionais da rede corporativa da empresa.

A mesma senha para acesso ao S.O./REDE libera acesso à Internet por meio da integração *Firewall*/AD. Seguindo todas as regras de filtros de conteúdo de Internet.

10. RESPOSTA A INCIDENTE DE SEGURANÇA

A Catálise reconhece que, não obstante todas as precauções de segurança que possam ser implantadas, não há como garantir totalmente a inviolabilidade de seu ambiente físico ou digital (local ou em nuvem).

Neste sentido, é compromisso da Catálise adotar processos claros e pré-definidos de resposta a qualquer incidente de segurança, considerando níveis de impacto e gravidade, de forma a garantir uma ação rápida para mitigar ao máximo seus danosos efeitos, bem como a total transparência junto aos interessados e autoridades públicas.

Notificações de incidentes de segurança, caso e assim que percebidos, devem ser efetuadas imediatamente para a área de TI e ao Comitê de Proteção de Dados e SI.

11. PLANO DE CONTINUIDADE DE NEGÓCIOS

A Catálise possui um Plano de Continuidade de Negócios - PCN, estruturado pela área de TI sob a coordenação do gestor da área de TI, o qual determina as diretrizes do acionamento, parâmetros para decisão de acionamento e ações em caso de acionamento.

A necessidade e o tipo de contingência serão determinados com base na importância para o negócio e o tempo de indisponibilidade aceitável para este recurso, sem afetar a continuidade dos negócios da Catálise. A definição dos critérios de importância e tempo aceitável de indisponibilidade é de responsabilidade do gestor da área de TI.

Tendo a Catálise seus serviços hospedados exclusivamente em nuvem pública o PCN adotará como prioridade, em caso de contingência, o acesso remoto aos serviços e restauro do ambiente lógico.

O PCN é um documento interno e confidencial, sendo vedada a sua divulgação a terceiros. Eventualmente a Catálise poderá elaborar um documento resumido do PCN, no qual estarão ocultadas informações internas e sensíveis da Catálise, para que seja fornecido a terceiros em processos de *due diligence* realizados em fase pré contratação com *leads* ou investidores. Neste caso a área de compliance da Catálise deverá ser envolvida com vistas a garantir a existência de um acordo de confidencialidade adequado firmado entre as partes.

11.1. Testes periódicos do PCN

O PCN deverá ser objeto de teste no mínimo a cada 12 meses, podendo tais testes serem realizados a qualquer momento caso necessário.

Documento de uso exclusivo da Catálise Capital Partners S.A.

12. A PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais – Lei 13.709/18 (LGPD) estabelece regras sobre como os dados pessoais (de pessoa física) devem ser tratados nos meios físicos ou digitais. O objetivo da lei é proteger os direitos de liberdade e privacidade dos titulares de dados pessoais.

Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração é considerada como tratamento de dados pessoais.

A LGPD determina que qualquer atividade de tratamento de dados pessoais deve respeitar a privacidade do titular envolvido. Dessa forma, a atividade deve trazer informações claras, precisas e de fácil acesso sobre:

- Como os dados pessoais serão tratados;
- Para qual finalidade esses dados serão usados;
- Quais são as medidas aplicadas para a segurança dessas informações; e
- Quais direitos o titular envolvido tem sobre os seus dados pessoais.

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

- **Finalidade:** propósitos legítimos, específicos, explícitos e informados ao titular.
- **Adequação:** compatibilidade do tratamento com finalidades informadas ao titular.
- **Necessidade:** limitação ao mínimo necessário para realização de suas finalidades.
- **Livre Acesso:** garantia, aos titulares, de consulta facilitada e gratuita.
- **Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados.
- **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis.
- **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger dados.
- **Prevenção:** adoção de medidas para prevenir ocorrência de danos face ao tratamento dos dados pessoais.
- **Não discriminação:** impossibilidade de realização do tratamento com fins discriminatórios.
- **Responsabilização e prestação de contas:** demonstração, pelo

Documento de uso exclusivo da Catálise Capital Partners S.A.

agente, da adoção de medidas eficazes e capazes de comprovar observância e cumprimento das normas de proteção de dados pessoais e eficácia dessas medidas.

A LGPD garante de forma não absoluta, o direito ao acesso, exclusão, revogação, dentre outros. Assim, qualquer atividade de tratamento que envolva dados pessoais deverá observar as regras trazidas pela LGPD (apresentadas em forma de princípios) e estar apta a atender todos os direitos garantidos aos titulares envolvidos.

A Catálise pela sua área de TI e pelo Comitê de Proteção de Dados Pessoais e Segurança da Informação tem o dever de adotar procedimentos internos com vistas a atender integralmente as exigências da LGPD.

12.1 Armazenamento de Dados Pessoais

Os dados pessoais das pessoas físicas ficarão armazenados na nuvem da Catálise Investimentos e alocados em diretórios específicos, de acordo com o responsável pelo tratamento, sendo seu acesso segregado por tipo de função e autenticado por senha criptografada.

Os dados pessoais permanecerão armazenados pelo tempo que for necessário, de acordo com a finalidade para a qual fora coletado e consentido, sendo designado o respectivo prazo de armazenamento para cada dado coletado.

12.2 Compartilhamento de Dados Pessoais

Preservando a privacidade, segurança e confidencialidade das informações, a Catálise poderá compartilhar os dados cadastrais registrados:

- Com parceiros estratégicos, prestadores de serviços e/ou fornecedores contratados;
- Para fins da Política de Privacidade ou em outras situações em que seu consentimento seja solicitado;
- Para cumprimento e execução de obrigações legais e regulatórias;
- Para cumprimento de solicitações e decisões de autoridades judiciais, administrativas ou arbitrais;
- Para investigação de possíveis infrações e análise de indícios ou situações suspeitas à luz das Leis de Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa e Anticorrupção (9.613/98, 12.683/12, 12.846/13, 13.260/16), entre outras normas correlatas;
- Para situações em que o compartilhamento seja necessário para criação, funcionamento e melhoria dos sistemas, das atividades, dos serviços da Catálise Investimentos junto aos parceiros estratégicos, bem como para atendimento das finalidades previstas na Política de Privacidade da Catálise Investimentos.

Nas situações em que o compartilhamento de dados seja necessário deve-se providenciar o preenchimento e assinatura de Acordo de Confidencialidade ou

Seigilo ou documento semelhante em que se formalize compromisso com a preservação e zelo sobre os dados pessoais recebidos.

13. TREINAMENTO

13.1 *Onboarding*

Todo Colaborador Catálise deverá receber treinamento e orientações relacionadas à SI da Empresa ainda na primeira semana de trabalho na Catálise. Tal treinamento deverá ser ministrado pela área de TI ou outra por esta designada, e será o momento em que o novo Colaborador receberá todas as normas internas da Empresa envolvendo as matérias de SI e proteção de dados pessoais.

13.2 Reciclagem

A área de TI deverá promover, no mínimo anualmente, treinamentos de reciclagem sobre a matéria SI a todos os Colaboradores Catálise. Tais treinamentos de reciclagem deverão abordar novos riscos observados na operação da Empresa, novas normas internas implantadas, novas ferramentas de segurança adotadas entre outras questões que visem atualizar o conhecimento e engajamento da equipe sobre a matéria.

13.3 Comunicação Interna

Serão continuamente realizados processos de comunicação interna com vistas a promover o contínuo debate e conscientização a respeito da SI. A área de TI e área de Recursos Humanos serão responsáveis por manter uma agenda de ações de comunicação interna neste sentido.

14. EXCEÇÕES E VIOLAÇÕES

Situações que não se encaixem ou estejam em desacordo com esta política, deverão ser submetidas ao Comitê de Proteção de Dados pessoais e Segurança da Informação, que analisará as circunstâncias e fundamentos, e deliberará em conjunto com a Diretoria a aprovação para tal exceção.

Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e eventuais processos criminais, se aplicáveis.

15. MANUTENÇÃO DOS ARQUIVOS

A Catálise manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo desta Política, pelo prazo mínimo de 10 (dez) anos, conforme legislação vigente.

16. VIGÊNCIA E REVISÃO

As diretrizes contidas nesta Política entram em vigor na data de sua publicação e permanecem vigentes por prazo indeterminado, devendo ser revisadas no mínimo anualmente.