CATÁLISE		POLÍTICA EXTERNA - CCP
Código	**Versão**	**Documento**
PEX CCP.01	**2ª**	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, CIBERNÉTICA E DE PROTEÇÃO DE DADOS**

Elaboração	Tecnologia da Informação		
Revisão	Compliance		
Aprovação	Comitê de Proteção de Dados Pessoais e Segurança da Informação	**Data**	14/11/2025

1. OBJETIVO

A Catálise Capital Partners S.A. e suas controladas adotam esta política para estabelecer diretrizes para garantir a integridade, confidencialidade e disponibilidade das informações do grupo Catálise, protegendo dados próprios e de terceiros contra acessos indevidos, vazamentos e incidentes de segurança. A política orienta ações para minimizar riscos, assegurar conformidade legal e promover boas práticas de segurança em ambientes físicos e digitais.

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. DIRETRIZES

Princípios de Segurança da Informação

A política se fundamenta nos pilares de integridade, confidencialidade e disponibilidade, garantindo que as informações sejam mantidas em seu estado

original, acessadas apenas por pessoas autorizadas e disponíveis sempre que necessário. Também são observados princípios como autenticidade, irretratabilidade, privilégio mínimo e proteção de dados pessoais conforme a LGPD.

Governança e Responsabilidades

A governança é conduzida pelo Comitê de Proteção de Dados e Segurança da Informação, responsável por definir ações, aprovar normas, acompanhar atualizações, responder a incidentes e promover treinamentos. O Encarregado de Dados (DPO) atua conforme a LGPD. A área de Tecnologia da Informação identifica vulnerabilidades, implanta soluções, realiza auditorias e testes de segurança.

Gestão de Acessos

Os acessos são controlados pelo princípio do menor privilégio, com identidade única para cada usuário, autenticação multifator e senhas complexas, que devem ser trocadas periodicamente. Há revisão contínua dos acessos e monitoramento para prevenir riscos. O acesso remoto é permitido mediante protocolos seguros, incluindo firewall, ZTNA e uso obrigatório de antivírus.

Equipamentos e Ferramentas

Os equipamentos fornecidos pela Catálise devem ser utilizados exclusivamente para atividades corporativas, estando sujeitos a inventário e monitoramento. É proibido o uso de softwares não licenciados, sendo obrigatória a homologação para novas ferramentas. Serviços em nuvem devem atender aos padrões mais rigorosos de segurança, como certificação TIER IV, e são submetidos a auditorias periódicas, incluindo testes de invasão (pentest).

Proteção de Dados Pessoais

O armazenamento é realizado em nuvem corporativa, com acesso segregado e criptografia. O compartilhamento de dados ocorre apenas mediante acordo de confidencialidade e para finalidades legítimas, como cumprimento de obrigações legais ou regulatórias. Todas as atividades seguem os princípios da LGPD: finalidade, adequação, necessidade, transparência, segurança e prevenção.

Prevenção e Resposta a Incidentes

Há monitoramento contínuo de acessos e trilhas de auditoria. Existe um Plano de Continuidade de Negócios (PCN) para contingências, com aplicação de testes anuais. Qualquer incidente deve ser comunicado imediatamente à área de TI e ao Comitê de SI.

Treinamento e Conscientização

São realizados treinamentos obrigatórios na admissão e reciclagens anuais para todos os colaboradores, além de comunicação interna contínua sobre normas e segurança.

5. REGRAS GERAIS DE SEGURANÇA

A Catálise adota práticas para garantir a segurança de seus sistemas e informações,

incluindo:

a) **Controle de acessos**: uso de autenticação multifator e revisão periódica de permissões.

b) **Uso de e-mail corporativo**: proibida a utilização de webmails externos.

c) **Monitoramento e auditoria:** rastreabilidade das atividades e registros de acessos.

d) **Proteção de equipamentos:** controle de dispositivos fornecidos pela empresa e regras para uso de equipamentos pessoais.

e) **Armazenamento e backup:** dados protegidos em ambiente seguro, com cópias de segurança periódicas.

f) **Ambiente físico seguro:** controle de acessos ao escritório e monitoramento de entradas.

6. EXCEÇÕES E VIOLAÇÕES

Situações não previstas ou em desacordo com esta política devem ser submetidas ao Comitê de Proteção de Dados e Segurança da Informação para análise e aprovação.

7. PENALIDADES E CONFORMIDADE

O não cumprimento desta política pode resultar em medidas disciplinares, incluindo desligamento e possíveis sanções legais. Revisões periódicas são conduzidas para garantir aderência a regulamentos e melhores práticas de mercado.

8. 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.