# POLÍTICA DE SEGURANÇA E CONTROLE DE ACESSO – PORTFOLIOHUB – LUIS GUSTAVO

A segurança da informação é um componente essencial na implantação do *PortfolioHUB – Luis Gustavo*, especialmente por envolver o uso de ferramentas colaborativas que requerem controle adequado de acesso, armazenamento e compartilhamento de dados. Esta política estabelece diretrizes básicas de segurança, mesmo em ambiente simulado, a fim de garantir a integridade, confidencialidade e disponibilidade das informações manipuladas ao longo do projeto.

## 1. Controle de Acesso às Pastas no Google Drive

A estrutura de pastas foi criada com níveis distintos de permissão:

- 01 – Documentação: acesso de edição apenas ao administrador.
- 02 – Prints e Evidências: acesso restrito ao criador; leitura compartilhada somente no PDF final.
- 03 – Segurança e Acesso: acesso exclusivo ao administrador (pasta com política e registros técnicos).
- 04 – Projetos: acesso de leitura para revisores fictícios.
- 05 – Apresentação Final: acesso compartilhado por link para fins de avaliação.

Todos os compartilhamentos foram realizados com a opção “Somente visualizar” para arquivos públicos e “Editor” apenas para o administrador.

## 2. Simulação de Gestão de Usuários

Embora a implantação tenha ocorrido em ambiente acadêmico simulado, foi prevista uma estrutura organizacional hipotética para fins didáticos:

- admin@xn--portfliogustavo-bvb.com– Administrador geral da plataforma;
- joao@xn--portfliogustavo-bvb.com – Colaborador com permissão de leitura em projetos;

- maria@xn--portfliogustavo-bvb.com – Revisor com permissão de sugestão em documentos do Docs.

Caso o Admin Console estivesse ativo, essas permissões seriam gerenciadas formalmente por meio de grupos e unidades organizacionais dentro do Google Workspace.

## 3. Boas Práticas Adotadas

- Todos os arquivos foram organizados em pastas nomeadas com critérios claros e padronizados.
- O compartilhamento de documentos se limitou a links privados ou contas específicas, evitando exposição pública desnecessária.
- Foi sugerida, via Google Gemini, a aplicação de autenticação em duas etapas (2FA), mesmo que não tenha sido implementada devido às limitações do ambiente.

## 4. Registro e Auditoria

- Prints das telas de configuração de acesso e permissões foram capturados e salvos na pasta 02 – Prints e Evidências.
- Os registros de compartilhamento serão incluídos no PDF final da entrega, como evidência da aplicação desta política.