

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

PENSE OCUPACIONAL

CONTEXTUALIZAÇÃO

A **PENSE OCUPACIONAL**, empresa especializada em saúde ocupacional, segurança do trabalho e gestão de pessoas, reconhece que a informação é um ativo estratégico e essencial para a continuidade de seus serviços.

Esta Política de Segurança da Informação (PSI) tem como objetivo estabelecer diretrizes para garantir a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações, em conformidade com:

- Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD);
- Lei Anticorrupção (Lei nº 12.846/2013);
- Normas ISO/IEC 27001, 27701 e 27002;
- Boas práticas de Governança do IBGC;
- Recomendações da CGU e demais órgãos fiscalizadores.

Todas as pessoas empregadas, estagiários, prestadores de serviços e parceiros da **PENSE OCUPACIONAL** devem cumprir integralmente esta política.

O descumprimento poderá acarretar sanções administrativas, civis e criminais, além de medidas disciplinares internas.

OBJETIVO

Definir princípios e normas para a proteção das informações e ativos digitais e físicos da **PENSE OCUPACIONAL**, assegurando que sejam utilizados de forma ética, segura, responsável e em conformidade com a legislação vigente.

PRINCÍPIOS

- **Confidencialidade:** acesso restrito somente a pessoas autorizadas.
- **Integridade:** proteção contra alterações não autorizadas ou acidentais.
- **Disponibilidade:** acesso garantido a quem de direito sempre que necessário.
- **Autenticidade:** garantia da origem legítima das informações.
- **Transparência:** tratamento de dados de acordo com a LGPD e com boa-fé.
- **Rastreabilidade:** registro e monitoramento das atividades de acesso e uso da informação.

DIRETRIZES PRINCIPAIS

- 1) Login e Senha
 - Cada usuário terá credenciais individuais, pessoais e intransferíveis.
 - Senhas devem ser alteradas periodicamente e sempre que houver suspeita de comprometimento.
 - É proibido compartilhar logins ou senhas.
- 2) E-mail Corporativo
 - Uso exclusivo para fins profissionais.
 - É proibido o envio de mensagens ofensivas, discriminatórias, fraudulentas ou que exponham informações sensíveis.
 - Deve ser utilizada a assinatura padrão da empresa.
- 3) Conexão à Internet e Wi-Fi
 - O acesso à rede interna será protegido por autenticação segura.
 - O uso indevido poderá ser rastreado.
 - Redes públicas devem ser evitadas.
- 4) Armazenamento e Compartilhamento de Arquivos
 - Utilizar apenas pastas e sistemas autorizados pela **PENSE OCUPACIONAL**.
 - Acesso concedido conforme a necessidade de cada área (princípio do menor privilégio).
 - Backups regulares serão realizados.
- 5) Dispositivos e Mídias
 - Todo dispositivo externo (pen drive, HD, etc.) deve ser previamente verificado quanto a vírus e malwares.
 - O colaborador é responsável pelos equipamentos sob sua guarda.
- 6) Confidencialidade das Informações
 - Informações pessoais, médicas, estratégicas e financeiras devem ser tratadas como confidenciais.
 - É proibido utilizá-las para benefício próprio ou de terceiros.
 - Todos devem assinar o Termo de Confidencialidade.
- 7) Publicidade de Dados e Mesa Limpa
 - A estação de trabalho deve ser bloqueada quando não estiver em uso.
 - Documentos físicos confidenciais devem ser guardados em armários trancados.
- 8) Responsável
 - A área de Tecnologia da Informação será responsável por criar e revogar acessos, monitorar incidentes e garantir atualizações de segurança.
- 9) Atividades Proibidas
 - Alterar configurações de equipamentos sem autorização.

- Instalar softwares não homologados.
- Armazenar arquivos pessoais em servidores corporativos.
- Baixar ou compartilhar conteúdos ilegais ou protegidos por direitos autorais.

ETAPAS PARA IMPLEMENTAÇÃO

- Aprovação pela Diretoria.
- Treinamento e conscientização de todos os colaboradores.
- Assinatura dos termos de responsabilidade e confidencialidade.
- Monitoramento contínuo e auditorias periódicas.
- Revisão da política a cada 12 (doze) meses ou quando necessário.

CONCLUSÃO

A **PENSE OCUPACIONAL** reafirma seu compromisso com a proteção da informação e a conformidade legal, promovendo uma cultura de ética, integridade e segurança.

A correta documentação e publicidade desta política pretende gerar impactos positivos e os resultados esperados com essa implementação, visam gerar transparência, cumprindo um dos pilares do compliance antifraudes.

Casos omissos nesta política serão tratados individualmente.

Versão:	Data:	Elaborado por:	Revisado por:	Aprovado por:
01	15/09/2025	Bárbara Maíra Advocacia Especializada	Rejane Silva	Conselho de Administração