

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Smartspace — Um time que transforma sempre caminha junto

# Sumário

1. Introdução
2. Palavra da Diretoria
3. Compromisso com a Informação
4. Programa de Segurança da Informação
5. Objetivos do Programa de Segurança
6. Comunicação da Política
7. Ambientes de Desenvolvimento
8. Violações e Incidentes de Segurança
9. Políticas Complementares
10. Responsabilidades do Sistema de Gestão de Segurança da Informação (SGSI)
  - › CEO
  - › Comitê de Segurança da Informação
  - › Alta Administração
  - › Setor de Desenvolvimento Humano Organizacional (DHO)
  - › Proprietários de Ativos
  - › Setor de Comunicação do Comercial & Marketing
11. Conformidade Legal e Regulamentar
12. Continuidade de Negócios
13. Revisão e Atualização
14. Conclusão



## *1. Introdução*

A Smartspace mantém um programa robusto de Segurança da Informação, que é a base de todas as atividades do grupo. Esta política se aplica a todos os colaboradores, incluindo funcionários, estagiários, aprendizes, dirigentes, empregados de empresas contratadas e terceiros que atuam ou prestam serviços em nome da Smartspace. A Política de Segurança da Informação tem como objetivo proteger as informações e garantir a continuidade do negócio, alinhando-se às exigências da ISO 27001 e da Lei Geral de Proteção de Dados (LGPD).

## *2. Palavra da Diretoria*

A diretoria da Smartspace reitera seu compromisso em manter as informações protegidas, prezando pela confidencialidade, integridade e disponibilidade de dados. Este compromisso é fundamental para garantir a confiança de nossos clientes, parceiros e colaboradores, além de assegurar a conformidade com as regulamentações legais. Todos os colaboradores e parceiros devem compreender e cumprir esta política, contribuindo ativamente para a segurança das informações da organização.

### *3. Compromisso com a informação*

Na Smartspace, a informação é um dos principais ativos da organização. A segurança da informação é essencial para o sucesso de nossas operações, uma vez que as oportunidades de negócio e o relacionamento com clientes e parceiros dependem da proteção e integridade dos dados que manipulamos. A informação segura fortalece a confiança no relacionamento com o mercado e permite a expansão dos negócios de forma responsável.

### *4. Programa de Segurança da Informação*

O Programa de Segurança da Informação da Smartspace é gerido pelo Sistema de Gestão de Segurança da Informação (SGSI), que abrange a implementação, monitoramento e revisão contínua das práticas de segurança. O programa assegura que as políticas de segurança sejam aplicadas em toda a empresa, em conformidade com as normas ISO 27001 e LGPD.

### *5. Objetivos do Programa de Segurança*

- ▶ **Confidencialidade, Integridade e Disponibilidade:** Proteger as informações e os ativos de informação da empresa, garantindo sua confidencialidade, integridade e disponibilidade.
- ▶ **Melhoria Contínua:** Manter um ciclo de melhoria contínua nos processos e controles de segurança, incluindo auditorias regulares e avaliações de risco.
- ▶ **Treinamento e Conscientização:** Realizar treinamentos regulares e campanhas de conscientização para colaboradores, reforçando o papel de cada um na proteção das informações.



## ***6. Comunicação da Política***

A Política de Segurança da Informação deve ser comunicada de forma clara e acessível a todos os colaboradores e partes interessadas. A divulgação ocorre por meio de treinamentos, campanhas de conscientização e comunicações internas, garantindo que todos compreendam suas responsabilidades. A política é revisada periodicamente, e quaisquer alterações são devidamente comunicadas a todos os envolvidos.

## ***7. Ambientes de Desenvolvimento***

Nos ambientes de desenvolvimento, testes e produção, os controles de segurança da informação são aplicados rigorosamente para garantir que a segurança seja mantida durante todo o ciclo de vida do desenvolvimento. A segmentação de ambientes e a proteção de dados são exigências fundamentais, assegurando que informações sensíveis não sejam expostas indevidamente. Todos os projetos de desenvolvimento de sistemas devem seguir as diretrizes de segurança definidas pela empresa.

## ***8. Violações e Incidentes de Segurança***

Qualquer violação da Política de Segurança da Informação ou incidente relacionado à segurança deve ser reportado imediatamente ao Comitê de Segurança da Informação. Todas as violações são investigadas, e ações corretivas são implementadas. A violação intencional ou negligente desta política pode resultar em ações disciplinares, incluindo desligamento, conforme previsto nos procedimentos internos.

## ***9. Políticas Complementares***

Esta Política de Segurança da Informação é complementada por um conjunto de políticas temáticas, que reforçam e sustentam o Sistema de Gestão de Segurança da Informação (SGSI), assegurando que os controles e processos de segurança sejam aplicados de forma abrangente e integrada em todas as áreas da organização.

## ***10. Responsabilidades do Sistema de Gestão de Segurança da Informação (SGSI)***

As responsabilidades no contexto do SGSI da Smartspace estão distribuídas da seguinte forma:

- ▶ CEO: O CEO garante que o SGSI seja implementado de acordo com esta política, assegurando a alocação de recursos adequados e o apoio necessário para a efetiva execução das iniciativas de segurança da informação.
- ▶ Comitê de Segurança da Informação: Responsável pela coordenação operacional do SGSI, garantindo que os processos e controles de segurança sejam aplicados corretamente e que os incidentes sejam tratados de forma eficaz.

- ▶ Alta Administração: A alta administração revisa o SGSI ao menos uma vez ao ano ou sempre que ocorrer uma mudança significativa, gerando um relatório formal para avaliar a eficácia e propor melhorias.

Setor de Desenvolvimento Humano Organizacional (DHO): Responsável pela implementação do programa de conscientização e treinamentos sobre

- ▶ segurança da informação, além da avaliação e implementação do plano de treinamento aplicável a todos que desempenham funções relacionadas à gestão de segurança da informação.
- ▶ Proprietários de Ativos: A proteção da integridade, disponibilidade e confidencialidade de cada ativo de informação é de responsabilidade do proprietário do ativo.
- ▶ Setor de Comunicação do Comercial & Marketing: Define quais informações relativas à segurança da informação serão comunicadas, para quais partes interessadas (internas e externas), por quem e quando.

## *II. Conformidade Legal e Regulamentar*

A Smartspace cumpre todas as legislações e regulamentações aplicáveis, incluindo a Lei Geral de Proteção de Dados (LGPD), garantindo que todas as informações pessoais e sensíveis sejam tratadas de maneira adequada e segura.

## *12. Continuidade de Negócios*

Planos de contingência e continuidade de negócios são mantidos e testados regularmente, visando garantir a resiliência dos sistemas de informação e minimizar os impactos de incidentes que possam comprometer a operação da empresa.

## *13. Revisão e Atualização*

Esta política é revisada anualmente ou sempre que houver necessidade de adequação a novas exigências legais ou mudanças significativas no ambiente de negócio ou tecnologia.

## *14. Conclusão*

A Política de Segurança da Informação da Smartspace é um pilar fundamental na proteção dos dados e na preservação da confiança de clientes e parceiros. Todos os colaboradores têm um papel essencial no cumprimento desta política e no fortalecimento da segurança da informação na organização.



**SMARTSPACE**

0800 724 8181

**SMARTSPACE - João Pessoa**

Av. Adolfo Loureiro França, 468 | João Pessoa, PB - Brasil

**SMARTSPACE - Miami**

1953 NW 93rd Avenue | Miami, FL - USA

**DIGI SOLUÇÕES DE COMUNICAÇÃO LTDA.**

CNPJ 06.126.611/0001-67

Smartspace