Mapa da Segurança da Informação: PSI e a ISO 27001

Navegando pela Segurança da Informação

No universo da segurança da informação, a Política de Segurança da Informação (PSI) e a norma ISO 27001 são dois pilares fundamentais, mas que atuam em níveis diferentes.

Para entender a relação entre eles, podemos usar uma analogia simples: a PSI é a bússola que aponta a direção desejada pela organização, enquanto **a ISO 27001 é o mapa detalhado que fornece a estrutura e as rotas para chegar a esse destino** de forma segura e reconhecida internacionalmente.

Analogia Fundamental: PSI como bússola + ISO 27001 como mapa = Navegação segura na segurança da informação

Política de Segurança da Informação (PSI)

O Que É

Documento de alto nível que estabelece diretrizes, princípios e objetivos gerais de segurança da informação

Propósito

Reflete a cultura e metas de negócio da empresa, servindo como declaração formal do compromisso da alta gestão

Pergunta Central

"O que queremos proteger e por quê?"

Uma Política de Segurança da Informação é essencialmente a proteção dos ativos de informação traduzida em compromisso organizacional formal e estruturado.

ISO 27001: O Sistema de Gestão

01

Abordagem Holística

Gerenciamento sistemático das informações sensíveis da empresa

02

Pilares CID

Garante confidencialidade, integridade e disponibilidade

03

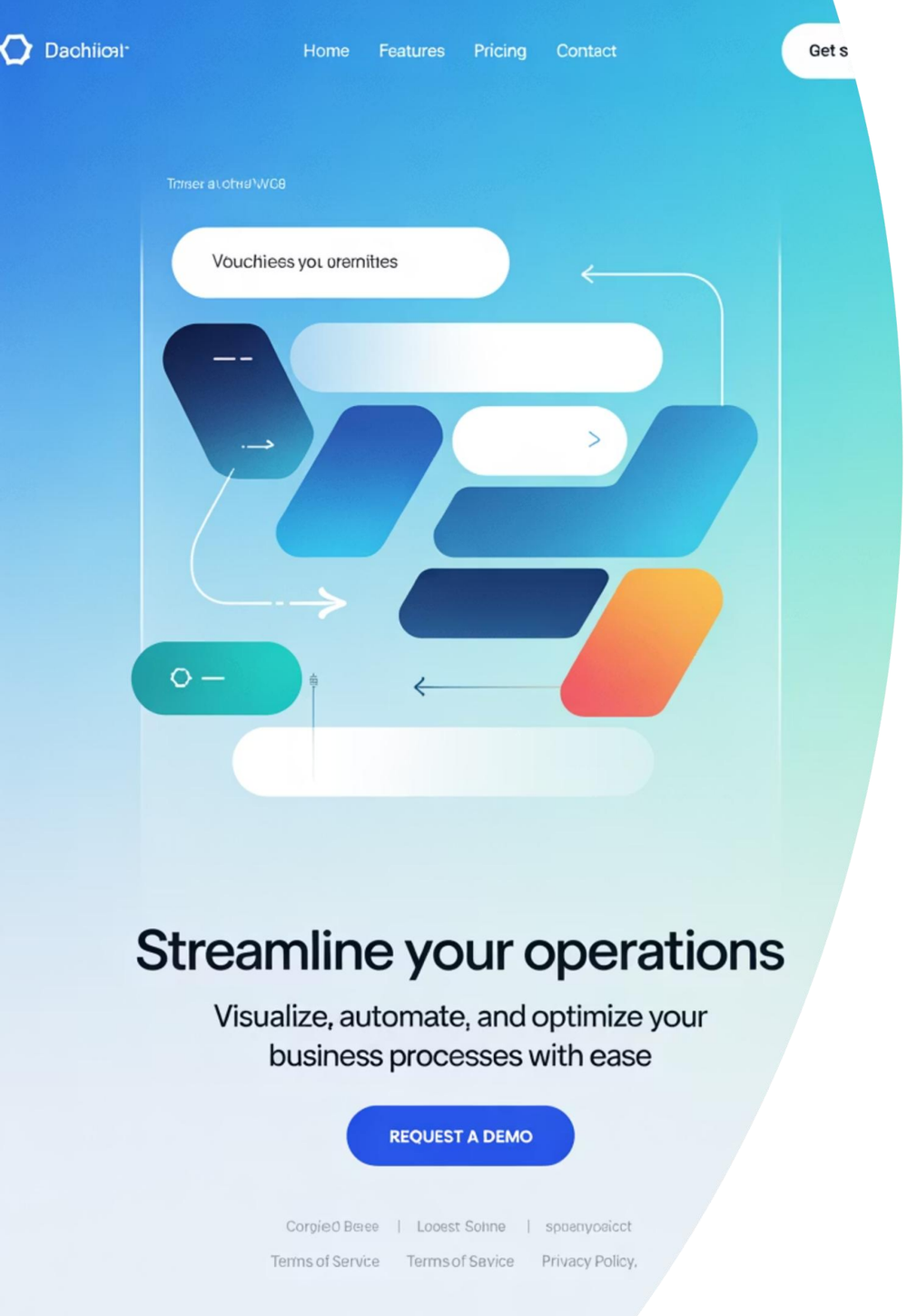
Gestão Baseada em Riscos

Não dita controles específicos, mas como gerenciar de forma abrangente

Definição Técnica

Principais Diferenças Detalhadas

Característica	Política de Segurança da Informação (PSI)	ISO 27001
Natureza	Documento estratégico e diretivo, específico da organização.	Padrão internacional e normativo para um sistema de gestão.
Escopo	Define as intenções e diretrizes gerais de segurança da informação da empresa.	Abrange todo o ciclo de vida de um SGSI, desde o planejamento até a melhoria contínua.



Comparativo Detalhado: Características Específicas

Nível de Detalhe

PSI: Geralmente, é um documento mais conciso e de alto nível.

ISO 27001: É um padrão detalhado com cláusulas e controles específicos (Anexo A) que orientam a implementação do SGSI.

Obrigatoriedade

PSI: É uma prática fundamental de boa governança, sendo um requisito da própria ISO 27001.

ISO 27001: A adoção é voluntária, mas a certificação confere um reconhecimento formal e internacional das práticas de segurança.

Foco e Público-Alvo

Foco da PSI

O "quê" e o "porquê" da segurança da informação na organização.

Foco da ISO 27001

O "como" gerenciar a segurança da informação de forma estruturada e baseada em riscos.

Público da PSI

Todos os colaboradores, parceiros e terceiros que têm acesso às informações da empresa.

Público da ISO 27001

Gestores de segurança, auditores, equipes de TI e a alta direção responsável pela implementação e manutenção do SGSI.

A Integração Perfeita: PSI + ISO 27001

Em suma, a PSI é uma peça-chave dentro do quebra-cabeça da ISO 27001.

PSI como Ponto de Partida

Declaração de intenções que norteia todas as ações do SGSI

ISO 27001 como Estrutura

Framework detalhado que fortalece e operacionaliza a política

Resultado Final

Segurança da informação robusta e reconhecida internacionalmente

Conclusão: Não se trata de uma escolha entre um e outro, mas sim de entender como a política interna (PSI) se encaixa e é fortalecida pela estrutura de gestão global (ISO 27001).