**Experimente o Smartsheet GRATUITAMENTE**

**MODELO DE PLANO**

**DE SEGURANÇA DE DADOS**

| HISTÓRICO DE VERSÕES |
| --- |
| VERSÃO | APROVADO POR | DATA DA REVISÃO | DESCRIÇÃO DA ALTERAÇÃO | AUTOR |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

PLANO DE SEGURANÇA DE DADOS

NOME DA EMPRESA

Endereço físico

Cidade, estado e CEP

endereçodosite.com

Versão 0.0.0

00/00/0000

1. **IDENTIFICAÇÃO DO SISTEMA**

Detalhes sobre o sistema, proprietário do sistema e número de usuários

1. **AMBIENTE DO SISTEMA**

Detalhes sobre interconexões do sistema, principais dispositivos e componentes de hardware e software

1. **REQUISITOS**

Detalhes sobre quaisquer requisitos de segurança de dados aplicáveis

* 1. **Controle de acesso**

Garanta que o sistema limite o acesso a usuários autorizados, defina o tipo de transações permitidas, limite algumas funções a usuários “com privilégios”, monitore o acesso remoto e controle a conexão de dispositivos móveis

* 1. **Conscientização e treinamento**

Garanta que todas as pessoas da organização estejam cientes dos riscos de segurança do sistema, recebam o treinamento adequado para realizar atividades de forma a proteger os dados e entendam indicadores de ameaças ou infiltrações

* 1. **Auditoria e prestação de contas**

Garanta que a organização tenha um sistema contínuo que monitore qualquer atividade incomum ou não autorizada no sistema

* 1. **Gerenciamento de configurações**

Estabeleça e mantenha configurações básicas em todo o sistema, incluindo o controle e o monitoramento de softwares instalados por usuários

* 1. **Identificação e autenticação**

Garanta que o sistema possa identificar usuários e dispositivos do sistema e imponha um mínimo de complexidade às senhas

* 1. **Resposta a incidentes**

Estabeleça um sistema que rastreie, documente e gere relatórios de incidentes que possam ter comprometido a segurança e que teste a capacidade das organizações de responder a um incidente

* 1. **Manutenção**

Realize manutenção contínua no sistema

* 1. **Proteção de mídias**

Limite o acesso à mídia digital do sistema a usuários autorizados e garanta que a mídia digital seja mantida segura de outras maneiras

* 1. **Segurança de pessoal**

Monitore as pessoas antes de permitir o acesso ao sistema e garanta que o sistema esteja protegido depois que as pessoas deixarem a organização

* 1. **Proteção física**

Limite o acesso aos sistemas físicos e equipamentos a pessoas autorizadas

* 1. **Avaliação de risco**

Avalie periodicamente os riscos de segurança na operação normal do sistema, busque vulnerabilidades e faça correções quando vulnerabilidades são encontradas

* 1. **Avaliação de segurança**

Avalie periodicamente os controles de segurança para garantir que eles sejam eficazes e faça correções quando necessário

* 1. **Proteção do sistema e das comunicações**

Monitore e proteja as comunicações de fora do sistema que são recebidas pelo sistema

* 1. **Integridade do sistema e da informação**

Identifique, informe e corrija falhas do sistema em tempo hábil, providencie proteção contra códigos maliciosos e monitore alertas e avisos de segurança

|  |
| --- |
| **AVISO DE ISENÇÃO DE RESPONSABILIDADE**Qualquer artigo, modelo ou informação fornecidos pela Smartsheet no site são apenas para referência. Embora nos esforcemos para manter as informações atualizadas e corretas, não fornecemos garantia de qualquer natureza, seja explícita ou implícita, a respeito da integridade, precisão, confiabilidade, adequação ou disponibilidade do site ou das informações, artigos, modelos ou gráficos contidos no site. Portanto, toda confiança que você depositar nessas informações será estritamente por sua própria conta e risco. |