Lista de dados sensíveis

A ISO 27001 e a ISO 27002 são normas internacionais que estabelecem boas práticas de segurança da informação, incluindo a proteção de dados pessoais sensíveis. Alguns tipos comuns de dados sensíveis que podem ser encontrados em um setor da Empresa x incluem:

1. Informações financeiras, como informações bancárias, dados de pagamento e informações fiscais;
2. Dados pessoais, como nomes, endereços, informações de contato e informações de identificação pessoal, como números de passaporte ou de carteira de motorista;
3. Informações médicas, como histórico médico, informações de saúde e informações de tratamento médico;
4. Informações de segurança, como informações de segurança pessoal e informações sensíveis sobre instalações;
5. Informações sobre a vida profissional, como informações de emprego, informações de salário e informações de benefícios;

Categoria 1: Dados altamente sensíveis

- Informações financeiras dos contribuintes.
- Informações pessoais dos funcionários da Empresa x, incluindo informações financeiras, de saúde e histórico de trabalho.

Categoria 2: Dados moderadamente sensíveis

- Informações do público coletadas através do setor de Comunicação.
- Informações dos vereadores, incluindo informações pessoais, políticas e votações.
- Informações jurídicas da Empresa x.

Categoria 3: Dados pouco sensíveis

- Informações de protocolo, incluindo agenda de eventos e lista de convidados.
- Informações de expediente, incluindo relatórios de atividades e correspondências.

É importante destacar que a segurança e proteção de todos os dados coletados pela Empresa x é crucial para garantir a privacidade e o cumprimento da LGPD. A implementação de medidas de segurança e controle rigorosas para cada categoria de dado é essencial para garantir a privacidade e a proteção dos dados. Além disso, é importante garantir que todos os funcionários envolvidos no processo estejam cientes das políticas e regulamentos de privacidade de dados da Empresa x.

---

1. Dados pessoais sensíveis:

- Setor de RH: Dados de saúde, religião, origem étnica e orientação sexual dos funcionários da Empresa x.
- Setor Jurídico: Dados sensíveis relacionados a processos judiciais.

Categoria: Altamente sensíveis Importância: Esses dados são confidenciais e podem afetar negativamente a vida pessoal e profissional das pessoas envolvidas, caso sejam divulgados de maneira inadequada.

2. Dados financeiros:

- Setor Financeiro: Dados bancários, informações sobre pagamentos e transações financeiras.

Categoria: Sensíveis Importância: Esses dados são confidenciais e podem ser utilizados para fins fraudulentos, caso sejam divulgados de maneira inadequada.

3. Dados de protocolo:

- Setor de Protocolo: Dados sobre reuniões, decisões tomadas e documentos oficiais.

Categoria: Sensíveis Importância: Esses dados são confidenciais e podem afetar negativamente a tomada de decisão e a reputação da Empresa x, caso sejam divulgados de maneira inadequada.

4. Dados de expediente:

- Setor de Expediente: Dados sobre documentos internos e processos administrativos.

Categoria: Moderadamente sensíveis Importância: Esses dados são confidenciais e podem afetar a eficiência dos processos administrativos da Empresa x, caso sejam divulgados de maneira inadequada.

5. Dados de comunicação:

- Setor de Comunicação: Dados sobre campanhas publicitárias, contatos com a mídia e informações relacionadas à imagem da Empresa x.

Categoria: Moderadamente sensíveis Importância: Esses dados são confidenciais e podem afetar a imagem da Empresa x, caso sejam divulgados de maneira inadequada.

6. Dados do vereador:

- Setor do Vereador: Dados pessoais, financeiros, informações sobre projetos de lei e contatos com eleitores.

Categoria: Sensíveis Importância: Esses dados são confidenciais e podem afetar a imagem e a carreira política do vereador, caso sejam divulgados de maneira inadequada.

A categoria e a importância dos dados são determinadas pela LGPD (Lei Geral de Proteção de Dados), que estabelece que é dever da Empresa x proteger esses dados de maneira adequada e garantir a privacidade dos indivíduos. Além disso, é importante seguir as normas e boas práticas estabelecidas pela ISO 27001 e ISO 27002, para garantir a segurança dos dados e evitar possíveis riscos. A ANPD (Autoridade Nacional de Proteção de Dados) também deve ser consultada para garantir o cumprimento de todas as regulamentações legais.