Política de Auditoria e Conformidade

Dados do documentos
ID Interno EVDOC: 51-8530
Data do documento: 2023-01-25
Versão do documento: 2023-01-25
Fluxo de aprovação EVDoc: 52-8530-02
Sigla / Denominação: PAC
Empresa: EVSolid (Aqui Referida como EV)
Responsável PCTSI: DSI (Departamento de Segurança da Informação)

1 – Objetivo

Esta política visa estabelecer diretrizes para monitorar a conformidade da empresa com as políticas de segurança e as regulamentações aplicáveis, incluindo a Lei Geral de Proteção de Dados (LGPD) e outras regulamentações relacionadas à proteção de dados pessoais.

2 – Escopo

Esta política se aplica a todos os funcionários, terceirizados e parceiros da empresa que coletam, armazenam, processam ou compartilham dados pessoais de titulares de dados.

3 – Regulamentações aplicáveis

A empresa deve cumprir todas as regulamentações aplicáveis relacionadas à proteção de dados pessoais, incluindo, mas não limitado a LGPD, Lei de Proteção de Dados.

4 – Responsabilidade

A organização é responsável por garantir que os dados pessoais de seus titulares sejam protegidos em conformidade com as regulamentações aplicáveis. A gestão é responsável por supervisionar a implementação desta política e garantir que ela seja revisada e atualizada regularmente.

5 – Auditorias internas

A organização realiza auditorias internas periódicas para avaliar a conformidade com as políticas de segurança e as regulamentações aplicáveis. Essas auditorias são realizadas por pessoas qualificadas e independentes, que devem ter acesso a todos os registros e informações necessárias para avaliar a conformidade da empresa. O objetivo dessas auditorias é identificar quaisquer lacunas ou deficiências nas políticas e práticas da empresa relacionadas à proteção de dados pessoais.
As auditorias internas devem incluir uma avaliação das políticas de segurança de dados da empresa, a eficácia dos controles e procedimentos implementados para proteger dados pessoais, a conformidade com as regulamentações aplicáveis, a adequação das medidas técnicas e organizacionais para proteger dados pessoais, e a eficácia do treinamento e conscientização fornecidos aos funcionários.
Os resultados das auditorias internas devem ser documentados e relatados à equipe de gestão da empresa. Os planos de ação corretiva devem ser desenvolvidos para abordar quaisquer não conformidades identificadas durante a auditoria.

6 – Métricas de conformidade

A organização estabelece métricas para monitorar sua conformidade com as políticas de segurança e as regulamentações aplicáveis. Essas métricas incluem indicadores quantitativos e qualitativos, que permitem avaliar o desempenho da empresa em relação à proteção de dados pessoais.
As métricas devem ser revisadas regularmente pela equipe de gestão da empresa, para garantir que continuem sendo relevantes e eficazes na avaliação da conformidade. A equipe de gestão deve desenvolver planos de ação corretiva para lidar com quaisquer não conformidades identificadas pelas métricas.

7 – Planos de ação corretiva

A organização deve desenvolver planos de ação corretiva para abordar quaisquer não conformidades identificadas pelas auditorias internas e externas, bem como pelas métricas de conformidade.

Os planos de ação corretiva incluem uma descrição detalhada das ações que serão tomadas para corrigir a não conformidade, incluindo responsabilidades, prazos e recursos necessários. A equipe de gestão da empresa deve revisar regularmente o progresso desses planos de ação corretiva e garantir que sejam implementados de maneira eficaz e oportuna.
A equipe de gestão deve garantir que a equipe de TI esteja ciente dos planos de ação corretiva, para garantir que as medidas corretivas sejam implementadas de maneira eficaz nos sistemas de informação da empresa.

Além disso, a equipe de gestão deve garantir que quaisquer violações da política de segurança de dados sejam relatadas e tratadas em conformidade com as políticas internas da empresa e com as regulamentações aplicáveis. Os planos de ação corretiva devem ser desenvolvidos para lidar com quaisquer violações relatadas.

8 – Revisão da política

A política de auditoria e conformidade deve ser revisada regularmente para garantir que continue relevante e eficaz. Quaisquer alterações devem ser comunicadas a todos os funcionários relevantes e treinamentos adicionais podem ser necessários. A periodicidade mínima é de um ano ou alteração em alguma legislação que impacte essa política.