



—— POLÍTICA DE SEGURANÇA DA INFORMAÇÃO ——

OBJETIVO

O objetivo da Política de Segurança da Informação é promover e divulgar as diretrizes e controles que devem ser estabelecidas e seguidas no intuito de proteger e preservar as informações corporativas a nível de confidencialidade, integridade, disponibilidade e privacidade alinhando-as à regulamentos, leis, normas nacionais e internacionais constituindo-se em uma normativa da organização formalizando seu compromisso com a segurança de informações e dados sensíveis do negócio e expandindo sua exigência de cumprimento a todos os seus colaboradores, além de, clientes (que atuem como fornecedor), parceiros, fornecedores e prestadores de serviços que atuem em nome da Proodus.

ESCOPO

A Política de Segurança da Informação deve ser seguida primordialmente pelos colaboradores da organização além das demais partes interessadas como os clientes (que atuem como fornecedor), parceiros, fornecedores e prestadores de serviços, atuando em nome da Proodus, os mantendo cientes e atualizados quanto aos controles de segurança implementados pela organização.

PRINCÍPIOS DA POLÍTICA

A PSI estabelece os seguintes princípios orientadores:

- 1 – Toda e qualquer informação gerada ou recebida através dos processos de trabalhos pertencem única e exclusivamente à organização.
- 2 – Todos os colaboradores e prestadores de serviços interno contratados deverão firmar o acordo de confidencialidade a fim de manter preservada as informações geradas durante os processos de trabalho.
- 3 – Todos os recursos disponíveis na empresa como equipamentos, informações e sistemas deverão ser utilizados única e exclusivamente para a realização das atividades profissionais.
- 4 – Os cuidados com as informações corporativas é um dever de todos.

COMUNICAÇÃO DA POLÍTICA

A Política de Segurança da Informação está divulgada nos seguintes meios:

- **Site Institucional:** www.produs.com.br (versão resumida)
- **Intranet Corporativa:** intranet.produs.com.br

RESPONSABILIDADES

6.1. Gestores das áreas

Responsáveis por zelar pela segurança das informações manuseadas pelas suas equipes nos seus processos de trabalho. Os gestores devem servir de exemplo quanto a aderência, seguimento, multiplicação dos controles de segurança da informação estabelecidas na PSI e incentivo no processo de melhoria contínua sobre a segurança da informação. Cabe aos gestores a divulgação da PSI para fornecedores, colaboradores recém-admitidos assim como manter suas equipes atualizadas sobre os aspectos e controles de segurança a fim de promover a consciência da proteção das informações.

6.2. Colaboradores

São as pessoas que formam as equipes envolvidas nos processos de trabalho e que manuseiam diariamente as informações da empresa. Os colaboradores podem fazer parte do quadro de efetivos, temporários ou prestadores de serviços, devendo estar cientes e comprometidos no seguimento das diretrizes da PSI.

6.3. Equipe Técnica

É a equipe formada por técnicos e analistas de TI envolvidos nos processos de suporte, gestão de infraestrutura e segurança da informação. São os responsáveis por estabelecer, manter, revisar e homologar os controles para a segurança das informações corporativas implementados no ambiente interno da empresa. Cabe a equipe técnica promover a conscientização dos demais colaboradores quanto a importância do seguimento da PSI e seu papel na preservação dos

dados assim como multiplicar o conhecimento técnico às demais áreas e agir como fiscalizadores do cumprimento dos controles internos a fim de manter a conformidade com a PSI.

6.4. Clientes, fornecedores e parceiros

As partes interessadas externas como clientes (atuando como fornecedor), fornecedores e parceiros são responsáveis em se manter comprometidos com a segurança sobre as informações geradas, tratadas e manuseadas dentro dos seus escopos de atuação e relacionamento com a organização. A Política de Segurança da Informação estabelecida e seguida pela Probus nos seus processos de negócios deve estar disponível no site institucional aos clientes, fornecedores e parceiros, para ciência, de modo que não haja alegação de desconhecimento e/ou isenção de culpa em eventos de violação de segurança que porventura os afetem.

6.5. Comitê de Segurança da Informação - CSI

O Comitê de segurança da informação - CSI é o responsável por analisar os incidentes de segurança da informação identificados e reportados a fim de chegar a sua causa raiz e promover soluções para eliminar ou minimizar a probabilidade de nova ocorrência.

O CSI deve ser convocado sempre na ocorrência de um incidente de segurança que possa ter comprometido algum aspecto de confidencialidade, disponibilidade e/ou integridade de informações corporativas. O CSI tem a sua composição fixa formada pela gestão da qualidade e gestão técnica e pode ser complementado pelo(s) gestor(es) da(s) área(s) envolvida(s), o(s) autor(es) envolvidos assim como mais recursos técnicos internos ou externos como analistas, especialistas e consultores.

CONTROLES DE SEGURANÇA

Todos os controles de segurança adotados visam garantir o pleno cumprimento dos objetivos dentro do escopo definido levando em consideração que os princípios de segurança da informação são comunicados e disponibilizados internamente na versão estendida desse documento para todos os colaboradores.

Demais partes interessadas que desejem ter acesso à versão completa, poderá solicitá-la por meio da ouvidoria interna através do e-mail ouvidoria@produs.com.br. As solicitações realizadas, passarão por devida análise e disponibilização em caso de aprovação.