PROTOCOLO GERAL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Introdução

A O2sistemas adota a presente Política de Segurança da Informação (PSI) com o objetivo de proteger a confidencialidade, integridade e disponibilidade das informações no âmbito de suas operações, visando mitigar riscos e garantir a conformidade com as leis e regulamentações aplicáveis.

Esta política é aplicável a todos os colaboradores, prestadores de serviço, parceiros e quaisquer partes envolvidas no tratamento e uso de informações relacionadas à empresa.

2. Objetivo

Esta Política de Segurança da Informação estabelece diretrizes e normas para assegurar a proteção dos ativos de informação da O2sistemas, promovendo um ambiente seguro e confiável que contribua para a continuidade e eficácia dos serviços prestados.

A PSI visa, ainda, reduzir o impacto de incidentes de segurança e fornecer uma base para a gestão adequada dos riscos de segurança da informação.

3. Princípios da segurança da informação

As diretrizes aqui estabelecidas são fundamentadas nos seguintes princípios:

- **Confidencialidade:** Garantia de que as informações serão acessadas apenas por pessoas autorizadas.
- **Integridade:** Proteção das informações contra alterações não autorizadas ou acidentais, garantindo sua exatidão e confiabilidade..
- **Disponibilidade:** Acesso contínuo e irrestrito às informações e sistemas necessários para o desempenho das atividades empresariais..

4. Âmbito de Aplicação

A Esta política se aplica a:

- Todos os colaboradores e terceirizados;
- Todos os sistemas, processos, dados e documentos;
- Equipamentos e infraestruturas físicas e tecnológicas utilizadas no tratamento da informação;
- Parceiros, fornecedores e prestadores de serviços que, de alguma forma, tenham acesso ou tratem informações da O2sistemas.

5. Diretrizes de Segurança da Informação

5.1 Controle de Acesso

O acesso aos sistemas e informações da O2sistemas será restrito, concedido apenas a usuários devidamente autorizados.

As informações são compartimentalizadas baseadas nas atribuições de cada pessoa.

Todas as contas de usuário devem possuir controle de identidade com senhas fortes e autenticação multifator, onde aplicável.

O nível de acesso será concedido com base no princípio do mínimo privilégio, garantindo que cada colaborador tenha acesso apenas às informações estritamente necessárias para o desempenho de suas funções.

5.2 Gestão de Ativos

Os ativos de informação (equipamentos, softwares, dados, documentos, entre outros) devem ser identificados, inventariados e classificados de acordo com seu valor e importância para a organização.

A responsabilidade pela proteção e uso adequado de cada ativo será atribuída a um gestor de ativos, que responderá pelo cumprimento das normas de segurança estabelecidas.

5.3 Classificação da Informação

As informações da O2sistemas serão classificadas de acordo com seu nível de criticidade e sensibilidade, podendo ser categorizadas como públicas, internas, confidenciais ou restritas.

Cada categoria terá normas específicas para manuseio, armazenamento e descarte seguro das informações, conforme diretrizes da empresa.

5.4 Proteção contra Ameaças e Vulnerabilidades

A O2sistemas adota medidas de segurança para proteger seus sistemas e informações contra ameaças internas e externas, ataques cibernéticos, vazamento de dados, roubo, acessos não autorizados e demais vulnerabilidades.

Entre as medidas estão o uso de firewalls, antivírus atualizados, controles de rede, bem como monitoramento contínuo para detecção e resposta a incidentes de segurança.

5.5 Uso Adequado dos Recursos de Informação

Todos os colaboradores, fornecedores e parceiros deverão fazer uso responsável e ético dos recursos tecnológicos e informacionais fornecidos pela O2sistemas. O uso dos ativos de TI deve estar de acordo com os propósitos organizacionais e com as políticas internas de segurança, sendo vedada a utilização para fins pessoais ou que estejam em desacordo com os valores e normas da empresa.

5.6 Gestão de Incidentes de Segurança

Todos os incidentes de segurança da informação devem ser reportados imediatamente à equipe responsável. A empresa dispõe de procedimentos específicos para a gestão e resposta a incidentes, incluindo detecção, análise, contenção, erradicação e recuperação, conforme as melhores práticas de gestão de incidentes.

5.7 Conformidade e Auditoria

A O2sistemas compromete-se a realizar auditorias periódicas e avaliações de conformidade para assegurar o cumprimento da PSI e identificar melhorias no ambiente de segurança da informação. As auditorias incluem a revisão das práticas, processos e controles, bem como a realização de testes de vulnerabilidade e auditorias de sistemas.

5.8 Treinamento e Conscientização

A empresa promoverá treinamentos periódicos para conscientizar seus colaboradores e parceiros sobre a importância da segurança da informação, incentivando boas práticas e fortalecendo a cultura de segurança no ambiente corporativo.

6. Responsabilidades

Colaboradores e Terceirizados: Responsáveis pelo uso adequado dos recursos de informação e pelo cumprimento das diretrizes estabelecidas nesta política.

Gestores: Devem assegurar que suas equipes compreendam e cumpram as normas de segurança da informação, atuando na gestão de acesso e proteção dos dados sob sua responsabilidade.

Área de Segurança da Informação: Responsável pela implementação, monitoramento e revisão desta política, bem como pelo tratamento de incidentes e pela realização de auditorias e treinamentos.

Parceiros e Fornecedores: Devem aderir às normas de segurança estabelecidas pela O2sistemase seguir as diretrizes de proteção de dados, mediante formalização contratual.

7. Consequências para o Não Cumprimento

O descumprimento das diretrizes desta política poderá resultar em medidas disciplinares e administrativas, que podem incluir advertências, suspensão ou até desligamento, dependendo da gravidade do incidente e da política interna de sanções da O2sistemas.

No caso de prestadores de serviço e terceiros, o descumprimento poderá resultar em penalidades contratuais e, quando aplicável, em sanções legais.

8. Revisão e Atualização da Política

A Política de Segurança da Informação será revisada periodicamente, pelo menos uma vez ao ano, ou sempre que se fizer necessário, a fim de manter sua eficácia e adequação às necessidades da O2sistemas e às legislações e regulamentações aplicáveis.

9. Disposições Finais

Esta Política de Segurança será de observância obrigatória por todos os colaboradores, parceiros, fornecedores e prestadores de serviços.

A conformidade com esta política visa garantir a proteção dos ativos de informação e a preservação da reputação e credibilidade da O2sistemas.