


POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Tipo	Política
		Versão	2.1
		Data	29/10/2024
Este documento faz parte do Sistema de Gerenciamento de Riscos da Ambipar Group			

1. APRESENTAÇÃO

A Ambipar atua em diversos segmentos para oferecer serviços e produtos completos voltados à gestão ambiental. Em franca expansão mundial, a Ambipar respeita as regras de compliance e responsabilidade socioambiental, prezando a ética e o pronto atendimento às demandas de seus clientes.

Sendo assim a política de segurança da Informação, também referida como PSI, é documento que orienta e estabelece as diretrizes corporativas da Ambipar para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários.

Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida internacionalmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

1. OBJETIVO

Este documento tem como objetivo garantir a confidencialidade, integridade, disponibilidade, legalidade, autenticidade e auditabilidade das informações da organização e de todos aqueles que fazem parte dela, tais como clientes, fornecedores, colaboradores e acionistas.

2. CAMPO DE APLICAÇÃO

Aplica-se a todos os administradores, funcionários, estagiários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento, ou com acesso a informações que pertençam a Ambipar ou a suas subsidiárias.

Todo e qualquer usuário de recursos computacionais da empresa tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

3. CONCEITOS

A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

- **Confidencialidade:** Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;
- **Disponibilidade:** Garante que a informação esteja disponível para as pessoas autorizadas sempre que se faça necessário;
- **Integridade:** Garante que a informação esteja completa e íntegra e que não tenha sido

modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

4. DA CRIAÇÃO DE PROCEDIMENTO ESPECÍFICO RELATIVO A ESTA POLÍTICA

A Ambipar manterá Procedimento Específico referente a esta Política contendo fluxo de procedimentos/processos e cautelas, observando os parâmetros e princípios estabelecidos nesta Política.

O PEPSI deverá ser aprovado por no mínimo 03 (três) diretores da Ambipar Participações e Empreendimentos S.A e conterá, dentre outros pontos:

1. Definições;
2. Classificação da Informação;
3. Responsabilidades;
4. Proteção de Dados Pessoais;
5. Política de senhas;
6. Tratamento/regras referentes a arquivos de Trabalho;
7. Tratamento/regras referentes a arquivos Pessoais;
8. Compartilhamento de Dados e Pastas;
9. Backup de arquivos;
10. Plano de Incidentes;
11. Uso da Internet com recursos providos pela Companhia;
12. Uso do Correio eletrônico;
13. Necessidade de novos sistemas/aplicativos ou equipamentos;
14. Impressão e outros;
15. Tecnologia com IA, cuidados a serem adotados;
16. Fake News e a responsabilidade no seu compartilhamento;
17. Uso de Antivírus;
18. Outros temas relevantes para a área de Tecnologia da Informação/Segurança da Informação;
19. Responsabilidades/alçadas para concessão de acessos;
20. Análise de riscos de segurança de dados e desenvolvimento na prática;
21. Plano de treinamentos sobre segurança de dados.

É dever de todos dentro da Ambipar:

Considerar a informação como sendo um ativo da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a Ambipar e deve sempre ser tratada profissionalmente.

É de responsabilidade do Diretor/Superintendente/ Gerente/Coordenador/Supervisor de cada área classificar a informação (relatórios, documentos, modelos, procedimentos, planilhas)

gerada por sua área de acordo com o nível de confidencialidade estabelecido neste documento.

São boas práticas:

- Bloquear o acesso ao computador sempre que sair da sua mesa de trabalho, mesmo que por alguns minutos;
- Manter mesas organizadas e documentos com informações confidenciais trancados, quando não os estiver utilizando.
- Não transmitir/compartilhar informações da Companhia sem autorização. Para maiores detalhes sobre o tema, indica-se a leitura conjunta da Política de Confidencialidade.

5. INTELIGÊNCIA ARTIFICIAL

O uso de Inteligência Artificial (IA) pela companhia deve estar em conformidade com as diretrizes de segurança da informação, protegendo dados e garantindo práticas éticas e seguras. A IA será utilizada em conformidade com as normas de proteção de dados, garantindo a privacidade das informações pessoais processadas ou verificadas.

Para maiores detalhes sobre o tema indicamos a leitura do PEPSI.

6. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA

É qualquer ato que:

- Qualquer conduta contrária as regras estabelecidas neste Política.
- Exponha a empresa a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados ou de informações ou ainda da perda de equipamento;
- Envolve a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos;
- Envolve o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

Qualquer conduta que possa resultar em vazamento de dados/informação não deve ser adotada e tampouco é permitida. A adoção de medidas estranhas ou contrárias a presente Política caracteriza falta grave passível de aplicação de penalidades e até mesmo rescisão motivada do Contrato de Trabalho ou Contrato de Parceria.

7. OUTROS

Qualquer outro assunto relacionado a Tecnologia da Informação/Segurança da Informação que não tenha sido abordado neste documento ou no PEPTI deverá ser informado ao Diretor de Tecnologia da Informação Corporativo para que orientações/diretivas sejam dadas.

8. PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave. O tratamento de eventual descumprimento deverá observar as regras previstas na Política de Tratamento de Denúncias e Gestão de Consequências.

9. VIGÊNCIA

O disposto no presente documento entrará em vigor na data de publicação do comunicado que o anunciar, sendo aprovada pelo Conselho de Administração.

AMBIPAR GROUP