POLITICA DE SEGURANÇA DA INFORMAÇÃO - PSI

[DPTI – Empresa xxxxxxxxxx]

INFORMAÇÕES DE CONTROLE DE DOCUMENTOS

Autor (Responsible)	**Head of IT / Líder TI / etc.**		
Dono (Accountable)	COO (Chief Operations Officer) / CIO / etc.		
Aprovado por	Conselho de Gestão (Management Board)		
Data Aprovação e Publicação	xx/xx/2020 / xx/xx/2021		
Público Alvo (Informed)	IT Dept.		
Políticas e Procedimentos Relacionados	PPD / PSI / PP / Código Conduta / Mapa do Fluxo de Dados		
Classificação de Segurança	Baixa ( )	Média ( )	Alta ( )

Controle de Revisões

Versão	Data	Responsável	Item/Escopo	Status *
1.0	01/03/2021	xxxxxxxxxxxxxxxxxx	Todo Documento	AP

*** INI (INICIADO) – AA / AP (AGUARDANDO APROVAÇÃO OU PUBLICAÇÃO) – PUB (PUBLICADO) – EXC (POLÍTICA EXCLUÍDA / DESATIVADA)**

ENVOLVIDOS (D-RACI)

Decision	Accountable	Responsible	Consulted	Informed
Todas as resoluções deste documento	COO	Head of IT	Conselho de Gestão, Líder de Gov. Corporativa, Líder de Finanças, Líder de RH e Gerencia de TI.	Todos os Colaboradores e demais envolvidos direta ou indiretamente

SUMARIO

TERMOS E DEFINIÇÕES

TI - Tecnologia da Informação.

DPTI - Departamento de Processos de Tecnologia da Informação.

CONFIDENCIALIDADE - Propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

INTEGRIDADE - Propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação.

DISPONIBILIDADE - Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

AUTENTICIDADE - Propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de alterações ao longo de um processo.

LEGALIDADE - Propriedade que garante que a informação respeita as legislações condizentes ao seu escopo de atuação.

CRIPTOGRAFIA - Processo de codificação de informações para que só o destinatário possa ler.

MIDIAS REMOVIVEIS - Dispositivos utilizados para o armazenamento e transporte de dados, tais como PenDrive, HD Externo, Cartão de Memória, DVDs, CDs, etc.

BACKUP - Refere-se à cópia de dados de um dispositivo para o outro com o objetivo de posteriormente recuperar estes dados, seja em caso eventual problema ou nas rotinas de simulação de incidentes. É também conhecido pelo termo “cópias de segurança”.

DISPOSITIVOS MÓVEIS - Quaisquer equipamentos eletrônicos portáteis para processamento de dados, armazenamento e comunicação, como: notebooks, tablets, smartphones, consoles portáteis, pendrive, tokens, entre outros.

E-MAIL - Meio de comunicação baseado no envio e na recepção de mensagens via rede de computadores, amplamente conhecido como correio eletrônico.

DATACENTER - Ambiente projetado para concentrar os equipamentos de processamento e armazenamento de dados de uma empresa.

CLOUD - Ambiente de infraestrutura de serviços de TI hospedados fora da organização, ou seja, em um fornecedor como: Amazon AWS, Microsoft Azure, Google Cloud, entre outros.

REDE – Conjunto de Equipamentos de comunicação que formam a Rede Física e Lógica por onde transitam os dados a serem processados.

LGPD – Lei Geral de Proteção de Dados Pessoais (13.709/2018)

INFORMAÇÃO SENSÍVEL – Qualquer tipo de informação ou de dados pessoais, física ou eletrônica que seja relacionada aos negócios e processos da Empresa (confidencial ou não).

1. Declaração de Política

A Gestão de Conformidades possui papel fundamental no contexto das organizações, interligando todos os processos da cadeia produtiva em vários setores, desde o nível operacional ao estratégico. Na [Empresa Template] (doravante denominada “Empresa”) o [Departamento de Processos de Tecnologia da Informação (DPTI)] em conjunto com a área de Compliance busca continuamente a efetiva utilização da informação como suporte às melhores práticas organizacionais no que tange aos seus processos e serviços, sempre assumindo que a transversalidade sobre vários eixos da organização atenda as exigências por agilidade, flexibilidade, continuidade, inovação e segurança.

Nesse contexto da segurança, o presente documento visa atender a busca por uma melhoria contínua nos processos e ferramentas para garantir a segurança da informação. Para alcançar esse resultado, este documento que é denominado como Política de Segurança da Informação (PSI), leva em consideração o melhor alinhamento possível entre as diretrizes estratégicas e o mapeamento de processos atuais da empresa, bem como as Políticas de Proteção aos Dados; logo, promovendo as mudanças planejadas com apoio total as decisões e as melhorias nos processos relativos a segurança da informação.

[nome responsável]

[função/cargo/papel]

2. Introdução

Segurança da informação é o termo que descreve o conjunto de controles utilizados para a proteção das informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade, autenticidade e legalidade, não estando a segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento.

Este documento estabelece um conjunto de diretrizes que possibilitam as partes interessadas da Empresa adotarem padrões de comportamento adequados com relação à utilização e preservação das informações. Foi elaborado pelo [DPTI] com base nas melhores práticas do mercado de TI.

2.1 Objetivo

A presente política tem por objetivo estabelecer e disseminar aos usuários as regras para utilização dos recursos de Tecnologia da Informação e orientá-los a utilizar esses recursos de maneira adequada, bem como estabelecer e definir os processos relacionados à segurança da informação no contexto operacional da organização.

Ademais, a Empresa entende que é estritamente essencial preservar as informações e processos tecnológicos em sua estrutura, sobretudo, quanto aos três principais atributos abaixo:

- **Integridade:** garantindo de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade**: garantindo de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade**: garantindo de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **Legalidade**: garantindo que a informação respeita as legislações condizentes ao seu escopo de atuação, principalmente, quanto à Legislação de Proteção de Dados Aplicável (LGPD).

2.2 Escopo

A Política de Segurança da Informação da Empresa aplica-se a todos os usuários, sejam eles colaboradores, prestadores de serviços, consultores, temporários e estagiários que estejam a serviço da instituição, incluindo toda a mão de obra terceirizada ou disponibilizada mediante convênios, parcerias ou quaisquer outras formas de atuação conjunta com outras empresas.

Para este documento, consideram-se recursos de Tecnologia da Informação equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pela Empresa.

As aplicações destas políticas também deverão ser implementadas no contexto "Default" das implementações operacionais da organização, conforme será visto no item 6 deste documento, bem como seguir as melhores práticas de segurança nos seguintes eixos de aplicação:

- Gerenciamento de Acesso e Identificação;
- Controles de Detecção;
- Proteção de Infraestrutura;
- Proteção de Dados (incluindo o PPD baseado na LGPD);
- Resposta a Incidentes.

2.3 Divulgação

A divulgação da política deve ser clara e ampla para que todos os usuários tenham acesso e possam compreendê-la.

3. Segurança da Informação

A informação da Empresa é um [illegible] protegido contra divulgação não autorizada, modificação [illegible] tomadas medidas prudentes para garantir que sua confidencialidade, integridade e disponibilidade não sejam comprometidas.

3.1 Classificação da Informação

A gestão da informação [illegible] tanto em âmbito interno como em âmbito externo. Entretanto, algumas informações [illegible] de sua geração, guarda, uso, transparência ou destruição – por seu imediatismo, conhecimento relacionado a projetos específicos e/ou provenientes dos sistemas de informação, diretórios de rede e banco de dados aos quais o usuário em geral tenha conhecimento por força das atividades profissionais – deverão ser tratadas como confidenciais e sigilosas.

A Política de Segurança da Informação é aplicável a todas as informações sob gestão da Empresa, incluindo aquelas que são:

- Armazenadas e transmitidas por meios eletrônicos (e-mail, sms, sites web, etc.);
- Armazenadas em qualquer tipo de mídia (pendrive, cartões de memória, dvd, cd, etc.);
- Transmitidas em conversas formais e informais;
- Impressas ou escrita em papel e/ou outros meios físicos similares;
- Geradas, recebidas, criadas e/ou tratadas no âmbito dos processos da organização;
- Demais informações relacionadas aos processos da Empresa.

A classificação da informação deverá ser realizada pelos Líderes de Setor (ou função compatível), e pelos colaboradores designados com esta atribuição. Entretanto, a responsabilidade pela atribuição do nível de classificação permanece com o Gestor Líder.