ORGANIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Histórico das Revisões

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Elaboração** | **Data** | **Revisão** | **Descrição** | **Aprovação** |
|  |  | 00 | Versão inicial |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. **OBJETIVO**

Estabelecer uma estrutura definida, aprovada e compreendida para a implementação, operação e gestão da segurança da informação e privacidade dentro da CLIENTEX através de papéis e responsabilidades alocados de acordo com as necessidades da empresa, em consonância com a Política de Segurança da Informação e Política de Privacidade da CLIENTEX e conforme definido nas normas ABNT NBR ISO/IEC 27001 e 27002, específicas para melhores práticas relacionadas à segurança da informação, conforme as normas ABNT NBR ISO/IEC 27701, 27018, 29100 e 29151, específicas para melhores práticas relacionadas privacidade juntamente com a norma ABNT NBR ISO/IEC 31000 específica para gestão de riscos

1. **JUSTIFICATIVA**

A estrutura da organização de segurança da informação e privacidade da CLIENTEX busca o comprometimento da direção da empresa conforme recomendado pelas normas ABNT ISO referenciadas e por se tratar de um tema corporativo envolvendo aspectos físicos, tecnológicos e humanos que sustentam a operação do negócio.

Assim sendo torna-se condição *sine qua non*, o apoio TOP DOWN, ou seja, mobilizando e envolvendo primeiramente a diretoria para depois atingir os demais níveis na hierarquia e todos os processos distribuídos da empresa.

1. **ORGANOGRAMA DE SI**

A estrutura da organização de segurança da informação da CLIENTEX deve obedecer ao seguinte organograma:

Relógio digital com números

Descrição gerada automaticamente com confiança baixa

1. **CARGOS – FUNÇÕES – RESPONSABILIDADES**

|  |  |  |
| --- | --- | --- |
| **Cargo/Função** | **Composição** | **Responsabilidades** |
| **Diretor de Segurança da Informação** | Profissional interno | * Definir e garantir a aderência da empresa às diretrizes de SI; * Assegurar que as metas da segurança da informação estão identificadas, e que atendem aos requisitos da organização e estão integradas aos processos relevantes da empresa; * Formular e aprovar a PSI; * Analisar a eficácia da implementação da PSI; * Fornecer os recursos necessários e claro direcionamento para a implantação da SI; * Aprovar as atribuições de tarefas e responsabilidades; |
| **Coordenador de Segurança da Informação** | Profissional interno | * Garantir que as atividades de SI são executadas conforme a PSI; * Identificar como conduzir as não-conformidades; * Avaliar a adequação e coordenar a implementação dos controles de SI; * Mapear e identificar as ameaças significativas ao ambiente e riscos de exposição da informação; * Identificar a necessidade de uma consultoria especializada em SI, seja estabelecida e disponibilizada dentro da organização; * Iniciar planos e programas para manter a conscientização da SI; * Garantir a conscientização de todos os funcionários e terceiros. |
| **Encarregado de Dados ou DPO** | Profissional com autonomia independente dentro da empresa  **(interno ou terceirizado)** | Baseado na norma ABNT ISO/IEC 27701 convém a este profissional:   * Centralizar e estar envolvido **em todas as questões relacionadas à privacidade e tratamento de dados pessoais**; * Buscar continuamente especialização na legislação, regulamentação e prática de proteção de dados; * Atuar como ponto de contato junto às autoridades de supervisão; * Receber comunicações da autoridade nacional (ANPD) e tomar providências; * Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e tomar providências; * Orientar funcionários e contratados sobre boas práticas referente à proteção de dados pessoais; * Coordenar desenvolvimento de procedimentos internos sobre qualquer tipo de tratamento de dados de forma correta. * Fornecer orientações em relação às avaliações de impacto de privacidade. |
| **Gerente de Tecnologia da Informação** | Profissional interno | * Garantir que as atividades de TI são executadas conforme diretrizes estabelecidas pela Coordenação de SI; * Assegurar a atualização dos ativos de TI da empresa; * Gerenciar vulnerabilidades do ambiente; * Realizar manutenções no ambiente conforme PSI e demais políticas internas relacionadas; * Apoiar a Coordenação na aplicação de controles de SI no ambiente tecnológico. |
| **Gestores** | USUÁRIOS responsáveis pelas diversas áreas da empresa | * Garantir a utilização dos ativos conforme regras definidas garantindo assim a sua proteção; * Assegure um adequado tratamento quando o ativo é excluído ou destruído; * Reportar os incidentes de SI e Violação de Privacidade. |
| **Comitê de SI e Privacidade** | 1. Diretor de SI 2. Coordenador de SI 3. Gerente de TI 4. Diretora Adm   (São exemplos e sugestões) | * Aprovar as metodologias e processos para SI e privacidade; * Avaliar a adequação e coordenar a implementação dos controles de SI e privacidade; * Avaliar as informações recebidas do monitoramento e da análise crítica dos incidentes de SI e privacidade, e recomendar ações apropriadas como respostas. |
| **Assessoria em SI** | Empresa terceirizada a ser definida pela Direção de SI | * Orientar adequadamente a CLIENTEX quando acionado; * Apoiar o time de resposta para casos em que exista Incidentes de Segurança ou Violação de Privacidade; * Outras funções e responsabilidades definidas pelo Comitê de Segurança da Informação. |
| **Assessoria Jurídica** | Empresa terceirizada com profissionais especializados em direito digital, a ser definida pela Direção de SI | * Orientar adequadamente a CLIENTEX quando acionado para casos e/ou situações que envolvam processos jurídicos. |

1. **PERIODICIDADE**

Cabe à direção da CLIENTEX revisar periodicamente este procedimento e avaliar a adequação, suficiência e eficácia dos procedimentos aqui definidos.