Política Institucional de Segurança da Informação e Privacidade de Dados

Informação Pública

Diretoria Executiva

Segurança da Informação

Controle e Histórico

Versão	Data	Autor(es) / Área	Motivo da Revisão	Revisor(es) / Área	Aprovador(es) / Área
0.1	11/08/2020	PG Advogados/ **DPO** - Operações	Criação do documento Política de Segurança da Informação	Carlos Renato P. Olivo/ **Segurança da Informação**	Carolina Schmid / **Chief Operations –** Jorge Pacca**/Presidência**
1.0	18/08/2020	PG Advogados/ **DPO** – Comitê Segurança da Informação	Revisão e Publicação do documento Política de Segurança da Informação	Carlos Renato P. Olivo/ **Segurança da Informação**	Carolina Schmid / **Chief Operations –** Jorge Pacca**/Presidência**
2.0	27/04/2023	Carlos Renato P. Olivo/ **Segurança da Informação**	Revisão e Publicação do documento Política de Segurança da Informação	Carlos Renato P. Olivo/ **Segurança da Informação**	Carolina Schmid / **Chief Operations –** Jorge Pacca**/Presidência**
3.0	04/05/2023	Peck Advogados/ **DPO**	Revisão e Publicação do documento Política de Segurança da Informação	Carlos Renato P. Olivo/ **Segurança da Informação**	Carolina Schmid / **Chief Operations –** Jorge Pacca**/Presidência**
4.0	12/12/2023	Peck Advogados/ **DPO**	Revisão e Publicação do documento Norma de Classificação de Informação	Carlos Renato P. Olivo/ **Segurança da Informação**	Carolina Schmid / **Chief Operations –** Jorge Pacca**/Presidência**
5.0	02/02/2024	Peck Advogados/ **DPO** - Carlos Renato P. Olivo/ **Segurança da Informação**	Revisão e Publicação do documento Norma de Classificação de Informação	Carlos Renato P. Olivo/ **Segurança da Informação**	Carolina Schmid / **Chief Operations –** Jorge Pacca**/Presidência**
6.0	09/10/2025	Carlos Renato P. Olivo/ **Segurança da Informação** Marcelo Terentin/**Segurança da Informação**	Adequação ao modelo institucional de normativos, atualização conforme as normas ISO/IEC 27001:2022 e 27701:2019, e consolidação das diretrizes estratégicas do SGSIP	Comitê de Segurança e Privacidade	Carolina Schmid / **Presidência**

Sumário

1. Introdução

As informações são ativos estratégicos indispensáveis à operação, reputação e continuidade da **Cleartech**. A proteção desses ativos, em conjunto com o respeito à privacidade, representa um compromisso institucional permanente.

Esta Política estabelece os princípios, compromissos e diretrizes gerais que orientam a **Cleartech** na implementação de controles, condutas e estruturas voltadas à segurança da informação e à proteção de dados pessoais.

A **Cleartech** reconhece que a efetividade da segurança não depende apenas de soluções técnicas, mas da atuação conjunta de processos, pessoas e tecnologia, com envolvimento ativo da alta direção, colaboradores e parceiros.

A Política de Segurança da Informação conta com o apoio integral da alta direção, que se compromete a promover uma cultura de segurança e a alocar os recursos necessários para sua implementação efetiva. É responsabilidade de todos, independentemente de cargo ou função, estarem cientes e cumprirem esta Política de Segurança da Informação, aplicando-a de forma consistente em suas atividades diárias e promovendo sua disseminação.

2. Objetivo

Formalizar o compromisso institucional da **Cleartech** com a proteção das informações, o respeito à privacidade e o fortalecimento da cultura de segurança organizacional.

Por meio deste instrumento, a **Cleartech** estabelece diretrizes estratégicas, princípios orientadores e responsabilidades institucionais que sustentam o funcionamento eficaz do Sistema de Gestão de Segurança da Informação e Privacidade (SGSIP).

Esta Política contribui para o alcance dos objetivos do SGSIP, como: assegurar a confidencialidade, integridade, disponibilidade e conformidade no tratamento de informações institucionais e dados pessoais

A política também busca assegurar que todos os colaboradores, parceiros e partes interessadas conheçam e cumpram os padrões de conduta, as práticas de proteção e os requisitos legais e contratuais aplicáveis à segurança e à privacidade no contexto das atividades organizacionais.

3. Abrangência

Aplica-se a todas as áreas, unidades organizacionais, processos, sistemas, ativos informacionais, pessoas e tecnologias sob responsabilidade ou controle da **Cleartech**, em qualquer ambiente físico ou lógico onde a organização atue.

Seu escopo inclui:

- Todos os colaboradores, terceiros, prestadores de serviço, parceiros, fornecedores, representantes e quaisquer outras partes que tenham acesso a informações, sistemas ou ativos da **Cleartech**;
- Todas as informações geradas, armazenadas, processadas ou transmitidas, em qualquer meio, formato ou suporte, incluindo dados pessoais e informações sensíveis;
- Infraestrutura tecnológica, sistemas corporativos, ambientes em nuvem, redes internas, dispositivos móveis e demais recursos de tecnologia da informação e comunicação utilizados nas operações da **Cleartech**.

Atividades realizadas presencialmente ou em regime remoto, incluindo o uso de dispositivos pessoais autorizados (BYOD) ou acesso remoto a sistemas da **Cleartech**.

O cumprimento das diretrizes estabelecidas nesta política é obrigatório e constitui responsabilidade direta das lideranças e de todos os envolvidos no tratamento da informação. As orientações específicas para cada tema abordado são complementadas por normas, procedimentos e demais instrumentos normativos do SGSIP.

As empresas controladas pela **Cleartech** devem, com base nesta Política, definir seus direcionamentos internos, considerando suas especificidades operacionais, exigências legais e regulatórias, garantindo aderência aos princípios do SGSIP.

4. Abreviações e Definições

Ameaça: Evento ou agente com potencial de causar impacto negativo à organização;

Ativo: Qualquer recurso com valor para a **Cleartech**, que requer proteção adequada;

Ativo Intangível: Recurso de valor não físico, como dados, imagem, marca ou conhecimento;

Autenticidade: Garantia de que a informação é fidedigna e atribuível ao seu emissor;

Backup: Cópia de segurança da informação, usada para recuperação em caso de perda ou falha;

CIDLA: Acrônimo dos princípios de segurança: Confidencialidade, Integridade, Disponibilidade, Legalidade e Autenticidade;

CISO: *Chief Information Security Officer* – responsável pela liderança da área de Segurança da Informação;

Colaborador: Pessoa com vínculo profissional com a **Cleartech**, incluindo terceiros e prestadores;

Confidencialidade: Acesso restrito à informação apenas por indivíduos autorizados;

CSIP: Comitê de Segurança da Informação e Privacidade – órgão de governança multidisciplinar do SGSIP;

DPO: *Data Protection Officer* – Encarregado pelo Tratamento de Dados Pessoais, conforme a LGPD;

Disponibilidade: Garantia de que a informação estará acessível quando necessário;

Gestor da informação: Responsável pela gestão do ciclo de vida da informação, incluindo classificação e controle de acesso;

Identidade Digital: Conjunto de credenciais que identificam um usuário em sistemas eletrônicos;

Incidente de Segurança da Informação: Evento que compromete ou ameaça à segurança das informações;

Informação: Conjunto de dados com valor organizacional, em qualquer suporte ou formato;

Integridade: Garantia de que as informações estejam íntegras e sem alterações não autorizadas durante o seu ciclo de vida;

Legalidade: Adesão às normas e leis vigentes no tratamento da informação;

PSI: Política de Segurança da Informação;

Recursos de Tecnologia da Informação: Infraestrutura física e lógica utilizada no tratamento da informação;

Risco: Probabilidade de uma ameaça causar impacto negativo;

SGSIP: Sistema de Gestão de Segurança da Informação e Privacidade, estrutura que integra políticas, controles e processos;

Violação: Descumprimento das regras previstas nos normativos da **Cleartech**.

5. Princípios e Diretrizes Gerais

A **Cleartech** adota princípios que norteiam a proteção da informação e a preservação da privacidade, em consonância com seus valores organizacionais e com a legislação aplicável.

O Sistema de Gestão de Segurança da Informação e Privacidade (SGSIP) está fundamentado nos pilares da confidencialidade, integridade e disponibilidade, assegurando que os dados e ativos informacionais sejam acessados, utilizados e protegidos de forma apropriada ao seu valor e sensibilidade.

As informações tratadas no âmbito das atividades da **Cleartech** são reconhecidas como ativos institucionais e devem ter sua propriedade formalmente atribuída, com responsabilidades relacionadas à classificação, uso e proteção.

A **Cleartech** assegura a proteção dos direitos de propriedade intelectual relacionados aos seus ativos informacionais, incluindo conteúdos técnicos, marcas e licenças.

Colaboradores, prestadores de serviço e parceiros têm o dever de respeitar o sigilo profissional, zelando pela confidencialidade das informações acessadas no exercício de suas funções.

A comunicação sobre segurança e privacidade deve seguir diretrizes formais, assegurando que as informações relevantes cheguem tempestivamente às partes interessadas internas e externas, conforme suas atribuições e responsabilidades.

As diretrizes apresentadas nas seções seguintes detalham a aplicação desses princípios, estruturadas conforme os domínios organizacionais de segurança da informação e privacidade cobertos pelo SGSIP.

5.1 Responsabilidades por Segurança da Informação

A **Cleartech** define e atribui responsabilidades de segurança da informação aos colaboradores e áreas, de forma a assegurar que a proteção dos ativos e o cumprimento das políticas e normas sejam devidamente aplicados.

As responsabilidades incluem:

- Cumprimento das políticas, normas, procedimentos e instruções de segurança da informação;

- Proteção dos ativos sob sua responsabilidade, de acordo com os níveis de classificação e controles aplicáveis;
- Comunicação imediata de incidentes ou fragilidades de segurança identificadas;
- Apoio às ações de melhoria contínua do Sistema de Gestão da Segurança da Informação e da Privacidade (SGSIP).

Essas responsabilidades são formalmente estabelecidas, comunicadas e revisadas periodicamente, garantindo clareza de papéis e deveres dentro da organização. Gestão de Ativos e Classificação da Informação

5.2 Gestão de Ativos e Classificação da Informação

5.2.1 Gestão de Ativos

A **Cleartech** deve manter um inventário atualizado de ativos informacionais críticos, com identificação de seus respectivos proprietários e classificação de acordo com o valor, a sensibilidade e a criticidade dos ativos. Esses ativos devem ser protegidos ao longo de todo o seu ciclo de vida, incluindo aquisição, uso, armazenamento, manutenção, transferência e descarte.

A manutenção, atualização ou correção de falhas técnicas deve ser realizada exclusivamente pelas áreas técnicas responsáveis, com registros apropriados e validação dos controles de segurança. O ciclo de vida dos ativos, desde a aquisição até o descarte, deve seguir práticas seguras, incluindo procedimentos adequados de descarte ou reutilização, conforme os requisitos estabelecidos pela **Cleartech** e pelas normas aplicáveis.

5.2.2 Classificação da Informação

A **Cleartech** estabelece um modelo institucional de classificação da informação com o objetivo de garantir a aplicação de medidas de segurança proporcionais ao grau de sensibilidade, valor e criticidade dos dados e ativos informacionais.

A classificação deve acompanhar todo o ciclo de vida da informação, da criação ao descarte e o controle de acesso. Sua aplicação deve estar formalmente definida conforme os papéis e responsabilidades descritos nos normativos complementares da organização.

5.3 Controles de Acesso e Identidade

A **Cleartech** controla o acesso físico e lógico aos seus ambientes, ativos e informações, adotando práticas que asseguram a proteção contra acessos não autorizados. Cada

colaborador deve possuir uma identidade digital individual, intransferível e, sempre que aplicável, de conhecimento exclusivo, sendo responsável por seu uso, proteção e sigilo. É expressamente vedado o compartilhamento, armazenamento, replicação, publicação ou qualquer uso indevido de credenciais próprias ou de terceiros.

A fim de garantir a eficácia desses controles, a **Cleartech** adota os princípios do menor privilégio (*least privilege*) e da real necessidade de conhecimento (*need to know*) na definição dos acessos. Adicionalmente, será exigida, sempre que possível, a utilização de autenticação multifator (MFA) para acesso a sistemas sensíveis, bem como a revisão periódica das permissões concedidas, visando assegurar a conformidade com os critérios de segurança estabelecidos.

5.4 Uso Aceitável de Recursos e Ativos de TIC (Tecnologia de Informação e Comunicação)

Os recursos de TIC fornecidos ou gerenciados pela **Cleartech** devem ser utilizados exclusivamente para fins profissionais, em conformidade com os normativos internos, respeitando os princípios éticos, legais e de segurança da informação.

É vedado o uso de dispositivos, repositórios ou canais de comunicação não autorizados para armazenamento, transmissão ou tratamento de informações corporativas.

O uso da internet e do correio eletrônico deve ocorrer exclusivamente por meios homologados, com responsabilidade e dentro dos limites definidos, visando à segurança, à produtividade e a proteção da imagem institucional.

A **Cleartech** adota práticas de mesa limpa e tela limpa, além de implementar controles destinados a assegurar o uso adequado dos ambientes de trabalho físico e digital.

O uso de dispositivos pessoais (BYOD) para acesso aos sistemas ou dados da **Cleartech** está sujeito à autorização formal e ao cumprimento dos requisitos mínimos de segurança.

5.5 Comportamento e Conduta Digital

O registro ou compartilhamento de imagens, áudios ou vídeos nas dependências da **Cleartech** sem autorização formal pode comprometer a confidencialidade das operações e a privacidade de colaboradores. Situações dessa natureza são reguladas por normativos específicos, devendo os colaboradores observarem rigorosamente as diretrizes vigentes sobre uso aceitável, conduta e proteção da informação.

O uso de mídias sociais em nome da **Cleartech** deve ocorrer exclusivamente quando expressamente necessário e autorizado, restrito a colaboradores cujas funções incluam essa atividade.

É proibida a publicação ou o compartilhamento de informações da **Cleartech** em redes sociais sem autorização prévia e formal. Todos os colaboradores devem agir com ética, discrição e responsabilidade, assegurando que suas manifestações pessoais não comprometam a imagem institucional, nem revelem informações operacionais, rotinas internas ou dados sensíveis.

O dever de preservar o sigilo profissional aplica-se igualmente a conteúdos publicados em plataformas digitais, permanecendo vigente mesmo após o desligamento.

5.6 Código de Conduta e Ética

O Código de Conduta e Ética da Cleartech estabelece princípios de integridade, respeito, responsabilidade e transparência nas relações profissionais. Define condutas intoleráveis, como vazamento de informações, assédio e práticas ilícitas, passíveis de sanções disciplinares. Todos os colaboradores devem conhecer e cumprir suas diretrizes, incluindo aquelas relacionadas à segurança da informação e privacidade, promovendo um ambiente ético e seguro. O descumprimento pode resultar em advertências, rescisões contratuais e sanções legais proporcionais a sua gravidade, avaliadas e aplicadas pelo Comitê de Ética.

5.7 Segurança Física e Ambiental

A **Cleartech** deve proteger seus ativos físicos e instalações críticas por meio da definição de perímetros de segurança e da implementação de controles compatíveis à criticidade das operações.

O acesso físico a áreas sensíveis deve ser restrito a pessoas formalmente autorizadas, com autenticação individual, rastreabilidade e mecanismos de monitoramento.

Medidas adicionais de proteção física podem incluir sistemas de controle de acesso, sensores ambientais e mecanismos de gestão de visitantes. A eficácia desses controles deve ser revisada periodicamente, considerando os riscos físicos, ambientais e operacionais.

As diretrizes operacionais específicas estão descritas em normas e procedimentos complementares da **Cleartech**.

5.8 Segurança no Trabalho Híbrido e Remoto

A **Cleartech** estabelece diretrizes institucionais para garantir que o trabalho híbrido e remoto seja conduzido com o mesmo nível de proteção aplicável às atividades presenciais. O cumprimento das políticas de Segurança da Informação e Privacidade é obrigatório em qualquer modalidade de trabalho, sendo responsabilidade do colaborador assegurar a confidencialidade, integridade e disponibilidade das informações corporativas e quaisquer incidentes ou não conformidades devem ser imediatamente comunicado pelos canais oficiais de reporte

São princípios aplicáveis:

- Utilização exclusiva de dispositivos corporativos ou devidamente autorizados, em conformidade com a Política de BYOD e com os controles técnicos exigidos;
- Adoção de conexões seguras, com uso obrigatório de VPN, autenticação multifator (MFA) e criptografia de dados em trânsito e em repouso;
- Manutenção de ambientes físicos adequados e seguros durante o trabalho remoto, com prevenção contra acessos não autorizados e observância das práticas de mesa limpa e tela limpa;
- Cumprimento integral das políticas, normas e procedimentos corporativos de segurança da informação e privacidade, independentemente do local de execução das atividades;
- Responsabilidade do colaborador em zelar pela proteção de credenciais, ativos e informações corporativas;
- Observância das normas de ergonomia e saúde ocupacional previstas em regulamentos internos e legislação aplicável, garantindo condições seguras de trabalho.

5.9 Segurança em Ambientes em Nuvem

A **Cleartech** deve adotar práticas seguras e controles específicos para proteção de ambientes em nuvem, observando os princípios de responsabilidade compartilhada, proteção de dados, controle de acesso, criptografia e conformidade regulatória.

A contratação de provedores deve seguir critérios rigorosos para seleção, contratação e monitoramento contínuo assegurando conformidade com normas e regulamentos internacionais aplicáveis, tais como ISO/IEC 27001, ISO/IEC 27701, a Lei Geral de Proteção de Dados Pessoais e o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR).

Adicionalmente, a **Cleartech** deve implementar controles técnicos apropriados, tais como criptografia de dados em repouso e em trânsito, gestão segura de configurações, segregação lógica e física dos ambientes, além de auditorias periódicas para assegurar a conformidade e eficácia dos controles estabelecidos

5.10 Segurança no Desenvolvimento de Sistemas Aquisição de Softwares e Gestão de Ciclo de Vida

O desenvolvimento, aquisição e integração de softwares na **Cleartech** devem incorporar requisitos de segurança desde as fases iniciais do ciclo de vida, assegurando a prevenção de vulnerabilidades e a conformidade com normas, contratos e exigências regulatórios.

Todos os sistemas, sejam internos ou de terceiros, devem ser avaliados quanto aos seus impactos sobre a segurança da informação e submetidos a validações apropriadas antes de entrarem em operação.

A **Cleartech** adota práticas seguras de desenvolvimento, incluindo a integração de requisitos de segurança ao ciclo de vida de sistemas, capacitação contínua das equipes técnicas e validações formais antes da liberação para ambientes produtivos.

5.11 Gestão de Vulnerabilidade e Patches

5.11.1 Análise de Vulnerabilidades Técnicas

A **Cleartech** deve manter um processo estruturado para identificar, analisar e tratar vulnerabilidades técnicas, alinhado à estratégia de segurança da informação e ao SGSIP. vulnerabilidades devem ser identificadas de forma contínua, classificadas conforme sua criticidade e tratadas com base em critérios de impacto, exposição e relevância dos ativos afetados.

5.11.2 Gestão de Patches e Atualizações de Segurança

A **Cleartech** mantém um processo formalizado para aplicação de atualizações de segurança (patches) em sistemas, aplicações e equipamentos sob sua responsabilidade. Essas atualizações devem ser priorizadas conforme critérios de criticidade e impacto operacional, seguindo prazos definidos internamente.

A aplicação dos patches deve ser registrada, monitorada e auditada periodicamente, em conformidade com as boas práticas e os requisitos regulatórios aplicáveis.

5.12 Gestão de Incidentes de Segurança e Privacidade

A **Cleartech** mantém um processo estruturado para a gestão de incidentes de segurança da informação, com o objetivo de garantir a identificação, resposta, recuperação e prevenção de eventos que comprometam a confidencialidade, integridade, disponibilidade ou privacidade das informações.

Todos os incidentes relevantes devem ser prontamente reportados pelos canais oficiais disponibilizados pela **Cleartech** e tratados conforme critérios e responsabilidades estabelecidos em normativo específico.

Os incidentes são analisados pela equipe de Segurança da Informação e, quando necessário, escalados ao Comitê de Segurança da Informação e Privacidade e à Alta Direção.

Quando envolverem dados pessoais, devem ser avaliados em conjunto com o Encarregado (DPO), garantindo a observância das obrigações legais e regulatórias, incluindo a notificação aos titulares e às autoridades competentes, conforme previsto na LGPD.

5.13 Continuidade de Negócios e Recuperação de Desastres

Os procedimentos de gestão da Continuidade de Negócios da **Cleartech** devem ser implementados em conformidade com os requisitos do Sistema de Gestão de Segurança da Informação e Privacidade (SGSIP), assegurando a disponibilidade, integridade e confidencialidade das informações críticas. Esses procedimentos abrangem planos de resposta, recuperação e restauração, conforme definidos no **Plano de Continuidade de Negócios (PCN)** e no **Plano de Recuperação de Desastres (PRD)**, garantindo a resiliência dos serviços essenciais e a retomada tempestiva das operações em cenários de interrupção.

A **Cleartech** deve manter e atualizar procedimentos estruturados para garantir a continuidade dos processos críticos de negócio e a recuperação tempestiva da infraestrutura tecnológica, em conformidade com os requisitos do Sistema de Gestão de Segurança da Informação e Privacidade (SGSIP).

5.14 Salvaguarda (backup)

A **Cleartech** deve assegurar a existência de mecanismos de salvaguarda (backup) das informações críticas, como parte integrante das estratégias de continuidade de negócios e recuperação de desastres.

Esses mecanismos devem garantir a disponibilidade e integridade dos dados essenciais, respeitando os requisitos legais e operacionais aplicáveis, e alinhando-se ao Plano de Continuidade de Negócios (PCN) e ao Plano de Recuperação de Desastres (PRD), de forma a viabilizar a restauração segura e oportuna das operações em caso de falhas ou interrupções relevantes.

5.15 Segurança na Gestão de Colaboradores, Terceiros e Fornecedores

A **Cleartech** deve assegurar que colaboradores, prestadores de serviço e fornecedores cumpram os requisitos de segurança desde o início de seu relacionamento com a organização até seu desligamento. Isso inclui verificações prévias, assinatura de termos de confidencialidade, concessão de acessos conforme o perfil funcional e orientação sobre o uso seguro das informações e sistemas.

Todos os terceiros com acesso a ativos da **Cleartech** devem estar vinculados a contratos com cláusulas de segurança, privacidade e conformidade legal. A **Cleartech** deve avaliar riscos associados a fornecedores, exigir controles compatíveis com o nível de criticidade dos serviços prestados e supervisionar a adesão às exigências contratuais e normativas aplicáveis.

As responsabilidades específicas e os critérios detalhados para qualificação, controle e monitoramento estão descritos em normativos complementares, incluindo as normas de segurança para dispositivos de terceiros, gestão de acessos e gestão de contratos com fornecedores.

5.16 Privacidade e Proteção de Dados Pessoais

A **Cleartech** assegura que o tratamento de dados pessoais seja realizado em conformidade com a Lei Geral de Proteção de Dados (LGPD) e demais legislações aplicáveis, bem como alinhado às melhores práticas internacionais. O tratamento observa os princípios de finalidade, adequação, necessidade, transparência, segurança e responsabilização, assegurando que os dados sejam utilizados apenas para propósitos legítimos e informados.

A governança de privacidade inclui a designação de Encarregado pelo Tratamento de Dados Pessoais (DPO), responsável por orientar a organização, apoiar a resposta a incidentes e interagir com titulares e autoridades competentes.

A **Cleartech** limita o tratamento de dados pessoais ao mínimo necessário e fundamentado em bases legais apropriadas, garantindo que transferências

internacionais ocorram apenas quando houver proteção adequada. Medidas técnicas e organizacionais são aplicadas para prevenir acessos não autorizados, alterações indevidas, perda ou destruição de dados, incluindo rotinas de retenção, descarte seguro e revisões periódicas de controles.

A organização assegura aos titulares o exercício pleno de seus direitos, como acesso, correção, exclusão, portabilidade e revogação do consentimento, disponibilizando canais de comunicação específicos para esse fim.

Colaboradores e prestadores de serviços participam de treinamentos regulares sobre privacidade e proteção de dados, fortalecendo a cultura organizacional de conformidade.

5.17 Gestão de Mudanças

A **Cleartech** deve assegurar que mudanças com impacto potencial na segurança da informação, privacidade ou funcionamento do SGSIP, incluindo alterações em ativos, processos, sistemas, controles ou requisitos legais, sejam avaliadas, autorizadas e implementadas de forma controlada.

O processo deve considerar riscos, envolver partes interessadas e prever, quando necessário, medidas de mitigação, validação e comunicação.

6. Papéis e Responsabilidades

A **Cleartech** adota uma estrutura de governança integrada para o Sistema de Gestão da Segurança da Informação e Privacidade (SGSIP), com responsabilidades distribuídas conforme os seguintes papéis:

6.1 Alta Direção

- Demonstrar comprometimento institucional com esta Política e com o SGSIP;
- Aprovar diretrizes, exceções, investimentos e recursos necessários para a segurança e privacidade da informação;
- Promover o alinhamento do SGSIP à estratégia e cultura organizacional, assegurando os recursos necessários à sua eficácia, resiliência e aprimoramento contínuo.

6.2 CISO – Chief Information Security Officer

- Definir e liderar a estratégia institucional de segurança da informação, alinhando-a aos objetivos organizacionais e às demandas de negócio;

- Coordenar o Sistema de Gestão da Segurança da Informação e Privacidade (SGSIP), com apoio do Comitê de Segurança e Privacidade, garantindo sua efetividade, coerência e atualização contínua;
- Avaliar e tratar riscos relacionados à segurança da informação, propondo medidas corretivas e preventivas;
- Apoiar auditorias internas e externas, assegurando a conformidade com os normativos de Segurança e Privacidade;
- Avaliar e aprovar formalmente exceções à Política de Segurança da Informação (PSI), quando justificadas e documentadas.

6.3 DPO – Encarregado pelo Tratamento de Dados Pessoais

- Coordenar o Sistema de Gestão da Privacidade da Informação (SGPI), assegurando sua aderência à LGPD e à ISO/IEC 27701;
- Avaliar riscos e apoiar a resposta a incidentes de privacidade e a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais;
- Promover a conformidade legal no tratamento de dados pessoais e atuar como canal de comunicação com titulares e autoridades.

6.4 Comitê de Segurança da Informação e Privacidade

- Apoiar a coordenação dos sistemas de gestão de segurança da informação e privacidade, contribuindo para sua efetividade e participando da avaliação de seus resultados e da implementação de melhorias contínuas;
- Participar do processo de elaboração, revisão e atualização das políticas, normas e procedimentos relacionados à segurança da informação, assegurando sua aderência às diretrizes organizacionais, requisitos legais e normas aplicáveis;
- Apoiar a identificação, avaliação e tratamento de riscos relacionados à segurança da informação e à privacidade de dados;
- Apoiar auditorias internas e externas, assegurando a conformidade com os normativos de Segurança e Privacidade;
- Garantir o engajamento dos colaboradores nas ações de capacitação e conscientização sobre segurança da informação e privacidade, promovendo a cultura organizacional de proteção dos dados.

6.5 Demais Áreas de Operações, Administração e Suporte

- Implementar controles técnicos e organizacionais sob sua responsabilidade, conforme os normativos do SGSIP e as diretrizes corporativas de segurança e privacidade;
- Integrar os requisitos de segurança da informação e proteção de dados pessoais aos processos, contratos, infraestrutura e gestão de pessoas, assegurando sua efetividade no contexto operacional;
- Apoiar os processos de gestão de mudanças, capacitação, tratamento de incidentes e conformidade legal, contribuindo para a maturidade e resiliência do SGSIP;
- Assegurar a aplicação das diretrizes e controles de segurança e privacidade nas atividades sob sua gestão, incluindo a correta classificação, proteção, rastreabilidade e controle dos ativos informacionais em todas as fases do seu ciclo de vida, promovendo a conformidade, a mitigação de riscos e o alinhamento às políticas institucionais.

6.6 Colaboradores

- Estar ciente e manter-se atualizado com esta Política de Segurança da Informação e Privacidade e demais documentos complementares;
- Cumprir a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais;
- Proteger suas credenciais e reportar prontamente e formalmente quaisquer suspeitas ou eventos de violação a área de Segurança da Informação;
- Utilizar ativos e informações com ética, responsabilidade e de acordo com os critérios de segurança e privacidade definidos;
- Cumprir esta Política, demais normativos relacionados e legislações vigentes, incluindo aquelas relacionadas às suas atividades profissionais.

7. Referências Normativas

7.1 Normas Internacionais

- **ISO/IEC 27001:2022:** Sistemas de Gestão de Segurança da Informação – Requisitos;
- **ISO/IEC 27002:2022:** Código de Prática para Controles de Segurança da Informação;

- **ISO/IEC 27701:2019:** Extensão à ISO/IEC 27001 e 27002 para Gestão da Privacidade da Informação – Requisitos e Diretrizes.

7.2 Normativos Corporativos

- A **Cleartech** mantém normativos internos complementares que detalham os controles de segurança, privacidade, continuidade e governança previstos nesta Política. Esses documentos incluem normas, procedimentos, planos e instruções aplicáveis ao SGSIP, assegurando a operacionalização das diretrizes aqui estabelecidas.

7.3 Legislação Brasileira

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei nº 12.965/2014 – Marco Civil da Internet.

8. Revisão e Aprovação

Este documento entra em vigor na data de sua publicação e deverá ser revisado e, quando necessário, atualizado a cada dois anos ou a qualquer tempo pela área de Segurança da Informação, por iniciativa própria ou mediante solicitação de partes diretamente envolvidas.

As atualizações devem seguir as diretrizes e procedimentos definidos na **Norma de Gestão de Mudanças Corporativa**, sendo obrigatória a formalização por meio do processo de gestão de mudanças vigente sempre que as alterações impactarem controles implementados, requisitos legais, contratuais ou regulatórios ou impactarem papéis, responsabilidades, procedimentos ou fluxos operacionais do SGSIP.

Todas as versões deste documento deverão ser aprovadas pela Diretoria Executiva da **Cleartech** antes de suas publicações e devidamente comunicadas por meio dos canais internos de comunicação institucional.

9. Disposições Finais

Este documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as demais Políticas, Normas e Procedimentos aplicáveis pela Cleartech.

Este normativo, bem como os documentos complementares, encontra-se disponíveis na Intranet corporativa da Cleartech, especificamente na plataforma Sharepoint, no site do Comitê de Segurança da Informação e Privacidade e na biblioteca de **Normativos Publicados.**

Toda e qualquer atividade em desacordo com as disposições contidas neste documento ou nos normativos complementares será reconhecida como violação e, consequentemente, será tratada conforme estipulado nas cláusulas contratuais pertinentes e na legislação aplicável, visando determinar responsabilidades e aplicar as sanções cabíveis.

10. Anexos

Não se aplica