1. Escopo e Objetivo

A presente Política de Segurança da Informação tem como objetivo estabelecer diretrizes e controles que assegurem a proteção de todas as informações tratadas pela Grand Thera, garantindo a sua **confidencialidade**, **integridade** e **disponibilidade**. A política visa mitigar riscos relacionados à segurança da informação, protegendo ativos contra acessos não autorizados, perdas, divulgação indevida, ou qualquer tipo de abuso, garantindo a conformidade com legislações vigentes, como **LGPD**, **GDPR**, **ISO 27001**, e diretrizes do **NIST**.

Além disso, essa política busca promover uma cultura organizacional voltada para a segurança da informação, assegurando que todos os envolvidos estejam cientes de suas responsabilidades e da importância de proteger os dados da empresa e de seus clientes.

Este documento se aplica a todos os ativos de informação, sejam eles físicos ou digitais, e a todos os colaboradores, parceiros, fornecedores, consultores e qualquer pessoa que tenha acesso às informações ou sistemas da Grand Thera. O escopo inclui redes, sistemas de informação, aplicativos, dispositivos móveis, bancos de dados e todo tipo de informação sensível ou confidencial processada, armazenada ou compartilhada pela organização.

A Grand Thera reconhece que a segurança da informação é um componente essencial para garantir a continuidade dos negócios e a confiança dos seus clientes, e por isso adota uma abordagem abrangente para garantir que todos os ativos estejam devidamente protegidos.

Os objetivos específicos incluem:

1. **Assegurar a proteção dos ativos de informação** contra ameaças internas e externas, garantindo que medidas adequadas de controle sejam implementadas para reduzir o risco de incidentes.

2. **Garantir a conformidade com as legislações e regulamentações aplicáveis** sobre proteção de dados e segurança da informação, de modo a evitar penalidades e assegurar a proteção dos direitos dos titulares dos dados.

3. **Mitigar os riscos** de violações de segurança e interrupções de serviço, estabelecendo planos de resposta a incidentes e procedimentos de recuperação que minimizem o impacto sobre as operações da empresa.

4. **Prover diretrizes e procedimentos claros** para o tratamento adequado das informações, de forma que todos os colaboradores saibam como proceder em diferentes situações que envolvam o uso, armazenamento e compartilhamento de dados.

5. **Promover uma cultura de segurança** entre todos os colaboradores, através de treinamentos contínuos e conscientização sobre boas práticas e diretrizes de segurança.

2. Governança e Responsabilidades

Como uma empresa comprometida com a excelência, a gestão da segurança da informação na Grand Thera deve ser conduzida de forma prática, onde cada papel e responsabilidade é atribuído de forma clara e objetiva. É fundamental que todos os colaboradores compreendam a importância da segurança da informação e atuem de forma responsável no tratamento dos dados. As responsabilidades incluem:

Direção Executiva:

- Aprovar a política de segurança e prover recursos necessários para sua implementação, garantindo que a segurança da informação seja parte integral da estratégia de negócios.
- Estabelecer uma cultura de segurança da informação e garantir o comprometimento com a conformidade, promovendo um ambiente seguro e confiável para todos os stakeholders.
- Realizar revisões periódicas das políticas e procedimentos para assegurar que estejam atualizados e alinhados com as melhores práticas e requisitos legais.

Liderança de Segurança da Informação (Cumulativa):

- A liderança em segurança da informação pode ser acumulada por um membro da equipe com conhecimento técnico, que será responsável por coordenar a implementação das diretrizes de segurança em todos os processos da empresa.
- Liderar a implementação das diretrizes de segurança e coordenar a resposta a incidentes, atuando como ponto focal para quaisquer questões relacionadas à segurança da informação.
- Monitorar o ambiente de tecnologia da informação e implementar medidas corretivas quando necessário para garantir que os controles de segurança sejam eficazes.

Comitê ou Encarregado de Proteção de Dados:

- Garantir a conformidade com LGPD/GDPR, atuando como o responsável por assegurar que as práticas da Grand Thera estejam em linha com as regulamentações de proteção de dados pessoais.

- Atuar como ponto de contato para titulares de dados e autoridades competentes, respondendo a dúvidas e solicitações relacionadas ao tratamento de dados pessoais.

- Na ausência de um encarregado formal, o comitê se estabelecerá inicialmente pela direção executiva, que designará membros qualificados para atuar como representantes de proteção de dados.

Todos os Colaboradores:

- Seguir todas as diretrizes estabelecidas na política de segurança, garantindo que suas ações estejam em conformidade com os procedimentos estabelecidos.

- Reportar comportamentos suspeitos ou potenciais incidentes de segurança de forma imediata, contribuindo para a identificação precoce de possíveis ameaças e a mitigação dos riscos.

- Participar de treinamentos e atividades de conscientização para se manter atualizado em relação às melhores práticas de segurança.

Parceiros e Fornecedores:

- Seguir as diretrizes da Grand Thera relacionadas à segurança da informação e garantir que informações sensíveis sejam tratadas adequadamente, em conformidade com as melhores práticas e regulamentações vigentes.

- Implementar medidas de segurança equivalentes ou superiores às exigidas pela Grand Thera, assegurando que o tratamento de informações sensíveis seja realizado de maneira segura e responsável.

3. Gestão de Riscos

A **gestão de riscos** na Grand Thera visa identificar, analisar, mitigar e monitorar os riscos relacionados ao tratamento de informações sensíveis, de forma proporcional ao tamanho e contexto da empresa. Considerando que a Grand Thera é uma empresa com time ágil e enxuto, a abordagem de gestão de riscos é prática e voltada para o contexto específico do negócio, assegurando que recursos sejam utilizados de forma eficiente. A abordagem segue as boas práticas da **ISO 27005**, do **framework NIST** e as exigências de conformidade das regulamentações de proteção de dados (LGPD e GDPR).

As etapas da gestão de riscos incluem:

Identificação dos Riscos:

- Identificar vulnerabilidades e ameaças potenciais que possam comprometer a segurança das informações, levando em consideração tanto fatores internos quanto externos que possam impactar a organização.

- Realizar mapeamento dos ativos de informação e classificar segundo sua criticidade, considerando o valor do ativo e o impacto potencial de sua perda ou comprometimento.

- Realizar entrevistas e workshops internos para garantir que todos os potenciais riscos sejam identificados, aproveitando o conhecimento dos colaboradores sobre seus respectivos processos.

Análise de Riscos:

- Avaliar o impacto e a probabilidade de ocorrência de cada risco identificado, estabelecendo uma matriz de risco que permita priorizar as ações de mitigação.

- Realizar **Avaliações de Impacto na Proteção de Dados** (DPIA) conforme exigência da LGPD/GDPR para atividades que envolvem dados pessoais, assegurando que os riscos para os direitos dos titulares sejam adequadamente avaliados e tratados.

- Envolver a liderança em segurança e a direção executiva na análise dos riscos mais críticos, garantindo que as decisões sejam tomadas com base em uma visão ampla do impacto no negócio.

Tratamento de Riscos:

- Definir controles de segurança adequados para mitigar ou eliminar os riscos identificados, considerando o apetite ao risco da Grand Thera e a viabilidade dos controles.

- Aplicar princípios de **Privacy by Design** e **Privacy by Default** para garantir que a privacidade seja integrada aos processos desde o início, assegurando que medidas de proteção sejam consideradas já na fase de planejamento dos projetos.

- Desenvolver planos de ação para cada risco identificado, com responsabilidades e prazos definidos para implementação das medidas de mitigação.

Monitoramento e Revisão:

- Realizar monitoramento contínuo dos riscos e da eficácia dos controles implementados, utilizando indicadores de desempenho para avaliar se as medidas adotadas estão gerando os resultados esperados.

- Revisar periodicamente a gestão de riscos para identificar novas ameaças e vulnerabilidades, promovendo melhorias contínuas e garantindo que a política de segurança esteja sempre alinhada às mudanças no ambiente de negócios e às novas tecnologias adotadas.

- Realizar auditorias internas de segurança periodicamente, para identificar eventuais falhas nos controles e assegurar a conformidade com as políticas e procedimentos estabelecidos.

Comunicação e Documentação:

- Manter registros simplificados sobre os riscos identificados, suas análises e as medidas tomadas para tratá-los, garantindo que haja uma documentação clara e acessível para consulta sempre que necessário.

- Garantir a comunicação interna clara sobre riscos, controles e responsabilidades entre os diferentes stakeholders envolvidos, promovendo um ambiente colaborativo e integrado na gestão da segurança da informação.

Promover reuniões periódicas para discutir os riscos identificados e os avanços nas ações de mitigação, assegurando o envolvimento de todos os colaboradores no processo de gestão de riscos.

4. Classificação da Informação

A Grand Thera adota um sistema de **classificação da informação** para assegurar que todos os dados sejam tratados de acordo com seu nível de sensibilidade e criticidade. As informações são classificadas em quatro níveis: **Público**, **Interno**, **Confidencial** e **Restrito**. Essa classificação visa garantir que apenas pessoas autorizadas tenham acesso a informações críticas, minimizando riscos de perda ou divulgação não autorizada.

- **Público**: Informações destinadas ao público em geral, cuja divulgação não causa prejuízos à organização. Exemplos incluem materiais de marketing e comunicados de imprensa.

- **Interno**: Informações restritas aos funcionários e colaboradores da organização. Embora não causem grandes prejuízos se divulgadas, sua exposição não é desejável. Incluem políticas internas e comunicados administrativos.

- **Confidencial**: Informações cuja divulgação não autorizada pode resultar em perdas financeiras, de imagem ou competitividade. Requerem controles de acesso e proteção rigorosos, como uso de criptografia. Exemplos são estratégias de negócios e dados de clientes.

- **Restrito**: Informações altamente sensíveis, cujo acesso é limitado a um grupo específico dentro da organização. A divulgação não autorizada pode causar danos significativos. Incluem segredos comerciais e projetos de pesquisa e desenvolvimento.

Todas as informações devem ser rotuladas e tratadas de acordo com seu nível de classificação. É responsabilidade de cada colaborador garantir que as informações estejam devidamente classificadas e protegidas conforme exigido.

5. Princípios de Privacidade e Proteção de Dados Pessoais

A Grand Thera está comprometida com a proteção dos **dados pessoais** de seus clientes, parceiros e colaboradores, seguindo os princípios estabelecidos pela **LGPD** e **GDPR**. Além disso, a Grand Thera possui uma política específica de proteção de dados pessoais, que complementa esta política de segurança da informação e fornece diretrizes detalhadas para o tratamento de dados pessoais. Esses princípios incluem **minimização dos dados**, **transparência**, **adequação**, **necessidade** e **segurança**.

- **Minimização de Dados**: Coletar e processar apenas os dados pessoais necessários para cumprir uma finalidade específica, evitando o tratamento de dados desnecessários.

- **Transparência**: Informar os titulares de dados sobre como seus dados serão utilizados, garantindo que haja clareza e compreensão sobre as práticas de tratamento.

- **Adequação e Necessidade**: Garantir que os dados coletados estejam de acordo com a finalidade informada ao titular e que sejam essenciais para a execução dessa finalidade.

- **Segurança**: Implementar medidas técnicas e organizacionais para proteger os dados pessoais contra acesso não autorizado, perdas ou incidentes.

- **Direitos dos Titulares**: Respeitar os direitos dos titulares de dados, incluindo o direito de acesso, correção, exclusão e portabilidade de seus dados pessoais. A Grand Thera possui processos para lidar com solicitações dos titulares de dados de forma eficiente e em conformidade com as regulamentações.

Além disso, todos os colaboradores devem aplicar os conceitos de **Privacy by Design** e **Privacy by Default**, garantindo que a privacidade seja considerada desde a concepção dos processos, produtos e serviços.

6. Gestão de Acessos

A **gestão de acessos** na Grand Thera visa garantir que apenas pessoas autorizadas tenham acesso aos recursos e informações da empresa, de acordo com suas responsabilidades e necessidades. Isso é feito por meio da aplicação dos princípios de **privilégio mínimo** e **segregação de funções**, além do uso de ferramentas de controle de identidade e autenticação.

- **Privilégio Mínimo**: Cada colaborador deve ter acesso apenas aos recursos e informações necessários para realizar suas atividades. Isso reduz o risco de acesso indevido a informações sensíveis.

- **Segregação de Funções**: Funções críticas que possam representar riscos à segurança da informação devem ser segregadas para evitar que uma única pessoa tenha controle completo de um processo. Isso ajuda a prevenir fraudes e erros.

- **Controle de Identidade e Autenticação**: Todos os acessos aos sistemas da Grand Thera devem ser feitos com autenticação, preferencialmente utilizando **métodos de autenticação multifator (MFA)**. Isso garante que apenas usuários autorizados tenham acesso aos sistemas.

- **Revisão Periódica de Acessos**: Todos os acessos devem ser revisados periodicamente para garantir que apenas pessoas que ainda necessitam das permissões as mantenham. Em caso de mudança de função ou desligamento de um colaborador, os acessos devem ser imediatamente revogados.

- **Registro e Monitoramento de Acessos**: Todos os acessos aos sistemas e informações devem ser registrados e monitorados para detectar e responder a qualquer atividade suspeita. Logs de acesso são armazenados e revisados de acordo com políticas de auditoria da empresa.

A implementação de controles de gestão de acessos é essencial para garantir a **confidencialidade**, **integridade** e **disponibilidade** das informações tratadas pela Grand Thera, assegurando um ambiente seguro e confiável para todos os seus processos.

7. Segurança Física e do Ambiente

A **segurança física e do ambiente** na Grand Thera é fundamental para garantir a proteção dos ativos de informação contra ameaças físicas, como acesso não autorizado, roubo, danos acidentais e desastres naturais. Atualmente,

a Grand Thera opera majoritariamente em regime de home office como estratégia de capitalização e absorção de maiores talentos. Essas políticas de segurança física se aplicam em momentos em que estabelecemos escritórios físicos para projetos e operações de negócios. Para isso, a empresa adota medidas que incluem:

- **Controle de Acesso Físico**: O acesso às instalações da Grand Thera é restrito a colaboradores autorizados e visitantes devidamente acompanhados. Áreas críticas, como salas de servidores, têm acesso limitado apenas a pessoas designadas.

- **Proteção de Equipamentos**: Todos os equipamentos que armazenam ou processam informações sensíveis devem ser protegidos contra danos físicos. Isso inclui o uso de racks seguros, sistemas de ventilação e proteção contra picos de energia.

- **Ambientes Seguros**: Áreas que contêm informações sensíveis devem ser monitoradas por câmeras de segurança e outros sistemas de vigilância. Alarmes e sistemas de controle de acesso garantem que apenas pessoas autorizadas tenham acesso a essas áreas.

- **Plano de Continuidade Física**: A Grand Thera possui procedimentos para recuperação de desastres que incluem medidas físicas, como redundância de infraestrutura e planos de evacuação, para assegurar a continuidade dos negócios em situações de emergência. **Controle de Acesso Físico**: O acesso às instalações da Grand Thera é restrito a colaboradores autorizados e visitantes devidamente acompanhados. Áreas críticas, como salas de servidores, têm acesso limitado apenas a pessoas designadas.

- **Proteção de Equipamentos**: Todos os equipamentos que armazenam ou processam informações sensíveis devem ser protegidos contra danos físicos. Isso inclui o uso de racks seguros, sistemas de ventilação e proteção contra picos de energia.

- **Ambientes Seguros**: Áreas que contêm informações sensíveis devem ser monitoradas por câmeras de segurança e outros sistemas de vigilância. Alarmes e sistemas de controle de acesso garantem que apenas pessoas autorizadas tenham acesso a essas áreas.

- **Plano de Continuidade Física**: A Grand Thera possui procedimentos para recuperação de desastres que incluem medidas físicas, como redundância de infraestrutura e planos de evacuação, para assegurar a continuidade dos negócios em situações de emergência.

- **Segurança no Home Office**: Para colaboradores que atuam em regime de home office, são adotadas medidas como:

    - Orientação sobre Ambiente Seguro: Os colaboradores devem configurar um ambiente seguro em suas residências, garantindo que dispositivos sejam utilizados em locais privados e seguros.

    - Proteção de Equipamentos: Todos os dispositivos utilizados no home office devem estar protegidos com criptografia, senhas seguras e softwares de segurança atualizados.

    - Rede Segura: Recomenda-se o uso de VPN (Virtual Private Network) para acessar os sistemas corporativos, garantindo a proteção dos dados durante o trânsito pela rede.

- Política de Mesa Limpa: Durante o trabalho remoto, é importante que os colaboradores adotem a prática de mesa limpa, assegurando que documentos confidenciais não sejam deixados em locais desprotegidos.

8. Gestão de Incidentes de Segurança

A **gestão de incidentes de segurança** visa identificar, reportar, responder e mitigar quaisquer incidentes que possam comprometer a segurança da informação. A Grand Thera adota uma abordagem estruturada para a gestão de incidentes, que inclui:

- **Identificação e Registro**: Qualquer incidente ou suspeita de incidente de segurança deve ser identificado e registrado por colaboradores, fornecedores ou parceiros. Um sistema de registro de incidentes é utilizado para garantir o acompanhamento de cada evento.

- **Resposta e Contenção**: Após a identificação, a equipe de segurança deve atuar rapidamente para conter o incidente, minimizando os impactos para a empresa e seus clientes. Isso inclui ações imediatas para isolar sistemas afetados e impedir o avanço do incidente.

- **Investigação e Análise**: Uma investigação detalhada é conduzida para determinar a causa raiz do incidente e avaliar os danos causados. A análise ajuda a definir medidas corretivas e preventivas para evitar a recorrência de problemas semelhantes.

- **Comunicação**: Em caso de incidente de segurança envolvendo dados pessoais, os titulares dos dados e as autoridades competentes serão informados conforme as exigências legais, seguindo as diretrizes da LGPD e GDPR.

- **Aprendizado e Melhoria Contínua**: A Grand Thera busca aprender com cada incidente, revisando processos e controles de segurança, garantindo melhorias contínuas para reduzir o risco de novos incidentes.

9. Criptografia e Proteção de Dados

A **criptografia** é um dos principais mecanismos utilizados pela Grand Thera para garantir a segurança dos dados em trânsito e em repouso. A empresa aplica técnicas de criptografia modernas para proteger informações sensíveis contra acessos não autorizados.

- **Criptografia de Dados em Trânsito**: Todos os dados enviados pela rede, especialmente informações pessoais e sensíveis, devem ser criptografados para garantir sua integridade e confidencialidade durante o tráfego. Isso inclui o uso de **TLS (Transport Layer Security)** em todas as comunicações externas.

- **Criptografia de Dados em Repouso**: Informações confidenciais armazenadas em servidores, bancos de dados ou dispositivos móveis devem ser protegidas por meio de criptografia, utilizando algoritmos seguros, como **AES (Advanced Encryption Standard)**.

- **Gestão de Chaves Criptográficas**: A Grand Thera adota práticas rigorosas para a gestão de chaves criptográficas, garantindo que as chaves sejam armazenadas de forma segura e apenas acessíveis a pessoas autorizadas.

- **Pseudonimização e Anonimização**: Quando possível, técnicas de pseudonimização e anonimização são aplicadas para proteger os dados pessoais, reduzindo o risco de identificação dos titulares em caso de vazamento.
- **Revisão e Atualização de Criptografia**: Os métodos e algoritmos de criptografia são revisados periodicamente para garantir que estejam alinhados às melhores práticas e padrões de segurança, assegurando que os dados da Grand Thera estejam sempre protegidos contra ameaças emergentes.

10. Continuidade de Negócios

A **continuidade de negócios** é essencial para garantir que as operações da Grand Thera possam ser mantidas ou rapidamente retomadas em caso de incidentes que comprometam a segurança da informação ou a infraestrutura da empresa. A Grand Thera adota uma abordagem preventiva para assegurar a resiliência dos negócios, contemplando diversas práticas e ações integradas que visam proteger e recuperar a continuidade operacional em situações adversas. Essas medidas são fundamentais para manter a confiança dos clientes e parceiros, garantindo que, mesmo em momentos de crise, a empresa seja capaz de fornecer seus serviços e cumprir seus compromissos.

- **Plano de Continuidade de Negócios (PCN)**: Um plano documentado que descreve as ações e os procedimentos necessários para assegurar a continuidade dos serviços essenciais durante situações de crise ou interrupções. Este plano é revisado e atualizado periodicamente para garantir que reflita as mudanças no ambiente de negócios e na infraestrutura de TI, incluindo procedimentos de comunicação interna e externa durante crises. O PCN cobre diferentes cenários, como interrupções de TI, falhas de comunicação, desastres naturais e outras possíveis emergências que possam impactar os serviços.

- **Identificação de Processos Críticos**: Os processos críticos para a operação da empresa são identificados e priorizados, de modo que possam ser restaurados rapidamente em caso de interrupção. Essa identificação envolve uma análise detalhada de todas as atividades da empresa, incluindo o impacto financeiro, legal e operacional que uma interrupção pode causar. Cada processo crítico possui planos de recuperação específicos, de modo a garantir uma retomada rápida e eficiente. Além disso, são estabelecidos níveis de tolerância a interrupções para cada processo, permitindo que a empresa tenha clareza sobre quais serviços devem ser restaurados em primeiro lugar.

- **Testes e Exercícios Regulares**: Testes de continuidade e simulações de cenários de crise são realizados regularmente para avaliar a eficácia do PCN e a capacidade de resposta dos colaboradores envolvidos. Esses exercícios incluem simulações de desastres naturais, falhas de TI e outras possíveis situações de risco, permitindo que a empresa identifique pontos de melhoria e aprimore continuamente seus processos de resposta a incidentes. Os resultados desses testes são documentados e usados para ajustar e melhorar o plano, garantindo que a empresa esteja sempre preparada para responder de forma eficaz.

- **Redundância de Infraestrutura**: Recursos de TI críticos possuem redundância, o que inclui servidores, armazenamento de dados e redes, para garantir a continuidade dos serviços em caso de falhas de hardware ou software. A redundância também abrange planos de backup de dados e replicação geográfica, garantindo que as informações estejam sempre disponíveis, mesmo que ocorram falhas em componentes específicos da infraestrutura. A Grand Thera também realiza auditorias regulares de seus recursos de redundância para garantir que eles estejam funcionando conforme o esperado e que os dados possam ser recuperados rapidamente.

11. Auditoria e Conformidade

A **auditoria e conformidade** são processos fundamentais para garantir que a Grand Thera esteja em conformidade com regulamentações e normas aplicáveis, além de verificar a aderência às políticas e procedimentos internos de segurança da informação. Esses processos são essenciais para garantir a transparência e a integridade das operações, além de reforçar a confiança dos clientes, parceiros e demais stakeholders. A auditoria também desempenha um papel crucial na identificação de áreas onde os controles podem ser aprimorados, garantindo que a empresa esteja continuamente evoluindo em termos de segurança.

- **Auditorias Internas e Externas**: A Grand Thera realiza auditorias internas periódicas para avaliar a conformidade com as políticas de segurança e identificar possíveis melhorias. Além disso, auditorias externas são realizadas por entidades independentes para garantir a conformidade com normas, como ISO 27001, LGPD e GDPR. As auditorias externas também servem como uma forma de validação da eficácia das práticas de segurança adotadas pela empresa, contribuindo para a melhoria contínua. A Grand Thera valoriza a independência das auditorias externas, pois isso traz maior credibilidade e confiança nos processos de segurança implementados.

- **Monitoramento de Conformidade**: A conformidade com as políticas de segurança e regulamentações é monitorada de forma contínua, garantindo que eventuais desvios sejam identificados e corrigidos prontamente. Ferramentas automatizadas são utilizadas para monitorar o cumprimento de requisitos de segurança e gerar relatórios periódicos, permitindo que a gestão tenha uma visão clara do status da conformidade em toda a organização. Além disso, são conduzidas verificações aleatórias para garantir que os controles estejam sendo aplicados de forma consistente em todas as áreas da empresa.

- **Correção de Não-Conformidades**: Quando uma não-conformidade é identificada, ações corretivas são definidas e implementadas para garantir que a falha não ocorra novamente, promovendo a melhoria contínua dos processos de segurança. Além disso, análises de causa raiz são realizadas para entender o motivo da falha e garantir que todas as medidas necessárias sejam adotadas para mitigar riscos futuros. Essas ações corretivas são acompanhadas de prazos definidos e responsáveis designados, garantindo que o processo de correção seja concluído de forma eficaz e dentro dos prazos estabelecidos.

- **Revisões Periódicas de Políticas**: As políticas de segurança da informação são revisadas regularmente para garantir que estejam alinhadas com as melhores práticas de mercado e as mudanças nas regulamentações aplicáveis. Essas revisões garantem que a empresa continue a atender aos requisitos legais e normativos de forma eficiente. Sempre que uma revisão é realizada, todos os colaboradores são informados sobre as mudanças, e, quando necessário, treinamentos específicos são oferecidos para garantir que todos estejam cientes e alinhados com as novas diretrizes.

12. Treinamento e Conscientização

O **treinamento e conscientização** são essenciais para garantir que todos os colaboradores da Grand Thera compreendam a importância da segurança da informação e saibam como aplicar boas práticas em seu dia a dia. Um ambiente de trabalho seguro depende do comprometimento de todos os envolvidos, desde os colaboradores até a alta direção, e a promoção da cultura de segurança é uma prioridade constante para a Grand Thera. A conscientização é vista como um elemento chave para a proteção dos ativos de informação, e, por isso, há um esforço contínuo para manter todos os colaboradores atualizados e comprometidos com a segurança.

- **Treinamentos Regulares**: A Grand Thera oferece treinamentos regulares sobre segurança da informação para todos os colaboradores, abordando temas como proteção de dados, identificação de ameaças e práticas seguras de trabalho, incluindo no contexto de home office. Esses treinamentos são adaptados às realidades dos diferentes setores da empresa, garantindo que todos compreendam como suas atividades podem impactar a segurança da informação. Além disso, os treinamentos são atualizados periodicamente para incorporar novas ameaças e tendências, garantindo que os colaboradores estejam sempre preparados para lidar com os desafios mais recentes.

- **Campanhas de Conscientização**: Campanhas periódicas são realizadas para reforçar a importância da segurança da informação e lembrar os colaboradores sobre práticas e comportamentos seguros, como o cuidado ao abrir e-mails suspeitos ou ao acessar redes não seguras. Essas campanhas utilizam diversos formatos, como e-mails, posters digitais, workshops e quizzes, para garantir que as mensagens sejam transmitidas de maneira eficaz e alcancem todos os públicos da empresa. O uso de diferentes abordagens visa maximizar o alcance e a retenção da mensagem entre os colaboradores, promovendo um ambiente de segurança proativo.

- **Responsabilidade Individual**: Todos os colaboradores têm a responsabilidade de proteger as informações da Grand Thera e devem adotar as melhores práticas em suas atividades diárias, garantindo que a segurança da informação seja parte da cultura organizacional.

  A empresa incentiva todos os colaboradores a reportarem incidentes ou comportamentos suspeitos imediatamente, promovendo uma cultura de transparência e colaboração. Essa responsabilidade individual é reforçada através de programas de reconhecimento, nos quais colaboradores que demonstram práticas exemplares de segurança são destacados e recompensados.

- **Treinamento Específico para Funções Críticas**: Colaboradores que desempenham funções críticas, como gestão de TI e proteção de dados, recebem treinamentos específicos, alinhados às responsabilidades e riscos associados às suas funções, assegurando que estejam preparados para lidar com situações que possam comprometer a segurança da informação.

  Esses treinamentos incluem práticas avançadas de gestão de incidentes, resposta a ataques cibernéticos e proteção de infraestrutura crítica. Além disso, esses colaboradores participam de workshops e conferências externas, garantindo que estejam sempre atualizados com as melhores práticas do mercado.

- **Avaliação de Eficácia dos Treinamentos**: A eficácia dos treinamentos e campanhas de conscientização é avaliada periodicamente, por meio de testes, simulações de incidentes e questionários de avaliação. Os resultados dessas avaliações são utilizados para ajustar o conteúdo e a abordagem dos treinamentos, garantindo que as necessidades de segurança da informação da empresa sejam atendidas de maneira eficiente.

  A empresa também realiza avaliações pós-incidente para determinar se os treinamentos fornecidos foram suficientes e identificar áreas onde mais melhorias são necessárias.

- **Promoção de Boas Práticas no Home Office**: Com a prevalência do trabalho remoto, a Grand Thera reforça continuamente a importância de seguir práticas seguras no home office, como o uso de redes seguras, a proteção de dispositivos com senhas fortes e o cuidado ao compartilhar informações.

  Essas orientações são integradas aos treinamentos regulares e acompanhadas de materiais informativos para apoiar os colaboradores no dia a dia. Além disso, são realizadas auditorias periódicas das práticas de home office para garantir que todos os colaboradores estejam seguindo as orientações e que a segurança das informações seja mantida, mesmo fora do ambiente corporativo.

13. Gestão de Vulnerabilidades

A **gestão de vulnerabilidades** visa identificar, avaliar, corrigir e monitorar as vulnerabilidades que possam existir nos sistemas e na infraestrutura da Grand Thera. Esse processo é essencial para reduzir a exposição a riscos e fortalecer a segurança dos ativos da organização. A Grand Thera adota práticas sistemáticas para a gestão de vulnerabilidades, garantindo que todas as fraquezas sejam tratadas de forma proativa.

- **Identificação de Vulnerabilidades**: A Grand Thera utiliza ferramentas automatizadas de varredura e análise para identificar vulnerabilidades nos sistemas, redes e aplicativos. Essas ferramentas são executadas regularmente e sempre que novas alterações são feitas na infraestrutura, garantindo que qualquer nova vulnerabilidade seja detectada rapidamente.

- **Avaliação de Vulnerabilidades**: Após a identificação, as vulnerabilidades são classificadas de acordo com a sua criticidade, levando em consideração o impacto potencial e a probabilidade de exploração. A empresa utiliza métricas como CVSS

(Common Vulnerability Scoring System) para priorizar as ações de correção, assegurando que as vulnerabilidades mais críticas sejam tratadas com maior urgência.

- **Correção e Mitigação**: Medidas corretivas são tomadas para eliminar ou mitigar as vulnerabilidades identificadas. Isso pode incluir a aplicação de patches, atualizações de software, mudanças de configuração ou adoção de novas ferramentas de proteção. Todas as correções são devidamente documentadas e acompanhadas até a sua conclusão.

- **Monitoramento Contínuo**: O monitoramento contínuo é realizado para garantir que as vulnerabilidades corrigidas não voltem a ocorrer e que novas fraquezas sejam identificadas e tratadas a tempo. Relatórios periódicos são gerados para dar visibilidade sobre o status das vulnerabilidades e as ações tomadas para mitigá-las.

14. Controle de Acesso a Aplicações e Sistemas

O **controle de acesso a aplicações e sistemas** é fundamental para garantir que apenas pessoas autorizadas possam acessar informações sensíveis e sistemas críticos da Grand Thera. A política de controle de acesso abrange desde a autenticação dos usuários até o gerenciamento de suas permissões, assegurando que os acessos sejam concedidos de acordo com as necessidades e responsabilidades de cada função.

- **Autenticação Multifator (MFA)**: Todos os acessos aos sistemas críticos da Grand Thera devem ser realizados mediante autenticação multifator (MFA). O uso de MFA proporciona uma camada adicional de segurança, tornando mais difícil o acesso não autorizado, mesmo que as credenciais de um usuário sejam comprometidas.

- **Controle Baseado em Funções**: O acesso aos sistemas é concedido com base no princípio do **privilégio mínimo** e na **segregação de funções**. Cada colaborador tem acesso apenas aos recursos necessários para o desempenho de suas atividades, minimizando a exposição a riscos e evitando acessos desnecessários a informações sensíveis.

- **Gestão de Identidades**: A gestão de identidades é feita de forma centralizada, garantindo que todas as contas de usuários sejam criadas, modificadas e removidas de acordo com as políticas internas de segurança. Quando um colaborador muda de função ou deixa a empresa, seus acessos são imediatamente ajustados ou revogados, garantindo que não haja riscos relacionados a acessos indevidos.

- **Revisão Periódica de Acessos**: São realizadas revisões periódicas das permissões concedidas aos colaboradores, assegurando que os acessos estejam sempre alinhados com as responsabilidades de cada função. Essas revisões ajudam a identificar e remover acessos desnecessários ou obsoletos, reduzindo o risco de exposição.

15. Gestão de Backups

A **gestão de backups** é essencial para garantir a disponibilidade e a recuperação de dados em caso de falhas, incidentes de segurança ou desastres. A Grand Thera adota uma política rigorosa de backups que abrange todas as informações críticas, assegurando que os dados possam ser recuperados de maneira rápida e eficiente sempre que necessário.

- **Frequência de Backups**: Backups regulares são realizados para garantir a proteção dos dados mais recentes. A frequência dos backups varia de acordo com a criticidade dos dados, com backups diários para informações mais sensíveis e backups semanais para dados menos críticos. A política de backups é revisada periodicamente para garantir que esteja alinhada com as necessidades da empresa.

- **Backups Incrementais e Totais**: A Grand Thera utiliza uma combinação de backups incrementais e totais para otimizar o uso de recursos e garantir a recuperação completa dos dados. Backups incrementais são realizados regularmente para armazenar apenas as mudanças desde o último backup total, garantindo uma recuperação eficiente em caso de necessidade.

- **Armazenamento Seguro**: Os backups são armazenados de forma segura, utilizando criptografia para proteger os dados contra acessos não autorizados. Além disso, cópias dos backups são armazenadas em locais geograficamente distintos, reduzindo o risco de perda de dados em caso de desastres naturais ou falhas de infraestrutura.

- **Testes de Recuperação**: Testes regulares de recuperação de backups são realizados para garantir que os dados possam ser restaurados rapidamente e de forma completa em caso de necessidade. Esses testes permitem identificar possíveis falhas nos procedimentos de backup e assegurar que todos os dados críticos estejam devidamente protegidos e acessíveis.

- **Política de Retenção**: A política de retenção de backups define por quanto tempo os backups são armazenados antes de serem descartados de forma segura. A Grand Thera mantém backups históricos por períodos definidos, garantindo que informações antigas possam ser recuperadas quando necessário, respeitando os requisitos legais e normativos aplicáveis.

16. Segurança no Desenvolvimento de Software

A **segurança no desenvolvimento de software** é um pilar importante para garantir que todas as aplicações da Grand Thera sejam desenvolvidas com práticas de segurança incorporadas desde o início do ciclo de desenvolvimento. Dessa forma, a empresa minimiza riscos de vulnerabilidades e assegura que os sistemas atendam aos mais altos padrões de proteção. Garantir a segurança em todas as fases do desenvolvimento não apenas protege os dados dos clientes, mas também fortalece a confiança na qualidade e integridade dos produtos oferecidos pela Grand Thera.

- **Secure Development Lifecycle (SDLC)**: A Grand Thera adota práticas de **ciclo de vida de desenvolvimento seguro (SDLC)**, garantindo que as melhores práticas de segurança sejam seguidas em todas as etapas de desenvolvimento, desde a concepção até o lançamento das aplicações. O SDLC envolve uma série de etapas cuidadosamente planejadas, incluindo análise de requisitos de segurança, design seguro, implementação, testes, lançamento e manutenção. Cada uma dessas etapas é revisada para garantir que os controles de segurança adequados estejam em vigor, minimizando riscos potenciais.

- **Revisão de Código**: Todos os códigos desenvolvidos são revisados quanto à presença de vulnerabilidades e aderência a padrões de segurança. A revisão pode ser realizada por pares ou automatizada, utilizando ferramentas que analisam o código em busca de vulnerabilidades comuns. Essa revisão envolve uma análise detalhada de diferentes aspectos do código, como controle de entrada, autenticação, criptografia e manuseio de erros. As revisões regulares ajudam a identificar possíveis melhorias no código, promovendo uma qualidade contínua dos softwares desenvolvidos.

- **Testes de Segurança**: Antes de o software ser lançado, são realizados testes de segurança, incluindo **testes de penetração** e **análises estáticas e dinâmicas**, onde os testes são realizados de acordo com a exigência e complexidade do projeto final, bem como as exigências e complexidades de cada ambiente e operação, visando se adequar ao real nível de criticidade. Isso ajuda a identificar falhas de segurança e a resolvê-las antes que o produto seja disponibilizado para uso. Os testes de penetração são realizados por especialistas internos ou externos que simulam ataques cibernéticos, garantindo que todas as vulnerabilidades possíveis sejam identificadas e mitigadas antes da entrega ao cliente. Além disso, a Grand Thera implementa **testes de regressão de segurança** sempre que alterações significativas são feitas no código, garantindo que melhorias contínuas não introduzam novos riscos.

- **Treinamento de Desenvolvedores**: Os desenvolvedores da Grand Thera recebem treinamentos regulares sobre segurança de software, incluindo práticas de codificação segura, análise de vulnerabilidades e uso de bibliotecas seguras. Dessa forma, garantimos que a equipe esteja sempre atualizada e capacitada a implementar as melhores práticas de segurança. Esses treinamentos também incluem **workshops práticos**, nos quais os desenvolvedores aprendem a identificar e mitigar vulnerabilidades específicas, simulando cenários reais de ataques. Ao integrar a segurança ao dia a dia dos desenvolvedores, a Grand Thera assegura que o conhecimento seja continuamente aplicado e aprimorado.

17. Segurança em Dispositivos Móveis e BYOD (Bring Your Own Device)

A Grand Thera reconhece que o uso de **dispositivos móveis** e a prática de **BYOD (Bring Your Own Device)** são comuns no ambiente de trabalho moderno, trazendo tanto flexibilidade quanto desafios para a segurança da informação. Para garantir a proteção dos dados corporativos em dispositivos móveis, a Grand Thera adota diretrizes específicas para o uso seguro desses dispositivos, garantindo que todos os colaboradores entendam as responsabilidades associadas ao uso desses equipamentos.

- **Política de BYOD**: A Grand Thera permite que os colaboradores utilizem seus próprios dispositivos para acessar sistemas e informações da empresa, desde que cumpram os requisitos de segurança definidos. Os dispositivos devem ser registrados, e os colaboradores devem concordar em seguir todas as políticas de segurança estabelecidas pela empresa. Além disso, a política de BYOD inclui orientações detalhadas sobre **práticas de segurança no uso dos dispositivos**, como não compartilhar o dispositivo com terceiros, manter o sistema operacional atualizado e evitar conexões a redes Wi-Fi públicas sem uma VPN.

- **Proteção de Dispositivos**: Todos os dispositivos que acessam dados da Grand Thera devem ser protegidos por senhas fortes, criptografia de dados e software de segurança atualizado. Além disso, deve ser utilizado um método de autenticação seguro, como **MFA (autenticação multifator)**, para garantir que apenas usuários autorizados possam acessar informações sensíveis. A Grand Thera também recomenda o uso de **soluções de segurança móvel**, como antivírus e detecção de ameaças, garantindo que os dispositivos estejam protegidos contra malware e outras ameaças cibernéticas. Caso um dispositivo seja comprometido, procedimentos claros estão definidos para notificação imediata e mitigação do risco.

- **Gerenciamento de Dispositivos Móveis (MDM)**: A Grand Thera utiliza uma solução de **Gerenciamento de Dispositivos Móveis (MDM)** para monitorar, gerenciar e proteger os dispositivos que acessam dados corporativos. A solução MDM permite que dispositivos sejam bloqueados ou apagados remotamente em caso de perda ou roubo, garantindo a proteção das informações. Além disso, o MDM permite **políticas de conformidade automatizadas**, onde dispositivos que não atendem aos requisitos de segurança são automaticamente impedidos de acessar os sistemas da empresa. Essa abordagem garante que todos os dispositivos em uso estejam em conformidade com as diretrizes de segurança, minimizando riscos para a organização.

- **Segregação de Dados Pessoais e Corporativos**: A empresa aplica soluções que garantem a segregação entre dados pessoais e dados corporativos nos dispositivos móveis, de forma a proteger as informações da Grand Thera sem invadir a privacidade dos colaboradores. Essa medida é essencial para assegurar que os dados corporativos sejam devidamente protegidos, mesmo quando armazenados em dispositivos pessoais. A segregação é realizada por meio de **containers de segurança** que criam ambientes isolados dentro dos dispositivos móveis, onde os dados da Grand Thera são armazenados e acessados de forma segura. Dessa forma, mesmo em caso de comprometimento de um dispositivo, os dados pessoais dos colaboradores permanecem protegidos, e os dados corporativos não são afetados.

18. Gestão de Logs e Monitoramento de Atividades

A **gestão de logs e o monitoramento de atividades** são fundamentais para identificar, analisar e responder a eventos suspeitos e possíveis incidentes de segurança dentro dos sistemas e redes da Grand Thera. Esse processo ajuda a garantir a integridade dos sistemas e a identificar atividades maliciosas, garantindo uma resposta rápida a ameaças emergentes. Além de detectar e responder a incidentes, a gestão de logs também desempenha um papel importante na identificação de possíveis falhas de segurança e na melhoria contínua dos processos.

- **Registro de Logs**: Todos os sistemas críticos da Grand Thera geram logs detalhados, incluindo registros de autenticação, acessos, atividades administrativas e alterações nos sistemas. Esses logs são armazenados de forma segura, garantindo que possam ser consultados para auditorias e investigações futuras. A retenção dos logs segue uma política de acordo com a criticidade das informações e requisitos legais, assegurando que estejam disponíveis por períodos suficientes para atender a possíveis auditorias ou investigações. Além disso, a Grand Thera aplica técnicas de criptografia para garantir a integridade e a confidencialidade dos logs armazenados, prevenindo acessos não autorizados e modificações indevidas.

- **Monitoramento Contínuo**: A Grand Thera realiza um monitoramento contínuo dos sistemas e das redes, utilizando ferramentas especializadas para identificar atividades suspeitas ou comportamentos fora do padrão. Esses sistemas de monitoramento emitem alertas em tempo real sempre que uma possível ameaça é detectada, permitindo uma resposta rápida e eficaz. As ferramentas de monitoramento são configuradas para identificar uma ampla gama de possíveis incidentes, desde tentativas de acesso não autorizado até alterações em arquivos críticos. A Grand Thera também utiliza **análise comportamental** para diferenciar entre atividades normais e anômalas, reduzindo falsos positivos e permitindo uma resposta mais focada.

- **Análise de Logs**: A análise regular dos logs é conduzida para identificar padrões de comportamento que possam indicar ameaças em potencial. Essa análise inclui a identificação de tentativas de acesso não autorizadas, comportamentos anômalos e outras atividades que possam comprometer a segurança dos sistemas da empresa. A Grand Thera utiliza ferramentas de **machine learning** para ajudar na análise dos logs, identificando padrões complexos que poderiam passar despercebidos em uma análise manual. Além disso, relatórios periódicos são gerados para que a equipe de segurança avalie as atividades e identifique oportunidades de melhoria nos processos de segurança.

19. Gestão de Senhas e Autenticação

A **gestão de senhas e autenticação** é um componente essencial para garantir que apenas pessoas autorizadas possam acessar os sistemas e informações da Grand Thera. O uso de credenciais fortes e a adoção de métodos de autenticação seguros são fundamentais para proteger os ativos da organização contra acessos não autorizados. Além disso, a Grand Thera mantém uma política rigorosa de **auditoria de senhas** para garantir que todas as credenciais estejam sempre em conformidade com as melhores práticas de segurança.

- **Política de Senhas**: Todos os colaboradores da Grand Thera são obrigados a seguir uma política rigorosa de senhas, que inclui o uso de senhas complexas, com comprimento mínimo, caracteres especiais e alteração periódica. Senhas fracas ou reutilizadas não são permitidas, e todas as contas devem ser protegidas por uma senha exclusiva. Além disso, a política de senhas exige que as credenciais sejam atualizadas em intervalos regulares, e colaboradores são notificados automaticamente quando suas senhas estão próximas do vencimento. Caso uma senha seja comprometida, procedimentos de emergência são acionados para garantir a segurança das contas afetadas.

- **Autenticação Multifator (MFA)**: Para acessos a sistemas críticos e dados sensíveis, a Grand Thera adota o uso de **MFA (autenticação multifator)**. A combinação de diferentes fatores de autenticação, como senhas e códigos de autenticação gerados em dispositivos separados, aumenta significativamente a segurança e reduz o risco de acessos indevidos. Além dos fatores tradicionais, a Grand Thera está implementando o uso de **biometria** para acessos a determinados sistemas, garantindo uma camada extra de proteção. A MFA também é aplicada em situações de acesso remoto, minimizando os riscos associados ao trabalho fora do ambiente corporativo.

- **Gestão Centralizada de Identidades**: A gestão de identidades e acessos é feita de forma centralizada, garantindo que todas as contas de usuário sejam criadas, alteradas ou desativadas de acordo com as políticas de segurança estabelecidas. Isso assegura que os acessos sejam devidamente controlados e revisados, minimizando o risco de contas inativas serem utilizadas de forma indevida. Ferramentas de **IAM (Identity and Access Management)** são utilizadas para automatizar processos e fornecer visibilidade sobre o status de cada conta, facilitando a gestão e o controle dos acessos dentro da organização.

- **Uso de Gerenciadores de Senhas**: A Grand Thera incentiva o uso de **gerenciadores de senhas** para que os colaboradores armazenem e gerenciem suas senhas de forma segura. Essas ferramentas permitem a criação de senhas únicas e complexas para cada sistema, reduzindo o risco associado ao uso de senhas fracas ou repetidas. Além disso, treinamentos periódicos são oferecidos para garantir que todos os colaboradores saibam utilizar as ferramentas de forma adequada, maximizando os benefícios e garantindo a proteção das credenciais.

20. Plano de Resposta a Incidentes

O **plano de resposta a incidentes** é uma parte crucial da estratégia de segurança da Grand Thera, garantindo que a empresa esteja preparada para lidar rapidamente com eventos que possam comprometer a segurança das informações e a continuidade dos negócios. Esse plano descreve como a organização identifica, gerencia e mitiga incidentes de segurança, assegurando uma resposta coordenada e eficaz. A Grand Thera mantém um plano robusto que é regularmente revisado e testado para garantir sua eficácia diante de diferentes tipos de ameaças.

- **Identificação de Incidentes**: A identificação de incidentes é feita através de um monitoramento contínuo dos sistemas e da infraestrutura. Qualquer atividade suspeita ou comportamento fora do padrão é imediatamente sinalizado para a equipe de segurança, que avalia a gravidade do evento e determina se ele constitui um incidente de segurança. Além disso, colaboradores são treinados para identificar sinais de possíveis incidentes e reportá-los imediatamente, contribuindo para uma resposta mais rápida e abrangente.

- **Notificação e Comunicação**: Assim que um incidente é identificado, um processo de notificação é iniciado, envolvendo todas as partes interessadas, incluindo gestores, equipe técnica e, quando necessário, clientes ou parceiros afetados. A comunicação rápida e clara é essencial para minimizar impactos e garantir uma resposta coordenada. A Grand Thera utiliza **canais de comunicação seguros** para garantir que as informações sobre o incidente sejam transmitidas de forma

protegida, evitando vazamentos de informações sensíveis.

- **Contenção e Erradicação**: Após a identificação do incidente, a equipe de segurança atua para conter a ameaça, impedindo que ela se espalhe ou cause mais danos. Em seguida, são tomadas ações para erradicar a causa do incidente, o que pode incluir a remoção de malware, o bloqueio de acessos não autorizados e a aplicação de patches de segurança. Ferramentas automatizadas são usadas para agilizar a contenção, enquanto a equipe de segurança investiga a origem do incidente para garantir que todas as causas sejam adequadamente tratadas.

- **Recuperação e Retomada de Operações**: Após a contenção e a erradicação do incidente, a Grand Thera se concentra na recuperação dos sistemas afetados e na retomada das operações normais. Planos de recuperação são executados para restaurar dados e funcionalidades, garantindo que os sistemas estejam seguros antes de serem colocados novamente em operação. A Grand Thera mantém **backups atualizados** que são utilizados para garantir uma recuperação rápida e completa, minimizando o impacto para os negócios e clientes.

- **Análise Pós-Incidente**: Depois que o incidente é resolvido, uma análise detalhada é conduzida para identificar as causas do problema e evitar futuras ocorrências. Lições aprendidas são documentadas e as políticas e controles de segurança são ajustados conforme necessário para fortalecer a postura de segurança da Grand Thera. Além disso, são realizados **workshops internos** para compartilhar os aprendizados com toda a equipe, promovendo uma cultura de melhoria contínua e preparação contra futuros incidentes.

21. Aceitação da Política

Todo colaborador ou terceiro que atua em nome ou no interesse da Grand Thera deve revisar esta Política e se comprometer com seus termos e condições. A política está disponível no portal da Grand Thera e em todas as plataformas internas da empresa, de modo a garantir o acesso e a transparência sobre o Programa de Integridade.

A adesão a esta Política é um pré-requisito para todos os colaboradores, prestadores de serviços e parceiros de negócio. A Grand Thera realiza sessões de integração e treinamentos regulares para assegurar que todos os envolvidos estejam plenamente informados sobre as diretrizes e obrigações estipuladas. É esperado que qualquer pessoa que tenha acesso à Política compreenda a sua importância e esteja comprometida com a implementação de suas práticas no dia a dia.

A Grand Thera também se compromete a revisar regularmente esta Política, garantindo que esteja sempre atualizada e em conformidade com as mudanças regulatórias e melhores práticas de mercado. Todos os colaboradores são incentivados a dar feedback sobre a Política, de modo a garantir que ela esteja sendo efetiva e aplicável em todas as situações. A transparência e a colaboração são elementos fundamentais para o sucesso contínuo da Grand Thera, e a aceitação desta Política é um reflexo do compromisso de cada profissional com esses valores.