



Norma de Procedimento TI e Segurança da Informação

Referência: 001-01
NP TISI
Data de emissão:
28/10/2021
Pág. 1

Assunto: Parâmetros de Segurança. Fiscalização Interna.

Índice

I.	OBJETIVO	2
II.	DEFINIÇÕES	2
III.	PRINCÍPIOS	5
IV.	DIRETRIZES.....	6
V.	APLICABILIDADE E CONFORMIDADE.....	7
VI.	TREINAMENTO, ATUALIZAÇÃO E DIVULGAÇÃO	8
VII.	ATRIBUIÇÕES E RESPONSABILIDADES	8
VIII.	SANÇÕES	10
IX.	PROCEDIMENTOS	11
X.	DOCUMENTOS RELACIONADOS	17

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		



Norma de Procedimento TI e Segurança da Informação

Referência: 001-01
NP TISI
Data de emissão:
28/10/2021
Pág. 2

Assunto: Parâmetros de Segurança. Fiscalização Interna.

I. OBJETIVO

1.1 Estabelecer diretrizes para assegurar a proteção dos ativos tecnológicos e de informação, garantindo confidencialidade, integridade e disponibilidade das informações e fluxos de processos, de acordo com os requisitos do negócio da Medical Life e com as leis e regulamentações permanentes.

1.2 Regular a utilização segura dos recursos que promovem o acesso aos dados e informações através de recursos de identificação, autenticação, autorização e auditoria, que permitam aos colaboradores, terceiros, fornecedores, parceiros, clientes e outras partes interessadas nos negócios da Medical Life seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

1.3 Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento, desta forma auxiliando a Medical Life a cumprir sua missão e reforçar seus valores.

II. DEFINIÇÕES

2.1 **Colaborador:** trabalhador da empresa, de todos os níveis hierárquicos, cargo, função, sexo ou forma de contratação.

2.2 **Dados e Informações:** Dados são a base para a informação, que pode ser quantificado, mas não qualificado. Já a informação é o resultado de um conjunto de dados que foram ordenados e organizados permitindo a transmissão de uma mensagem compreensiva dentro de um determinado contexto.

2.3 **Terceiro:** Toda pessoa física ou jurídica que não seja colaborador interno ou não fizer parte da Medical Life, mas que seja contratado para auxiliar no desempenho de suas atividades, tais como parceiros, representantes, fornecedores, consultores,

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

prestadores de serviços em geral, organizações da sociedade civil (ONGs), entre outros.

2.4 **Auditabilidade:** Uma característica dos sistemas de informação modernos que é medida pela facilidade com que os dados podem ser substanciados, permutando-os com os documentos de origem e ao ponto em que os auditores possam confiar nos processos de controle pré-verificados e monitorados.

2.5 **Auditabilidade:** Uma característica dos sistemas de informação modernos que é medida pela facilidade com que os dados podem ser substanciados, permutando-os com os documentos de origem e ao ponto em que os auditores possam confiar nos processos de controle pré-verificados e monitorados.

2.6 **Integridade:** Propriedade que garante que a informação processada seja mantida em seu estado original, protegendo-a de alterações indevidas, intencionais, ou acidentais, tanto no momento da sua guarda ou transmissão.

2.7 **Confidencialidade:** Propriedade que garante e estabelece limites de acesso às informações, permitindo o acesso apenas a pessoas autorizadas.

2.8 **Confidencialidade:** Propriedade que garante e estabelece limites de acesso às informações, permitindo o acesso apenas a pessoas autorizadas.

2.9 **Disponibilidade:** Propriedade que garante que pessoas autorizadas obtenham acesso à ativos de informações e ativos físicos sempre que for necessário para o desempenho de suas atividades.

2.10 **Conformidade:** Processo de garantia do cumprimento de um requisito, podendo ser obrigações empresariais com as partes interessadas (investidores, empregados, credores etc.) e com aspectos legais e regulatórios relacionados à administração das empresas, dentro de princípios éticos e de conduta estabelecidos pela Alta Administração da Medical Life;

2.11 **Recursos de segurança:** Métodos utilizados no setor de TI para promover o uso dos dados de uma forma segura. Assim, os recursos nada mais são do que o uso da criptografia de dados, do programa antivírus, da proteção de rede, do

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

desenvolvimento de planos de recuperação, entre outros, utilizados constantemente pelas empresas.

2.12 Recursos de segurança: Métodos utilizados no setor de TI para promover o uso dos dados de uma forma segura. Assim, os recursos nada mais são do que o uso da criptografia de dados, do programa antivírus, da proteção de rede, do desenvolvimento de planos de recuperação, entre outros, utilizados constantemente pelas empresas.

2.13 Segurança da Informação: É o conjunto de ações e controles que tem como objetivo garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, contribuindo para o cumprimento dos objetivos estratégicos da companhia;

2.14 Incidente de Segurança da Informação: Evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades e que afete algum dos aspectos da segurança da informação: confidencialidade, integridade ou disponibilidade;

2.15 Sistemas: refere-se a todos os sistemas de informação, computadorizados ou não, e suas bases de dados, arquivos físicos, arquivos digitais e mídia processada e armazenada por eles, o software de aplicação e de operação, e as operações de computador dentro de uma determinada organização, incluindo, mas não limitado a computadores centrais (mainframes ou servidores), sistemas intermediários e de apoio, mini e micro sistemas, redes locais, metropolitanas, e de longa distância, computadores pessoais (desktops e laptops), estações de trabalho e servidores, redes de telecomunicações (roteadores, pontes, etc), quaisquer novas tecnologias atualmente em desenvolvimento, e quaisquer outros computadores especializados localizados em áreas funcionais (departamentos) onde os dados são transmitidos, distribuídos ou processados por quaisquer meios. Todos estes sistemas e todos os dados neles residentes são considerados propriedade da Empresa e devem ser protegidos como tal por todos os colaboradores.

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

2.16 **Risco de Segurança da Informação:** Riscos associados à violação da confidencialidade, disponibilidade e integridade das informações da companhia nos meios físicos e digitais.

III. PRINCÍPIOS

3.1 A Política de Segurança da Informação tem por princípios a proteção dos dados, informações e conhecimento classificados como sigilosos, a preservação do direito pessoal e coletivo no que se refere à intimidade e ao sigilo das correspondências eletrônicas, informações e comunicações individuais, e possuem total aderência da alta administração da organização.

3.2 São observados por todos na execução de suas funções, incluindo colaboradores, terceiros, fornecedores, parceiros, clientes e outras partes interessadas nos negócios da Medical Life, que a eles tenham expressamente aderido.

3.3 São as bases para as ações ou linhas de conduta de segurança que atuam como guia para a sua implementação e a gestão da Segurança da Informação:

- **Estabelecer a Segurança da Informação em toda a empresa:** a Segurança da Informação é tratada em nível organizacional, de acordo com a tomada de decisões que levem em consideração todos os processos críticos de negócio da Medical Life.
- **Adotar uma abordagem baseada em riscos:** a Segurança da Informação é fundamentada em decisões baseadas em riscos como perda da vantagem competitiva, conformidade, responsabilidade civil, interrupções operacionais, danos à reputação e perdas financeiras.
- **Promover um ambiente positivo de segurança:** a Segurança da Informação é estruturada com base na análise do comportamento humano, observando as crescentes necessidades de todas as partes interessadas, através da conscientização e maturidade dos colaboradores fortalecendo

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		



Norma de Procedimento TI e Segurança da Informação

Referência: 001-01
NP TISI
Data de emissão:
28/10/2021
Pág. 6

Assunto: Parâmetros de Segurança. Fiscalização Interna.

um dos elementos fundamentais para manter o nível apropriado de Segurança.

IV. DIRETRIZES

4.1 Toda informação elaborada, adquirida, manuseada, armazenada, transportada e/ou descartada nas dependências e/ou em ativos da Medical Life é considerada patrimônio da empresa e deve ser utilizada exclusivamente para os interesses legítimos da empresa.

4.2 Todos os colaboradores, estagiários, terceiros, fornecedores e parceiros, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e salvaguarda dos ativos e informações de que sejam usuários ou com os quais tenham contato, assim como dos ambientes físicos e computacionais a que tenham acesso, independentemente das medidas de segurança implantadas.

4.3 O acesso lógico, o controle de acesso físico e o uso da informação da Medical Life devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas inerentes ao seu cargo ou função, para atender os interesses legítimos dos negócios da empresa.

4.4 Os incidentes de segurança devem ser identificados, monitorados, comunicados e devidamente tratados de forma a reduzir riscos no ambiente, evitando interrupção das atividades e não afetar o alcance dos objetivos estratégicos da Medical Life.

4.5 A Medical Life pode monitorar o acesso e a utilização de seus ativos tecnológicos, como dos ambientes, equipamentos e sistemas da informação, de forma que ações indesejáveis ou não autorizadas sejam detectadas e impedidas.

4.6 A Medical Life pode auditar periodicamente as práticas de Segurança da Informação, de forma a avaliar a conformidade das ações de seus colaboradores, estagiários, terceiros, fornecedores e parceiros em relação ao estabelecido nesta Política e na legislação aplicável.

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		



Norma de Procedimento TI e Segurança da Informação

Referência: 001-01
NP TISI
Data de emissão:
28/10/2021
Pág. 7

Assunto: Parâmetros de Segurança. Fiscalização Interna.

V. APLICABILIDADE E CONFORMIDADE

5.1 Essa Norma de Procedimento é aplicada à Medical Life, seus colaboradores e terceiros interessados, abrangendo todas as atividades desenvolvidas, de acordo com as regras definidas pela área de Compliance.

5.2 Aplica-se essa norma a toda forma de utilização, armazenamento de dados e informações em qualquer aparelho eletrônico de comunicação ou de armazenamento, estações de trabalho, computadores, aparelhos portáteis, sistemas, internet, correio eletrônico, redes sociais, impressoras, mídias removíveis e em papel.

5.3 Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação vigente.

5.4 É também obrigação de cada colaborador se manter atualizado em relação a esta Política de Segurança da Informação e às Normas e Procedimentos relacionados, buscando orientação do seu gestor ou da Gerência de TI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

5.5 A divulgação de informações ou dados a terceiros não autorizados não é permitida sem a aprovação por escrito da Administração no nível apropriado.

5.6 O uso pessoal de todos os sistemas, instalações, dados, informações, equipamentos, ou qualquer outro ativo da Medical Life não é permitido sem a aprovação por escrito da Administração no nível apropriado. Além disso, os Gestores da Medical Life não devem assumir qualquer tipo de compromisso por meio do uso de mídia eletrônica e recursos de software de rede sem a aprovação por escrito da Administração.

5.7 Todos os colaboradores devem manter sigilo sobre todas as suas senhas, procedimentos de acesso e controles relacionados, sendo pessoal e intransferível.

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

5.8 Qualquer violação desta política e/ou procedimentos relacionados e/ou leis relacionadas, seja voluntária ou involuntária, será tratada de acordo com as leis e regulamentações vigentes.

VI. TREINAMENTO, ATUALIZAÇÃO E DIVULGAÇÃO

6.1 Um programa de conscientização, educação e treinamento em Segurança da Informação é disponibilizado para garantia dos objetivos, princípios e diretrizes definidas nesta Política de Segurança da Informação.

6.2 O programa deve ser seguido adequando-se às necessidades e responsabilidades específicas de cada colaborador, estagiário, terceiro, fornecedor e parceiro da Medical Life.

6.3 Da mesma forma, o conteúdo da Política é amplo e constantemente atualizado e divulgado. A releitura desta Política, mesmo que não seja diretamente solicitada, deve ser feita periodicamente para melhor entendimento.

VII. ATRIBUIÇÕES E RESPONSABILIDADES

7.1 Responsabilidade da Gestão

- É responsabilidade da Alta Administração da Medical Life (incluem-se Gestores, Conselho de Administração, Comitê de Diretoria, Comitê de Direção de TI, e demais integrantes) gerenciar os sistemas de computação, de telecomunicações, e de segurança da informação da empresa.
- O Presidente da Medical Life (ou outro colaborador autorizado pelo Conselho de Administração) deve estabelecer uma Equipe de Gestão que efetivamente utilize e otimize os recursos dos sistemas da empresa, e o potencial dos ativos de informação consistente com sólidas práticas profissionais, Leis nacionais, padrões da indústria, e requisitos regulatórios.
- Os diversos sistemas, dados e componentes de infraestrutura serão monitorados continuamente para garantir que funcionem adequadamente

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

e tenham a capacidade de atender às necessidades e requisitos atuais e futuros da Medical Life.

- A Equipe de Gestão deve ser responsável e conduzir os estudos de viabilidade relativos à aquisição de soluções de TI e ao desenvolvimento, implementação, conversão de sistemas e dados, revisão dos sistemas, operação dos sistemas, e treinamento de pessoal para todos os sistemas da empresa.
- Também é responsabilidade da Alta Administração garantir que os procedimentos estejam em vigor para que esses sistemas operem em caso de desastres ou outras calamidades.

7.2 Área de Segurança da Informação

- Gerenciar, coordenar, orientar, avaliar e promover a implantação das ações, atividades e projetos relativos à Segurança da Informação na Medical Life, promovendo ações de interesse da empresa, programas educacionais e de conscientização do capital humano.

7.3 Colaboradores, estagiários, terceiros, fornecedores, parceiros e partes interessadas da empresa

- Conhecer e cumprir as normas e orientações estabelecidas nesta Política e demais Regulamentos que compõem a Política de Segurança da Informação da Medical Life;
- Informar as situações que comprometam a segurança das informações nas unidades organizacionais da Medical Life, através do Canal de Denúncias e Relatos, presente no Código de Ética da empresa;
- Toda informação criada, modificada no exercício das funções e qualquer informação contida em mensagens do correio eletrônico corporativo deve ser tratada como referente ao negócio da Medical Life, não devendo ser considerada como pessoal, particular ou confidencial, mesmo que arquivadas na sua pasta pessoal;

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

- Garantir que seja conhecida e cumprida a proibição de compartilhamento ou negociação de credenciais (ID, senhas, crachás, tokens e similares);
- Garantir que os requisitos de Segurança da Informação constem nas aquisições e/ou implementações tecnológicas.

VIII. SANÇÕES

8.1 Todas as garantias necessárias ao cumprimento desta Política estão estabelecidas formalmente com os colaboradores da Medical Life.

8.2 O descumprimento da Política é considerado uma falta grave e poderá acarretar a aplicação de sanções previstas em lei, assim como advertências conforme regulamentos internos e nas disposições contratuais.

8.3 Todas as disposições legais e demais normas da Medical Life, como o Código de Ética, devem ser rigorosamente observadas.

8.4 As sanções decorrentes do descumprimento das regras estabelecidas nesta Norma de Procedimento ou de outras Políticas Internas serão definidas e aplicadas pelo Compliance Officer a seu critério razoável, garantido ao Colaborador, contudo, amplo direito de defesa. O Compliance Officer poderá, consideradas as circunstâncias do caso e a seu critério razoável, concordar com o não cumprimento de determinadas regras.

8.5 É de responsabilidade de todos os Colaboradores (próprios e de Terceiros) comunicar qualquer violação e suspeita de violação aos requisitos desta Política. As comunicações de violação e suspeita de violação, identificadas ou anônimas, podem ser feitas diretamente ao Diretor de Compliance.

8.6 Todos os incidentes informados de suspeitas de violação desta Política serão investigados imediatamente e de forma apropriada. Se, depois da investigação, verificar-se que ocorreu uma conduta que infringe as regras dessa Política, serão tomadas medidas corretivas imediatas e exemplares, sempre de acordo com as circunstâncias, gravidade e a lei aplicável.

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

8.7 Qualquer colaborador, fornecedor, prestador de serviço, agente intermediário e outros parceiros que viole qualquer disposição desta Política estará sujeito a sanções disciplinares previstas no Código de Conduta da Medical Life, listadas abaixo:

- Advertência por escrito;
- Suspensão;
- Demissão sem justa causa;
- Demissão por justa causa;
- Exclusão do fornecedor, parceiro ou agente intermediário;
- Ação judicial.

IX. PROCEDIMENTOS

9.1 Aquisição de recursos de TI e atualização Sistêmica

- A área de Compras da Medical Life será acionada na obtenção de soluções de TI, incluindo o desenvolvimento ou atualização de sistemas, a prestação de serviços de manutenção, suporte, consultoria, treinamento, e toda e qualquer aquisição relacionada com tecnologia da informação.
- Todas as compras de TI serão administradas pela gerência da Medical Life e por indivíduos ou entidades funcionais designadas, e as etapas identificadas no processo de compras corporativas devem ser seguidas para a sua obtenção.

9.2 Instalação de equipamentos, softwares, e instalações físicas

- O Departamento de Tecnologia da Informação está autorizado a instalar todos os equipamentos e softwares necessários (servidores, terminais, impressoras, modems, roteadores, switches, etc) e supervisionar o projeto e a conclusão de todas as instalações físicas (edifícios, cabeamento, salas de informática, salas de rede, sistemas de proteção, etc.) que podem ser

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

necessárias para suportar os sistemas de computação, de telecomunicações, e de segurança da informação da Medical Life.

- Os colaboradores não têm permissão para instalar quaisquer dispositivos e/ou softwares em quaisquer estações de trabalho atribuídos a eles pela Medical Life.
- Não é permitida a transferência de informações da Empresa, sejam quaisquer arquivos, equipamentos, dispositivos e dados em qualquer forma, para dentro ou fora das dependências, instalações e sistemas da Empresa.
- Toda instalação ou aquisição deverá ser solicitada ao Departamento de Tecnologia da Informação.

9.3 Controles gerais de TI e de sistemas e aplicativos

- O estabelecimento, desenvolvimento, manutenção, revisão e melhoria de um programa completo de segurança abrangendo sistemas e telecomunicações, e de suas respectivas infraestruturas e dados, é de responsabilidade do Presidente ou outro pessoal de gestão autorizado da Medical Life.
- Os sistemas, dados, componentes de infraestruturas e informações relacionadas serão resguardados, protegidos de forma a proporcionar um ambiente operacional seguro.
- Os controles e segurança que devem existir incluem, mas não se limitam a: controles administrativos, proteção física de datacenter, controles operacionais, segurança de dados, informações e comunicações, desenvolvimento de sistemas, controles de manutenção, controles de aplicativos, e controles de centros computacionais.

9.4 Controles de operações

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

- A Medical Life deve estabelecer controles operacionais (políticas, procedimentos e tecnologias) para garantir que os centros computacionais sejam operados de maneira confiável.
- Esses controles incluem, mas não se limitam a controles sobre o acesso presencial, controles sobre o pessoal de operações, controles de manutenção de equipamentos de informática e de telecomunicações, e controle sobre mídias de arquivamento e instalações de armazenamento.

9.5 Segurança de Dados, Informação e Comunicação

- A Medical Life deve manter controles de integridade e segurança para a proteção de todos os sistemas de computação e telecomunicações, dados e informações.
- Esses controles também têm a intenção de cobrir os riscos decorrentes do potencial uso indevido de recursos dos sistemas de informática e telecomunicações.
- O estabelecimento desses controles deve incluir, mas não se limitar a: controles lógicos de acesso (sistema operacional, sistema de banco de dados, software aplicativo), segurança de rede e acesso local, identificação e autenticação de usuários, firewalls, controles criptográficos (criptografia, hashing etc.), controles de transmissão de mensagens (e-mail, telecomunicações, etc.), métodos de classificação de recursos de informação, retenção e descarte de informações, e um mecanismo de monitoramento, análise e resolução de incidentes de violação de dados e segurança.

9.6 Controles de aplicativos

- A equipe de TI autorizada da Medical Life garantirá por meio de mecanismos específicos (por exemplo, auditoria de TI) que todos os sistemas e aplicativos são desenvolvidos e operam com controles indicativos para garantir a precisão das informações. Estes podem ser:

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

controles de entrada, controles de processamento, controles de base de dados, controles de telecomunicações e controles de saída.

9.7 Controles dos centros computacionais

- Será responsabilidade do Departamento de Tecnologia da Informação da Medical Life (neste caso, o Coordenador - TI) garantir que os procedimentos operacionais de controle dos centros computacionais estejam em vigor.
- Estes podem incluir: biometria para determinar o acesso às instalações, procedimentos de backup e recuperação, monitoramento do desempenho do sistema (sistema operacional, banco de dados, rede), gerenciamento e resolução de problemas, procedimentos de controle de integridade e desempenho de aplicações, procedimentos de armazenamento em nuvem, procedimentos de teste do plano de recuperação de desastres, e procedimentos de monitoramento de incidentes de segurança e de violação de dados.

9.8 Continuidade dos sistemas de TI

- A administração da Medical Life deve garantir que os sistemas e procedimentos de backup adequados sejam estabelecidos e operados para todos os sistemas de computação e telecomunicações.
- Esses sistemas de backup devem ser estabelecidos para proteger a Empresa no caso de uma avaria imprevista ou de uma grande catástrofe.
- A Medical Life deve desenvolver e manter um plano que aborda o risco de que tais eventos possam ocorrer e isso deve exigir o planejamento de alternativas de processamento de sistemas de computação (incluindo, mas não limitado a instalações, equipamentos, procedimentos, etc.) para que possa garantir a continuidade dos negócios.
- Os requisitos para a continuidade dos sistemas de TI podem incluir, minimamente: identificação de sistemas críticos; avaliação de instalações

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

de processamento alternativas; planos de backup e recuperação documentados, procedimentos de teste, procedimentos de avaliação de contingência, procedimentos de armazenamento off-site; recuperação de dados e de equipamentos; e uma apólice de seguro.

9.9 Padrões de Segurança

- As normas de segurança dos sistemas de informação definem os critérios, regras e procedimentos mínimos estabelecidos pela Alta Administração da Medical Life e ratificados pelo Conselho de Administração, cuja implementação é necessária para ajudar a garantir o cumprimento da Política Segurança da Informação.
- Estes são implementados por vários funcionários (incluindo, mas não limitado ao Coordenador de TI, gerente de segurança, administrador de segurança do sistema, usuários finais, gerentes de divisão de TI etc.). Estes devem detalhar a especificação de cada procedimento e/ou controle a ser implementado.
- O Medical Life pratica a disseminação da cultura de Segurança da Informação aos seus funcionários, prestadores de serviços e estagiários por meio de treinamentos específicos focados em garantir a confidencialidade, integridade e disponibilidade das informações.

9.10 Padrões de segurança da informação adotados pela empresa:

- Proteção da informação: é diretriz que independentemente da forma apresentada que pode ser de forma básica, eletrônica, escrita ou falada ou como ela é compartilhada, armazenada ou transmitida, a informação seja utilizada unicamente à finalidade à qual foi autorizada pelo gestor da informação e não seja utilizada em meios não autorizados, e que toda informação de propriedade do Medical Life seja protegida de forma a não comprometer a sua confidencialidade, integridade ou disponibilidade.

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		



Norma de Procedimento TI e Segurança da Informação

Referência: 001-01
NP TISI
Data de emissão:
28/10/2021
Pág. 16

Assunto: Parâmetros de Segurança. Fiscalização Interna.

- Gestão, controle de acessos e rastreabilidade: os acessos às informações são realizados somente mediante autorização do responsável pela informação e são restritos a pessoas autorizadas.
- Autenticação: todo funcionário, estagiário ou prestador de serviços possui apenas um identificador (login) de acesso à informação.
- Prevenção contra vírus, arquivos e softwares maliciosos: a organização tem controles para prevenir que vírus e outros tipos de softwares maliciosos entrem e se espalhem nos sistemas de informação por meio de arquivos e softwares não homologados cuja instalação e uso são proibidos.
- Manutenção e cópias de segurança: a organização conta com procedimentos específicos para garantir a recuperação de dados e informações quando necessário.
- Classificação dos dados e das informações: a organização adota cinco categorias para efeitos de classificação da informação, Público; Interno; Confidencial; Confidencial restrito; ou secreto.
- Mesa limpa e descarte de informações: a Medical Life tem práticas orientadas aos funcionários, prestadores de serviço e estagiários para que não deixem informações à mostra e as descartem sempre que necessário.
- Confidencialidade: todos os contratos firmados com a Medical Life possuem cláusula de confidencialidade.
- Utilização dos recursos da informação: a Medical Life possui práticas em que apenas softwares disponibilizados e equipamentos configurados de acordo com o padrão da organização podem ser usados pelos funcionários, prestadores de serviço e estagiários.
- Prevenção a vazamento de informações: a Medical Life tem controles e políticas que previnem o vazamento de informações estabelecendo boas práticas para uso de correio eletrônico, acesso à internet, acesso remoto, uso de telefones móveis, comportamento dos funcionários, prestadores de

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		

serviços e estagiários em locais públicos e na troca de informações com fornecedores.

- Tratamento de incidentes cibernéticos: a Medical Life conta com mecanismos para prevenção de ameaças de origem cibernética. Todo e qualquer incidente de segurança cibernética, passa por uma análise e é classificado de acordo com o impacto causado pelo incidente, que pode ser crítico ou baixo de acordo com a classificação vigente. Caso um incidente de origem cibernética seja identificado pelo público geral, o mesmo deverá ser reportado pelo e-mail ti@medicalhealthrio.com.br.
- Gestão de continuidade de negócios: Identificando procedimentos e infraestrutura alternativa para proteger as pessoas, a reputação, os valores e os compromissos com os públicos relacionados. A Medical Life possui mecanismos de acionamento dos planos de continuidade de negócios em caso de desastres, tanto de origem cibernética como operacional.

X. DOCUMENTOS RELACIONADOS

- Carta de Compromisso da Diretoria
- Código de Ética;
- Norma de Procedimento de Gestão de Riscos;
- Constituição da República Federativa do Brasil;
- Lei nº 12.846/2013 (Lei Anticorrupção);
- Lei 13303/16 (Lei das Estatais);
- Decreto Federal nº 8.420/2015;
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD);
- ISO 19600 – Sistema de Gestão de Compliance;
- ISO 37001 – Sistema de Gestão Antissuborno;
- Lei Federal 9279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes);

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		



Norma de Procedimento TI e Segurança da Informação

Referência: 001-01
NP TISI
Data de emissão:
28/10/2021
Pág. 18

Assunto: Parâmetros de Segurança. Fiscalização Interna.

- Lei Federal 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);
- Lei de Crimes Cibernéticos – Lei 12.737/2012;
- Marco Civil da Internet – Lei 12.965/2014;
- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código e prática para a gestão da segurança da informação;
- Lei RJ 7753/17 (Lei sobre Programa de Integridade nas Empresas que contratarem com a Administração Pública);
- Lei Federal 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados).

Elaborado: Isabelle Moriggi	Assistente de Compliance		Próxima Revisão:
Revisado: Eloísa Guntzel	Gerente de Compliance		OUTUBRO/2025
Aprovado: Flavia Gerbassi	DDO		