SUMÁRIO

1. INTRODUÇÃO

A informação utilizada pela **IMPULSO** é um ativo valioso e deve ser gerida de forma adequada para assegurar sua disponibilidade, integridade, confidencialidade e privacidade, independentemente do meio pelo qual é coletada. A segurança e a privacidade das informações devem ser garantidas ao longo de todo o seu ciclo de vida, desde a coleta até o descarte seguro.

A **IMPULSO** estabelece sua Política de Segurança da Informação Externa ("Política") como parte integrante do seu Sistema de Gestão de Segurança e Privacidade da Informação ("SGSI/SGPI"), alinhando-se às melhores práticas e normas internacionalmente reconhecidas. Fica instituída esta Política, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação e privacidade da **IMPULSO**.

2. OBJETIVO

O objetivo desta Política é assegurar níveis adequados de proteção às informações da Companhia e àquelas sob sua responsabilidade, assegurando a confidencialidade, integridade e disponibilidade dos dados, bem como a privacidade de todas as partes envolvidas.

Além disso, esta Política tem como objetivos específicos:

- **I.** Estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;
- **II.** Estabelecer orientações gerais de segurança da informação e privacidade, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confidencialidade, privacidade e autenticidade das informações;
- **III.** Estabelecer competências e responsabilidades quanto à segurança da informação e privacidade;
- **IV.** Nortear a elaboração das políticas, procedimentos e outros documentos complementares necessários à efetiva implementação da segurança da informação e privacidade;
- **V.** Promover o alinhamento das ações de segurança da informação e privacidade com as estratégias de planejamento organizacional da **IMPULSO**.

3. ABRANGÊNCIA

Esta Política aplica-se a todos(as) os(as) funcionários(as), fornecedores e parceiros que possuam algum tipo de acesso aos ativos de informação da **IMPULSO**. Ela abrange todos os dados, sistemas, redes, dispositivos, aplicativos e processos envolvidos na coleta, armazenamento, processamento e transmissão de informações, independentemente do meio ou formato.

4. DEFINIÇÕES

Para o entendimento claro e consistente desta Política, são adotadas as seguintes definições:

Alta Liderança: Grupo de pessoas que formam o núcleo principal de liderança na Companhia, geralmente representado pelo CEO e liderados diretos.

Ativo(s) de Informação: Um "ativo de informação" pode ser compreendido como qualquer conteúdo, escrito ou não, que tenha valor ou relevância ao seu proprietário. Para a **IMPULSO**, serão

compreendidos como "ativos de informação" todos os documentos, arquivos, dados, relatórios, e-mails, impressos, bases de dados, contratos, propostas comerciais, bem como quaisquer informações ou dados que estejam relacionados à operação, estratégia, funcionamento, estrutura ou características da Companhia.

Controle de Acesso: Medidas para garantir que o acesso a ativos seja autorizado e restrito com base nos requisitos de negócios e segurança.

Companhia: A Impulso – Retail Media RD Saúde **("IMPULSO")**.

Confidencialidade: Refere à proteção de informações que não devem ser acessadas por indivíduos não autorizados.

Integridade: Está relacionado à plenitude do armazenamento dos dados, isto é, a garantia de que as informações não serão alteradas, excluídas ou manipuladas de forma indevida ou não autorizada.

Disponibilidade: Garantir que a informação possa ser obtida sempre que for necessário, isto é, que esteja sempre disponível para quem precisar dela no exercício de suas funções.

Titular(es): Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

5. DECLARAÇÃO

A **IMPULSO** reafirma seu compromisso com a segurança da informação e privacidade, implementando e monitorando rigorosamente seus controles para assegurar a confidencialidade, integridade, disponibilidade e privacidade de todos os ativos de informação. A atuação da Companhia é pautada pelo cumprimento das legislações vigentes e das melhores práticas de segurança da informação e privacidade.

6. DOS PRINCÍPIOS E DIRETRIZES

As ações de segurança da informação e privacidade da **IMPULSO** são guiadas pelos princípios que regem a boa governança corporativa e a responsabilidade empresarial, incluindo os seguintes princípios:

I. **Disponibilidade, integridade, confidencialidade, privacidade e autenticidade das informações:** Garantir que as informações estejam sempre acessíveis a quem precisa, sejam precisas e confiáveis, estejam protegidas contra acessos não autorizados e sua origem seja verificável.

II. **Continuidade dos processos e serviços essenciais:** Assegurar que os processos e serviços críticos para o funcionamento da **IMPULSO** e o atendimento aos clientes sejam mantidos de acordo com o SLA estabelecido, mesmo diante de eventuais incidentes de segurança da informação e/ou privacidade.

III. **Economicidade da proteção dos ativos de informação:** Proteger os ativos de informação de maneira eficaz e eficiente, otimizando recursos e garantindo o melhor retorno sobre os investimentos em segurança da informação e privacidade.

IV. Respeito ao acesso à informação, proteção de dados pessoais e privacidade: Assegurar que o acesso à informação seja equilibrado com a necessidade de proteger dados pessoais e respeitar a privacidade dos indivíduos, em conformidade com a legislação aplicável.

V. Responsabilidade do usuário: Estabelecer que todos os usuários de informação são responsáveis por suas ações, especialmente aquelas que possam comprometer a segurança dos ativos de informação.

VI. Alinhamento estratégico: Alinhar a presente Política com o planejamento estratégico da **IMPULSO**, garantindo coerência entre as medidas adotadas, os objetivos de negócio e as normas internas de segurança da informação e privacidade.

VII. Conformidade com legislação e regulamentos: Assegurar que todas as atividades de segurança da informação e privacidade estejam em conformidade com as leis e regulamentos aplicáveis, incluindo, mas não se limitando à Lei Geral de Proteção de Dados Pessoais ("LGPD") e outras legislações aplicáveis.

VIII. Educação e comunicação: Fomentar uma cultura de segurança da informação e privacidade por meio de programas contínuos de educação e comunicação, garantindo que todos(as) os(as) funcionários(as) estejam cientes de suas responsabilidades e das melhores práticas de segurança da informação e privacidade.

IX. Melhoria contínua: Promover a melhoria contínua das práticas de segurança da informação e privacidade, adaptando-se às novas ameaças e tendências tecnológicas.

6.1 Estas diretrizes constituem os principais pilares da gestão de segurança da informação e privacidade norteando a elaboração de políticas, procedimentos e documentos complementares no âmbito da **IMPULSO** e objetivam a garantia dos princípios básicos de segurança da informação e privacidade estabelecidos nesta Política.

6.2 As políticas, procedimentos e documentos complementares de segurança da informação e privacidade da **IMPULSO** devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação e privacidade.

6.3 As ações de segurança da informação e privacidade devem:

I. Considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade da **IMPULSO**;

II. Ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;

III. Visar à prevenção da ocorrência de incidentes.

6.4 O investimento necessário em medidas de segurança da informação e privacidade deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos à **IMPULSO**.

6.5 Toda informação gerada, custodiada, manipulada, utilizada ou armazenada pela **IMPULSO** constitui um ativo de informação e deve ser protegida de acordo com as diretrizes estabelecidas pela Companhia.

6.6 Pessoas e sistemas devem operar com o menor nível de privilégio e o mínimo acesso necessário para a execução de uma tarefa específica.

6.7 A presente Política e suas atualizações, bem como as políticas específicas de segurança da informação e privacidade da **IMPULSO** devem ser amplamente divulgadas a todos(as) os(as) funcionários(as) com o objetivo de promover sua observância, conscientização e a formação de uma cultura sólida de segurança da informação e privacidade.

6.8 Os(As) funcionários(as) da **IMPULSO** devem ser continuamente capacitados em procedimentos de segurança da informação e privacidade e no uso correto dos ativos de informação durante o desempenho de suas funções, visando a minimizar possíveis riscos à segurança da informação e privacidade.

6.9 As ações de capacitação mencionadas no item 6.8 acima, deverão contar com orientações atualizadas sobre as políticas internas da Companhia e capacitar os(as) funcionários(as) para lidar com aspectos de privacidade e segurança da informação no dia a dia de suas atividades.

6.10 Todos os contratos de prestação de serviços celebrados entre a **IMPULSO** e seus fornecedores devem incluir uma cláusula específica estabelecendo que o fornecedor declara ter ciência desta Política de Segurança da Informação, bem como com quaisquer outras políticas ou normas correlatas.

7. PAPÉIS E RESPONSABILIDADES

7.1 A estrutura de Gestão de Segurança da Informação e Privacidade é composta por:

I. **Alta Liderança:** Responsável por garantir que as demais lideranças da **IMPULSO** conheçam e estejam comprometidas com as diretrizes da presente Política e por alocar os recursos necessários, de acordo com o que for cabivel e razoável, para a implementação da presente Política.

II. **Encarregado (DPO):** Responsável por manter a presente Política atualizada, comunicar mudanças relevantes, assegurar que a Alta Liderança da Companhia esteja ciente do seu conteúdo e comprometida com o seu cumprimento, bem como assegurar que as respectivas áreas de negócio sejam devidamente comunicadas a respeito da importância de uma gestão eficaz de segurança da informação e privacidade na Companhia. O Encarregado também é responsável por promover uma cultura de segurança da informação e privacidade na Companhia; orientar os(as) funcionários(as) e reforçar a relevância da presente Política na Companhia; além de analisar as comunicações de incidentes e avaliar a probabilidade da sua verdadeira ocorrência e comunicar o incidente à Agência Nacional de Proteção de Dados ("ANPD") e aos Titulares afetados, sempre que necessário.

III. **Segurança e Tecnologia da Informação:** Responsável por monitorar eventos de tecnologia que possam representar um risco potencial ou concreto de materializar um incidente; atuar diretamente para resolver o incidente, avaliando, propondo, implementando e fiscalizando a implementação das medidas físicas, técnicas e organizacionais necessárias para a sua resolução definitiva; contribuir com o Encarregado para a avaliação e classificação do incidente, fornecendo as informações técnicas necessárias.

IV. **Todos os Usuários:** Todos(as) os(as) funcionários(as) ou fornecedores que tenham acesso aos sistemas e informações da **IMPULSO** são responsáveis por cumprir esta Política, bem como as diretrizes, medidas e procedimentos associados. Devem agir de forma a proteger a confidencialidade, integridade e disponibilidade e a privacidade das informações, reportando imediatamente para o Encarregado quaisquer incidentes de segurança da informação e/ou privacidade, potenciais ou confirmados.

7.2 Esta Política, juntamente com os demais documentos de segurança da informação e privacidade derivados desta Política, faz parte do arcabouço normativo da Gestão de Segurança da Informação e Privacidade da **IMPULSO**.

7.3 A Gestão da Segurança da Informação e Privacidade é composta, no mínimo, pelos seguintes processos:

I. **Tratamento da informação:** Processos relacionados à classificação, armazenamento, transmissão, e descarte seguro de informações sensíveis e confidenciais;
II. **Segurança física e do ambiente:** Medidas para proteger instalações físicas e o ambiente de TI contra acessos não autorizados, danos ou interferências;
III. **Gestão de incidentes em segurança da informação e privacidade:** Processos para detectar, responder e recuperar-se de incidentes de segurança da informação e privacidade que possam comprometer a confidencialidade, integridade, disponibilidade e/ou privacidade das informações;
IV. **Gestão de ativos:** Inventário e controle de ativos de informação, assegurando sua proteção adequada ao longo de seu ciclo de vida;
V. **Gestão do uso dos recursos operacionais e de comunicações:** Normas para o uso seguro e adequado de recursos como e-mail, acesso à internet, mídias sociais e serviços de computação em nuvem;
VI. **Controles de acesso:** Implementação de mecanismos de controle para garantir que apenas indivíduos autorizados tenham acesso a recursos e informações específicos;
VII. **Gestão de riscos:** Identificação, avaliação e tratamento de riscos associados à segurança da informação e privacidade;
VIII. **Gestão de continuidade:** Planejamento e implementação de medidas para assegurar a continuidade dos processos críticos de negócio em caso de incidentes de segurança da informação ou interrupções;
IX. **Auditoria e conformidade:** Processos para avaliar a conformidade com a política de segurança da informação, normas internas, e regulamentações externas, incluindo auditorias regulares.

7.4 Para cada um dos processos que constituem a Gestão de Segurança da Informação e Privacidade, deve ser observada a pertinência de elaboração de políticas, procedimentos e outros documentos como orientações ou manuais que disciplinem ou facilitem o seu entendimento em conformidade com a legislação vigente e melhores práticas de segurança da informação e privacidade.

7.5 Esses processos formam a base da Gestão da Segurança da Informação e Privacidade na **IMPULSO**. As políticas, procedimentos e outros documentos que regem esses processos devem, no mínimo, abranger os seguintes aspectos:

I. Conformidade com as diretrizes da LGPD e demais normativos e orientações emitidas pela ANPD.
II. Classificação da informação de acordo com seu nível de confidencialidade e criticidade, determinando os controles de segurança apropriados.

III. Proteção de dados contra acessos não autorizados e eventos acidentais ou ilícitos de destruição, perda, alteração, comunicação, ou qualquer forma de tratamento inadequado ou ilegal.

IV. Uso aceitável das informações e a utilização adequada de mídias de armazenamento.

V. Controle da entrada e saída de ativos de informação das instalações da Companhia.

VI. Definição e proteção dos perímetros de segurança da Companhia.

VII. Controles de acesso baseados no princípio do menor privilégio.

VIII. Procedimentos para identificação, contenção, erradicação e recuperação de incidentes, bem como atividades pós-incidente.

IX. Critérios para a comunicação de incidentes aos titulares de dados pessoais e à ANPD, quando aplicável.

X. Política de Gestão e Resposta a Incidentes de Segurança da Informação.

XI. Política de Gestão de Ativos da Companhia, incluindo a proteção dos ativos, sua classificação segundo a criticidade, manutenção de inventário atualizado de ativos, uso aceitável dos ativos, mapeamento de vulnerabilidades e ameaças, monitoramento de ativos conforme princípios legais, e investigação de sua operação quando houver indícios de quebra de segurança e privacidade.

XII. Utilização adequada dos recursos operacionais e de comunicações fornecidos pela **IMPULSO**, assegurando que sejam utilizados apenas para fins profissionais e em conformidade com princípios éticos, evitando comportamentos que comprometam a reputação da Companhia.

XIII. Políticas para acesso à internet, incluindo o *download* de arquivos e a proibição do uso de sites inadequados e da instalação de software não autorizado.

XIV. Regras para o uso de mídias sociais, a divulgação de informações, o uso de contas pessoais para fins profissionais e a interação nas mídias sociais.

XV. Políticas e procedimentos de controle de acesso, incluindo o uso de Múltiplo Fator de Autenticação (MFA), controles de autorização baseados no princípio do menor privilégio, segregação de funções, auditorias, e gestão de acessos para ativos de informação.

XVI. Gestão de riscos de segurança da informação e privacidade, incluindo a análise do ambiente e ativos da Companhia, identificação e documentação de riscos, avaliação e tratamento de riscos, e implementação de controles de segurança.

XVII. Gestão de Continuidade de Negócios, incluindo o Plano de Continuidade para manter as atividades em caso de incidentes de segurança da informação e realização de testes periódicos para garantir a eficácia do plano.

XVIII. Gestão de Mudanças nos ativos de informação, baseada em relatórios de avaliação e tratamento de riscos, com designação de papéis e responsabilidades e criação de um processo formal para solicitação e documentação de mudanças.

XIX. Auditoria e conformidade da organização, incluindo um Plano de Verificação de Conformidade que defina unidades abrangidas, aspectos a serem verificados, atividades a serem realizadas, documentos necessários, e elaboração de Relatório de Avaliação de Conformidade com recomendações.

7.6 A **IMPULSO** realiza auditorias internas periódicas de segurança da informação e privacidade para garantir conformidade com esta Política e com outros requisitos de segurança da informação e privacidade aplicáveis.

7.7 As atividades, produtos e serviços desenvolvidos pela **IMPULSO** devem cumprir os requisitos de privacidade e proteção de dados pessoais estabelecidos em leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes.

8. DAS VEDAÇÕES E DISPOSIÇÕES FINAIS

8.1 São vedadas as seguintes ações em relação à segurança da informação e privacidade:

I. O uso de informações e recursos de tecnologia da informação da **IMPULSO** para fins não autorizados ou incompatíveis com as atividades profissionais, incluindo, mas não se limitando a, uso pessoal, atividades ilícitas, imorais ou qualquer uso que possa comprometer a segurança, privacidade e a integridade dos sistemas e dados.

II. A instalação de qualquer *software* ou a alteração de parâmetros de configuração de computadores da **IMPULSO** de maneira diferente daquelas autorizadas pelo departamento de Tecnologia da Informação, bem como o uso de *softwares* ilegais (sem licenciamento).

III. A transferência e o armazenamento de dados ou informações profissionais por meio de ferramentas de armazenamento em nuvem não homologadas pela **IMPULSO**.

IV. O uso de ferramentas que visam ocultar os acessos à internet ou burlar os controles de segurança.

V. Uso de mídias removíveis e/ou tecnologias portáteis que proporcionem o armazenamento e transporte de dados, como *pen drives*, cartões de memória, HD externo, entre outros.

VI. A desativação, remoção ou a alteração de configurações dos programas de antivírus, exceto se autorizado pelo departamento de Tecnologia da Informação.

VII. A gravação de arquivos particulares (músicas, filmes, fotos etc.) nos diretórios de rede da **IMPULSO**.

VIII. Qualquer tipo de *upload/download* de informações de propriedade da **IMPULSO** ou de seus clientes em sites não autorizados, que efetuem manipulação da informação ou conversão de arquivos, sem prévia autorização.

IX. O cadastro do endereço de correio eletrônico (e-mail) corporativo em redes sociais ou outros sites e serviços sem relação com as finalidades legítimas aos negócios da **IMPULSO.**

X. A replicação, sincronização ou cópia de segurança (*backup*) do conteúdo de e-mails contendo informações corporativas da **IMPULSO** para qualquer serviço em nuvem não homologado pela **IMPULSO.**

XI. O acesso, armazenamento, transmissão, processamento e/ou impressão de material de conteúdo impróprio, tais como: pedofilia, pornografia, erotismo, violência, terrorismo, racismo, intolerância.

XII. A violação da propriedade intelectual da **IMPULSO** ou de outras empresas da RD Saúde, quer seja por meio da utilização indevida de imagens, textos, *softwares*, marcas ou pela cópia indevida de originais ou conversão do formato desses.

XIII. Utilizar a internet para violar, de qualquer forma, o direito de pessoas, empresas, organizações ou governos, inclusive, mas não somente, os de propriedade intelectual, autorais, marcas, patentes, privacidade, segredos de indústria ou segredos de negócios.

XIV. O uso do correio eletrônico *(e-mail)* para envio de mensagens que possam comprometer a imagem da **IMPULSO** perante seus clientes e a comunidade em geral ou que possam causar prejuízo moral e/ou financeiro à **IMPULSO** ou a terceiros.

XV. O envio e armazenamento de mensagens que sejam consideradas: correntes, spams, pornográficas, eróticas, obscenas, discriminatórias, ilegais, ofensivas, perturbadoras, racistas, imorais ou que violem direitos de imagem e/ou propriedade intelectual, bem como forjar, adulterar mensagens de e-mail ou simular a identidade de outra pessoa ao enviar uma mensagem.

8.2 As denúncias de violação, bem como os casos omissos e as dúvidas sobre esta Política devem ser submetidas ao Encarregado da **IMPULSO** e devem ser feitas no endereço eletrônico encarregado@impulsomidia.com.

8.3 Esta Política deverá ser revisada periodicamente, com frequência mínima anual, ou sempre que houver mudanças significativas nos requisitos legais, regulamentares ou nos processos internos da **IMPULSO**.