POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Data de emissão e aprovação: 15/08/2024	**Data da revisão:** 15/08/2024	**Versão:** 2.0
Elaborado por: Diretoria de Operações	**Aprovado por:** Diretoria	

CLÁUSULA PRIMEIRA - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS

1. INTRODUÇÃO

PÚBLICO

Conforme definição da norma NBR ISO/IEC 17799: 2005, a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegido. Nesse diapasão a Política de Segurança da Informação prima pela proteção dos dados produzidos, coletados ou de conhecimento da INFINITY IT SERVICES de diversos tipos de ameaça, para garantir a integridade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

Assim, a Política de Segurança da Informação (PSI) é uma declaração formal da INFINITY IT SERVICES acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda ou de seu conhecimento, devendo ser cumprida por todos os seus funcionários, parceiros e clientes.

Por princípio, a segurança da informação deve abranger três aspectos básicos, que são dispostos nesta Política conforme destacados a seguir:

- Confidencialidade: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação com o regular monitoramento dos responsáveis;
- Integridade: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações com a salvaguarda dos métodos de processamento;
- Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

2. ABRANGÊNCIA

Todos os funcionários, executivos, prestadores de serviços, consultores, clientes, fornecedores, parceiros diversos e demais contratados que estejam a serviço e compartilhem e/ou utilizem ativos corporativos da INFINITY IT SERVICES. Esta Política também reflete a governança aplicada aos temas de proteção de Dados Pessoais pela INFINITY IT SERVICES. A observância desta Política é obrigatória e reflete a legislação e regulamentação aplicáveis relacionadas à Lei Geral de Proteção de Dados.

3. OBJETIVO

Garantir a integridade, confidencialidade, conformidade e autenticidade da informação necessária para a realização dos negócios da INFINITY IT SERVICES junto aos seus Clientes, com o objetivo de proteger os dados porventura tratados, os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

4. DOCUMENTOS DE REFERÊNCIA

- NBR ISO/IEC 17799:2005
- ABNT 21:204.01-010
- ISO 27001 e 27002
- Lei 9.609/98 – Lei do Software
- Lei 12.965/2014 - Marco Civil da Internet.
- Lei 13.709/18 – LGPD

5. TERMOS E DEFINIÇÕES

- TI: Tecnologia da Informação;
- Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada por meio de softwares;
- Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados;
- Colaborador(es): Funcionários ou Prestadores de serviços contratados pela INFINITY IT SERVICES para execução de serviços;
- Terceiros: Clientes e seus prepostos e Fornecedores e seus prepostos;
- Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: Pen Drive, cartão de memória entre outros;
- USB: É um tipo de conexão "ligar e usar" que permite a ligação de periféricos sem a necessidade de desligar o computador;
- VPN (Virtual Private Network): Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da INFINITY IT SERVICES;
- Softwares de Mensageria: São programas que permitem a usuários se comunicarem remotamente (à distância), por meio de conexão com a Internet;
- Firewall: É um dispositivo de uma rede de computadores que tem por objetivo aplicar um procedimento de segurança a um determinado ponto da rede.
- Documentos: Contratos ou correspondências de cunho negocial ou operacional disponibilizados pela INFINITY IT SERVICES ou seus contratantes.

6. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

6.1. DEFINIÇÃO

Cabe a todos os Colaboradores e Terceiros cumprir fielmente a Política de Segurança da Informação. Os Colaboradores da INFINITY IT SERVICES devem sempre que necessário buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados em seu ambiente e sempre que possível mesmo no ambiente de Terceiros; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela INFINITY IT SERVICES; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente a empresa quando do descumprimento ou violação desta Política, por meio do e-mail: dpo@infinityitservices.com.br.

6.2. RESPONSABILIDADE DE CADA ÁREA

6.2.1. ÁREA OPERACIONAL DE TECNOLOGIA DA INFORMAÇÃO

- Cabe a área propor ajustes, melhorias, aprimoramentos e modificações desta Política e submeter para aprovação de Sócios e Diretores com periodicidade máxima de 12 (doze) meses;

- Convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política; prover todas as informações de gestão de segurança da informação solicitadas por Diretores/sócios.

- Colher a assinatura do Termo de Adoção da Política de Segurança da Informação de todos os colaboradores (terceiros, estagiários, temporários, CLT's, associados, sócios e outros);

- Colher a assinatura do Termo de Sigilo e Confidencialidade (NDA) dos funcionários e estagiários, arquivando-o nos respectivos prontuários;

- Indicar aos seus colaboradores, conforme os documentos firmados, que existe a cessão de propriedade intelectual para a INFINITY IT SERVICES e obrigação de não concorrência.

- Informar, prontamente, à equipe de TI (Controle de Acesso), todos os desligamentos, afastamentos e modificações no quadro funcional da empresa.

- Manter atualizado os controles sobre os acessos a sistema de Terceiros com a indicação do responsável, horário, meio, objetivo e ambiente acessados;

- Estabelecer os ativos de informação que mantêm acesso privilegiado tais como: sistemas operacionais instalados nos servidores e em estações de trabalho, banco de dados, servidores web (front-end), servidores de aplicação web (web application), servidores de correio e proxy web, dispositivos de redes de dados (switches, roteadores e firewalls);

6.2.2. DIRETORES/ SÓCIOS

a) Aprovar os termos da Política de Segurança da Informação e suas revisões periódicas. Incentivar e difundir os preceitos estabelecidos pela INFINITY IT SERVICES para assegurar a Segurança da Informação em todo o seu tratamento.
b) Fica o sócio Rodolfo Bento Matos, Diretor de Operações, nomeado como Encarregado de Proteção de Dados (DPO) conforme Anexo I - Termo de Nomeação de Encarregado de Proteção de Dados (DPO);

c) É de responsabilidade dos Sócios da INFINITY IT SERVICES estabelecer critérios relativos ao nível de confidencialidade da informação gerada pela empresa de acordo com os critérios a seguir:

i) Pública: É uma informação da INFINITY IT SERVICES ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma. São exemplos de informação pública: Editais de licitação e Informações disponibilizadas no site;

ii) Confidencial: É uma informação da INFINITY IT SERVICES e/ou de seus Contratantes que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à INFINITY IT SERVICES ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou colaboradores. São exemplos de informações confidenciais: Exames e diagnósticos de pacientes, informações disponíveis nos sistemas de Clientes e dados cadastrais de funcionários.

iii) Restrita: É toda informação que pode ser acessada somente por usuários da INIFINITY IT SERVICES explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. São exemplos de informações restritas: código fonte e arquitetura de um projeto.

6.2.3. COLABORADORES E PRESTADORES DE SERVIÇO

a) Seguir Políticas e Procedimentos: Cumprir todas as políticas e procedimentos de segurança da informação estabelecidos pela organização.
b) Proteção de Senhas: Manter senhas seguras e não as compartilhar com terceiros.
c) Identificação de Ameaças: Relatar imediatamente qualquer atividade suspeita ou violação de segurança à equipe de segurança da informação.
d) Uso Adequado dos Recursos: Utilizar os recursos de TI e sistemas de informação de acordo com as políticas estabelecidas, evitando o acesso não autorizado.
e) Treinamento em Segurança: Participar de treinamentos regulares de conscientização em segurança da informação para estar ciente das melhores práticas.
f) Acesso Controlado: Acessar apenas os sistemas e informações estritamente necessários para a execução de suas funções.
g) Confidencialidade: Manter a confidencialidade das informações da organização e não divulgar a terceiros sem autorização.

7. PROCESSO DE DIVULGAÇÃO DA PSI

7.1. A Política de Segurança da Informação deve ser de conhecimento de todos os Colaboradores, portanto deve ser amplamente divulgada, inclusive e principalmente para novos colaboradores. Os métodos de divulgação, serão:

a. Campanhas internas de conscientização;
b. Treinamentos mandatórios de funcionários e parceiros com atualizações anuais;

c. Site público da INFINITY IT SERVICES onde permanecerá disposta de maneira que seu conteúdo possa ser consultado a qualquer momento.

8. PROPRIEDADE INTELECTUAL

8.1. É de propriedade da INFINITY IT SERVICES, todos os "designs", criações, softwares, produtos ou procedimentos desenvolvidos por qualquer funcionário/prestador durante o curso de seu vínculo com a INIFINITY IT SERVICES, de forma que a reprodução e/ou comercialização sem a autorização expressa dos sócios da INFINITY IT SERVICES é crime punível pelo que preceitua o Código Penal e a Lei 9.610 de 19 de fevereiro de 1998, sem exclusão da responsabilização civil pelos danos provocados à INFINITY IT SERVICES. Eventual disposição diferente só será admissível se expressamente disposta em contrato.

9. SEGURANÇA DA INFORMAÇÃO

9.1. DIRETRIZES

Para assegurar a confidencialidade, integridade e disponibilidade da Informação obtida, coletada ou produzida pela INFINITY IT SERVICES, esta deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, divulgação não-autorizada, acidentes e outras ameaças.

Assim, para atingir os objetivos da INFINITY IT SERVICES, os Colaboradores devem prover uma cultura proativa de salvaguarda das informações por meio de ações que evidenciem um comportamento seguro e consistente com o objetivo de proteção, devendo permanecerem engajados com os procedimentos e instruções periodicamente compartilhadas por meio do Código de Boas Práticas e treinamentos regulares.

A INFINITY IT SERVICES se compromete a prover Campanhas contínuas de conscientização de Segurança da Informação que serão utilizadas para monitoramento e controle destas diretrizes.

9.1.1. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

a) As máquinas (servidores) que armazenam sistemas da INFINITY IT SERVICES estão em ambiente protegido – CLOUD DA MICROSOFT AZURE e ORACLE CLOUD, com acessos controlados e devidamente monitorados.
b) O acesso às dependências da empresa com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização dos sócios. Exceto para eventos e treinamentos organizados pela própria empresa.
c) É dever de todos os Colaboradores respeitar áreas e projetos de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada um.

9.2. REQUISITOS DE SEGURANÇA NO AMBIENTE TECNOLÓGICO

9.2.1. DIRETRIZES GERAIS

a) Todo acesso as informações e aos ambientes tecnológicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuadamente pela área de Tecnologia da Informação;

b) O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.
c) O Provedor de serviços em cloud contratado deverá manter controles adequados de proteção de perímetro que mitiguem ataques sobre falhas de códigos de desenvolvimento, invasões, vazamento de informações entre outros.

9.2.2. DIRETRIZES ESPECIFICAS

a) Sistemas: Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida;
b) Cópia de segurança (Backup): apenas quando contratado junto a terceiros, deve ser testado e mantido atualizado para fins de recuperação em caso de desastres por prazo determinado;
c) É vedado ao colaborador executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos, sem a observância do procedimento específico, ou ainda executar qualquer ação que provoque a indisponibilidade de serviços, a instalação de equipamentos, armazenamento de arquivos ou mesmo promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa ou de terceiros;
d) Também é vedado enviar informações confidenciais (autorizadas) para e-mails externos sem proteção. No mínimo, o arquivo deve contar com a proteção de uma senha “robusta”.
e) A base de dados armazenada em cloud deve obrigatoriamente estar segregada dos demais clientes do provedor ou em contêiner multi tenant, ou ainda, tenha os acessos segregados por compartilhamento.
f) Os ambientes (desenvolvimento, homologação e produção) criados nos provedores de Cloud devem permanecer isolados, não sendo possível a comunicação entre eles.

10. DA GESTÃO DE ACESSOS

10.1. DIRETRIZES

A empresa implementará mecanismos adequados de controle de acesso para garantir que apenas usuários autorizados possam acessar os recursos e dados na nuvem. Será adotada uma abordagem baseada no princípio do menor privilégio, garantindo que os usuários tenham apenas as permissões necessárias para desempenhar suas funções.

10.2. DEFINIÇÕES

a) Tipos de Acesso:
   I. Privilegiado: acessar recursos ou informações críticas dentro da organização com um nível de autorização elevado, ou seja, informações ou sistemas que desempenham funções essenciais na operação ou manutenção dos sistemas de informação da empresa;
   II. Terceiros: O acesso de terceiros é o acesso concedido a indivíduos, organizações ou entidades externas à organização, que podem precisar interagir com sistemas

ou informações internas por motivos específicos, como fornecedores, prestadores de serviços, parceiros de negócios ou consultores externos.

III. Comum: refere-se ao acesso concedido a usuários regulares ou funcionários da organização que precisam acessar informações ou recursos em seu curso normal de trabalho. Esse acesso é concedido com base nas necessidades do trabalho e é geralmente restrito a áreas específicas relevantes para as funções do usuário

10.3. REQUISITOS PARA A CONCESSÃO DE ACESSOS E DIRETRIZES PARA REVISÃO

a) Necessidade de Negócio: Qualquer solicitação de acesso a sistemas ou informações deve ser justificada com base na necessidade de negócios. Os solicitantes devem explicar como o acesso apoiará suas responsabilidades e funções.
b) Autorização por E-mail: As solicitações de acesso devem ser acompanhadas por uma autorização por e-mail de um supervisor ou gerente responsável, confirmando a necessidade do acesso.
c) Verificação de Identidade: Antes da concessão de acesso, os solicitantes devem passar por um processo de verificação de identidade para garantir que são quem afirmam ser.
d) Aprovação da Equipe de Segurança: As solicitações de acesso devem ser revisadas e aprovadas pela equipe de segurança da informação ou por um comitê de acesso, garantindo que estejam em conformidade com as políticas de segurança.
e) Revisão de Necessidade Contínua: A equipe de TI deve revisar continuamente se os usuários ainda têm uma necessidade comercial justificável para o acesso concedido. Se a necessidade não existir mais, o acesso deve ser revogado imediatamente.
f) Revisão de Privilégios: Os privilégios de acesso devem ser revisados para garantir que não tenham sido aumentados sem autorização ou que não tenham sido explorados de maneira inadequada.
g) Revisão de Logs e Monitoramento: Os registros de acesso e atividade devem ser revisados regularmente em busca de atividades suspeitas ou violações de segurança.
h) Ação Corretiva: Qualquer problema identificado durante a revisão deve ser tratado prontamente. Isso pode incluir a revogação de acesso, treinamento adicional ou ações disciplinares, conforme apropriado.

10.4. GESTÃO DE ACESSOS PRIVILEGIADOS

a) Identificação de Funções Privilegiadas: Identificar as funções e cargos que exigem acesso privilegiado aos sistemas e informações. Isso pode incluir administradores de sistemas, administradores de banco de dados, gerentes de segurança da informação, entre outros.
b) Documentação de Justificativa: Exigir que todas as solicitações de acesso privilegiado sejam devidamente documentadas, incluindo uma justificativa clara de porque a pessoa precisa de acesso privilegiado.
c) Revisão da Necessidade Contínua: Periodicamente, revisar se os titulares de acesso privilegiado ainda têm uma necessidade legítima e contínua de acesso privilegiado. Isso deve ser feito em intervalos regulares, como trimestralmente.
d) Procedimentos de Emissão e Revogação: Estabelecer procedimentos claros para a emissão e revogação de privilégios de acesso privilegiado. Isso deve incluir aprovações por membros da alta administração.
e) Justificativa por Escrito: Toda solicitação de acesso privilegiado deve ser acompanhada por uma justificativa por escrito, explicando por que o acesso é necessário para o desempenho das funções do solicitante.

f) Aprovação de Autoridades Competentes: As solicitações de acesso privilegiado devem ser aprovadas por autoridades competentes, como o CTO (Chief Technology Officer) ou ou COO (Chief Operations Officer).
g) Mínimo Privilégio: Adote o princípio do "princípio do privilégio mínimo", o que significa que os usuários devem receber apenas os privilégios necessários para realizar suas tarefas, e não mais.

11. POLÍTICA DE GERENCIAMENTO DE MUDANÇAS

11.1. DIRETRIZES

Garantir que todas as alterações nos sistemas, infraestrutura e processos de TI sejam planejadas, avaliadas, autorizadas e implementadas de forma controlada para minimizar riscos à segurança da informação e ao ambiente tecnológico. Esta política se aplica a todos os sistemas de informação, infraestrutura de TI e processos relacionados à organização.

10.2. RESPONSABILIDADES

a) A equipe de TI é responsável por planejar, avaliar, testar e implementar todas as mudanças tecnológicas.
b) A Diretoria de Tecnologia é responsável por revisar e autorizar todas as mudanças propostas.
c) A equipe de Segurança da Informação deve avaliar o impacto das mudanças na segurança.
d) Os usuários finais devem relatar qualquer impacto adverso decorrente das mudanças.

11.3. PROCESSO DE GERENCIAMENTO DE MUDANÇAS

a) Solicitação de Mudança: Qualquer alteração deve ser solicitada e documentada, incluindo sua justificativa, escopo e impacto.
b) Avaliação de Impacto: A equipe de TI avaliará o impacto potencial da mudança na segurança da informação e no ambiente tecnológico.
c) Aprovação e Autorização: A Diretoria de TI revisará as solicitações e autorizará ou negará a implementação das mudanças.
d) Planejamento e Testes: As mudanças autorizadas serão planejadas e testadas em um ambiente controlado antes da implementação.
e) Implementação: A mudança será implementada de acordo com o plano aprovado.
f) Monitoramento e Avaliação: A equipe de TI monitorará a mudança após a implementação e avaliará seu impacto.
g) Documentação e Comunicação: Todas as mudanças e seus resultados serão documentados e comunicados aos interessados.
h) Controle de Mudanças de Emergência: Mudanças de emergência podem ser realizadas quando necessário para evitar danos à segurança ou à continuidade dos negócios. No entanto, essas mudanças devem ser documentadas e revisadas retrospectivamente pela Diretoria de TI;

12. DO MONITORAMENTO E RESPOSTAS A INCIDENTES

12.1. DIRETRIZES

Garantir a detecção precoce, o registro adequado e a resposta eficaz a incidentes de segurança da informação para proteger os ativos e a confidencialidade, integridade e disponibilidade das informações da organização. Esta política se aplica a todos os sistemas de informação, infraestrutura de TI e processos relacionados à organização.

12.2. RESPONSABILIDADES

a) A equipe de Segurança da Informação é responsável pelo monitoramento contínuo de eventos de segurança e pela resposta a incidentes.
b) Os administradores de sistemas devem cooperar com a equipe de Segurança da Informação e notificar imediatamente qualquer incidente detectado.
c) Os usuários finais devem relatar incidentes de segurança de imediato à equipe de TI.

12.3. PROCESSO DE MONITORAMENTO E RESPOSTA A INCIDENTES

a) Monitoramento Contínuo: A equipe de Segurança da Informação monitora continuamente os sistemas e redes em busca de eventos e indicadores de comprometimento de segurança.
b) Detecção de Incidentes: Quando um evento suspeito é identificado, ele é analisado para determinar se constitui um incidente de segurança da informação.
c) Classificação de Incidentes: Os incidentes são classificados em níveis de gravidade com base no impacto potencial, como crítico, alto, médio ou baixo.
d) Notificação e Documentação: Se um incidente é confirmado, a equipe de resposta a incidentes é notificada imediatamente. O incidente é documentado de forma detalhada, incluindo a hora de detecção, origem, natureza e impacto.
e) Isolamento e Contenção: Se necessário, medidas imediatas de isolamento e contenção são implementadas para impedir a disseminação do incidente e minimizar danos.
f) Análise Forense: A equipe de resposta a incidentes conduz uma análise forense para determinar a natureza e a extensão do incidente, bem como sua causa raiz.
g) Resposta e Recuperação: Com base na análise, é desenvolvido um plano de resposta que inclui ações para mitigar os impactos do incidente e restaurar a operação normal.
h) Notificação às Partes Interessadas: As partes interessadas, como a alta administração e autoridades regulatórias, são notificadas de acordo com as políticas de notificação estabelecidas.
i) Lições Aprendidas e Melhorias: Após a conclusão da resposta ao incidente, uma revisão é realizada para aprender com o incidente e implementar melhorias nos controles de segurança.
j) Revisão Contínua: O processo de monitoramento e resposta a incidentes é revisado e aprimorado continuamente para se adaptar às ameaças emergentes.

13. DO PLANO DE CONTINUIDADE DE NEGÓCIOS E OS RISCOS DA OPERAÇÃO

13.1 DIRETRIZES

Este plano de continuidade de negócios e mitigação de riscos visa proteger as operações críticas da organização, garantindo que as ações corretivas sejam tomadas em situações de crise e que a organização possa continuar a operar com o mínimo de interrupção possível. Ele está alinhado com a política de segurança da informação da organização e enfatiza a importância da preparação e da gestão de riscos.

13.2 PROCESSO DE CONTINUIDADE DE NEGÓCIO

a) Avaliação de Riscos: Realizar avaliações de risco para identificar ameaças à segurança da informação e os riscos associados a interrupções operacionais.
b) Identificação de Ativos Críticos: Identificar os ativos de informação críticos e os processos de negócios dependentes desses ativos.
c) Estratégias de Recuperação: Estabelecer estratégias de recuperação para operações críticas, incluindo locais de recuperação alternativos, sistemas de backup e planos de ação.
d) Procedimentos de Resposta a Incidentes: Ter procedimentos documentados para responder a incidentes, incluindo ação imediata, investigação, mitigação e recuperação.
e) Comunicação: Estabelecer planos de comunicação claros para notificar as partes interessadas internas e externas em caso de interrupções ou incidentes.
f) Testes e Exercícios: Realizar exercícios regulares para testar a eficácia do plano de continuidade de negócios e garantir que a equipe esteja preparada.
g) Treinamento e Conscientização: Treinar a equipe de continuidade de negócios e conscientizar todos os funcionários sobre seus papéis em situações de crise.
h) Revisão e Atualização: Revisar o plano de continuidade de negócios periodicamente para garantir sua relevância e eficácia.
i) Conformidade: Garantir que o plano de continuidade de negócios esteja em conformidade com as regulamentações e padrões de segurança aplicáveis.
j) Mitigação de Riscos: Implementar medidas proativas de mitigação de riscos para reduzir a probabilidade e o impacto de incidentes de segurança da informação.

14. DISPOSIÇÕES FINAIS

Esta política entrará em vigor a partir de sua data de aprovação pela Diretoria Conselho de Administração. A revisão de seu conteúdo se dará a cada 12 (doze) meses ou sempre que necessário.

15. HISTÓRICO DE ALTERAÇÕES

Data	Versão	Área	Descrição da Atividade
15/10/2023	1.0	Diretoria de Operações	Aprovação para Publicação
15/08/2024	2.0	Diretoria de Operações	Aprovação para Publicação

ANEXO I – PROTEÇÃO E PRIVACIDADE DE DADOS

1. . CLÁUSULA PRIMEIRA – DA PROTEÇÃO DE DADOS LEI 13.709/18

As partes comprometem-se mutuamente ao cumprimento da Lei 13.709.2018, a "Lei Geral de Proteção de Dados" (LGPD), bem como das demais normas aplicáveis ao tema, das regulamentações emanadas pela Autoridade Nacional de Proteção de Dados e demais órgãos reguladores.

1.1. DOS AGENTES DE TRATAMENTO

1.1.1. DA CONTRATANTE – CONTROLADORA DE DADOS

A. Na relação estabelecida por força do presente Contrato, nos moldes da LGPD, a CONTRATANTE declara ser inteira e exclusivamente responsável pelo(a):

I. conteúdo das comunicações e/ou informações transmitidas em decorrência dos serviços objeto do presente Contrato;
II. propositura de alterações ou adequações no sistema para atendimento da LGPD;
III. utilização dos serviços disponibilizados no SISTEMA seguindo as regras aplicáveis à estrita finalidade do tratamento de dados coletados, respeitada a base legal aplicável;
IV. uso e publicação de comunicações e/ou informações através dos serviços objeto do presente Contrato;
V. confidencialidade dos dados gerados pela utilização do SISTEMA e armazenados em seu ambiente.

B. A CONTRATANTE reconhece e concorda que os Dados Pessoais acessados e/ou de qualquer forma disponibilizados à CONTRATADA foram coletados e disponibilizados de forma lícita e garante que:

I. observa todos os princípios para o tratamento de dados previstos na LGPD;
II. não obstante o SISTEMA vedar determinadas ações dos titulares de dados, com fundamento nas bases legais determinadas pela Lei, é capaz de respeitar os direitos dos titulares de dados, nos termos do art. 18, da LGPD;
III. adota as medidas técnicas e organizacionais possíveis e necessárias à proteção dos Dados Pessoais dos titulares e à sua completa adequação às legislações aplicáveis;
IV. observa e avalia todas as instruções, normas e boas práticas acerca da matéria, além de todas as salvaguardas necessárias, antes de instruir o tratamento de dados à CONTRATADA.

1.2. DA CONTRATADA – OPERADORA DE DADOS

A. As Partes reconhecem e acordam que a CONTRATADA figura como Operadora de Dados Pessoais, nos termos do art. 5º, VII, da Lei Geral de Proteção de Dados Pessoais ("LGPD"), e realizará o tratamento de Dados Pessoais em nome e sob instrução da CONTRATANTE, controladora desses dados (art. 5º, VI, da LGPD).

B. A CONTRATADA declara e garante que somente realizará o tratamento dos dados pertencentes ou de posse da CONTRATANTE para os fins descritos neste Contrato, observando a finalidade, necessidade e adequação do tratamento, em conformidade com a legislação vigente, bem como se compromete a:

I. adotar medidas de segurança, técnicas e administrativas aptas a proteger os Dados Pessoais, em seu ambiente, de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, informando à CONTRATANTE, periodicamente e/ou sempre que solicitado, via relatório detalhado, as medidas tomadas nesse sentido;
II. adotar os padrões técnicos mínimos determinados pela autoridade nacional para tornar aplicável o disposto no item anterior, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de Dados Pessoais sensíveis;
III. controlar e restringir o tratamento dos dados aos profissionais necessários para as respectivas atividades, que deverão ser instruídos sobre a forma adequada de tratamento, sem os revelar a terceiros salvo sob consentimento da CONTRATANTE;
IV. abster-se de criar cópias, modificar, adulterar, revelar a terceiros e/ou, de qualquer forma, transferir Dados Pessoais sem a ciência e consentimento por escrito da CONTRATANTE.
V. não divulgar e/ou compartilhar Dados Pessoais com terceiros não envolvidos na presente relação contratual, salvo mediante consentimento por escrito da CONTRATANTE;
VI. não realizar qualquer atividade de tratamento de Dados Pessoais por meios particulares, não oficiais e/ou não aprovados pela CONTRATANTE;
VII. realizar o tratamento de Dados Pessoais sensíveis, somente quando inevitável e em conformidade com o disposto no art. 11 da LGPD, restringindo-se às finalidades previstas neste Contrato, com adoção de todas as medidas possíveis e necessárias ao resguardo desses dados e com atenção à sensibilidade das informações;
VIII. reportar à CONTRATANTE, no prazo de 24 (vinte e quatro) horas corridas, a ocorrência de qualquer incidente envolvendo o tratamento de Dados Pessoais e/ou de eventuais solicitações por Parte do titular;
IX. garantir que as suas políticas de segurança sigam padrões e boas práticas de mercado, como por exemplo a família da ISO 27000, considerando as extensões 27701, além de 27799 e 27018 quando aplicáveis;
X. observar as Políticas da CONTRATANTE, em especial a Política de Privacidade e a Política de Segurança da Informação.
XI. comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados pessoais, em conformidade com o artigo 9º da Resolução CD/ANPD nº 15, de 24 de abril de 2024, sobre qualquer

incidente de segurança que possa causar risco ou dano relevante, no prazo máximo de três (3) dias úteis, salvo disposição em contrário prevista em legislação específica.

C. A CONTRATADA declara que para fins desta contratação, não armazenará e/ou extrairá cópia(s) (backups) dos Dados da CONTRATANTE e/ou de seus Clientes em decorrência da prestação do serviço ora CONTRATADA, sendo a CONTRATANTE exclusivamente a responsável pelo armazenamento e/ou eventuais backups em seu ambiente tecnológico.

1.3. DO TRATAMENTO DE DADOS

A. As Partes declaram que na presente contratação, a CONTRATADA apenas realiza eventualmente o tratamento de "acesso" a Dados Pessoais dos clientes da CONTRATANTE. Considerando esta premissa, todo e qualquer tratamento de Dados Pessoais no âmbito deste Contrato observará o prazo de vigência contratual e as disposições contidas neste instrumento.
B. Se necessária a continuidade de qualquer atividade de tratamento após o término da vigência contratual, essa necessidade deverá ser objeto de comunicação escrita entre as Partes, no prazo de 10 (dez) dias que antecedem o término da vigência, devendo ser indicada sua finalidade e adequação, observando-se as boas práticas existentes para tanto, garantindo a segurança da informação mesmo após o término do Contrato.
C. Após o prazo acima referido, a CONTRATADA se compromete a eliminar eventuais dados que ainda esteja sob seu tratamento, de forma idônea e segura, apresentando cópia dos dados em formato legível para a contratante antes de sua exclusão definitiva e fornecer evidências do procedimento realizado para tanto. Havendo a utilização de mídias, elas devem também ser destruídas, observando padrões de mercado, como NIST 800-88.
D. As Partes deverão manter o registro das atividades de tratamento de dados envolvidas nesta contratação.

1.4. LIMITAÇÃO DE RESPONSABILIDADE

A. Em caso de responsabilização da CONTRATADA por danos atribuíveis, exclusivamente a ações da CONTRATANTE, fica assegurado àquela o direito de regresso, nos termos do art. 42, §4º, da LGPD, c/c art. 934, do CC, sem prejuízo do ressarcimento das despesas administrativas e jurídicas incorridas, inclusive honorários advocatícios;
B. A CONTRATADA não será responsável por violações dos dados e informações extraídas em decorrência da prestação de serviço, ora contratado, resultantes de atos de funcionários, prepostos ou de pessoas autorizadas pela CONTRATANTE e nem daquelas resultantes da ação criminosa ou irregular de terceiros ("hackers") que ocorram no ambiente da CONTRATANTE.

1.5. Caso a CONTRATADA aja em desconformidade com as instruções oferecidas pela CONTRATANTE, nos moldes da legislação vigente, será equiparada à figura de Controlador

de dados pessoais, respondendo integralmente por qualquer dano referente ao tratamento de dados pessoais.

1.6. Caso a CONTRATANTE e a CONTRATADO atuem como Controladores de dados pessoais, cada uma das Partes será integralmente responsável pelos tratamentos de dados realizados pelas partes ou sob suas ordens, devendo agir conforme as melhores práticas para garantir a segurança da informação e as responsabilidades delimitadas neste Contrato.

2. CLÁUSULA SEGUNDA - CONFIDENCIALIDADE E SIGILO DAS INFORMAÇÕES

2.1. As Partes, por si, seus empregados, prepostos ou representantes, obrigam-se a manter absoluto sigilo sobre as operações, dados, materiais, pormenores, informações, documentos, especificações técnicas ou comerciais, inovações e aperfeiçoamentos tecnológicos ou comerciais, inclusive quaisquer programas, rotinas ou arquivos que, no curso da execução do presente Contrato tenham sido ou venham a ser revelados ou confiados em qualquer razão pelas Partes, sendo consideradas informações confidenciais e que não deverão ser reveladas a terceiros, salvo com expressa anuência da Parte reveladora. As Partes comprometem-se ainda, incondicionalmente, a não usar, comercializar, reproduzir ou dar ciência a terceiros, omissiva ou comissivamente, as informações acima referidas, sem a anuência da outra parte.

2.2. Estas obrigações de confidencialidade possuem caráter irrevogável e irretratável. A infração de quaisquer destas obrigações cominará o dever da Parte infratora, incluindo Partes signatárias e/ou pessoas por elas envolvidas, direta ou indiretamente nas atividades relacionadas a este Contrato, de indenizar a Parte prejudicada nas eventuais perdas e danos, materiais ou morais, que tiver sofrido em virtude da infração constatada.

2.3. Mesmo depois de rescindido o presente CONTRATO, as Partes continuarão obrigadas e responsáveis com relação às disposições sobre sigilo e confidencialidade, nos moldes da legislação vigente.

2.4. As informações disponíveis ao público, exceto se forem resultado de violação deste contrato pela PARTE infratora ou seus Representantes, não estarão incluídas no compromisso de confidencialidade contraído nesta cláusula.

2.5. Caso a CONTRATADA seja solicitada, com base em lei ou regulamento aplicável, ou seja, obrigada por lei ou regulamento aplicável ou por processo judicial ou arbitral, ou por ordem de autoridade governamental, a revelar quaisquer Informações, deverá fornecer apenas Informações na medida necessária para cumprir a lei, regra ou decisão em questão; e, se legalmente possível, requerer à respectiva autoridade tratamento confidencial à Informação.

3. CLAUSULA TERCEIRA - DESCARTE SEGURO DE INFORMAÇÕES DE CLIENTES

3.1 OBJETIVO

O Operador de Dados, doravante referido como "Operador", está comprometido em assegurar o descarte seguro e apropriado das informações de clientes conforme exigido pela legislação aplicável à proteção de dados e privacidade.

3.2 PRAZO PADRÃO DE DESCARTE

3.2.1 Salvo disposição em contrário neste contrato, o Operador se compromete a manter as informações do cliente apenas pelo tempo estritamente necessário para cumprir as finalidades para as quais foram coletadas.

3.2.2. O prazo padrão de retenção das informações de clientes é de 180 dias a partir da data em que as informações não são mais necessárias para as finalidades especificadas no contrato.

3.3 PROCEDIMENTO DE DESCARTE SEGURO

3.3.1. Ao final do prazo de retenção ou quando as informações não forem mais necessárias, o Operador adotará medidas adequadas e seguras para destruir ou anonimizar as informações de clientes, de forma a impedir a recuperação ou o uso indevido.

3.3.2. O Operador se compromete a utilizar práticas de descarte seguro que estejam em conformidade com os padrões de segurança da informação relevantes e as melhores práticas da indústria.

3.4 CLAÚSULAS CONTRATUAIS ESPECIFICAS

Caso as partes tenham acordos específicos em relação ao período de retenção ou descarte seguro das informações de clientes, esses acordos prevalecerão sobre as disposições deste contrato.

3.5 RESPONSABILIDADE DO CONTROLADOR DE DADOS

O Controlador de Dados, doravante referido como "Controlador", concorda em fornecer instruções claras e detalhadas ao Operador sobre os prazos de retenção e o descarte seguro das informações de clientes, sempre que essas instruções não estejam especificadas neste contrato.