RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 16 de julho de 2021

Histórico de Revisões

Data	Versão	Descrição	Autor
16/07/2021	1.0	Conclusão da primeira versão do relatório	Paulo Perrotti/ Aline Figueiredo/ Bianca Ribeiro
10/05/2022	1.1	Revisão periódica	Douglas Avila

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. **Referência:** Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador
Ideal Odonto (quando coleta dados)

Operador
Ideal Odonto (quando atua por conta e ordem de terceiros)

Encarregado	
Douglas Avila	
E-mail Encarregado	**Telefone Encarregado**
douglas.avila@idealtrends.com.br	0800 730 7373

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

2.1 - A Ideal Odonto realiza tratamento de dados pessoais para prestação de serviço de planos odontológicos. Portanto, precisa elaborar relatório informando todos os dados coletados e recebidos, finalidade do tratamento, compartilhamento e armazenamento, no intuito de apresentar todas medidas e mecanismos de mitigação de riscos adotados pelo controlador no processo de tratamento de dados, conforme descreve o artigo 5º, inciso XVII da LGPD.

2.2 - No caso da instituição em questão, o RIPD relata a finalidade do tratamento, ou seja, a avaliação dos propósitos do tratamento; demonstra a adequação de acordo com as avaliações de compatibilidade das finalidades pretendidas conforme o contexto do tratamento; quais medidas de segurança são aplicadas para proteger os dados pessoais de eventuais acessos não autorizados; a revisão da necessidade dos dados tratados, considerando tratar somente o estritamente necessário para a

finalidade; e prevenção de problemas.

2.3 - Avaliação dos programas, sistemas de informação ou processos existentes ou a serem implementados geraram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do RIPD.

2.4 - A Ideal Odonto implementa diversos processos, projetos, sistemas e serviços que envolvem o tratamento de expressiva quantidade e diversidade de dados pessoais. Tais dados envolvem informações pessoais, dados sensíveis, dados profissionais.

3 – DESCRIÇÃO DO TRATAMENTO

3.1 - NATUREZA DO TRATAMENTO

3.1.1 - Os dados pessoais são recebidos mediante envio de dados dos clientes para a Ideal Odonto. Após o recebimento, os dados são transferidos e armazenados em Servidores, Sistema Cloud, E-mails. A Ideal Odonto realiza o processamento sobre os dados pessoais recebidos e disponibiliza os dados para utilização de seus colaboradores para a prestação de serviços de planos odontologicos. A Ideal Odonto transfere os dados fornecidos pelos clientes para prestadores de serviços e terceirizados para o desenvolvimento dos serviços contratados.

3.1.2 - A Ideal Odonto coleta e manipula dados de seus funcionários e colaboradores, para realização de gestão da empresa.

3.1.3 - Constam no banco de dados as informações dos Clientes, Usuários do site, Colaboradores, Funcionários, Candidatos, Anunciantes, Prestadores de Serviços, Fornecedores e Terceiros.

3.1.4 - De acordo com as informações recebidas, para que ocorra o bom desempenho dos negócios, a Ideal Odonto recebe, coleta e trata os seguintes dados por departamento:

(i) **Comercial**: O Departamento Comercial tem acesso aos seguintes dados:
Clientes: Nome, telefone, WhatsApp, e-mail, domínio, CNPJ, informações públicas da própria Receita Federal, Endereço, Responsável legal pela empresa, CNPJ do contratante, e-mail e telefone do cotador, IP do cotador, região do cotador. Dados pessoais de donos de empresas, dados das empresas e de seus funcionários
A captação de clientes é feita via mídias sociais e Google, onde os dados extraídos são lançados em planilhas.

(ii) **Contas a pagar**: O Departamento de contas a pagas tem acesso aos seguintes dados:
Colaborador: Nome, cargo, CPF, RG e dados bancários.
Dados completos de fornecedores PJ e PF para que seja possível a realização

de pagamentos e apuração fiscal.
Dados completos de fornecedores PJ e clientes PF, para que seja possível a emissão de NFs de entrada e saída. Consulta de situação financeira no mercado.

(iii) **Contas a receber**: O Departamento de contas a receber tem acesso aos seguintes dados:
Documentos dos clientes PJ e PF: CPF, RG e CNPJ.
Dados pessoais dos Clientes PJ e PF: Nome, Data de Nascimento, Endereço, Conta, Agência, Banco, Tipo de conta. Acesso ao anexo do contrato assinado, telefones, e-mail, contatos, histórico de tratativas, parcelas e pagamentos.

(iv) **Jurídico**: O Departamento Jurídico tem acesso aos seguintes dados:
Clientes PF: Nome, CPF, planilhas com informações do processo, troca de e-mails com informações das partes e processos e minutas de acordos.
Clientes PJ: CNPJ, Endereço, Razão Social, planilhas com informações do processo, troca de e-mails com informações das partes e processos e minutas de acordos.

(v) **Marketing**: O Departamento de Marketing tem acesso aos seguintes dados:
Audiovisual – Nome do responsável legal pela empresa, CNPJ do contratante, e-mail, telefone e cartão de crédito.
Dados pessoais dos clientes internos e externos são repassados de acordo com a demanda solicitada.
Dados empresariais da empresa do Grupo Ideal que solicitou alguma locução profissional como CNPJ, Nome, telefone, e-mail, cartão de crédito. Todos os materiais brutos e editados pelo setor são armazenados na nuvem, inclusive documentos assinados por clientes internos e externos. Documentos com informações das solicitações dos clientes internos e externos.
Vídeos e fotos de pacientes, depoimentos após o tratamento, Termos de autorização de uso da imagem.

(vi) **Operações**: O Departamento de Operações tem acesso aos seguintes dados:
Nome do paciente, nome da empresa, RG, CPF, CNPJ, Endereço, Telefone, E-mail, Cartão do SUS, questionário impresso sobre alguns dados de saúde (guardado em armário trancado), cartão de crédito dos pacientes (fica gravado os últimos 4 dígitos), fotos da boca e rosto dos pacientes, data de nascimento dos pacientes, profissão, consulta de títulos protestados, agenda dos dentistas, dados dos dentistas, atestados, simulação de tratamento e rastreamento de envio, diagnósticos para o tratamento, tipo de tratamento, valores dos tratamentos, e-mail de fornecedores.

(vii) **RH:** O Departamento de RH coleta os seguintes dados:
Colaboradores/Funcionários: Nome, CPF, RG, PIS, CTPS, Data de Nascimento, Nome dos pais, endereço, Sexo, Estado Civil, Naturalidade,

Nacionalidade, filiação sindical, Dados bancários (Conta, Agência, Banco, Tipo de conta), Salário, Remuneração variável, Benefícios, Telefone particular, Telefone corporativo, E-mail particular, E-mail corporativo, Formação acadêmica, Experiências anteriores, Regime trabalhista, Data Admissão, Data Desligamento, atestados, biometria (antes da pandemia, agora o controle de ponto é via sistema mediante login e senha do colaborador), avaliação de desempenho.

(viii) **Plataforma**: A Plataforma coleta os seguintes dados:
No momento do cadastro do usuário – nome da empresa, nome do responsável, e-mail, CNPJ, telefone, cargo, informações sobre o modelo de negócio da empresa.
Quando solicita um orçamento – Nome, e-mail, empresa, telefone, campo para autorização de recebimento de promoções e novidades da Ideal Odonto, e propostas sem compromisso de outros fornecedores.

3.1.5 - Constam nas informações prestadas que a Ideal Odonto compartilha esses dados coletados com seus colaboradores, parceiros de negócios e terceirizados para que estes realizem algum tipo de tratamento desses dados, voltados para a prestação de serviço de plataforma de geração de negócios para indústrias.

3.1.6 - São coletados dados de saúde, biometria e filiação a sindicato de funcionários e colaboradores pelo Departamento de RH. Para tal tratamento, o funcionário responsável pelo recebimento e tratamento desses dados deverá obter o consentimento do titular do dado e atender todos os requisitos da LGPD, uma vez que tais dados são considerados sensíveis.

3.1.7 - A Ideal Odonto utiliza os seguintes sistemas: MPI Sistemas (responsável por pegar briefing, conteúdos, e imagem dos clientes), Gmail (envio de cópias de contrato aos clientes) Sensedata (históricos e jornadas com dados de clientes) e Painel de Ideal Odonto (responsável por centralizar todas as informações de cadastro dos clientes e contatos comerciais recebidos).

3.1.8 – O Departamento de RH utiliza os seguintes sistemas: Alterdata (cadastros de todos os colaboradores e clientes), Impulse Up (Avaliação de desempenho), Trello, Drive, Ahgora Ponto (controle ponto via login e senha do colaborador).

3.1.9 – O Departamento de Marketing utiliza os seguintes sistemas e ferramentas para edição de fotos e videos: Pacote Adobe, Pro Tools, Elements Envato, Vimeo, Locução, Adobe Stock, Drive, Planilhas e Docx Google.

3.1.10 - Os funcionários podem baixar programas nas máquinas sem autorização do TI para realizar o procedimento.

3.1.11 - Os empregados e colaboradores podem utilizar mídias removíveis (pen drive, HD externo,

celular, dentre outros) nas máquinas.

3.2 – ESCOPO DO TRATAMENTO

3.2.1 - Os dados pessoais tratados pela Ideal Odonto abrangem:

- **Informações de identificação pessoal**: Nome, CPF, RG, PIS, CTPS, Data de Nascimento, endereço, Sexo, Estado Civil, Naturalidade, Nacionalidade, Dados bancários, Telefone, E-mail.

- **Dados sensíveis:** Dados de saúde, Biometria, Filiação sindical, Atestados.

- **Dados profissionais**: Salário, Remuneração variável, Benefícios, Formação acadêmica, Experiências anteriores, Regime trabalhista, Data Admissão, Data Desligamento, avaliação de desempenho.

- **Dados familiares (composição familiar):** Nome dos pais.

- **Dados de identificação eletrônica:** Endereço IP, Tela de uso, Informações digitadas.

3.2.2 - A Ideal Odonto, no departamento de RH, poderá realizar o tratamento dos atestados médicos apresentados pelos empregados e colaboradores para verificação de absenteísmo. Para tal tratamento, o colaborador responsável pelo recebimento e tratamento desses dados deverá obter o consentimento do titular do dado e atender todos os requisitos da LGPD, uma vez que tais dados são considerados sensíveis.

3.2.3 - A frequência de tratamento dos dados pessoais é realizada no horário comercial em dias úteis, visando a prestação de serviços de plataforma de geração de negócios para indústrias.

3.2.4 - A abrangência do tratamento de dados pessoais é referente ao território brasileiro, mas pode ampliar para outras localidades, em razão da utilização de serviços "cloud".

3.3 – CONTEXTO DO TRATAMENTO

3.3.1 - A natureza do relacionamento dos titulares dos dados com a Ideal Odonto no âmbito da prestação de serviço de planos de saúde é centrada no contrato de prestação de serviço a ser realizado ao cliente, o qual é responsável por informar dados referente a relação contratual.

3.3.2 – A natureza do relacionamento dos titulares dos dados (funcionários e colaboradores) com a Ideal Odonto é referente a relação de trabalho voltado a gestão de negócios da empresa, sendo os funcionários e colaboradores responsável por informar dados profissionais, pessoais e sensíveis.

3.3.3 – Nenhuma informação referente aos dados pessoais dos indivíduos é comunicada aos titulares. Os titulares dos dados não têm acesso as informações armazenadas na Ideal Odonto.

3.3.4 - Poderão ser tradados dados pessoais de crianças e adolescentes.

3.3.5 - Em relação ao tratamento de dados pessoais de crianças e adolescentes, deve-se solicitar o consentimento de ao menos um representante legal (artigo 14, §1º da LGPD).

3.3.6 - O tratamento de dados deve ser realizado de acordo com a expectativa do titular de dados, de acordo com a leis e regulamentos, e conforme política de privacidade para ciência do titular dos dados sobre o tratamento dos dados e a possibilidade de consentir o manuseio desses dados pessoais pela Ideal Odonto.

3.3.7 - A Ideal Odonto utiliza recursos de segurança e está implantando uma Política de Treinamento para sensibilização referente a privacidade e proteção de dados.

3.4 – FINALIDADE DO TRATAMENTO

3.4.1 - A finalidade do tratamento dos dados pessoais da Ideal Odonto é baseada na execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; no consentimento do titular do dado; legitimo interesse do controlador, para prestação de serviços de plataforma geração de negócios para indústrias.

3.4.2 Os resultados pretendidos pelos titulares de dados pessoais são: divulgar seus produtos para compradores e representantes de todo o Brasil.

3.4.3– A Ideal Odonto equilibra seus interesses com os dos indivíduos com os quais ela tem relacionamento.

4 – PARTES INTERESSADAS CONSULTADAS

4.1 – As partes interessadas consultadas foram: gerentes dos departamentos.

4.2 – Os gerentes dos departamentos apontaram os dados coletados e determinados pontos de vulnerabilidade da gestão do departamento, tais como não tem bloqueio de mídias removíveis, acesso físico a arquivos e pastas em papel, acesso não controlado a áreas com dados pessoais, acesso a dados não necessários para a finalidade da área, envio de dados pessoais por e-mail.

5 – NECESSIDADE E PROPORCIONALIDADE

5.1 – FUNDAMENTAÇÃO LEGAL

5.1.1 - As operações realizadas pela Ideal Odonto sobre os dados pessoais limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (LGPD, art. 6º, III).

5.1.2 - A LGPD estabelece, em seu artigo 7º, rol taxativo para o processamento válido de tratamento de dados pessoais. No caso da Ideal Odonto, as hipóteses de tratamento de dados pessoais são: **consentimento do titular; execução do contrato e legítimo interesse do controlador**.

5.1.3 – Quando a Ideal Odonto necessita tratar dados baseando-se no legítimo interesse do

controlador (LGPD, art. 10), esse tratamento de dados pessoais é indispensável; ou não há outra base legal possível de se utilizar para alcançar o mesmo propósito; ou esse processamento de fato auxilia no propósito almejado.

5.2 – QUALIDADE E MINIMIZAÇÃO DOS DADOS

5.2.1 - Consta no banco de dados da Ideal Odonto informações excessivas mantidas além do necessário para o objetivo organizacional da empresa. Tal costume deve ser modificado em um próximo relatório de impacto, atentando-se para o término da finalidade do tratamento do dado coletado, com a sua consequente eliminação da base de dados. Deve ser evitando a coleta de dados que não são necessários para o estabelecimento.

5.2.2 – Os dados coletados devem ser claros e relevantes para a finalidade original e devidamente atualizados. É necessário constituir uma nova metodologia de armazenamento de dados para informações que já atingiram a finalidade do tratamento e estão apenas armazenados no banco de dados, sem qualquer critério ou funcionalidade.

5.3 – MEDIDAS PARA ASSEGURAR CONFORMIDADE DO OPERADOR

5.3.1 – Realizar vistoria sobre os processos de tratamento de dados executados na empresa a fim de avaliar se esses processos estão em conformidade com as diretrizes definidas pelo controlador, a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).

5.4 – MEDIDAS PARA ASSEGURAR DIREITOS DO TITULAR DOS DADOS

5.4.1 – O canal de comunicação está disponibilizado para que os titulares dos dados pessoais possam demandar as solicitações previstas pelo art. 18º da LGPD. A Política de Privacidade da Ideal Odonto informa sobre o direito que o titular dos dados pessoais tem de realizar qualquer uma das referidas solicitações. A Política de Privacidade pode ser encontrada no link .https://docs.google.com/document/d/e/2PACX-1vQ1n-EEppyZWIghqJNmLBq82LUCwSIc7tZA2iovdRKUJKLp2dsY59ak1WFuLl-RYA/pub Caso o usuário identifique alguma falha ou vulnerabilidade de segurança no sistema, é possível reportá-la também para o Encarregado, no e-mail: douglas.avila@idealtrends.com.br

5.4.2 Quando solicitado pelo titular do dado pessoal, a Ideal Odonto fornecerá informações de privacidade (confirmação de existência ou o acesso a dados pessoais) por meio de e-mail ou sob forma impressa, de acordo com a solicitação do referido titular.

5.5 – SALVAGUARDAS PARA AS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

5.5.1 – A Ideal Odonto não realiza qualquer tipo de transferência internacional de dados.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

6.1 - Os contratos deverão atender a uma avaliação de risco, selecionados e identificados de acordo com a sua sensibilidade no que se refere à coleta, tratamento e armazenamento de dados, em "baixa, média ou alta" sensibilidade. Neste sentido, antes de definir tais medidas, salvaguardas e mecanismos junto a clientes, colaboradores e fornecedores em geral, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais.

6.2 – Para cada sensibilidade, será utilizada uma minuta contratual ou documento, bem como um procedimento específico, a fim de garantir a mitigação de risco.

6.3 - Para cada risco identificado, define-se: a sensibilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento ("baixa, média ou alta" sensibilidade), confrontando-se os seguintes critérios:

(i) Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

(ii) Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

(iii) Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

6.4 - A título de informação, é destacada a seguir uma lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais. O nível de probabilidade, impacto e nível de riscos devem ser avaliados de acordo com o contexto de cada caso. Os doze primeiros riscos representam riscos de privacidade obtidos da norma ISO/IEC 29134:2017 seção 6.4.4.

	Risco referente ao tratamento de dados pessoais
R01	Acesso não autorizado.
R02	Modificação não autorizada.
R03	Perda.
R04	Roubo.
R05	Remoção não autorizada.

R06	Coleção excessiva.
R07	Informação insuficiente sobre a finalidade do tratamento.
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.
R11	Retenção prolongada de dados pessoais sem necessidade.
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).
R14	Reidentificação de dados pseudonimizados.

7 – MEDIDAS PARA TRATAR OS RISCOS

7.1 A Ideal Odonto adota medidas de segurança, técnicas e administrativas suficientes a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46.), dentro de um limite de risco aceitável para a corporação.

7.2 A equipe de SI, comandada pelo Encarregado de Dados - Data Protection Officer (DPO) da Ideal Odonto, é responsável por coordenar e supervisionar o cumprimento das políticas e procedimentos em toda a Ideal Odonto no tocante à confidencialidade, integridade e segurança de seus ativos de informação. O DPO deve aplicar as políticas definidas, identificar áreas de preocupação e implantar as mudanças apropriadas de acordo com as necessidades. As responsabilidades especificas incluem:

- ➢ Tomar decisões pertinentes às Políticas de Segurança da Informação e seu conteúdo.
- ➢ Aprovar, antecipadamente, exceções a estas políticas com base em análise caso-a-caso.
- ➢ Coordenar, anualmente, uma verificação de risco formal para identificar novas ameaças e vulnerabilidades e identificar controles apropriados para minimizar qualquer novo risco.
- ➢ Rever anualmente as políticas e procedimentos de segurança da informação para manter a adequação face às emergentes necessidades de negócio ou ameaças à segurança.
- ➢ Consultar anualmente as demais áreas de negócios e verificar a segurança de cada uma delas.
- ➢ Aplicação das políticas e procedimentos de segurança da informação de acordo com sua aplicabilidade a todos os ativos de informação.
- ➢ Administração das contas de usuários e gerenciamento de autenticação.

7.3 SEGURANÇA DA INFORMAÇÃO – SI

A proteção bem-sucedida dos sistemas da Ideal Odonto requer que vários departamentos e grupos sigam consistentemente uma visão compartilhada de segurança. A Segurança da Informação trabalha com os gerentes, administradores e usuários de sistemas dos departamentos no desenvolvimento de políticas, normas e procedimentos de segurança para ajudar na proteção dos ativos da Ideal Odonto. A Segurança da Informação é um departamento dedicado ao planejamento, educação e conscientização sobre segurança. As responsabilidades específicas da Segurança da Informação incluem:

- ➢ Criar políticas e procedimentos de segurança da informação quando necessário.
- ➢ Manter e atualizar Políticas e procedimentos de segurança da informação existentes.
- ➢ Rever anualmente as políticas e auxiliar a administração com o processo de aprovação.
- ➢ Agir como um departamento central de coordenação para implantação das políticas de Segurança da Informação.
- ➢ Criar, manter e distribuir procedimentos de resposta a incidentes e de encaminhamento.
- ➢ Monitorar e analisar alertas de segurança e distribuir informações ao pessoal apropriado de segurança, técnico e da administração da unidade de negócios.
- ➢ Fazer a revisão dos registros. Verificar qualquer exceção identificada.
- ➢ Restringir e monitorar o acesso a áreas restritas e informação confidencial. Assegurar que os

controles adequados estejam disponíveis onde houver informações e dados confidenciais e sensíveis.

7.4 ACESSO ÀS INFORMAÇÕES

Toda informação confidencial ou sensível deve ser protegida por controles de acesso para assegurar que não seja divulgada, modificada, apagada ou inutilizada indevidamente. Os logs devem rastrear todo acesso a tais dados e identificar por quem e quando tais dados foram acessados. Os colaboradores autorizados a visualizar informações em um determinado nível de classificação serão autorizados a acessar informações somente naquele nível ou em nível inferior com base na necessidade de acesso. Todo acesso aos sistemas deve ser configurado para negar acesso a tudo além daquilo que um usuário específico necessite ter acesso no desempenho de sua função profissional. O acesso a sistemas ou aplicativos contendo informações confidenciais, sensíveis ou privadas deve observar o processo de solicitação de acesso às informações. Todas as solicitações necessitam da aprovação da equipe de segurança da Ideal Odonto. O acesso a dados que excedam a função autorizada do colaborador também deve observar o processo de solicitação de acesso às informações e deve incluir limites documentados atinentes a tal acesso (ex. fonte de acesso, limites de tempo de acesso, etc).

7.5 SEGURANÇA DA INFORMAÇÃO - SI

- ➢ Monitorar alertas específicos de sistemas e aplicativos em sistemas críticos (ex. falha do firewall, reinicializações do sistema, etc.)
- ➢ Notificar as partes apropriadas no caso de falha do sistema de segurança ou evento de segurança.
- ➢ Assegurar que as regras de segurança aplicadas aos firewalls e roteadores sejam suficientes para proteger as redes e ativos corporativos da Ideal Odonto de ataques externos e de acesso não autorizado.
- ➢ Certificar-se de que as regras de segurança aplicadas aos firewalls e roteadores sejam suficientes para evitar eventos internos de segurança saiam da rede da Ideal Odonto.
- ➢ Rever todas as solicitações de alteração da regra de segurança para roteadores e firewalls de forma a atingir a conformidade com a política antes da submissão através do processo de gerenciamento de modificações.
- ➢ Certificar-se de que todos os protocolos/serviços autorizados através dos firewalls e roteadores estejam devidamente documentados
- ➢ Certificar que protocolos perigosos, tais como FTP, TELNET, POP3, IMAP e SNMP (com autenticação implementado) tenham passado pela avaliação de risco, tenham uma necessidade comercial corrente documentada, e estejam protegidos conforme a norma de segurança documentada.
- ➢ Monitorar ativamente eventos de segurança do firewall e do roteador para identificar incidentes externos de segurança.
- ➢ Realizar revisões de todas as regras definidas de firewall e roteador.

7.6 POLÍTICA DE ANTIVÍRUS

7.6.1 APLICABILIDADE DA POLÍTICA

Todos os sistemas geralmente afetados por vírus tais como servidores, Workstations e laptops nas redes da Ideal Odonto devem seguir esta política.

7.6.2 CONFIGURAÇÃO DE SOFTWARE

Todos os sistemas aplicáveis devem estar configurados com software antivírus aprovados pela Segurança da Informação-SI. A solução antivírus deve ser capaz de detectar, remover e proteger contra todos os tipos de software malicioso tais como vírus, Trojans, worms, spyware, adware e rootkits. O software deve estar configurado para receber atualizações automáticas, executar varreduras periódicas, registrar eventos com vírus em uma solução central de logging, e os usuários finais não devem ser capazes de configurar ou desabilitar o software.

7.7 PLANO E PROCEDIMENTOS DE RESPOSTA A INCIDENTES

7.7.1 APLICABILIDADE DA POLÍTICA

Toda detecção e resposta a incidentes, especialmente relacionado a sistemas críticos, deve seguir esta política. Os colaboradores devem estar cientes de suas responsabilidades na detecção de incidentes de segurança para facilitar o plano e os procedimentos de resposta a incidentes. Todos os colaboradores têm a responsabilidade de auxiliar nos procedimentos de resposta a incidentes dentro de sua área específica de responsabilidade. Alguns exemplos de incidentes de segurança que o colaborador pode reconhecer em suas atividades diárias incluem, sem limitação:

- Roubo, dano ou acesso não autorizado (ex. logins não autorizado, desaparecimento de papéis de sua mesa, cadeados quebrados, falta de arquivos de log, alerta de um guarda de segurança, evidência em vídeo de uma invasão ou de entrada física não programada ou autorizada).
- Fraude – informações imprecisas dentro de bases de dados, logs, arquivos ou registros impressos.
- Comportamento anormal do sistema (ex. reinicialização não programada do sistema, mensagens inesperadas, erros anormais em arquivos de log do sistema ou em terminais).
- Notificações sobre eventos de segurança (ex. alertas de integridade de arquivos, alarmes de detecção de intrusos, e alarmes de segurança física). Todos os colaboradores, independentemente de suas responsabilidades profissionais, devem estar cientes dos identificadores de potenciais incidentes e de quem notificar nestas situações.

7.7.2 PROCEDIMENTOS DE NOTIFICAÇÃO E REPORTE DE INCIDENTES

A Segurança da Informação-SI deve ser notificada imediatamente de qualquer real ou suposto incidente envolvendo os ativos informáticos da Ideal Odonto, mais especificamente, de qualquer sistema crítico. Caso não esteja claro se a situação deve ou não ser considerada um incidente de

segurança, a Segurança da Informação-SI deve ser contatado para avaliar a situação. Com exceção dos passos descritos abaixo, é imperativo que qualquer ação investigativa ou corretiva seja tomada somente pelo pessoal da Segurança da Informação-SI ou sob sua supervisão, para assegurar a integridade do processo de investigação e recuperação de incidentes. Quando confrontado com uma situação potencial, você deve fazer o seguinte:

- ➢ Preserve as evidências. Se o incidente envolver um sistema informático comprometido, não alterar o estado do sistema informático. O seguinte deve ser feito: o Não desligar o computador ou tentar reinicializá-lo. o Desconectar imediatamente o computador da rede, desconectando o cabo de rede. O computador deve permanecer ligado e todos os programas em execução devem ser mantidos ativos. Não alterar o estado do equipamento.
- ➢ Reportar o incidente de segurança. o Contatar a Segurança da Informação-SI sobre qualquer incidente suposto ou real. O número de telefone do Segurança da Informação-SI deve ser conhecido por todos os colaboradores e deve conectar a uma pessoa fora do horário comercial. o Ninguém deve comunicar a qualquer outra pessoa, além de seu(s) supervisor(es) ou o Segurança da Informação-SI, sobre qualquer detalhe ou circunstância envolvendo qualquer real ou suposto incidente. Toda comunicação com as autoridades legais ou o público será coordenada pelo Segurança da Informação-SI.
- ➢ Documentar qualquer informação que você tenha conhecimento enquanto aguarda pela resposta do Segurança da Informação-SI ao incidente. Se possível, isto deve incluir a data, hora e a natureza do incidente. Qualquer informação que você possa fornecer ajudará na definição da resposta adequada.

Identificado qualquer tipo de incidente, deverá ser preenchida a Notificação de Incidente de Segurança e enviada ao responsável pela equipe de Segurança da Informação-SI e para o Encarregado de Dados.

7.7.3 GESTÃO DE MUDANÇAS

Qualquer alteração ou mudança no que se refere ao processamento de dados e segurança da informação (tais como teste de todas as regras configuradas do firewall, roteador e switch), incluindo identificação, registro, aprovação formal de mudanças significativas, teste, avaliação de impactos e rollback, deve ser submetida à Diretoria da Ideal Odonto e validada previamente pelo DPO, de maneira registrada, formalizada e devidamente justificada, antes que estas alterações ou mudanças sejam efetivamente executadas, a fim de evitar qualquer tipo de impacto negativo no atendimento dos clientes, sempre mantendo-se a privacidade e confidencialidade das informações.

7.7.4 CLASSIFICAÇÃO DA GRAVIDADE DO INCIDENTE

A Segurança da Informação-SI tentará, primeiramente, determinar se o incidente de segurança justifica uma resposta formal. Em casos em que o incidente de segurança não demandar uma resposta a incidentes, a situação será encaminhada à respectiva área de TI para assegurar que todos os serviços de suporte tecnológico necessários sejam prestados. As seguintes descrições devem ser utilizadas para determinar qual resposta a Segurança da informação-SI deverá adotar:

- Nível 1 – Uma ocorrência de atividade potencialmente não amigável (ex., finger, telnet não autorizada, port scan, detecção de vírus corrigida, pico de desempenho inesperado, etc.).
- Nível 2 – Ocorrência de uma tentativa clara de obtenção de informação ou acesso não autorizado (ex., tentativa de download de arquivos de senhas protegidas, de acesso à área restritas, contaminação por vírus bem sucedida de um sistema não crítico em um computador, varredura de vulnerabilidade não autorizada, etc.) ou uma segunda ocorrência de ataque Nível 1.
- Nível 3 – Tentativa séria ou real violação da segurança (ex. ataque multi-prong, recusa de tentativa de serviço, infecção por vírus de um sistema ou rede críticos, buffer/stack overflow bem sucedidos, acesso não autorizado bem sucedido a informações ou sistemas críticos ou sensíveis, quebra de cadeado, roubo de papéis, etc.) ou um segundo ataque de Nível 2. Qualquer incidente de Nível 1 verificado em sistemas que armazenem informações confidenciais ou sensíveis ou originados em sistemas internos não autorizados é classificado como Nível 2.

7.8 RESPOSTA A INCIDENTES

7.8.1 RESPOSTA TÍPICA

As respostas podem incluir ou proceder através dos seguintes estágios: identificação, classificação de severidade, contenção, erradicação, recuperação e análise de causa raiz resultando no aprimoramento dos controles de segurança. As seguintes ações devem ser tomadas pela Segurança da Informação-SI após o incidente ter sido identificado e classificado.

7.8.1.1 Nível 1 Conter e Monitorar 1. Se possível, registrar o usuário, endereço de IP e domínio do intruso. Utilizar controles tecnológicos aprovados para bloquear, temporária ou permanentemente, o acesso do invasor. Manter vigilância contra futuras tentativas de invasão deste usuário ou endereço de IP.

7.8.1.2 Nível 2 Conter, monitorar e Alertar 1. Colher e proteger as informações associadas à intrusão. Utilizar controles tecnológicos aprovados para bloquear, temporária ou permanentemente, o acesso do invasor. Pesquisar a origem da conexão. Contatar o Provedor de Serviço de Internet (ISP) e solicitar mais informações referentes à tentativa e o intruso. Pesquisar os riscos potenciais relacionados ao método de intrusão utilizado e reavaliar para uma classificação de incidente mais elevada e contenção, erradicação e recuperação, conforme descrito para incidentes de Nível 3. Após a identificação, informar o usuário malicioso que está ciente de suas ações e adverti-lo sobre recriminações futuras, no caso de haver uma nova tentativa. Se um colaborador for o usuário malicioso, a administração deve trabalhar junto ao Recursos Humanos-RH para lidar devidamente com a violação da norma de Uso Aceitável.

7.8.1.3 Nível 3 Conter, Erradicar, Recuperar e executar Análise de Causa Raiz 1. 2. Conter a intrusão e decidir qual ação a ser tomada. Considerar a desconexão dos cabos de rede, aplicando ACLs altamente

restritivos, desativando ou isolando o port switch, userID, e encerrar a sessão do usuário/mudança de senha, etc. Colher e proteger as informações associadas à intrusão através de métodos offline. Caso haja a necessidade de perícia, o Segurança da Informação-SI trabalhará com os departamentos jurídico e administrativo para identificar os respectivos especialistas. Notificar a administração sobre a situação e mantê-los informados do andamento de cada um dos passos seguintes. Eliminar os meios de acesso do intruso e qualquer vulnerabilidade relacionada. Pesquisar a origem da conexão. Contatar o DPO e solicitar mais informações sobre a tentativa e o intruso, lembrando-lhes de sua responsabilidade em assisti-lo nesta questão. Pesquisar riscos potenciais associados ou danos causados pelo método de intrusão utilizado.

7.9 NOTIFICAÇÕES AUTOMÁTICAS DE SEGURANÇA DO SISTEMA

Todo sistema automático de detecção de intrusão dentro do ambiente da Ideal Odonto, incluindo sensores de detecção de intrusão e sistemas de verificação de integridade, será configurado para notificar automaticamente o Segurança da Informação-SI sobre qualquer comprometimento potencial ou ataque. Adicionalmente, qualquer detecção automática ou manual de pontos de acesso sem fio não autorizados deve acionar o Plano de Resposta a Incidentes.

7.10. DA POLÍTICA DE INTEGRIDADE

Os colaboradores declaram que estão cientes, conhecem, entendem e cumprem integralmente, na condução de suas atividades, toda a legislação anticorrupção a ela aplicável, em especial, mas sem limitar, a Lei n.º 12.846/2013 e o Decreto nº 8.420/2015, bem como a toda e qualquer outra legislação antissuborno ou anticorrupção aplicável, assim como as normas e exigências constantes das políticas internas da Ideal Odonto, as quais teve acesso e declara ter ciência, abstendo-se de qualquer atividade que constitua uma violação a tais dispositivos.

Os colaboradores declaram, garantem e aceitam que, com relação a este Manual, não praticarão nem tentarão praticar qualquer demanda, exigência, cobrança ou obtenção para si e para outrem de vantagem indevida ou promessa de vantagem indevida, a pretexto de influir em ato praticado por agente público e/ou privado, restando expresso, ainda, que nenhum favorecimento, taxa dinheiro ou qualquer outro objeto de valor foi ou será pago, oferecido, doado ou prometido pelos colaboradores, direta ou indiretamente.

PARÁGRAFO SEGUNDO:

Os colaboradores também se obrigam a cumprir todas as leis anticorrupção aplicáveis e garante que não irão, em razão deste Manual, ou de quaisquer outras transações comerciais, transferir qualquer ativo de valor, direta ou indiretamente, a qualquer pessoa do setor privado ou funcionários do Governo ou de empresas controladas pelo governo, a fim de obter ou manter qualquer outro benefício ou vantagem indevida. Os colaboradores garantem que nenhum dinheiro pago será utilizado a título de

compensação ou de outra forma será usado para pagar qualquer vantagem ou benefício, em violação da lei aplicável.

PARÁGRAFO TERCEIRO:
Os colaboradores declaram e garantem que não se encontram, de qualquer modo e a qualquer título, direta ou indiretamente (I) sob investigação em virtude de denúncias de suborno e/ou corrupção; (II) no curso de um processo judicial e/ou administrativo ou foram condenados ou indiciados sob a acusação de corrupção ou suborno; (III) listados em alguma entidade governamental, tampouco conhecidos ou suspeitos de práticas de terrorismo e/ou lavagem de dinheiro; (IV) sujeitos a restrições ou sanções econômicas e de negócios por qualquer entidade governamental; e (V) banidos ou impedidos, de acordo com qualquer lei que seja imposta ou fiscalizada por qualquer entidade governamental.

Os colaboradores notificarão prontamente, por escrito, a Ideal Odonto acerca do recebimento de qualquer notificação de qualquer entidade governamental – qualquer dos Poderes e administração pública direta ou indireta - relacionada a fatos ou investigações relativas a atos de corrupção, a respeito de qualquer suspeita ou violação do disposto nas Leis Anticorrupção, e ainda de participação em práticas de suborno ou corrupção, assim como o descumprimento de qualquer declaração prevista nesta Cláusula.

O não cumprimento de quaisquer regras anticorrupção aplicáveis pelos Colaboradores será considerada uma infração grave e conferirá a Ideal Odonto o direito de rescindir de imediato o Contrato, ficando os colaboradores obrigados a eximir a Ideal Odonto quaisquer ações, perdas e danos decorrentes de tal descumprimento. Os colaboradores ficarão responsáveis por indenizar a Ideal Odonto contra todo e qualquer dano que este suporte em razão do descumprimento das obrigações e declarações estabelecidas nesta Cláusula.

7.11 – POLÍTICA DE BYOD – "BRING YOUR OWN DEVICE"

Os Colaboradores que trazem seus próprios equipamentos para a Ideal Odonto, tais como aparelhos celulares, tablets ou qualquer outro equipamento, se comprometem aos seguintes termos:

– O equipamento é de completa responsabilidade do proprietário;
– Que o conteúdo armazenado é de responsabilidade do proprietário;
– Que o proprietário declara que todos os softwares possuem licença regular sob pena de responder isoladamente sobre qualquer incidente de pirataria;
– Que o proprietário deverá fazer uso de requisitos mínimos de segurança da informação tais como, mas não se limitando a antivirus, antispyware, senha de bloqueio, criptografia;
– Que o proprietário tem o dever de realizar backup de todas as informações pertinentes à empresa e

de salvá-las na rede corporativa;
– Que o equipamento está sujeito a monitoramento e a inspeção física por parte da empresa;
– Que o equipamento está sendo colocado à disposição da empresa como beneficiária de uso temporário e parcial, em caráter não oneroso, sem qualquer responsabilidade por parte da empresa;
– Que a empresa não se responsabiliza pela perda, deterioração, furto, extravio, quebra do equipamento, e se isso vier a ocorrer o proprietário deverá avisar a empresa imediatamente;
– Que o proprietário se compromete a portar o equipamento de forma discreta e com o máximo de zelo possível, para evitar incidentes e vazamentos de informação da empresa;
– Que o mero acesso ou uso do equipamento ou recursos de informação pelo proprietário, por si só, não configura sobreaviso ou sobre jornada, sendo um ato de liberalidade, proatividade e iniciativa dele.
- Que o equipamento não esteja sendo utilizado para coleta, tratamento e armazenamento de quaisquer dados da Ideal Odonto. Qualquer utilização do equipamento pessoal para fins profissionais deve ser reportada à equipe de SI e ao Encarregado de Dados.

7.12 – CLASSIFICAÇÃO DA INFORMAÇÃO E DOS ATIVOS

A informação e os ativos são caracterizados em termos de valor, requisitos legais, sensibilidade e criticidade, para evitar modificação ou divulgação não autorizada.
Neste sentido, os ativos são caracterizados por: Públicos, Internos e Confidenciais.

A Diretoria, com a orientação e suporte da equipe de SI, comandada pelo Encarregado de Dados - Data Protection Officer (DPO) da Ideal Odonto, e do Coordenador de cada área, designa os responsáveis, custodiantes e usuários das informações de acordo com a classificação.

Para cada tipo de ativo (público, interno ou confidencial), a Ideal Odonto tem critérios específicos de armazenamento, backup, transmissão e descarte seguro para informações impressas e eletrônicas, em todo o ciclo de vida.

8 – DOCUMENTOS PRODUZIDOS E IMPLANTADOS PELA IDEAL ODONTO

8.1 – Departamento de TI

1) NORMA DE CLASSIFICAÇÃO DA INFORMAÇÃO
2) NORMA DE CONTINUIDADE DE NEGÓCIO
3) NORMA DE GERENCIAMENTO DE SEGURANÇA
4) NORMA DE GESTÃO DE MUDANÇAS
5) NORMA DE GESTÃO DE PERÍMETRO
6) NORMA DE GESTÃO DE VULNERABILIDADE
7) NORMA DE USO ACEITÁVEL DAS TECNOLOGIAS

8) PLANO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS
9) PLANO DE RESPOSTA A INCIDENTE
10) POLÍTICA DE ARMAZENAMENTO, ANONIMIZAÇÃO E DESCARTE
11) POLÍTICA DE GESTÃO DE CRISE
12) POLÍTICA DE RESPOSTA DE INCIDENTE

8.2 – Departamento de RH

1) MANUAL DE GESTÃO DE RISCOS, CONTROLES DE SEGURANÇA, POLÍTICAS E PROCEDIMENTOS PARA OS SISTEMAS DE INFORMAÇÃO
2) NOTIFICAÇÃO DE INCIDENTE DE SEGURANÇA
3) POLÍTICA DE CONTRATAÇÃO E SELEÇÃO DE CANDIDATOS
4) POLÍTICA DE PRIVACIDADE PARA COLABORADORES DO GRUPO IDEAL
5) POLÍTICA DE PRIVACIDADE E DADOS PESSOAIS GRUPO IDEAL
6) TERMO DE RESPONSABILIDADE

8.3 – Departamento Comercial

1) POLÍTICA PRIVACIDADE CLIENTES LGPD Ideal Odonto
2) POLÍTICA DE COOKIES

9 – APROVAÇÃO

Esta seção visa formalizar a aprovação do RIPD por meio da obtenção das assinaturas do Responsável pela elaboração do RIPD, pelo encarregado e pelos profissionais que representam a empresa.

O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição.