





RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS
2ª EDIÇÃO – RIPD 2023/2024

MEMBROS DO COMITÊ LGPD / DPO SMS

Santa Marcelina Saúde

2024, V. 01



SUMÁRIO	
HISTÓRICO DE REVISÕES.....	3
OBJETIVO.....	4
INTRODUÇÃO.....	4
ETAPAS DO RIPD.....	4
1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO	5
2 – NECESSIDADE DE ELABORAR O RELATÓRIO.....	5
3 – DESCRIÇÃO DO TRATAMENTO.....	6
4 – PARTES INTERESSADAS CONSULTADAS	7
4.1 – MATURIDADE DA LGPD NA INSTITUIÇÃO	7
a) Contato do DPO.....	7
b) Diretiva de Proteção de Dados	7
c) FAQ – Perguntas e Respostas Frequentes.....	8
d) Política de Privacidade	8
e) Requerimento de Informações	8
f) Relatório de Impacto 22/23	8
g) Lei 13709-LGPD	8
4.2 – COLETA DE DADOS	8
4.2.1 – RESULTADOS OBTIDOS	9
4.3 – GOVERNANÇA	16
4.3.1 – METODOLOGIA.....	16
4.3.2 – DINÂMICA DE REUNIÕES E AÇÕES DO COMITÊ LGPD SMS.....	17
4.3.3 – INSTRUMENTOS UTILIZADOS	17
4.3.4 – MATERIAL DE APOIO AUDIO VISUAL.....	18
5 – NECESSIDADE E PROPORCIONALIDADE	18
5.1 – PRÓXIMAS ETAPAS A SEGUIR.....	19
6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS.....	20
7 – MEDIDAS PARA TRATAR OS RISCOS	20
8 – AÇÕES A SEREM DESENVOLVIDAS EM RESPOSTA AOS RESULTADOS OBTIDOS.....	21
9 – PRINCIPAIS AVANÇOS EM RELAÇÃO À 1ª FASE LGPD SMS (RIPD 22/23).....	22
10 – CONCLUSÃO	23
11 – APROVAÇÃO.....	24



Acesso em: <https://aztelecom.com.br/5-topicos-que-voce-nao-pode-perder-sobre-lgpd/>

Histórico de Revisões

Data	Versão	Descrição	Autor
01/03/2024	1.0	Conclusão do processo de elaboração da primeira versão do relatório	DPO

[Handwritten signatures and initials in blue ink]

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).

INTRODUÇÃO

Visando analisar e documentar como as atividades desta instituição afetam a privacidade e a proteção de dados pessoais dos indivíduos, no acesso, processamento, armazenamento, transmissão etc., considerando a tipologia de dados pessoais das comunidades (interna e externa) que se relacionaram ou se vinculam com as unidades de saúde do grupo Santa Marcelina Saúde, e com a finalidade de cumprir o previsto na Lei Geral de Proteção de Dados (LGPD), objetivo deste relatório de impacto é garantir que a organização compreenda plenamente os riscos associados ao processamento de dados pessoais e tome medidas adequadas para proteger os direitos e liberdades dos indivíduos, conforme exigido pela legislação de proteção de dados.

No entanto, a gestão das bases pertencentes as unidades de saúde, pacientes, colaboradores e prestadores de serviço, deverão alinhar suas estratégias, para alinhamento com a matriz. Devendo algumas ressalvas de mitigação relacionadas ao arquivamento e manipulação desses dados ou mesmo aos documentos digitais armazenados relacionados a eles. Sendo assim, o foco de proteção de dados pessoais da SMS, considerando o do fluxo da informação em dois principais contextos, paciente e familiares em busca de tratamento, profissionais, colaboradores, em uma percepção da Gestão de Pessoas, sendo o presente relatório uma ferramenta essencial para garantir que esta organização esteja em conformidade com a legislação de proteção de dados, prezando por práticas sólidas de proteção da privacidade, promovendo a confiança e o respeito dos indivíduos.

ETAPAS DO RIPD

- 1 – Identificação dos Agentes de Tratamento e do Encarregado
- 2 – Necessidade de Elaborar o Relatório
- 3 – Descrição do Tratamento
- 4 – Partes Interessadas Consultadas
- 5 – Necessidade e Proporcionalidade
- 6 – Identificação e Avaliação de Riscos
- 7 – Medidas para Tratar os Riscos



1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador	
Santa Marcelina Saúde	
Operador	
Santa Marcelina Saúde	
Encarregado	
Carlos da Silva	
E-mail Encarregado	Telefone Encarregado
dpo@santamarcelina.org	(11)2070-6203

Art. 5º Para fins desta Lei, considera-se:

VI – Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII – Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII – Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019).

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

O RIPD deve ser elaborado e/ou atualizado, por existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

- uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;
- rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada; (LGPD, art. 12 § 2º);
- tratamento de dado pessoal sobre “origem racial ou étnica, convicção religiosa, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (LGPD, art. 5º, II);
- processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20);
- tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);

- tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);
- tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);
- alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e
- reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

Ademais, é importante esclarecer que, por taxativa previsão da LGPD (Art. 4º), as disposições da Lei não são aplicadas ao tratamento de dados pessoais nas seguintes situações:

- I - Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
- II - Realizado para fins exclusivamente jornalísticos, artístico e acadêmico (aplicando-se a esta última hipótese os arts. 7º e 11 da LGPD);
- III - realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações.

3 – DESCRIÇÃO DO TRATAMENTO

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da natureza, escopo, contexto e finalidade do tratamento.

Reitera-se que a LGPD (art. 5º, X) considera tratamento “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

O principal objetivo é fornecer um cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, proporcionando subsídios para avaliação e tratamento de riscos no SMS.

Visando a conformidade com o acima referenciado, realizamos minuciosamente a verificação e validação de cada etapa descrita a seguir:

- Dados coletados;
- Dados pessoais sensíveis;
- Volumetria de dados coletados;
- Volume de dados utilizados;
- Finalidade da coleta dos dados;
- Armazenamento dos dados.

4 – PARTES INTERESSADAS CONSULTADAS

Foi realizado no nível institucional da SMS, a aplicação de ferramentas de forma on-line para realização do Diagnóstico Situacional LGPD SMS 2023 (2ª fase), o qual constituiu em levantar o nível de conhecimento e envolvimento dos colaboradores com a temática e práticas para aplicação da LGPD, dentro do grupo SMS.

Uma segunda ferramenta utilizada para obtenção dos tipos de dados que estavam sendo capturados pela instituição, foi a Classificação de Risco Referente ao Tratamento de dados pessoais, a qual visa identificar juntos aos Gestores de Unidade e Serviços, a atual condução nas unidades sobre o tratamento e guardas dos dados pessoais.

4.1. MATURIDADE DA LGPD NA INSTITUIÇÃO

Em 01/11/2019 foi criado o Comitê para a Implantação Institucional da Lei Geral de Proteção de Dados da Santa Marcelina saúde, Sendo formado por uma equipe de multiprofissional, deliberado pela Presidência da Casa de Saúde Santa Marcelina, o qual iniciou com a finalidade da implantação institucional da Lei Geral de Proteção de Dados e outras providências afins, considerando publicação em portaria específica como ato da Diretoria que designa a forma, metodologia, periodicidade e entregas do presente trabalho.

Em junho 2023, foi encerrado o primeiro ciclo sobre a condução da LGPD no grupo Santa Marcelina Saúde, contando com a conclusão do primeiro relatório de impacto à Proteção de Dados Pessoais (RIPD 2023 -1ªfase).

Link para acesso ao relatório:

https://santamarcelina.org/wp-content/uploads/2023/08/15.06.2023_RIPD_LGPD_SANTA-MARCELINA-SAUDE1.pdf

No segundo semestre de 2023, deu início a uma nova fase de consentimento aos gestores de Unidade e Serviços sobre a manutenção diária visando a LGPD no grupo SMS, levando a uma nova aplicação de formulários online para colaboradores e gestão, objetos estes, que são o alicerce do presente relatório (RIPD 2024 – 2ª fase).

INSTRUMENTOS OFICIAIS E PÚBLICOS CRIADOS EM DECORRÊNCIA DO COMITÊ.

A inclusão no site institucional (<https://santamarcelina.org/>) de um menu exclusivo para a demanda da LGPD, com a segmentação abaixo:

a) Contato do DPO

Acesso: <https://santamarcelina.org/contato-dpo>

Nesta seção, são divulgadas informações sobre o tratamento de dados pessoais realizado pela Rede de Saúde Santa Marcelina, compreendendo a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desse tratamento em cumprimento ao disposto no inciso I do art. 23 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

b) Diretiva de Proteção de Dados

Acesso: <https://santamarcelina.org/wp-content/uploads/2021/06/LGPD-SANTA-MARCELINA-SAUDE.pdf>

Este documento é destinado ao público interno e externo da Casa de Saúde Santa Marcelina e suas filiais e/ou departamentos, e busca demonstrar de maneira clara, as condutas institucionais adotadas para o cumprimento dos requisitos legais, observando a Lei Geral de Proteção de Dados, sua política de privacidade e a interação com outros preceitos e princípios institucionais que são parte do Programa de Integridade, como o Manual Institucional de Diretrizes, Boas Práticas e Condutas Éticas – Política de Compliance da Rede de Saúde Santa Marcelina.

c) **FAQ - Perguntas e Respostas Frequentes sobre A LGPD – Lei Geral de Proteção de Dados na Rede de Saúde Santa Marcelina** – Acesso: <https://santamarcelina.org/faq-lgpd/>

d) **Política de Privacidade** - Acesso: <https://santamarcelina.org/politica-de-privacidade>

Política de Privacidade, Acesso e Uso de Cookies Institucional da Casa de Saúde Santa Marcelina, seus departamentos e filiais, e sua integração com a política de Compliance, dentre outras providências.

e) **Requerimento de Informações** - <https://santamarcelina.org/requerimento-de-informacoes/>

Possibilitando o canal direto com o DPO, para a solicitação do cliente sobre informações de tratamento dos seus dados pessoais.

f) Relatório de Impacto 22/23

https://santamarcelina.org/wp-content/uploads/2023/08/15.06.2023_RIPD_LGPD_SANTA-MARCELINA-SAUDE1.pdf

g) Lei 13709-LGPD

<https://santamarcelina.org/wp-content/uploads/2023/08/L13709-LGPD.pdf>

4.2. COLETA DE DADOS

No segundo semestre de 2024, foi a aplicação dos formulários online para todos os colaboradores da grupo SMS, , com o objetivo de conhecer, mapear a guarda e o tratamento de dados pessoais pelas unidades, possibilitando identificar os pontos críticos e maiores dificuldade encontradas pelos colaboradores e conseqüentemente propor momentos pedagógicos direcionados a temáticas específicas, conforme resultado das pesquisas, e assim aprimorar as medidas padronizadas de tratamento e fortalecimento da segurança da guarda dos dados pessoais.

4.2.1 RESULTADOS OBTIDOS:

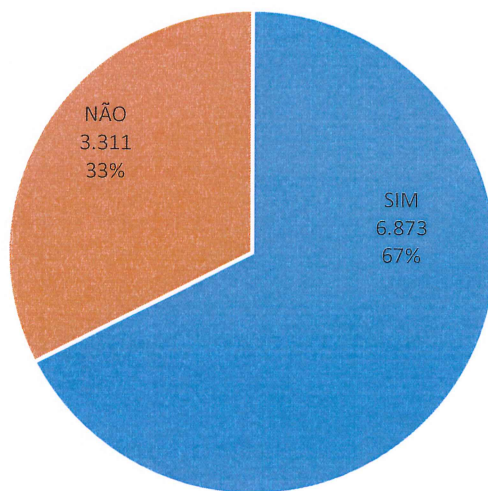
- FORMULÁRIO DE DIAGNÓSTICO SITUACIONAL LGPD 2023 (2ª FASE) – Colaboradores

O quadro abaixo, representa o percentual de respostas ao Formulário de Diagnóstico Situacional em relação ao número de colaboradores do grupo Santa Marcelina Saúde, das respectivas unidades.

UNIDADE	TOTAL DE COLABORADORES	RESPOSTAS	% RESPOSTAS
RASTS 11 - ITAQUERA/GUAIANASES/TIRADENTES	5.675	3.036	53,50%
RASTS 10 - SÃO MIGUEL / ITAIM PAULISTA	4.528	2.086	46,07%
HOSPITAL SANTA MARCELINA - MATRIZ	4.797	1.746	36,40%
OSS HOSPITAL CIDADE TIRADENTES	1.514	1.114	73,58%
OSS SANTA MARCELINA ITAIM PAULISTA	1.436	1.008	70,19%
OSS SANTA MARCELINA DE ITAQUAQUECETUBA	1.401	836	59,67%
HOSPITAL SANTA MARCELINA DE RONDONIA	423	167	39,48%
HOSPITAL SANTA MARCELINA SAÚDE - SÃO BERNARDO DO CAMPO	400	129	32,25%
HOSPITAL SANTA MARCELINA DE SAPEZAL	85	61	71,76%
TOTAL GERAL	20.259	10.183	53,66%

Fonte: Coleta de Dados 2023-2024

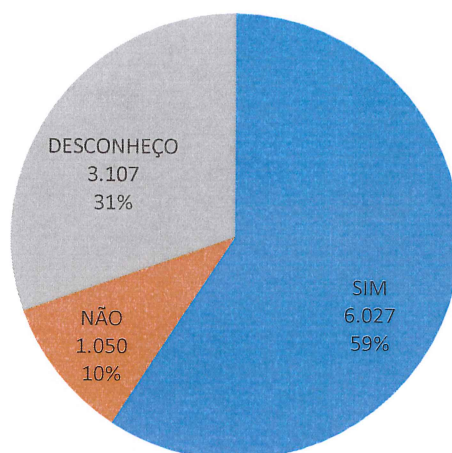
1. VOCÊ JÁ PARTICIPOU DE ALGUM MOMENTO FORMATIVO OU PEDAGÓGICO SOBRE LGPD?



Fonte: Coleta de Dados 2023-2024

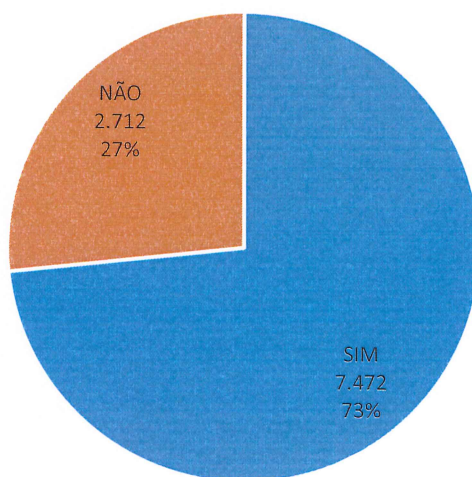
Handwritten signatures and initials in blue ink.

2. NO ÚLTIMO ANO, HOUVE ALGUMA INICIATIVA A RESPEITO DE PLANEJAMENTO SOBRE AS AÇÕES DE LGPD NO SEU SERVIÇO?



Fonte: Coleta de Dados 2023-2024

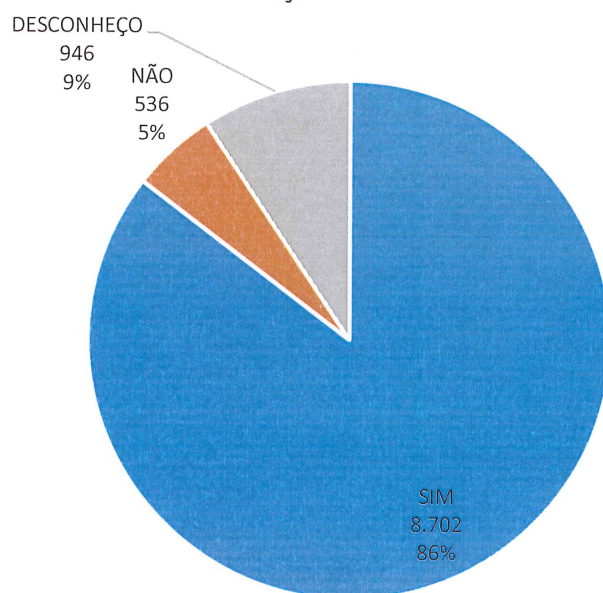
3. COMO TITULAR DE DADOS, VOCÊ CONHECE QUAIS SÃO OS DIREITOS PROTEGIDOS PELA LGPD?



Fonte: Coleta de Dados 2023-2024

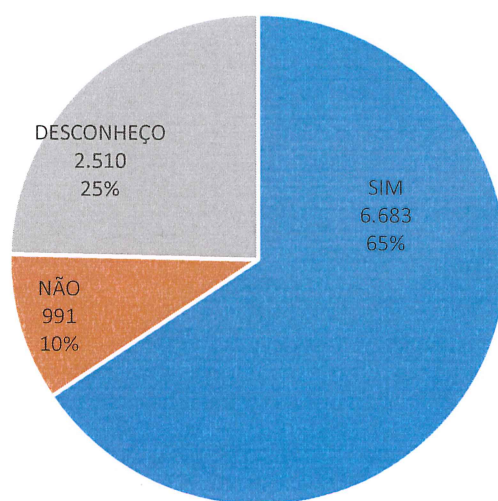
[Handwritten signatures and initials]

4. O SEU PROCESSO DE TRABALHO PODE SER CONSIDERADO SEGURO E COM A PRIVACIDADE RESPEITADA COMO PREMISSAS DA PROTEÇÃO DE DADOS?



Fonte: Coleta de Dados 2023-2024

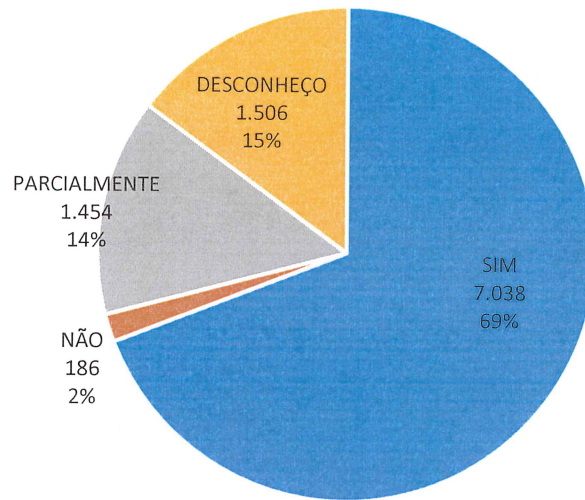
5. EXISTEM MELHORIAS NO SEU SERVIÇO E PROCESSO DE TRABALHO A RESPEITO DA LGPD QUE DEPENDEM DE SUA PARTICIPAÇÃO?



Fonte: Coleta de Dados 2023-2024

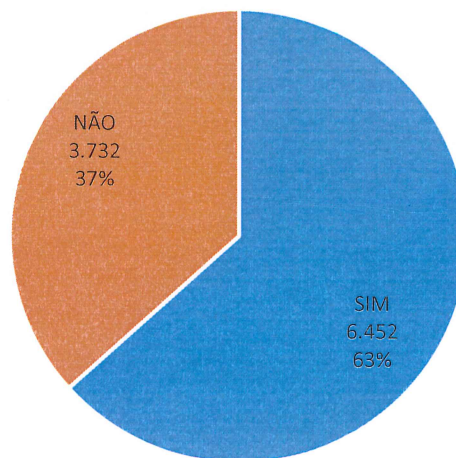
[Handwritten signatures and initials]

6. SUA EMPRESA POSSUI POLÍTICAS, PROCEDIMENTOS E MEDIDAS PROTETIVAS (CONTROLES DE ACESSO, CRIPTOGRAFIA, MODIFICAÇÃO DE DADOS, ANONIMIZAÇÃO DE DADOS) QUE PROPORCIONAM SEGURANÇA E GARANTEM A CONFORMIDADE COM OS REGULAMENTOS/LEIS DE PRIVACIDADE?



Fonte: Coleta de Dados 2023-2024

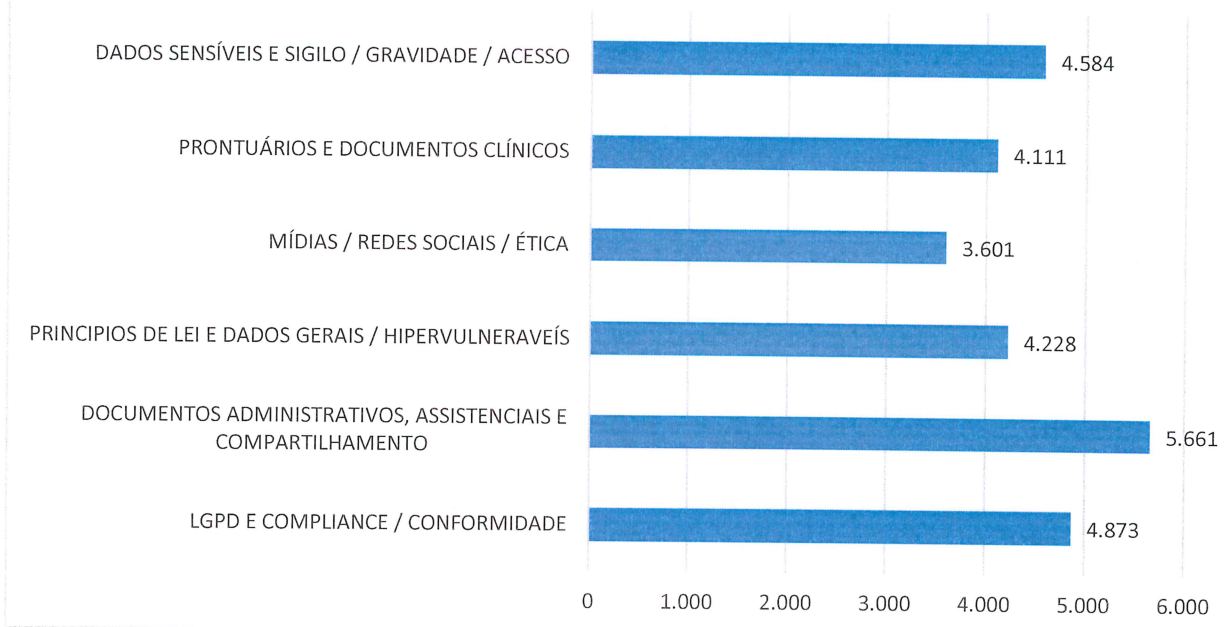
7. VOCÊ SABE DIFERENCIAR DADOS PESSOAIS GERAIS DE DADOS PESSOAIS SENSÍVEIS (LEI 13.709/2018 – ART 5º, I e II)?



Fonte: Coleta de Dados 2023-2024

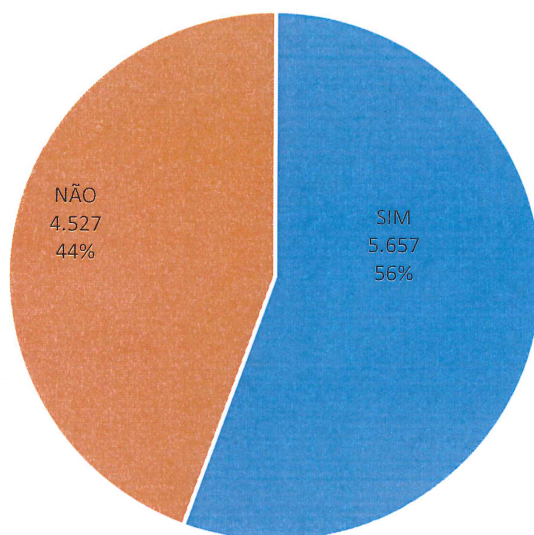
Handwritten signatures and initials in blue ink.

8. QUAIS OS TEMAS ABAIXO VOCÊ GOSTARIA DE SE APRIMORAR COM RELAÇÃO À LGPD?



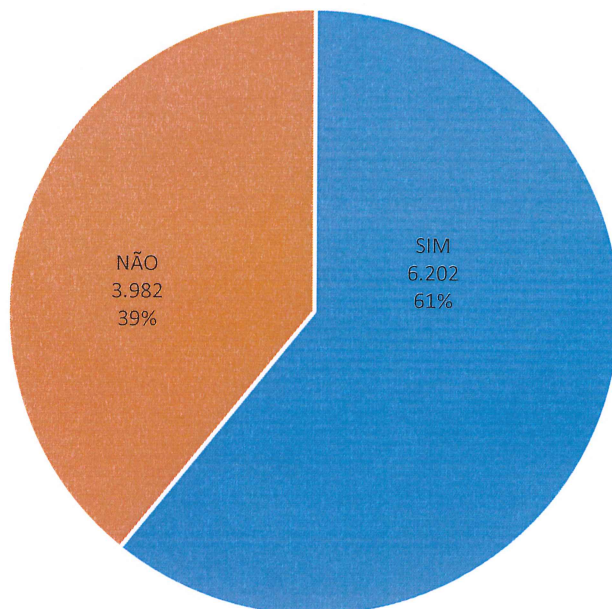
Fonte: Coleta de Dados 2023-2024

9. VOCÊ JÁ FEZ A LEITURA DO MATERIAL SOBRE LGPD PRESENTE NO SITE INSTITUCIONAL?



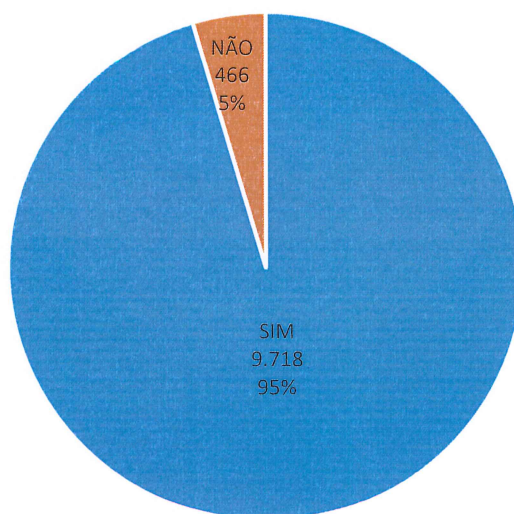
Fonte: Coleta de Dados 2023-2024

10. VOCÊ JÁ FEZ A LEITURA DO MATERIAL SOBRE COMPLIANCE PRESENTE NO SITE INSTITUCIONAL?



Fonte: Coleta de Dados 2023-2024

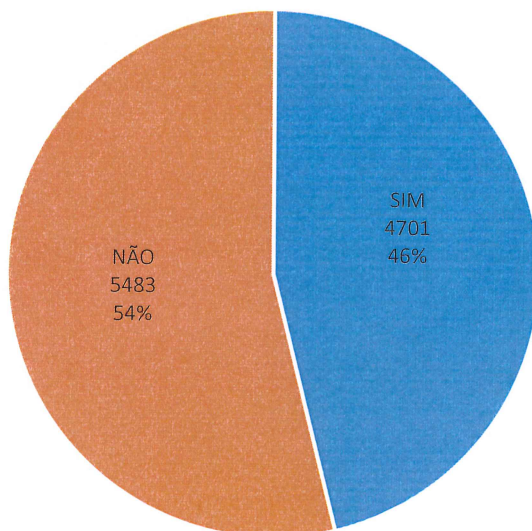
11. VOCÊ CONSIDERA IMPORTANTE FAZER OS MOMENTOS DE CAPACITAÇÃO ATRAVÉS DA AAGAPE SANTA MARCELINA?



Fonte: Coleta de Dados 2023-2024

[Handwritten signatures and initials in blue ink]

12. VOCÊ CONHECE NA ÍNTEGRA A LEI GERAL DE PROTEÇÃO DE DADOS (LEI 13.709/2018)?



Fonte: Coleta de Dados 2023-2024

[Handwritten signatures and initials]

4.3 GOVERNANÇA:

A governança na LGPD (Lei Geral de Proteção de Dados) refere-se aos processos, políticas e estruturas organizacionais estabelecidos para garantir o cumprimento eficaz dos requisitos da lei.

Institucionalmente, foi constituído um time multidisciplinar, contando com colaboração entre tecnologia; processos de negócios e jurídico; governança da privacidade; processos orientados a dados; transparência, permitindo assim, um equilíbrio de forças e skills para o desenvolvimento das atividades do comitê.

Para reforçar as ações e mapeamento da abrangência da LGPD na Instituição, foi criado um ambiente on-line para que o comitê pudesse se apropriar e discutir a Lei Geral de Proteção de Dados, assim como estabelecer diretrizes institucionais e estratégias, a fim de garantir sua efetiva implantação e cumprimento. Este ambiente criado é um espaço colaborativo na construção, apropriação de conhecimentos e aproximação dos participantes em torno deste objetivo comum.

O processo de governança na LGPD é fundamental para garantirmos que nossas operações sejam de forma ética, transparente e responsável no tratamento de dados pessoais, promovendo a confiança dos indivíduos e o cumprimento das exigências legais.

4.3.1 METODOLOGIA

O comitê multiprofissional foi formado a partir de deliberação da Presidência da Casa de Saúde Santa Marcelina para fins de implantação institucional da Lei Geral de Proteção de Dados e outras providências afins, considerando publicação em portaria específica como ato da Diretoria que designa a forma, metodologia, periodicidade e entregas do presente trabalho.

A metodologia que desenvolvemos para criarmos um ambiente para sustentação da LGPD na SMS, consistiu em um conjunto de ferramentas e aplicabilidades, que nos permitiram realizar um mapeamento amplo do momento inicial da instituição e nos apoiar a evoluímos no padrão a que chegamos hoje.

Para que pudéssemos aplicar a LGPD (Lei Geral de Proteção de Dados) de forma eficaz, procuramos seguir uma metodologia estruturada, seguindo alguns preceitos fundamentais da LGPD, conforme descrito abaixo:

1. **Conscientização e Treinamento:** Iniciando com a conscientização sobre a LGPD em toda a instituição, desde a alta administração até os funcionários de linha de frente. Oferecendo treinamento detalhado sobre os princípios e requisitos da LGPD e o impacto das políticas de proteção de dados nas operações diárias.
2. **Mapeamento de Dados:** Realizando um inventário completo dos dados pessoais que a instituição coleta, armazena, processa e compartilha. Incluindo identificar a origem dos dados, a finalidade do processamento, os meios de armazenamento e as partes envolvidas no processamento.
3. **Análise de Riscos e Impacto à Privacidade:** Realizando uma avaliação detalhada dos riscos associados ao tratamento de dados pessoais e identificando possíveis ameaças à segurança dos dados, como vazamentos, acessos não autorizados ou violações de privacidade, e ainda, avaliando o impacto potencial dessas ameaças nos direitos e liberdades dos titulares dos dados.
4. **Desenvolvimento de Políticas e Procedimentos:** Com base na análise de riscos, desenvolvemos políticas e procedimentos claros para governar o tratamento de dados pessoais. Isso inclui políticas de privacidade, consentimento, segurança da informação, retenção de dados e resposta a incidentes de segurança.

5. **Implementação de Medidas Técnicas e Organizacionais:** Implementamos medidas técnicas e organizacionais para garantir a segurança dos dados pessoais e o cumprimento dos requisitos da LGPD, incluindo o controle de acesso, a pseudo-anonimização, a anonimização a minimização de dados e a auditoria de segurança.

6. **Monitoramento e Revisão Contínua:** Estabelecemos um programa de monitoramento contínuo para garantir que as políticas e procedimentos de proteção de dados sejam seguidos adequadamente. Visando realizar auditorias periódicas para avaliar o cumprimento da LGPD e faça ajustes conforme necessário.

7. **Resposta a Incidentes:** Visando desenvolver um plano de resposta a incidentes para lidar com violações de dados pessoais de maneira rápida e eficaz, incluindo procedimentos para notificar as autoridades competentes e os titulares dos dados afetados, conforme exigido pela LGPD.

Ao seguirmos essas metodologias, visamos garantir uma aplicação eficaz da LGPD e demonstrar o compromisso institucional com a proteção da privacidade e dos direitos dos titulares dos dados pessoais.

4.3.2 DINÂMICA DE REUNIÕES E AÇÕES DO COMITÊ LGPD SMS

A dinâmica das ações do comitê foi composta por reuniões sempre a partir da presença de um núcleo permanente, que não se alterou e estiveram semanalmente reunidos, pelo período máximo de uma hora para a execução do planejamento. Os demais participantes foram integrados conforme as ações e atividades de concentração e dispersão, com as demandas e encomendas subsidiada pela discussão dos assuntos. Foi elaborado um cronograma a ser seguidos, o qual foi aprovado pela Direção e divulgado, com a finalidade de garantia das agendas se fizessem prioritárias para estes encontros, os quais foram secretariados com produção de atas, formalizando a participação e suas entregas. Além disso a instituição produziu o seu regulamento, visando disciplinar os aspectos gerais e orientações para a Lei Geral de Proteção de Dados, tendo caráter geral a todas as unidades, serviços e departamentos integrantes da Rede de Saúde Santa Marcelina. Foram realizadas adequações ao Manual Institucional de Diretrizes, Boas Práticas e Condutas Éticas – Política de Compliance, vigente desde 2016. Como estratégia de disseminação de conteúdo, a Casa de Saúde Santa Marcelina se valeu, dentre outras medidas, do ambiente virtual da AAGAPE Santa Marcelina, como repositório de conteúdo e fonte de consulta, além de ações específicas de treinamentos e capacitações presenciais, considerando a uniformização de conceitos e práticas, as quais foram convertidos posteriormente em política institucional.

4.3.3 INSTRUMENTOS UTILIZADOS:

Como estratégia inicial de disseminação de conteúdo, a Casa de Saúde Santa Marcelina se valeu, dentre outras ferramentas, o ambiente virtual da AAGAPE Santa Marcelina, como repositório de conteúdo e fonte de consulta, além de ações específicas de treinamentos e capacitações presenciais, considerando a uniformização de conceitos e práticas que foram convertidas em política institucional.



4.3.4 MATERIAL DE APOIO ÁUDIO VISUAL:

Foram criados vídeos institucionais, no intuito de instruir os colaboradores ao consentimento e cultura da LPGD SMS, assim como instrumento orientador no preenchimento dos formulários requisitados pelo comitê LGPD aos representantes das unidades / setores.

- Orientações no preenchimento do formulário Diagnóstico situacional LGPD 2023(Colaboradores):

Link de acesso: <https://www.youtube.com/watch?v=9Sc5oDHLog4>

- Orientações no preenchimento do formulário LGPD - Classificação de Risco Referente ao Tratamento de Dados Pessoais (gestores):

Link de acesso: <https://www.youtube.com/watch?v=PGH2URv1rwI>

5 – NECESSIDADE E PROPORCIONALIDADE

Todos os dados coletados nas operações cotidianas do SMS, são criteriosamente elegidos no intuito de atender a real necessidade de utilização dos dados, levando em consideração a sua finalidade e proporcionalidade, de forma que não tenhamos informações demasiadas e que não sejam necessários e essenciais para o atendimento do serviço proposto, consequentemente respeitando ao princípio da minimização de dados, ou seja, se os dados coletados se limitam ao mínimo necessário para o atingimento da finalidade proposta, sendo pertinentes, proporcionais e não excessivos. Ainda, esforços são realizados para garantir a qualidade dos dados, exatidão, clareza, relevância e atualização, em conformidade com informações de direitos dos titulares e assim atendendo o previsto no art. 18 da LGPD.

Em relação à natureza do tratamento:

- Considerando o estágio atual, deve admitir-se que os documentos e/ou formulários em papel constituem a forma predominante dos ativos de informações da SMS, inclusive de dados pessoais coletados, e esse material é ainda a principal fonte de arquivamento;
- No entanto, pode dizer-se que a maioria das demais operações (produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração) sendo os ativos de dados pessoais por meio de processamento de Sistema de Gestão Hospital;
- Essas relações não são poucas e se iniciam na própria SMS, onde encarregados realizam o tratamento de dados pessoais em nome da Instituição. Mas existem também outras operações como, por exemplo, a difusão que permite a divulgação e/ou a propagação desses dados para fora da Hospital, como em casos de pesquisas clínica e relatório epidemiológicos;
- A principal solução de tratamento e guarda da informação é o Sistema MV, no qual são manipulados os diversos prontuários dos pacientes. De acordo com o perfil de acesso (autenticado pelo usuário e senha), módulos correspondentes às especificidades dos usuários são disponibilizados.



Em relação ao escopo do tratamento:

- Além dos dados usuais de identificação (Nome, CPF, Sexo,...), rastreamento (endereço, telefone, e-mail...).
- Em relação aos dados sensíveis, pode dizer-se que o cadastro de dados sobre “origem racial ou étnica”, “referente à saúde”, “nome social”, “genético ou biométrico” são efetivados a todos os pacientes.

Em relação ao contexto do tratamento:

- No caso da SMS, o contexto do tratamento de dados pessoais está relacionado à execução de regulamentos e/ou políticas públicas, devidamente previstas em lei. Nesse sentido, o tratamento para cumprimento de obrigação legal ou regulatória pela SMS é uma hipótese inerente ao serviço público em geral, ficando assim a Instituição dispensada, em tese, do consentimento dos titulares para tal.

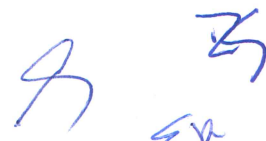
5.1 ETAPAS A SEGUIR

1) Aprimorar as ferramentas hoje existentes, a fim de estar em conformidade com as novas mudanças e definições da **Autoridade Nacional de Proteção de Dados (ANPD)**, na Lei Geral De Proteção de Dados (LGPD), evitando assim sanções e penalidades por não cumprimento da lei, as quais regem o **Regulamento de Dosimetria e Aplicação de Sanções Administrativas**, o qual possibilita que a ANPD aplique as punições necessárias para cada caso.

2) Atualização do momento pedagógico com os colaboradores do grupo SMS, visando reforçar a temática da LGPD na instituição.

3) Aplicação dos Formulários:

- LGPD SMS - Diagnóstico Situacional dos Prestadores De Serviços (2024) – Gestores
- LGPD SMS - Diagnóstico Situacional dos Prestadores De Serviços (2024) – Colaboradores

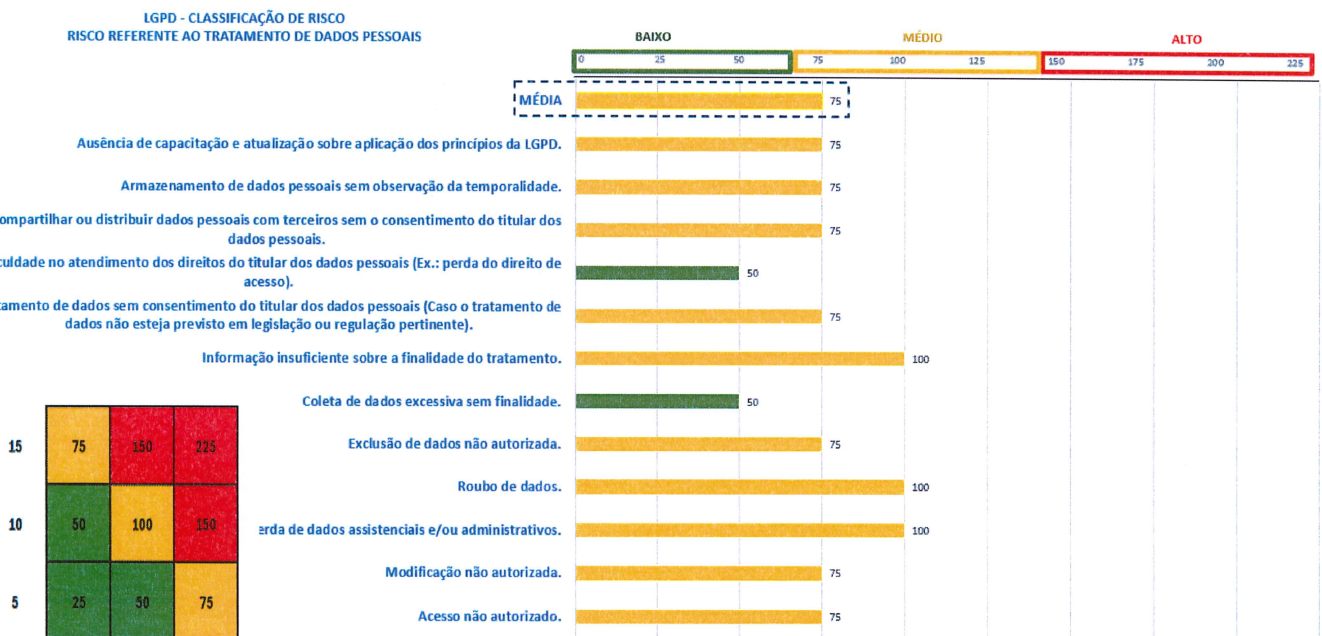


6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Com a finalidade de mantermos a conformidade com a legislação e proteger os dados pessoais dos titulares. Realizamos um processo detalhado para realizar essa identificação e avaliação das manipulações e guardas dos dados pessoais.

Nessa etapa, deve-se verificar todas as fontes de riscos e a respectiva consequência para os direitos das pessoas titulares.

Representados abaixo os níveis teóricos de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança. Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:



Fonte: Coleta de Dados 2023-2024

7 – MEDIDAS PARA TRATAR OS RISCOS

Entendemos como primordial algumas medidas compartilhadas com os integrantes da SMS para lidarmos com os riscos, com os exemplos a seguir:

[Handwritten signatures and initials]

MEDIDA	DESCRIÇÃO
1	Atualização de momentos pedagógicos para capacitação e de sensibilização a respeito da LGPD aos integrantes do SMS;
2	Constante revisão das informações sobre as respectivas finalidades dos dados em todos os formulários de cadastros, consultas, processos e relatórios (físicos e digitais) da SMS;
3	Reforçar a orientação aos colaboradores de possíveis sanções aos responsáveis em todos os locais físicos (gavetas, arquivos, depósitos etc.) de retenção de dados pessoais na SMS;
4	Monitorar se o controle de acesso aos setores internos, pelos colaboradores está devidamente identificado;
5	Monitorar a proteção lógica nos sistemas (atualizações de antivírus, senhas e demais acessos);
6	Registrar logs de acesso e alteração ou eliminação de dados com identificador, data e hora da ligação, IP;
7	Monitorar do nível de segurança dos sites externos, (utilização do protocolo https e TLS na comunicação dos e-mails);
8	Monitorar a salvaguarda dos dados (backups diários, redundância, plano de Disaster Recovery em sites fisicamente distintos).

Adoção de medidas de segurança, técnicas e administrativas para 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.

A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis, até um risco de nível alto, devidos aos benefícios do processamento dos dados pessoais e as dificuldades de mitigação, mas é altamente recomendável que em casos de houver um risco residual de nível alto, a instituição consulte a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.

8. AÇÕES A SEREM DESENVOLVIDAS EM RESPOSTA AOS RESULTADOS OBTIDOS

Com a finalidade de propagar o conhecimento sobre a LGPD (Lei Geral de Proteção de Dados), as instituições podem adotar uma variedade de medidas para garantir que seus funcionários, parceiros comerciais e outras partes interessadas compreendam as implicações da legislação e estejam preparados para cumpri-la. Algumas dessas medidas incluem:

Treinamento e conscientização: Realizar programas de treinamento regulares para os colaboradores em todos os níveis da instituição, abordando os princípios básicos da LGPD, as responsabilidades individuais e as melhores práticas para proteger os dados pessoais.

Material educacional: Fornecer materiais educacionais, como guias, manuais e infográficos, que explicam de forma clara e acessível os requisitos da LGPD e as etapas necessárias para garantir a conformidade.

Sessões informativas: Realizar sessões informativas ou palestras sobre a LGPD, onde especialistas internos ou externos possam discutir os aspectos-chave da legislação, responder a perguntas e fornecer orientação prática.

Comitê de privacidade: Estabelecer por meio do comitê de privacidade, o monitoramento e coordenação dos esforços de conformidade com a LGPD, garantindo a aplicação consistente dos princípios de proteção de dados em toda a instituição.

Comunicação interna: Integrar informações sobre a LGPD na comunicação interna da organização, incluindo boletins informativos, intranet e outros canais de comunicação utilizados para garantir que os funcionários estejam atualizados sobre as políticas e procedimentos relacionados à proteção de dados.

Avaliação de competências: Realizar avaliações periódicas das competências e conhecimentos dos funcionários em relação à LGPD, identificando áreas de melhoria e oferecendo oportunidades de treinamento adicional, conforme necessário.

Parcerias externas: Colaborar com consultorias especializadas, escritórios de advocacia ou outras organizações externas que possuam experiência em privacidade de dados para fornecer orientação e suporte na implementação da LGPD.

Recursos online: Disponibilizar recursos online, como documentos técnicos, webinars e cursos de e-learning, para facilitar o acesso ao conhecimento sobre a LGPD, especialmente para funcionários remotos ou em locais geograficamente dispersos.

Ao adotar essas medidas, as organizações podem garantir que todos os envolvidos estejam adequadamente informados e preparados para cumprir os requisitos da LGPD, promovendo uma cultura de privacidade de dados e reduzindo o risco de violações.

9. PRINCIPAIS AVANÇOS EM RELAÇÃO À 1ª FASE LGPD SMS (RIPD 22/23)

Em relação a experiência obtida na 1ª fase da LGPD na instituição e seus principais avanços, podemos destacar

1. **Abrangência mais ampla:** Conseguimos abranger uma gama mais ampla de áreas e processos dentro da organização, refletindo a compreensão mais detalhada das implicações da LGPD em todas as operações.
2. **Mapeamento de dados mais detalhado:** Permitiu termos um mapeamento mais detalhado dos dados pessoais processados pela organização, identificando com mais precisão onde os dados estão armazenados, quem tem acesso a eles e como são utilizados.
3. **Avaliação de riscos mais abrangente:** Baseados no nível de conhecimento cada colaborador, nos auxilia na avaliação de riscos pode ser mais abrangente e sofisticada, levando em consideração uma variedade de fatores,

como a sensibilidade dos dados, a probabilidade de violações e as possíveis consequências para os titulares dos dados,

4. **Inclusão de salvaguardas e medidas de segurança:** Nos permitiu uma análise mais detalhada das medidas de segurança existentes e a identificação de lacunas que precisavam ser abordadas para garantir a conformidade com a LGPD, com a contribuição dos colaboradores.

5. **Envolvimento das partes interessadas:** Contribuiu em um maior envolvimento dos colaboradores, de modo que nos auxiliou na elaboração do relatório de impacto, garantindo uma compreensão mais completa das questões relacionadas à privacidade de dados.

6. **Atualização contínua:** Entendimento de uma rotina a ser projetada, para ser atualizada regularmente, refletindo as mudanças nas práticas de negócios, na legislação e nas melhores práticas de privacidade de dados.

Essas são as principais pontuações de avanços, que o presente relatório de impacto da LGPD pôde apresentar em relação a versão anterior, refletindo a evolução contínua das práticas de privacidade de dados e a adaptação às exigências regulatórias em constante mudança.

10 - CONCLUSÃO

Em suma, o relatório de impacto da LGPD revela a complexidade e abrangência dos desafios enfrentados pela nossa organização na conformidade com essa legislação crucial de proteção de dados. Identificamos áreas de vulnerabilidade, implementamos medidas corretivas e fortalecemos nossas políticas e práticas de privacidade. No entanto, reconhecemos que a jornada rumo à plena conformidade é contínua e exige um compromisso constante com a proteção dos dados pessoais de nossos clientes, funcionários e parceiros. Apesar dos desafios, estamos confiantes de que, com diligência e investimento contínuo em recursos e educação, podemos não apenas atender aos requisitos da LGPD, mas também fortalecer nossa reputação como uma organização comprometida com a privacidade e segurança dos dados.



11 – APROVAÇÃO

Declaro por meio deste documento que revisei e aprovo o Relatório de Impacto da LGPD elaborado pelo comitê LGPD Santa Marcelina Saúde.

O Relatório de Impacto da LGPD é uma análise abrangente e detalhada dos efeitos da Lei Geral de Proteção de Dados em nossa instituição, incluindo uma avaliação dos riscos associados ao tratamento de dados pessoais e as medidas de mitigação propostas.

Ao aprovar este relatório, reconheço a importância da conformidade com a LGPD para garantir a proteção dos direitos e liberdades dos titulares dos dados e o compromisso desta organização em agir de acordo com os requisitos legais e éticos relacionados à proteção de dados pessoais.

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	
MEMBROS DO COMITÊ LGPD SMS	
 Charles Neris dos Santos Santa Marcelina Saúde Coordenador de TI Corporativo	 Renato Vieira da Rocha Hospital Santa Marcelina Coordenador de TI Corporativo TI
ENCARREGADO  Carlos da Silva Carlos Silva Hospital Santa Marcelina Gerente Corporativo de TI	REPRESENTANTE DO COMITÊ LGPD SMS  Eliza Yukie Inakake  Gustavo R. de Oliveira CAB/RJ 106.400 Casa de Saúde Santa Marcelina Assessoria Presidência Metrícula 13.935
REPRESENTANTE LEGAL DO CONTROLADOR  Ir Rosane Ghedin  Ir. Rosane Ghedin Diretora - Presidência Casa de Saúde Sta. Marcelina	

São Paulo, 01 de março de 2024

2
2/2

Comitê de Privacidade e Proteção de Dados – LGPD - SANTA MARCELINA SAÚDE | ITAQUERA

Subcomitê de Privacidade e Proteção de Dados – LGPD - SANTA MARCELINA SAÚDE | ITAIM PAULISTA

Subcomitê de Privacidade e Proteção de Dados – LGPD - SANTA MARCELINA SAÚDE | ITAQUAQUECETUBA

Subcomitê de Privacidade e Proteção de Dados – LGPD - SANTA MARCELINA SAÚDE | ITAIM PAULISTA

Subcomitê de Privacidade e Proteção de Dados – LGPD - SANTA MARCELINA SAÚDE | SÃO BERNARDO DO CAMPO

Subcomitê de Privacidade e Proteção de Dados – LGPD - SANTA MARCELINA SAÚDE | SAPEZAL

Subcomitê de Privacidade e Proteção de Dados – LGPD - SANTA MARCELINA SAÚDE | PORTO VELHO

Subcomitê de Privacidade e Proteção de Dados – LGPD - SANTA MARCELINA SAÚDE | ATENÇÃO PRIMÁRIA A SAÚDE

Handwritten signature and initials in blue ink, located in the bottom right corner of the page. The signature appears to be 'R' followed by some scribbles, and there are some other marks nearby.



SANTA MARCELINA
Saúde