



# RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

3ª edição 2025/2026

MEMBROS DO COMITÊ LGPD / DPO SMS



2026, 1ª VERSÃO.



**SANTA MARCELINA**  
Saúde

**Sumário**

Histórico de Revisões.....4

OBJETIVO .....4

INTRODUÇÃO.....4

ETAPAS DO RIPD.....4

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO DE DADOS (DPO).....5

2 – JUSTIFICATIVA PARA A ELABORAÇÃO DO RELATÓRIO.....5

3 – DESCRIÇÃO DO TRATAMENTO.....6

4 – IDENTIFICAÇÃO DAS PARTES INTERESSADAS CONSULTADAS.....7

    4.1 – MATURIDADE DA LGPD NA INSTITUIÇÃO.....7

        INSTRUMENTOS OFICIAIS E PÚBLICOS CRIADOS EM DECORRÊNCIA DO COMITÊ.....8

            a) Contato do DPO.....8

            b) Diretiva de Proteção de Dados.....8

            c) FAQ – Perguntas e Respostas Frequentes sobre a LGPD.....8

            d) Política de Privacidade.....8

            e) Requerimento de Informações.....8

            f) Relatório de Impacto 2022/2023.....9

            g) Relatório de Impacto 2023/2024.....9

            h) Lei nº 13.709/2018 – LGPD.....9

    4.2 – COLETA DE DADOS.....9

        4.2.1 – RESULTADOS OBTIDOS.....9

            - FORMULÁRIO DE DIAGNÓSTICO SITUACIONAL LGPD 2025 (3ª FASE) – GESTORES.....9

            - FORMULÁRIO DE DIAGNÓSTICO SITUACIONAL LGPD 2025 (3ª FASE) – NÃO GESTORES...32

    4.3 – GOVERNANÇA.....50

        4.3.1 – METODOLOGIA.....50

        4.3.2 – DINÂMICA DE REUNIÕES E AÇÕES DO COMITÊ LGPD SMS.....51

        4.3.3 – INSTRUMENTOS UTILIZADOS.....52

        4.3.4 – MATERIAL DE APOIO ÁUDIO VISUAL.....52

5 – ANÁLISE DE NECESSIDADE E PROPORCIONALIDADE.....53

6 – METODOLOGIA ADOTADA PARA IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS.....53

7 – MEDIDAS PARA TRATAR OS RISCOS .....55

8 - RESUMO DAS AÇÕES E O PLANO DE AÇÃO 2025-2026..... 55

9 - PRINCIPAIS AVANÇOS EM RELAÇÃO À 2ª FASE LGPD SMS (RIPD 23/24) .....57

# RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

MEMBROS DO COMITÊ LGPD / DPO SMS

10 – SEGURANÇA DA INFORMAÇÃO.....	57
11 – CONCLUSÃO.....	58
12 – APROVAÇÃO.....	60

## OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) 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

Considerando-se as operações de tratamento (acesso, processamento, armazenamento, transmissão, etc.) e a tipologia de dados pessoais das comunidades (interna e externa) que se relacionam ou se vinculam com as unidades de saúde do grupo Santa Marcelina Saúde (SMS), em princípio, as hipóteses previstas na Lei Geral de Proteção de Dados (LGPD) demonstram ser mais abrangentes. No entanto, a gestão das bases pertencentes às unidades de saúde, pacientes, colaboradores e prestadores de serviços deverá alinhar suas estratégias à matriz. Devem ser feitas algumas ressalvas de mitigação relacionadas ao arquivamento e à manipulação desses dados, bem como aos documentos digitais armazenados a eles relacionados. Sendo assim, o foco da proteção de dados pessoais da SMS considera o fluxo da informação em dois principais contextos: pacientes e familiares em busca de tratamento, e profissionais e colaboradores, sob a perspectiva da Gestão Estratégica de Pessoas. Nesse sentido, o presente relatório configura-se como uma ferramenta essencial para garantir que a Organização esteja em conformidade com a legislação de proteção de dados, prezando por práticas sólidas de proteção da privacidade e promovendo a confiança e o respeito dos indivíduos.

## ETAPAS DO RIPD

- 1 – Identificação dos Agentes de Tratamento e do Encarregado de Dados (DPO)
- 2 – Justificativa para a Elaboração do Relatório
- 3 – Descrição do Tratamento
- 4 – Identificação das Partes Interessadas Consultadas
- 5 – Análise de Necessidade e Proporcionalidade
- 6 – Metodologia adotada para Identificação e Avaliação de Riscos
- 7 – Medidas para Tratamento dos Riscos
- 8 – Resumo das Ações e o Plano de Ação 2025-2026
- 9 – Principais Avanços em Relação à 2ª Fase LGPD SMS (RIPD 23/24)
- 10 – Segurança da Informação
- 11 – Conclusão
- 12 – Aprovação

**1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO DE DADOS (DPO)**

<b>Controlador</b>	
Santa Marcelina Saúde	
<b>Operador</b>	
Santa Marcelina Saúde	
<b>Encarregado de Dados (DPO)</b>	
Carlos da Silva	
<b>Contato do DPO</b>	
<b>e-mail:</b> dpo@santamarcelina.org	<b>telefone:</b> (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 Agência Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 15.352, de 2026).

**2 – JUSTIFICATIVA PARA A ELABORAÇÃO DO RELATÓRIO**

No caso da SMS, o RIPD deve ser elaborado e/ou atualizado devido à possibilidade de ocorrência de 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 à 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);
- Tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, caso ocorra vazamento (LGPD, art. 42);
- Tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);

- Alterações nas leis, resoluções e regulamentos aplicáveis à privacidade, políticas e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, entre outros; 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 previsão expressa da LGPD (art. 4º), as disposições da lei não se aplicam ao tratamento de dados pessoais nas seguintes situações:

I - Quando realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - Quando realizado para fins exclusivamente jornalísticos, artísticos ou acadêmicos (aplicando-se a esta última hipótese os arts. 7º e 11 da LGPD);

III - Quando 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, do escopo, do contexto e da 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 de dados pessoais, proporcionando subsídios para avaliação e mitigação de riscos na SMS.

Visando à conformidade com o acima referenciado, realiza-se a minuciosa 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 – IDENTIFICAÇÃO DAS PARTES INTERESSADAS CONSULTADAS

Foi realizada, no nível institucional da SMS, a aplicação de ferramentas on-line para a realização do Diagnóstico Situacional LGPD SMS 2025, o qual teve como objetivo levantar o nível de conhecimento e envolvimento dos colaboradores com a temática e as práticas de aplicação da LGPD, dentro do grupo SMS.

Uma segunda ferramenta utilizada para a identificação dos tipos de dados capturados pela Instituição foi a Classificação de Risco Referente ao Tratamento de Dados Pessoais, a qual visa identificar, junto aos Gestores de Unidade e Serviços, a condução atual dos serviços quanto ao tratamento e à guarda 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 este formado por uma equipe multiprofissional, deliberada pela Presidência da Santa Marcelina Saúde. O Comitê teve como finalidade a implantação institucional da Lei Geral de Proteção de Dados e demais providências afins, considerando a publicação em portaria específica, como ato da Diretoria que designa a forma, a metodologia, a periodicidade e as entregas do presente trabalho.

Em junho de 2023, foi encerrado o primeiro ciclo sobre a condução da LGPD no grupo Santa Marcelina Saúde, com a conclusão do RIPD 2023 (1ª fase).

No segundo semestre de 2023, teve início uma nova rodada de consentimento junto aos Gestores dos serviços sobre a manutenção das práticas relacionadas à LGPD no grupo SMS, o que levou a uma nova aplicação de formulários online para Colaboradores e Gestores. Esses instrumentos constituem o alicerce do presente relatório (RIPD 2024 – 2ª fase).

Dando continuidade ao Programa Anual de LGPD, este relatório detalha a terceira etapa (RIPD 2026 – 3ª fase), fundamentada nos resultados da pesquisa de conscientização aplicada entre dezembro de 2025 e janeiro de 2026. Os dados coletados por meio de formulários eletrônicos com os colaboradores da rede Santa Marcelina Saúde consolidam o amadurecimento do processo iniciado nos ciclos anteriores e permitem a melhoria contínua na tomada de decisão, fortalecendo o Programa de Privacidade da Instituição.

## **INSTRUMENTOS OFICIAIS E PÚBLICOS CRIADOS EM DECORRÊNCIA DO COMITÊ**

Foi realizada a inclusão, no site institucional (<https://santamarcelina.org/>) de um menu exclusivo destinado às demandas relacionadas à LGPD, estruturado com as seguintes seções:

### **a) Contato do DPO**

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

Nesta seção, divulgam-se 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 adotadas 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 Santa Marcelina Saúde, bem como às suas filiais e/ou departamentos, e tem como objetivo demonstrar, de forma clara, as condutas institucionais adotadas para o cumprimento dos requisitos legais previstos na Lei Geral de Proteção de Dados. O documento também contempla a Política de Privacidade Institucional e sua interação com outros preceitos e princípios institucionais integrantes do Programa de Integridade, como o Manual Institucional de Diretrizes, Boas Práticas e Condutas Éticas – Política de Compliance da Santa Marcelina Saúde.

### **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/>

Apresenta a Política de Privacidade, Acesso e Uso de Cookies Institucional da Santa Marcelina Saúde, abrangendo seus departamentos e filiais, bem como sua integração com a Política de Compliance e demais diretrizes institucionais pertinentes.

### **e) Requerimento de Informações**

Acesso: <https://santamarcelina.org/requerimento-de-informacoes/>

Disponibiliza canal direto com o DPO para a solicitação, por parte do titular, de informações relacionadas ao tratamento de seus dados pessoais.

**f) Relatório de Impacto 2022/2023**

**g) Relatório de Impacto 2023/2024**

**h) Lei nº 13.709/2018 – LGPD**

**4.2. COLETA DE DADOS**

Com o objetivo de reforçar o compromisso institucional com a Transparência e a Segurança da Informação, entre dezembro de 2025 e janeiro de 2026, foi realizada a aplicação de um Questionário de Conscientização sobre a LGPD (Lei Geral de Proteção de Dados) junto aos Gestores e Colaboradores da SMS.

Tal ação teve como finalidade identificar o nível de maturidade das equipes e os pontos sensíveis que demandam maior atenção. Com base nos resultados obtidos, serão propostos momentos pedagógicos direcionados a temáticas específicas, visando ao aprimoramento dos padrões de tratamento e segurança dos dados.

A medida integra o Programa Contínuo de Governança e Conformidade em Proteção de Dados, buscando não apenas avaliar o nível de conhecimento das equipes, mas também promover a disseminação de Boas Práticas no Tratamento de Dados Pessoais.

Parte-se do entendimento de que a Proteção de Dados constitui responsabilidade compartilhada, sendo o engajamento de todos fundamental para assegurar a privacidade e a confiança de clientes, parceiros e colaboradores.

Os resultados obtidos permitem direcionar, de forma mais estratégica, as próximas etapas do Plano de Ação, contribuindo para que as operações institucionais permaneçam alinhadas às exigências legais e aos mais elevados padrões de ética digital.

**4.2.1 RESULTADOS OBTIDOS:**

**- FORMULÁRIO DE DIAGNÓSTICO SITUACIONAL LGPD 2025 (3ª FASE) – GESTORES**

Com base nos dados levantados, 671 (seiscentos e setenta e um) Gestores foram convidados a participar da coleta em diferentes serviços da Rede. Desse total, 377 (trezentos e setenta e sete) responderam ao Formulário, o que corresponde a uma taxa de engajamento de aproximadamente 56%.

Os resultados demonstram diferenças entre os serviços, com índices de resposta que variam entre 30% e 100%, indicando distintos níveis de aderência das lideranças às práticas institucionais de Proteção de Dados.

**RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)**

MEMBROS DO COMITÊ LGPD / DPO SMS

Observa-se que os serviços com maior adesão ao instrumento de coleta foram o Hospital Geral de Guaianases, com 100% de participação, e o Hospital Cidade Tiradentes, com 86%. Em contrapartida, os resultados também possibilitam a identificação de serviços que podem demandar um reforço nas ações de conscientização institucional, além das iniciativas de formação e comunicação relacionadas à Proteção de Dados e à Segurança da Informação.

A avaliação desses indicadores contribui para a compreensão do nível de maturidade institucional no que diz respeito à cultura de Proteção de Dados Pessoais e Segurança da Informação. A partir dessas informações, torna-se possível direcionar estratégias de capacitação e campanhas de conscientização voltadas aos Gestores que apresentam menor nível de aderência, fortalecendo as práticas de tratamento seguro e responsável de dados pessoais no âmbito da rede Santa Marcelina Saúde.

<b>Unidade</b>	<b>Total Colaboradores</b>	<b>Responderam</b>	<b>% Responderam</b>
OSS SANTA MARCELINA RASTS 11 ITAQUERA/GUAIANASES/TIRADENTES	153	102	67%
OSS SANTA MARCELINA-RASTS 10 SAO MIGUEL E ITAIM PAULISTA	108	61	56%
HOSPITAL SANTA MARCELINA	200	60	30%
OSS SANTA MARCELINA DE ITAQUAQUECETUBA	67	43	64%
OSS SANTA MARCELINA ITAIM PAULISTA	54	39	72%
OSS HOSPITAL CIDADE TIRADENTES	42	36	86%
HOSPITAL SANTA MARCELINA DE RONDONIA	20	13	65%
HOSPITAL SANTA MARCELINA SAÚDE - SÃO BERNARDO DO CAMPO	13	11	85%
HOSPITAL SANTA MARCELINA DE SAPEZAL	9	7	78%
OSS SANTA MARCELINA HOSPITAL GERAL DE GUAIANASES	5	5	100%
<b>Total Geral</b>	<b>671</b>	<b>377</b>	<b>56%</b>

Fonte: Coleta de Dados 2025-2026

Apresenta-se abaixo o Questionário de Gestores, organizado por questões, incluindo a alternativa correta, objetivo, finalidade, índice de acerto, aplicação na matriz de risco e resultado do impacto:

1) Um colaborador de uma clínica de radiologia recebe por e-mail o resultado de um exame de imagem de um paciente. Para agilizar o atendimento, ele encaminha o e-mail para o grupo de WhatsApp da equipe de plantão, que inclui técnicos e enfermeiros, para que a avaliação seja feita rapidamente. A conduta adotada pelo colaborador está correta?

**Finalidade:**

- Demonstrar que, embora a finalidade seja agilizar o processo, o meio utilizado pode não ser o mais seguro ou necessário, considerando a existência de sistemas internos próprios da Instituição.
- Ensinar sobre o risco de uso de dispositivos ou softwares não autorizados pela área de Tecnologia da Informação da Santa Marcelina Saúde.

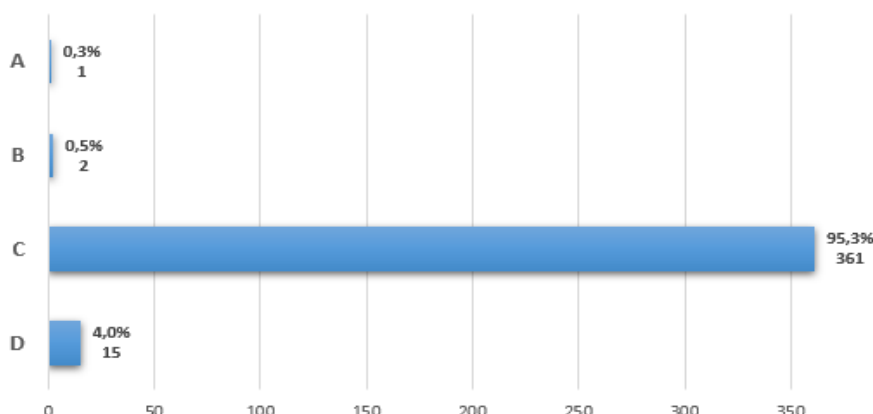
**Objetivo:**

- Diferenciar Dados Pessoais de Dados Pessoais Sensíveis;
- Reforçar o Princípio da Necessidade previsto na LGPD;
- Esclarecer aspectos relacionados à Responsabilidade Civil.

**Alternativas:**

- A) Sim, já que o grupo de WhatsApp é restrito a profissionais da saúde, garantindo a confidencialidade do paciente.
- B) Sim, pois a velocidade no compartilhamento de informações é vital para a saúde do paciente, justificando a ação.
- C) Não, pois mesmo em um grupo de equipe, o compartilhamento de dados sensíveis, como resultados de exames, deve ser realizado em plataformas seguras e com controle de acesso, não em aplicativos de mensagens genéricos.**
- D) Não, a menos que o paciente tenha dado um consentimento expresso para o uso do WhatsApp, o que torna a ação segura

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	95,3%
<b>ÍNDICE DE ERRO (em percentual)</b>	4,7%

2) Sobre o prontuário do paciente, a LGPD determina que:

**Finalidade:**

- Reforçar a cultura institucional de Proteção de Dados na Santa Marcelina Saúde;
- Consolidar o entendimento sobre o acesso restrito às informações;
- Prevenir riscos Jurídicos e Institucionais.

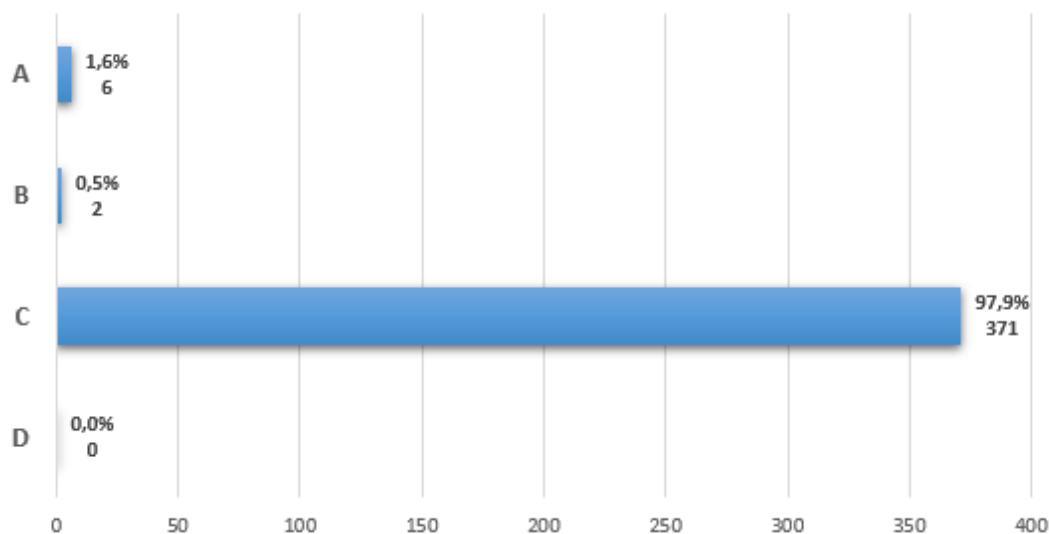
**Objetivo:**

- Desenvolver a conscientização ética no tratamento de dados;
- Reduzir que possam representar riscos ao tratamento de dados pessoais;
- Fortalecer a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

**Alternativas:**

- A) Deve ser acessado apenas pelo paciente.
- B) Pode ser compartilhado em treinamentos internos livremente.
- C) De ser acessado somente por profissionais autorizados e envolvidos no cuidado.**
- D) Pode ser utilizado em pesquisas sem necessidade de anonimização.

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

INDICE DE ACERTO (em percentual)	97,9%
INDICE DE ERRO (em percentual)	2,1%

3) Em relação ao uso de senha compartilhada entre colaboradores de uma mesma equipe para acessar sistemas vinculados aos Serviços de Saúde, assinale a alternativa correta:

**Finalidade:**

- Reforçar a cultura de responsabilidade individual;
- Promover boas práticas de Segurança da Informação;
- Reduzir riscos Operacionais e Jurídicos.

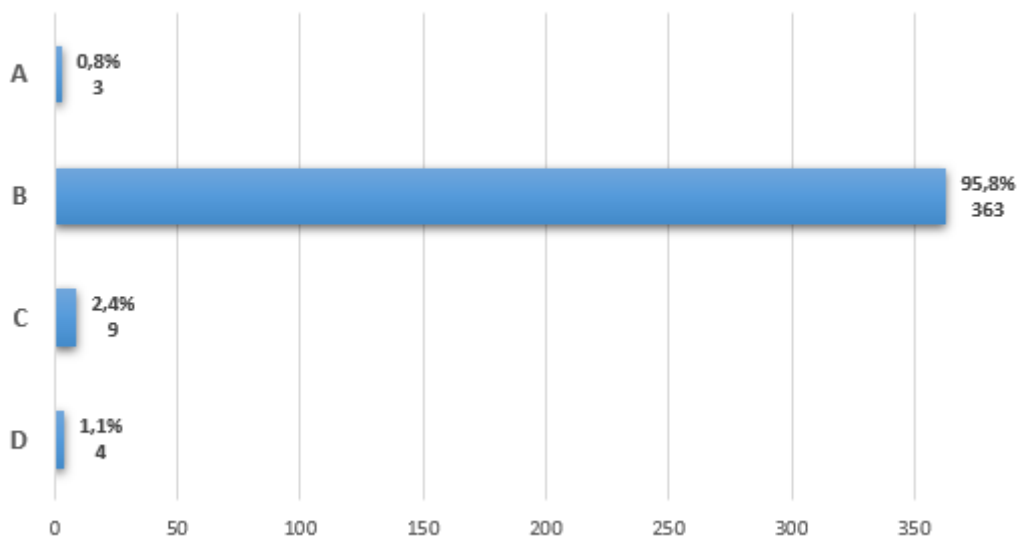
**Objetivo:**

- Consolidar o entendimento sobre o controle de acesso;
- Padronizar condutas internas;
- Estimular comportamentos éticos e responsáveis.

**Alternativas:**

- A) É permitido para agilizar os processos.  
**B) Não é permitido, pois compromete a segurança e a rastreabilidade de acessos.**  
 C) É permitido apenas se for para acessar um prontuário do paciente.  
 D) Não, ao menos que seja compartilhada com toda a equipe.

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

INDICE DE ACERTO (em percentual)	95,8%
INDICE DE ERRO (em percentual)	4,2%

4) Considere uma situação em que, foi criada uma pesquisa de satisfação para avaliar a percepção dos pacientes no atendimento feito pela Instituição. Nesse cenário, à luz da LGPD, é correto afirmar que:

**Finalidade:**

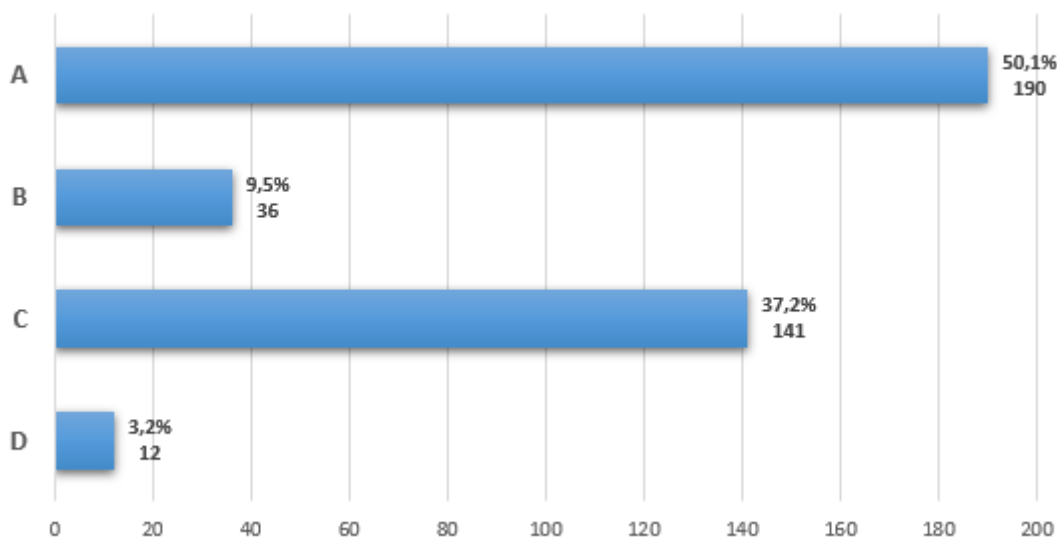
- Consolidar o princípio da minimização de dados;
- Desenvolver o pensamento crítico sobre formulários institucionais;
- Prevenir riscos regulatórios e reputacionais.

**Objetivo:**

- Fortalecer a cultura de privacidade desde a concepção dos processos;
- Estimular o desenho responsável de formulários e pesquisas;
- Integrar a LGPD à rotina administrativa.

**Alternativas:**

- A) A instituição deve coletar somente os dados estritamente necessários para a finalidade da pesquisa, por exemplo: nome, e-mail e telefone para contato.**
- B) A instituição pode solicitar todos os dados pessoais do paciente para ter um banco de dados completo, desde que deixe claro que a finalidade principal é a pesquisa.
- C) A instituição deve criar um formulário anônimo, sem a possibilidade de identificar o paciente, para garantir o anonimato.
- D) A instituição pode coletar o máximo de informações possível, incluindo RG e CPF, pois isso permite cruzar dados e aprofundar os resultados da pesquisa.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	50,1%
<b>ÍNDICE DE ERRO (em percentual)</b>	49,9%

5) Uma profissional da área administrativa, por curiosidade, acessa o prontuário eletrônico de um colega de trabalho que está internado. Acerca da conduta adotada pela profissional, assinale a afirmativa correta.

**Finalidade:**

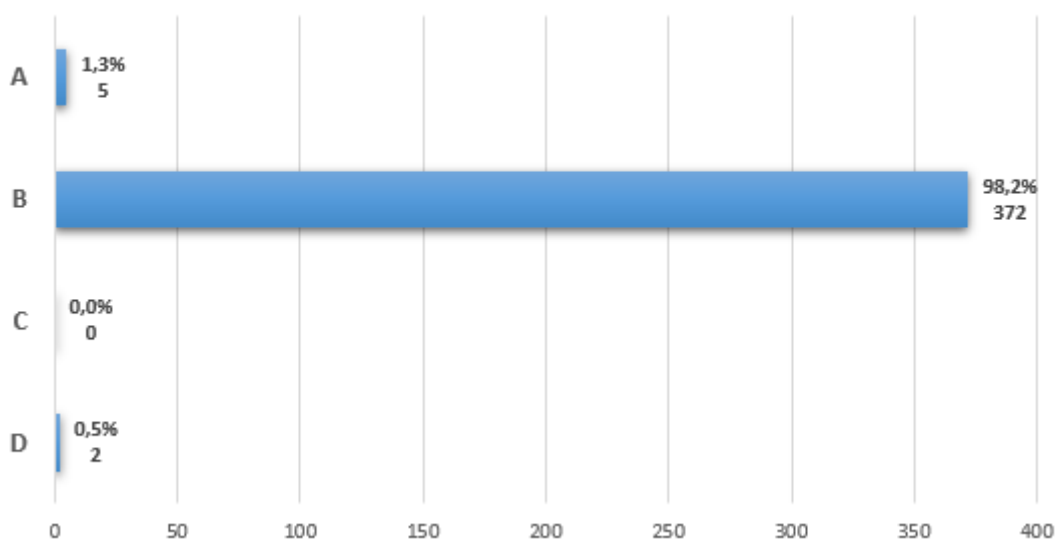
- Reforçar o conceito de “acesso por necessidade”;
- Fortalecer a cultura de confidencialidade;
- Sensibilizar os colaboradores quanto à responsabilidade individual.

**Objetivo:**

- Reforçar o dever de sigilo profissional;
- Reduzir riscos jurídicos e reputacionais;
- Promover o alinhamento entre a ética profissional e a LGPD.

**Alternativas:**

- A) É permitido, desde que o profissional não divulgue os dados obtidos.
- B) Não é permitido e configura uma grave violação de confidencialidade e privacidade do paciente.**
- C) É permitido, mas apenas para profissionais que trabalham há mais de 5 anos na Instituição.
- D) Não é permitido, exceto para situações que envolvam colaboradores da mesma Instituição.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>INDICE DE ACERTO (em percentual)</b>	98,2%
<b>INDICE DE ERRO (em percentual)</b>	1,8%

6) Sobre o armazenamento do prontuário físico do paciente, assinale a alternativa correta:

**Finalidade:**

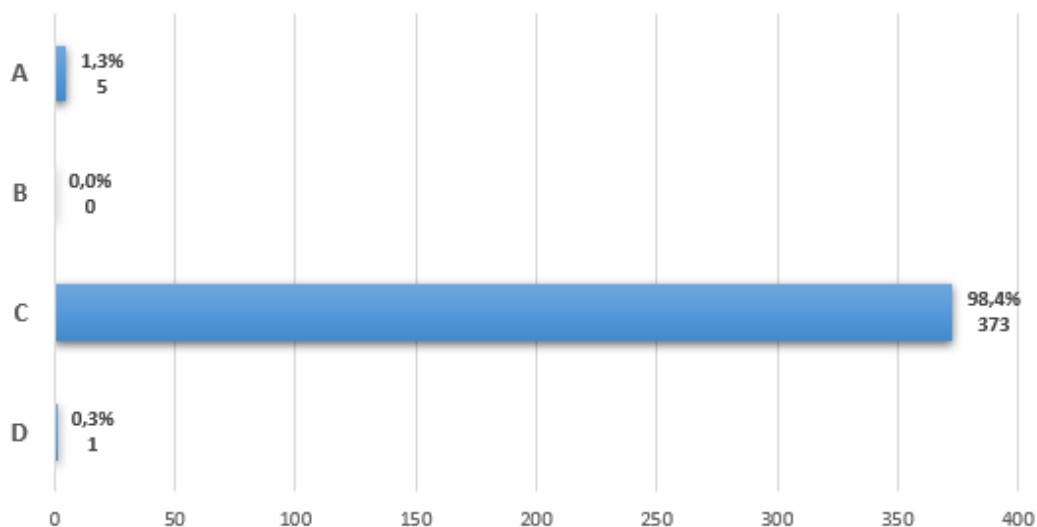
- Sensibilizar os colaboradores quanto à responsabilidade no manuseio documental;
- Prevenir Incidentes de Segurança.

**Objetivo:**

- Consolidar boas práticas de guarda documental;
- Reduzir vulnerabilidades físicas;
- Preparar os colaboradores para auditorias e inspeções.

**Alternativas:**

- A) O documento deve ser armazenado em um local de fácil acesso aos pacientes e colaboradores.
- B) O colaborador deve imprimir e arquivar em local acessível a todos.
- C) O colaborador deve armazenar em local seguro e com controle de acesso.**
- D) O colaborador pode manter no celular pessoal para consultas rápidas.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	98,4%
<b>ÍNDICE DE ERRO (em percentual)</b>	1,6%

7) Uma profissional de saúde decide publicar fotos do ambiente Hospitalar ou do Serviço de Saúde nas suas redes sociais, incluindo imagens de pacientes em tratamento, sendo que tais registros não apresentam seus rostos. A conduta praticada pela profissional está correta?

**Finalidade:**

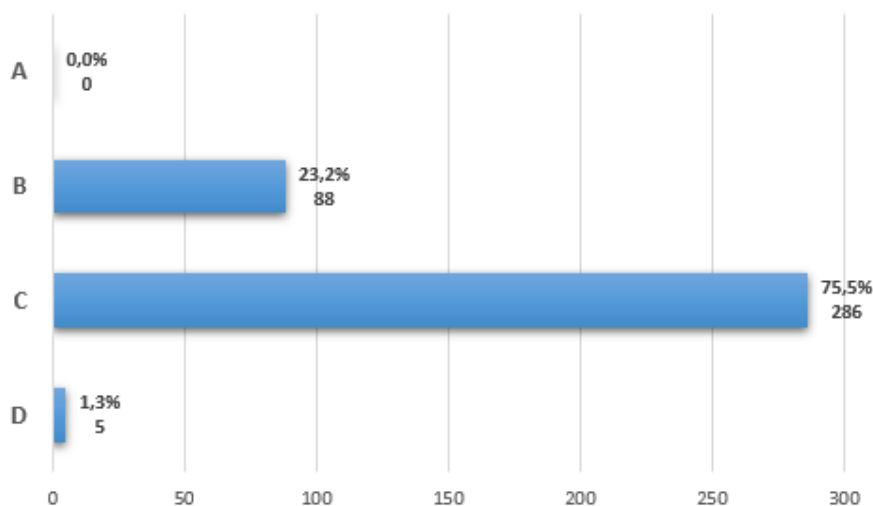
- Sensibilizar os colaboradores quanto aos riscos de exposição em redes sociais;
- Reforçar o conceito de dado pessoal identificável;
- Proteger a imagem institucional da Santa Marcelina Saúde.

**Objetivo:**

- Desenvolver a consciência digital responsável;
- Prevenir a exposição indevida em redes sociais;
- Fortalecer a cultura de ética e privacidade.

**Alternativas:**

- A) Sim, porque o foco da foto é o trabalho, e não há nomes ou rostos de pacientes.
- B) Não, a menos que a instituição e todos os pacientes nas fotos tenham assinado uma autorização para a publicação.
- C) Não, pois a imagem de uma pessoa, mesmo sem identificação, pode ser considerada um dado pessoal sensível, e a divulgação de um paciente em tratamento pode violar sua privacidade.**
- D) Sim, pois se trata de um ambiente público e não há identificação do paciente, tornando a imagem segura para divulgação.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>INDICE DE ACERTO (em percentual)</b>	75,5%
<b>INDICE DE ERRO (em percentual)</b>	24,5%

8) Durante o plantão em uma unidade Hospitalar ou do Serviço de Saúde, o técnico de enfermagem é solicitado por um paciente para que encaminhasse os resultados do seu exame, via WhatsApp. Considerando a Política da Boa Prática referente ao Uso do WhatsApp no Ambiente de Trabalho, é correto afirmar que:

**Finalidade:**

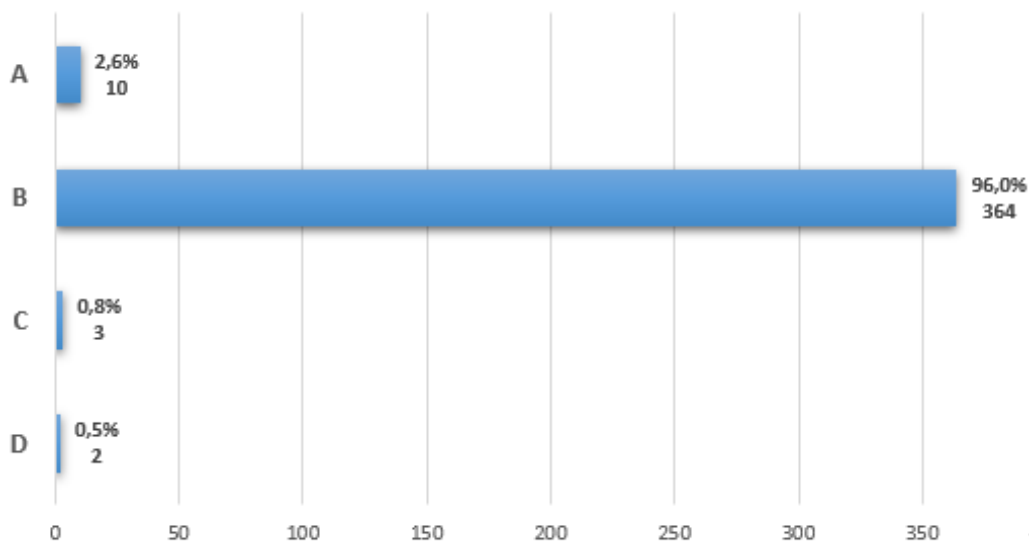
- Reforçar os limites do uso de aplicativos pessoais;
- Consolidar a cultura de Segurança da Informação;
- Prevenir Incidentes de Vazamento.

**Objetivo:**

- Fortalecer a observância das políticas internas;
- Reduzir vulnerabilidades operacionais;
- Padronizar as condutas de comunicação com pacientes.

**Alternativas:**

- A) A solicitação feita pelo paciente está em conformidade com as regras de avaliação dispostas na Política.
- B) É vedado o compartilhamento de informações sensíveis ou estratégicas via WhatsApp.**
- C) É permitido o compartilhamento do resultado, tendo em vista que a maioria dos pacientes usa essa ferramenta e a velocidade é crucial em casos de saúde.
- D) É permitido apenas se o resultado do exame for enviado em um grupo familiar do paciente.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	96,0%
<b>ÍNDICE DE ERRO (em percentual)</b>	4,0%

9) Ao criar relatórios com dados estatísticos de pacientes, para realização de análise críticas a partir de pesquisa interna, pode-se interpretar:

**Finalidade:**

- Reforçar o conceito de minimização e proteção das informações;
- Sensibilizar os colaboradores quanto ao risco de Reidentificação;
- Fortalecer a governança em pesquisas internas.

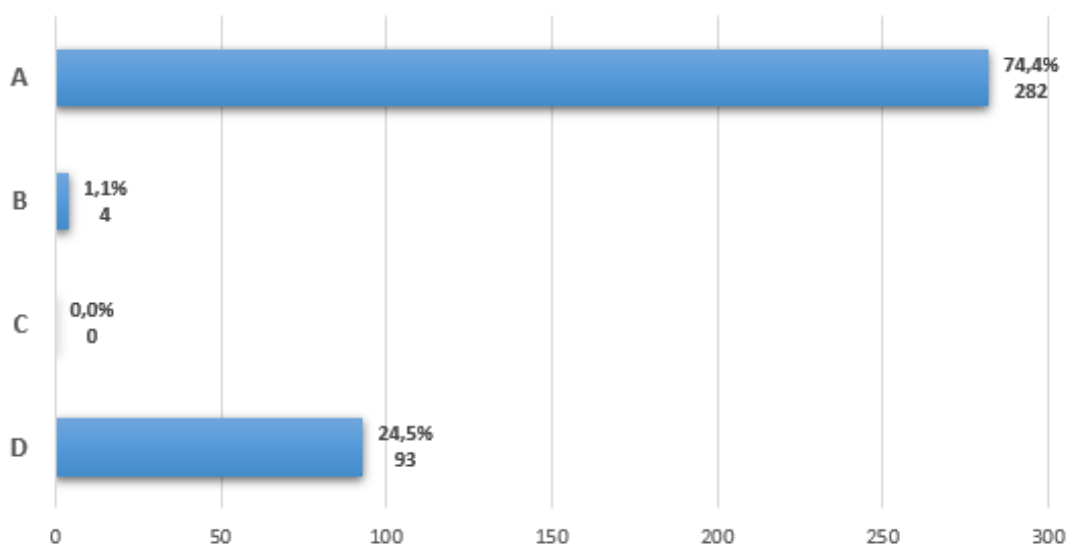
**Objetivo:**

- Desenvolver a cultura de proteção de dados desde a origem das análises;
- Evitar o uso excessivo de dados identificáveis;
- Reduzir o risco de vazamento em relatórios internos.

**Alternativas:**

- A) A obrigatoriedade de anonimização ou pseudoanonimização dos dados.  
 B) A utilização de dados pessoais, tais como: nome e CPF, sem restrição.  
 C) A divulgação de tais informações para fins de marketing.  
 D) Nenhuma das alternativas elencadas acima.

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

INDICE DE ACERTO (em percentual)	74,4%
INDICE DE ERRO (em percentual)	25,6%

10) Um colaborador encontra documentos impressos com exames de pacientes esquecidos na sala de reuniões. Sobre a conduta descrita acima, assinale a alternativa correta:

**Finalidade:**

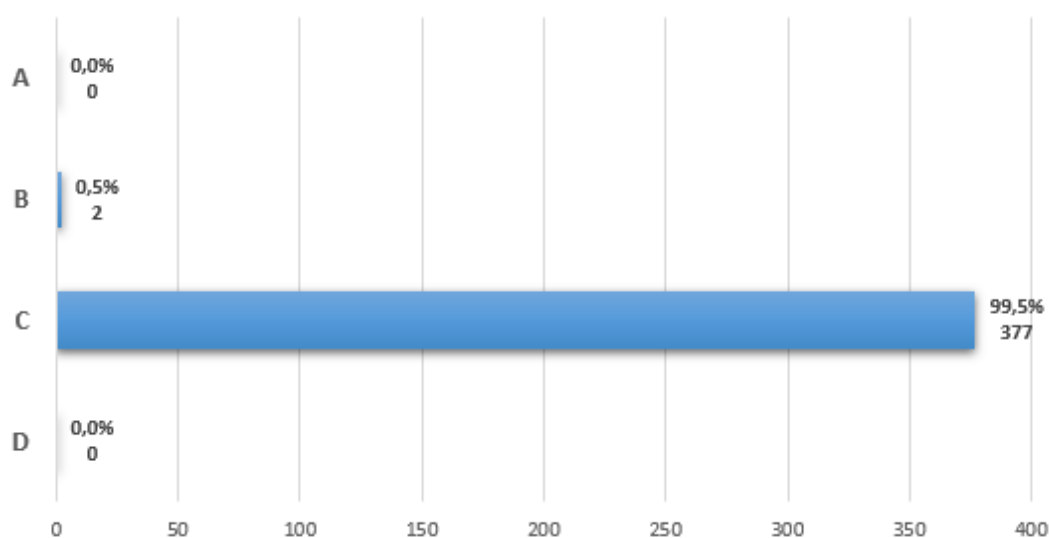
- Reforçar a responsabilidade coletiva;
- Sensibilizar os colaboradores quanto ao risco físico da informação;
- Estimular uma postura proativa.

**Objetivo:**

- Reduzir o risco de vazamento acidental;
- Integrar a LGPD à rotina administrativa;
- Fortalecer a governança documental.

**Alternativas:**

- A) Deve guardar os documentos consigo para posterior consulta.  
 B) Jogar no lixo comum ou reciclável.  
**C) Entregar à área responsável pela guarda de documentos para registro.**  
 D) Deixar na mesa, pois alguém vai recolher.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	99,5%
<b>ÍNDICE DE ERRO (em percentual)</b>	0,5%

11) Com relação ao envio de dados de pacientes, assinale a alternativa correta:

**Finalidade:**

- Reforçar o uso de canais oficiais;
- Consolidar a cultura de Segurança da Informação;
- Mitigar riscos jurídicos e reputacionais.

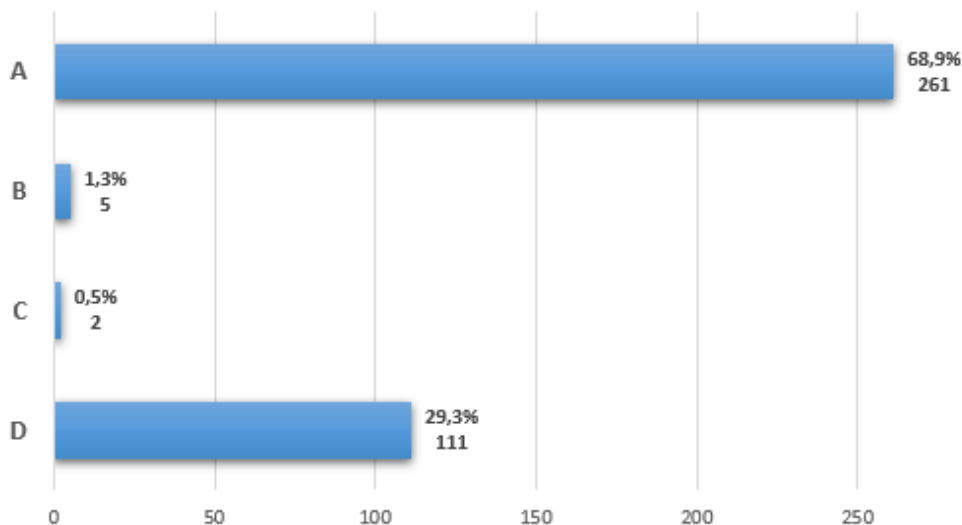
**Objetivo:**

- Fortalecer a governança digital;
- Reduzir vulnerabilidades operacionais;
- Estimular a responsabilidade individual no compartilhamento de dados.

**Alternativas:**

- A) **Devem ser formalizados por e-mail institucional com destinatário conhecido, fazendo menção do teor do assunto que está sendo enviado.**
- B) Não devem ser formalizados e os arquivos disponíveis nos anexos podem ser enviados em todos os formatos (PDF, Word, JPG, entre outros).
- C) Podem ser encaminhados via WhatsApp ou e-mail pessoal.
- D) Nenhuma das alternativas anteriores.

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	68,9%
<b>ÍNDICE DE ERRO (em percentual)</b>	31,1%

12) Quanto ao uso de sistemas relativos aos Serviços de Saúde em computadores pessoais dos colaboradores, assinale a opção correta:

**Finalidade:**

- Reforçar o controle do ambiente tecnológico;
- Sensibilizar os colaboradores quanto ao risco ampliado fora da rede corporativa;
- Promover a responsabilidade digital.

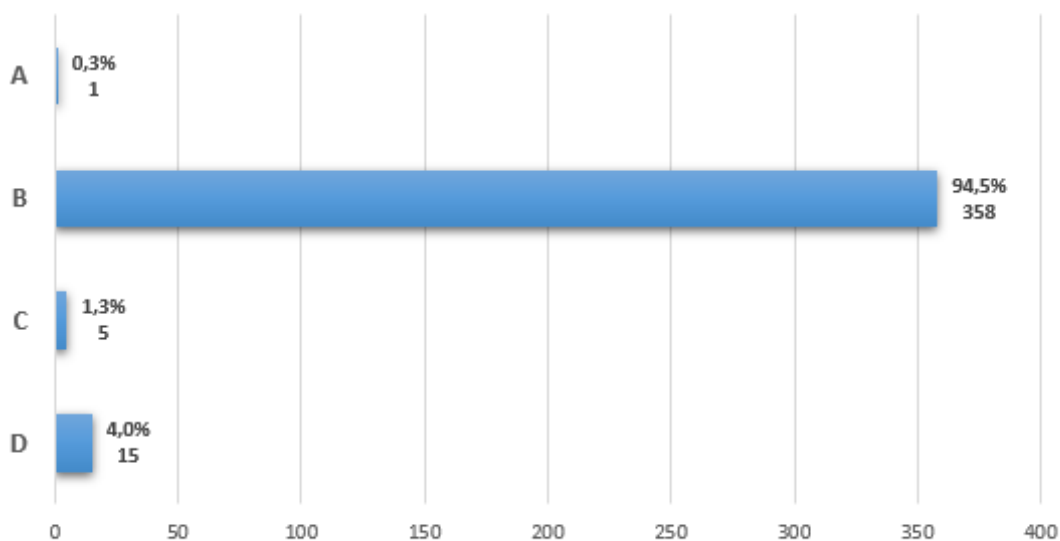
**Objetivo:**

- Padronizar as regras de acesso remoto;
- Reduzir vulnerabilidades tecnológicas;
- Fortalecer a cultura de segurança da informação.

**Alternativas:**

- A) É recomendado pela Instituição utilizar os sistemas sem autorização, visando a facilitação do acesso.
- B) Só pode ocorrer com a autorização prévia, adotando medidas de segurança.**
- C) Não é necessário solicitar a prévia autorização para utilização dos sistemas dos Serviços de Saúde.
- D) Todas as alternativas estão corretas.

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

<b>INDICE DE ACERTO (em percentual)</b>	94,5%
<b>INDICE DE ERRO (em percentual)</b>	5,5%

13) Observando as boas práticas em relação ao compartilhamento de senhas, assinale a alternativa correta:

**Finalidade:**

- Reforçar a responsabilidade individual;
- Consolidar a cultura de Segurança Digital;
- Prevenir falhas de rastreabilidade.

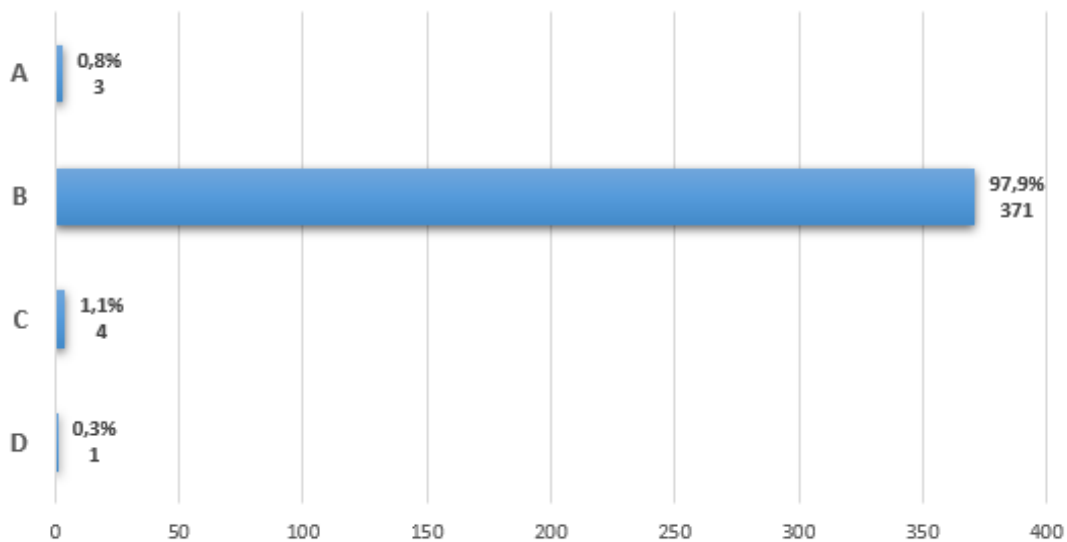
**Objetivo:**

- Reduzir vulnerabilidades humanas;
- Integrar a LGPD à rotina operacional;
- Promover o comportamento ético e responsável.

**Alternativas:**

- A) A senha de acesso ao sistema deve ser compartilhada entre colegas de plantão.  
**B) A senha de acesso ao sistema deve ser individual, forte e intransferível.**  
 C) A senha de acesso ao sistema deve ser simples para lembrar facilmente.  
 D) A senha de acesso ao sistema deve ser escrita em uma agenda de fácil acesso para todos.

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	97,9%
<b>ÍNDICE DE ERRO (em percentual)</b>	2,1%

14) No segmento da saúde, os profissionais têm acesso a informações sensíveis. Por isso, o compartilhamento de dados pessoais deve sempre observar a finalidade legítima e os princípios previstos na LGPD. Nesse contexto, imagine que um colaborador do Hospital ou do Serviço de Saúde compartilhou uma planilha com dados pessoais de pacientes para um terceiro e você teve ciência disso. Diante desse cenário, qual das alternativas a seguir apresenta a melhor medida para mitigar o risco:

**Finalidade:**

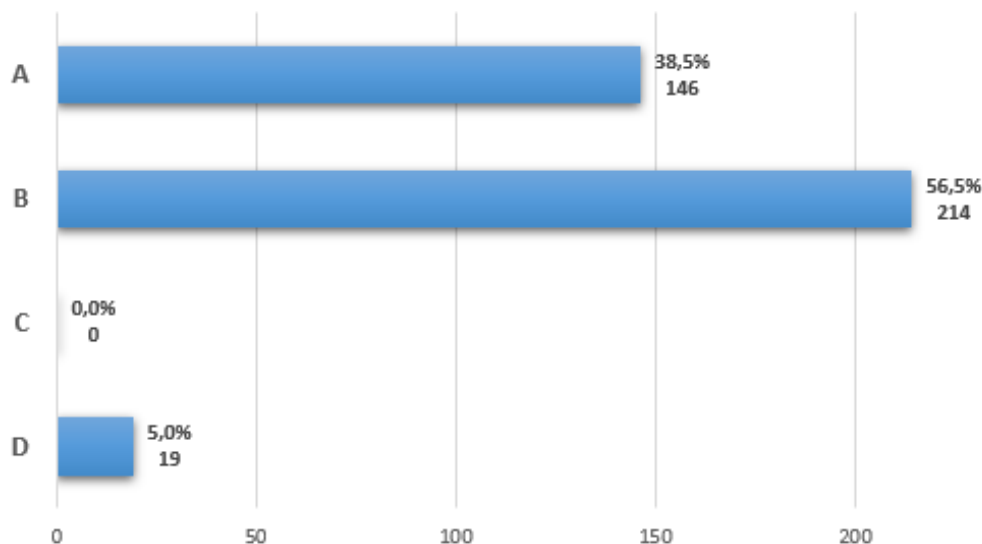
- Reforçar a importância do canal oficial de reporte;
- Consolidar a cultura de transparência e responsabilidade;
- Reduzir impactos jurídicos e reputacionais.

**Objetivo:**

- Reduzir o risco de agravamento do dano;
- Fortalecer a governança e a accountability;
- Integrar a LGPD à prática cotidiana dos colaboradores.

**Alternativas:**

- A) Comunicar ao Encarregado de Dados Pessoais da Santa Marcelina Saúde.**  
 B) Comunicar ao Líder Responsável pela área consultando sobre a autorização e a ocorrência existente.  
 C) Não comunicar a nenhuma das partes (Instituição e Gestão) sobre o ocorrido.  
 D) Nenhuma das alternativas anteriores se aplica corretamente ao caso.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	56,5%
<b>ÍNDICE DE ERRO (em percentual)</b>	43,5%

15) L.M foi visitar seu pai no Serviço de Saúde da Santa Marcelina e ao ingressar na enfermaria começou a tirar fotos e fazer vídeos para encaminhar para sua tia. Nas imagens e vídeos captados constavam registros de outros pacientes e familiares presentes no local. Diante do caso prático, assinale a alternativa correta:

**Finalidade:**

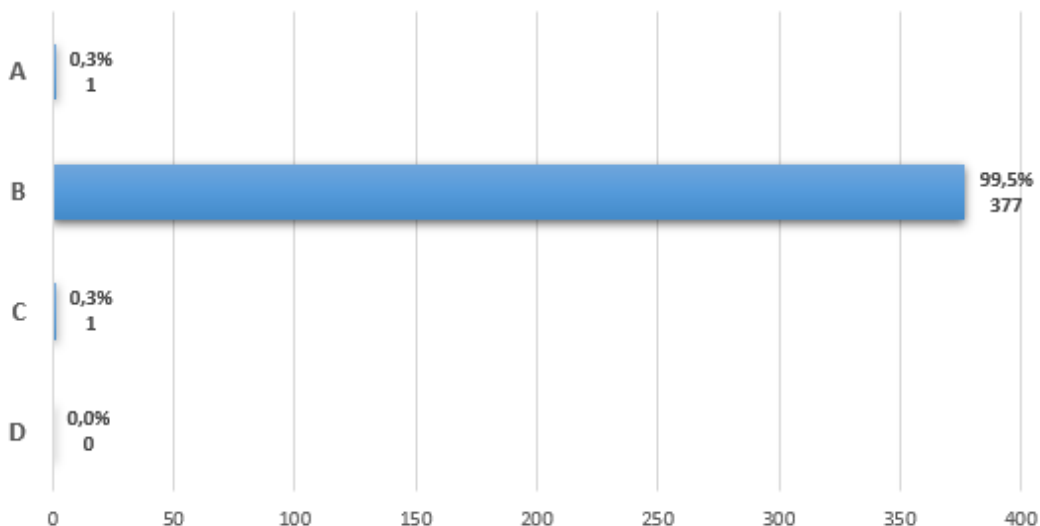
- Sensibilizar os colaboradores quanto ao risco indireto;
- Reforçar a proteção do ambiente hospitalar;
- Prevenir danos reputacionais.

**Objetivo:**

- Integrar a LGPD à rotina assistencial;
- Reduzir o risco reputacional;
- Desenvolver uma postura preventiva por parte dos colaboradores.

**Alternativas:**

- A) É permitido tirar fotos ou filmar dentro do Serviço de Saúde sem autorização.
- B) Não é permitido tirar fotos ou filmar dentro do Serviço de Saúde sem autorização, sendo que tais condutas violam os direitos de privacidade dos pacientes e familiares.**
- C) É permitido tirar fotos ou filmar dentro do Serviço de Saúde, sendo que tais condutas não violam os direitos de privacidade dos pacientes e familiares.
- D) É permitido tirar apenas fotos, sendo vedada a gravação de vídeos dentro da Instituição.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	99,5%
<b>ÍNDICE DE ERRO (em percentual)</b>	0,5%

16) Quanto ao uso de dados pessoais de pacientes em aulas ou treinamentos internos, assinale a alternativa correta:

**Finalidade:**

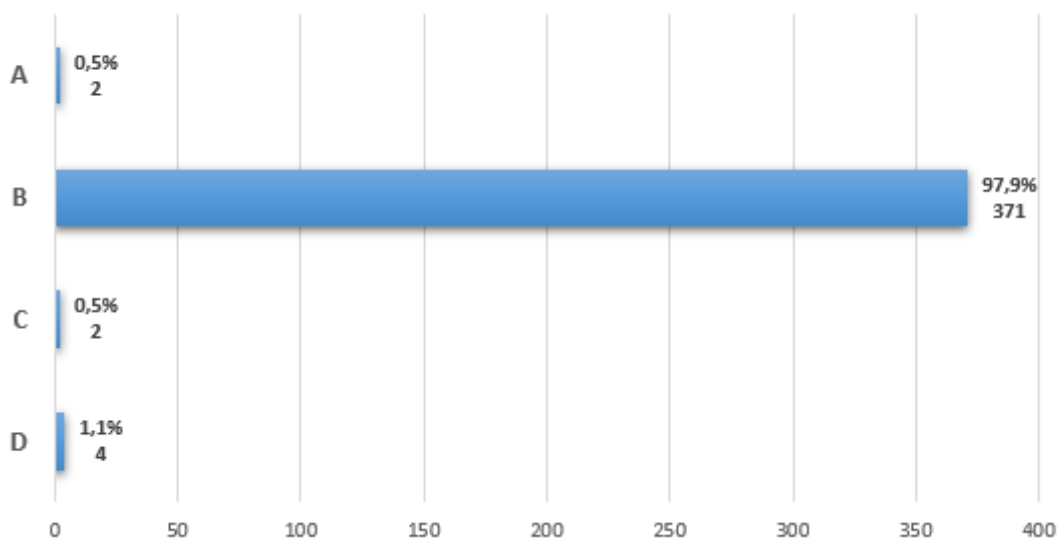
- Reforçar o Princípio da Minimização;
- Consolidar boas práticas educacionais;
- Prevenir a exposição indevida.

**Objetivo:**

- Reduzir o risco de exposição indevida;
- Padronizar o uso de casos clínicos em treinamentos;
- Promover a ética profissional alinhada à legislação.

**Alternativas:**

- A) É permitido a utilização de dados pessoais em apresentações, sem restrição do teor.  
**B) É permitido se houver anonimização de dados pessoais.**  
 C) É permitido se o professor for médico.  
 D) É permitido com autorização verbal.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	97,9%
<b>ÍNDICE DE ERRO (em percentual)</b>	2,1%

17) Sobre o uso de redes sociais corporativas para divulgação de eventos com fotos de colaboradores, assinale a alternativa correta:

**Finalidade:**

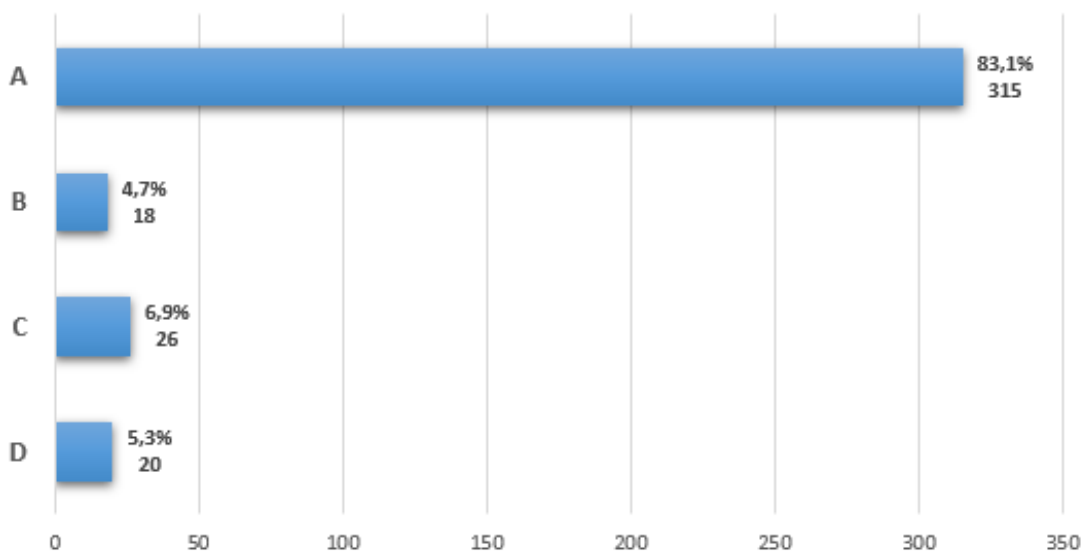
- Reforçar a cultura de respeito à imagem;
- Consolidar boas práticas de comunicação institucional;
- Sensibilizar os colaboradores quanto ao uso responsável de redes sociais.

**Objetivo:**

- Reduzir riscos reputacionais e trabalhistas;
- Promover a cultura de consentimento informado;
- Fortalecer a governança institucional.

**Alternativas:**

- A) Deve ser feito apenas com consentimento dos colaboradores.**  
 B) Não requer nenhuma autorização das partes.  
 C) É proibido em qualquer situação.  
 D) É permitido se não mencionar nomes.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	83,1%
<b>ÍNDICE DE ERRO (em percentual)</b>	16,9%

18) Durante análise de resultados laboratoriais, o profissional deve:

**Finalidade:**

- Reforçar o princípio da necessidade;
- Consolidar a cultura de confidencialidade assistencial;
- Prevenir vazamentos informais.

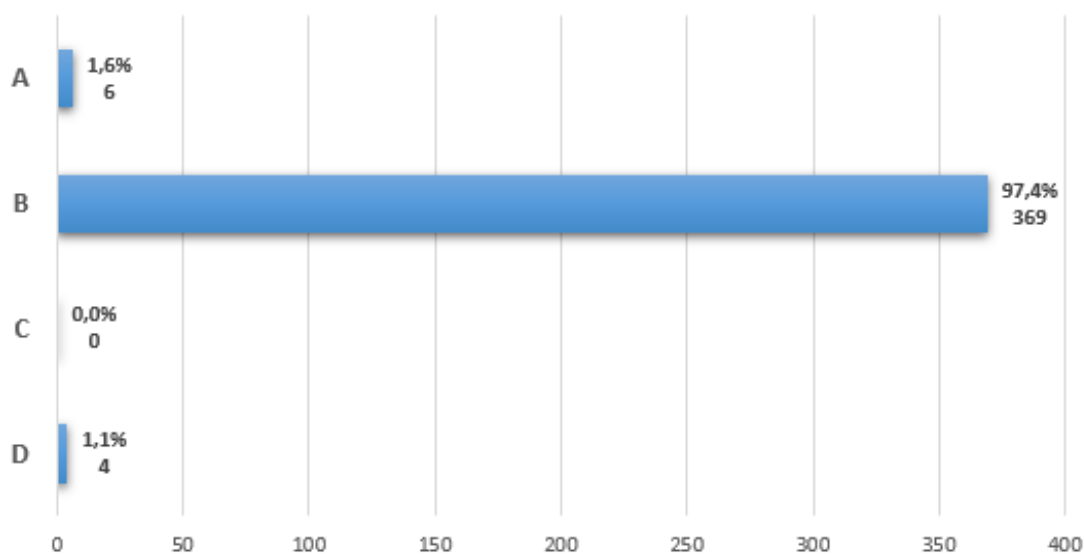
**Objetivo:**

- Fortalecer a ética profissional;
- Padronizar condutas assistenciais;
- Mitigar risco jurídicos e reputacionais.

**Alternativas:**

- A) Compartilhar as informações com toda a equipe de plantão.  
 B) **Discutir apenas com os profissionais diretamente envolvidos no caso.**  
 C) Divulgar no grupo de WhatsApp.  
 D) Enviar cópia à Gestão Estratégica de Pessoas (GEP).

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

INDICE DE ACERTO (em percentual)	97,4%
INDICE DE ERRO (em percentual)	2,6%

19) Um médico está em uma visita domiciliar e, para registrar informações do paciente, usa seu tablet pessoal, que não possui as mesmas medidas de segurança do sistema da instituição. No presente caso, assinale a afirmativa correta sobre a conduta do médico.

**Finalidade:**

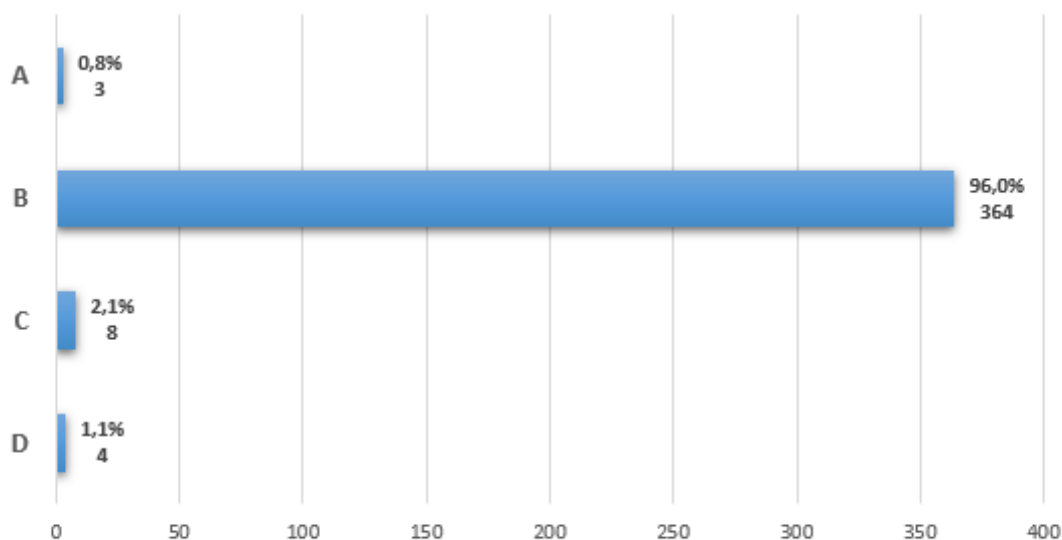
- Reforçar os limites do uso de dispositivos pessoais (BYOD);
- Sensibilizar os colaboradores quanto aos riscos fora do ambiente hospitalar;
- Fortalecer a responsabilidade profissional.

**Objetivo:**

- Reduzir riscos cibernéticos;
- Fortalecer a governança digital;
- Proteger dados sensíveis em qualquer ambiente.

**Alternativas:**

- A) É aceitável, pois o uso de dispositivos pessoais é uma forma de agilizar o trabalho e o registro de informações.
- B) **Não é aceitável, pois o registro de dados de pacientes deve ser feito apenas em dispositivos institucionais e plataformas seguras, que garantem a proteção e a rastreabilidade das informações.**
- C) É aceitável, desde que o médico tenha total confiança no sistema de segurança de seu tablet.
- D) Não é aceitável, pois os dados devem ser registrados apenas em prontuários físicos e não eletrônicos.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	96,0%
<b>ÍNDICE DE ERRO (em percentual)</b>	4,0%

20) Uma equipe de pesquisa decide usar uma planilha para compilar dados de pacientes, como resultados de exames e históricos de tratamento, a fim de agilizar a análise de um estudo. O acesso à planilha é compartilhado com todos os membros da equipe e não possui senha. A prática adotada pela equipe de pesquisa está em conformidade com a LGPD?

**Finalidade:**

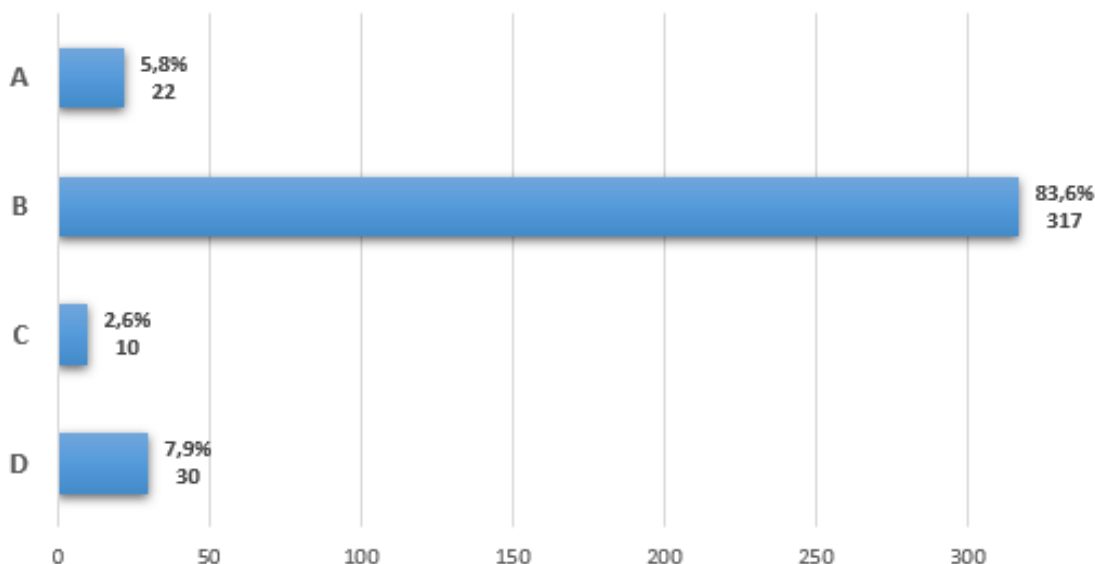
- Reforçar a segurança em projetos de pesquisa;
- Sensibilizar os pesquisadores quanto ao risco do uso de ferramentas informais;
- Consolidar a cultura de proteção de dados desde a concepção dos projetos.

**Objetivo:**

- Reduzir o risco de vazamento de dados sensíveis;
- Fortalecer a governança acadêmica;
- Desenvolver a responsabilidade coletiva na equipe de pesquisa.

**Alternativas:**

- A) Sim, pois os dados estão armazenados em plataformas seguras e acessíveis apenas à equipe de pesquisa.
- B) **Não, pois a ausência de senha e controle de acesso à planilha compromete a segurança de dados pessoais sensíveis, violando os princípios da LGPD.**
- C) Sim, desde que os membros da equipe tenham assinado um termo de confidencialidade.
- D) Não, pois a LGPD proíbe qualquer uso de dados pessoais em pesquisas científicas.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

INDICE DE ACERTO (em percentual)	83,6%
INDICE DE ERRO (em percentual)	16,4%

21) Um pesquisador de uma universidade, para um estudo científico, solicita ao Hospital ou ao Serviço de Saúde o acesso a um banco de dados com informações de pacientes. Para que esse uso esteja de acordo com a LGPD, a Instituição de Saúde deve:

**Finalidade:**

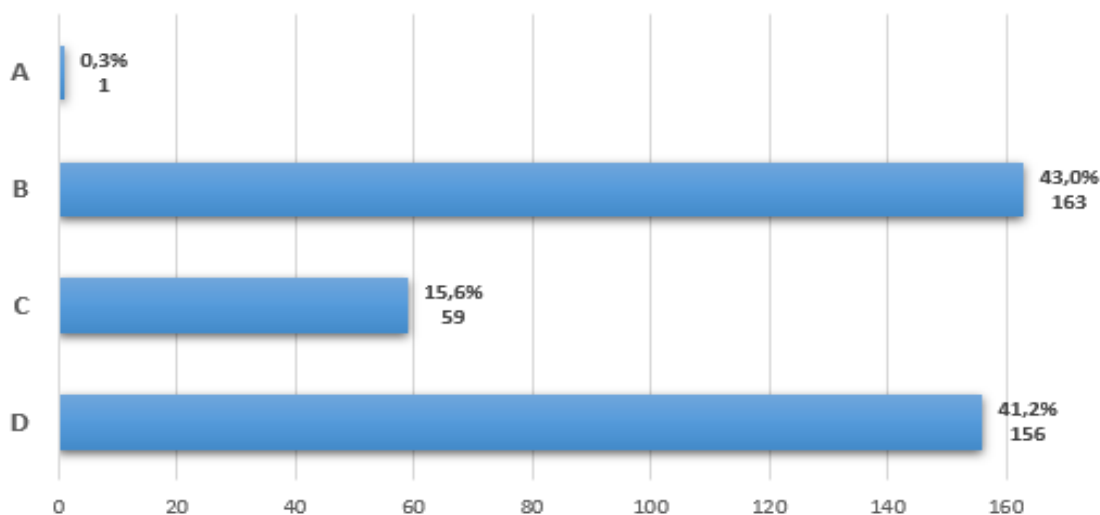
- Reforçar a governança em pesquisa;
- Sensibilizar os colaboradores sobre a minimização e a anonimização de dados;
- Reduzir riscos Jurídicos e Reputacionais.

**Objetivo:**

- Fortalecer a cultura de Proteção por Desenho (privacy by design);
- Reduzir vulnerabilidades no intercâmbio acadêmico;
- Consolidar a accountability institucional.

**Alternativas:**

- A) Fornecer o banco de dados completo ao pesquisador, pois a finalidade acadêmica é considerada uma justificativa legítima para o uso dos dados.
- B) Compartilhar os dados após a aprovação do Comitê de Ética em Pesquisa (CEP) da instituição, já que essa aprovação garante a conformidade com a lei.
- C) **Compartilhar os dados, mas somente se o pesquisador assinar um Termo de Comprometimento de Utilização de Dados (TCUD), comprometendo-se a não divulgar as informações.**
- D) Fornecer o banco de dados apenas após a completa anonimização ou pseudonimização das informações, garantindo que os dados não possam ser vinculados a nenhum paciente específico.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

INDICE DE ACERTO (em percentual)	15,6%
INDICE DE ERRO (em percentual)	84,4%

**- FORMULÁRIO DE DIAGNÓSTICO SITUACIONAL LGPD 2025 (3ª FASE) – NÃO GESTORES**

Observa-se que, do total de 20.167 colaboradores elegíveis, 10.387 participaram da aplicação dos questionários, representando uma taxa de adesão de 57%. Verifica-se variação significativa entre os serviços, com índices de participação que oscilam entre 22% e 84%, evidenciando diferentes níveis de engajamento institucional.

Destacam-se positivamente os serviços com maior adesão, como o Hospital Santa Marcelina de Sapezal (84%) e o Hospital Santa Marcelina Saúde – São Bernardo do Campo (73%). Em contrapartida, os resultados também possibilitam a identificação de serviços que podem demandar um reforço nas ações de conscientização institucional, além das iniciativas de formação e comunicação relacionadas à Proteção de Dados e à Segurança da Informação.

Esses dados subsidiam a análise de risco, indicando a necessidade de considerar o grau de cobertura da amostra na avaliação da maturidade institucional em proteção de dados pessoais.

Unidade	Total Colaboradores	Responderam	% Responderam
OSS SANTA MARCELINA RASTS 11 ITAQUERA/GUAIANASES/TIRADENTES	5.902	3.406	58%
OSS SANTA MARCELINA-RASTS 10 SAO MIGUEL E ITAIM PAULISTA	4.857	2.651	55%
HOSPITAL SANTA MARCELINA	3.917	1.060	22%
OSS HOSPITAL CIDADE TIRADENTES	1.238	1.018	66%
OSS SANTA MARCELINA DE ITAQUAQUECETUBA	1.573	870	55%
OSS SANTA MARCELINA ITAIM PAULISTA	1.396	551	39%
HOSPITAL SANTA MARCELINA DE RONDONIA	436	305	70%
HOSPITAL SANTA MARCELINA SAÚDE - SÃO BERNARDO DO CAMPO	351	255	73%
OSS SANTA MARCELINA HOSPITAL GERAL DE GUAIANASES	410	198	48%
HOSPITAL SANTA MARCELINA DE SAPEZAL	87	73	84%
<b>Total</b>	<b>20.167</b>	<b>10.387</b>	<b>57%</b>

Fonte: Coleta de Dados 2025-2026

Descreve-se, a seguir, o Questionário de Não Gestor estruturado por questões, contemplando a alternativa correta, o objetivo, a finalidade, o índice de acerto, a aplicação na matriz de risco e a avaliação do impacto.

1) O que significa a sigla LGPD?

**Finalidade:**

- Consolidar o conhecimento básico e uniforme;
- Estabelecer uma base comum de entendimento;
- Reforçar a identidade normativa, incluindo políticas internas, procedimentos operacionais e materiais que a fundamentam.

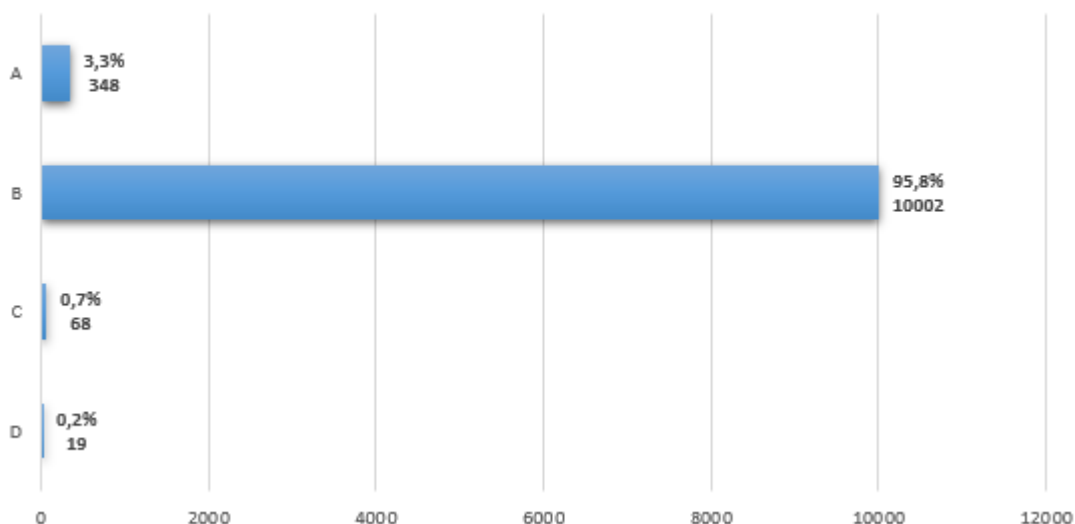
**Objetivo:**

- Nivelar o conhecimento básico sobre proteção de dados;
- Introduzir formalmente o marco regulatório aplicável;
- Promover a conscientização normativa entre os colaboradores.

**Alternativas:**

- A) Lei Geral de Proteção aos Direitos do Titular  
 B) **Lei Geral de Proteção de Dados Pessoais**  
 C) Lei Geral de Proteção ao Deficiente  
 D) Lei Geral de Proteção ao Devedor

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	95,8%
<b>ÍNDICE DE ERRO (em percentual)</b>	4,2%

2) Qual é o principal objetivo da LGPD?

**Finalidade:**

- Garantir a conformidade legal dos processos de tratamento de dados pessoais;
- Promover a cultura de Proteção de Dados;
- Proteger os direitos dos Titulares de Dados Pessoais.

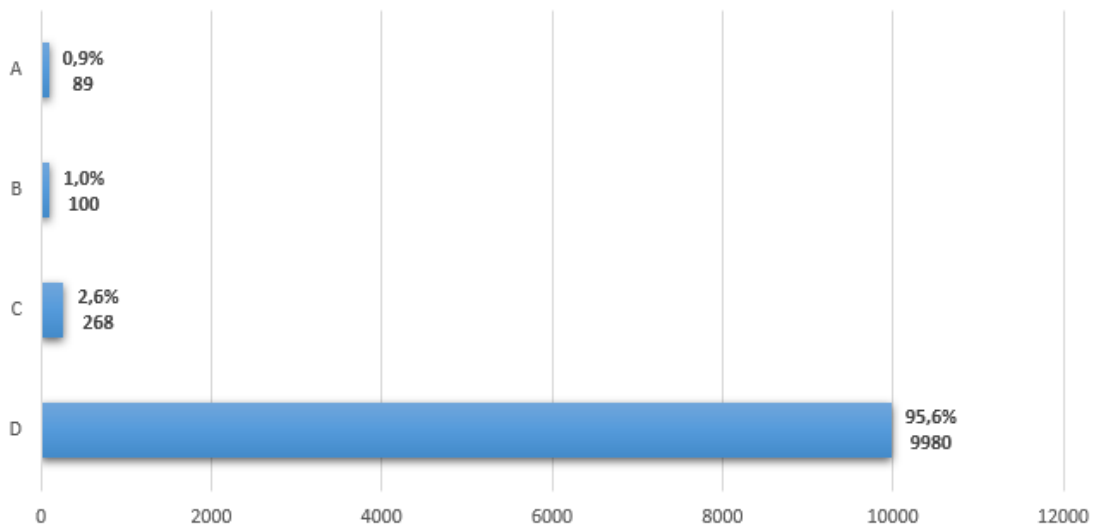
**Objetivo:**

- Assegurar que o tratamento de dados pessoais seja realizado de forma responsável, ética e segura, com respeito aos direitos fundamentais, promovendo a conformidade legal, a confiança institucional e a proteção efetiva dos titulares.

**Alternativas:**

- A) Proteger os direitos fundamentais de salvaguarda das crianças e dos adolescentes.
- B) Proteger os direitos fundamentais dos idosos e dos deficientes.
- C) Proteger os direitos fundamentais dos necessitados.
- D) **Proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.**

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

<b>INDICE DE ACERTO (em percentual)</b>	95,6%
<b>INDICE DE ERRO (em percentual)</b>	4,4%

## 3) Em que ano a LGPD entrou em vigor no Brasil?

**Finalidade:**

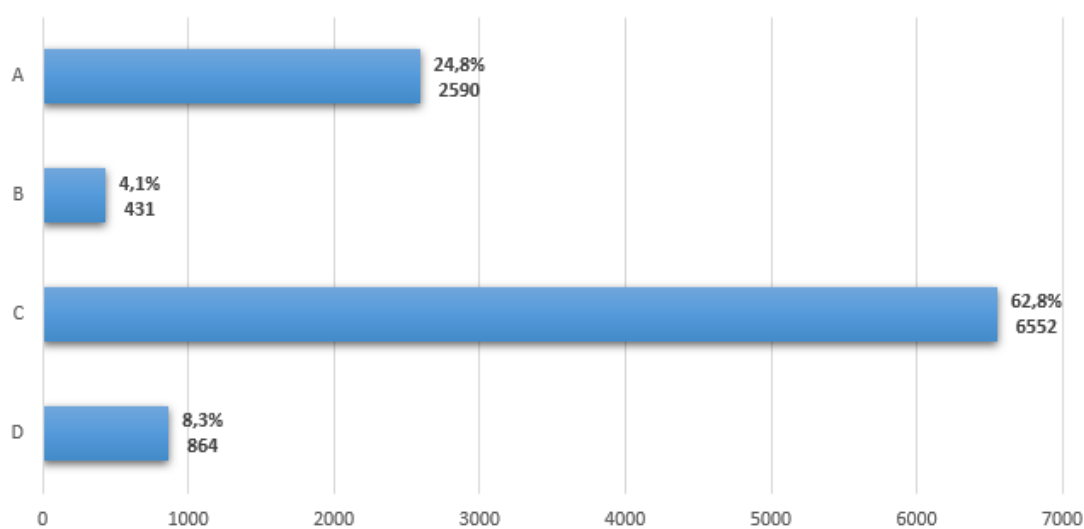
- Verificar o conhecimento dos colaboradores quanto ao marco temporal de vigência da LGPD no Brasil;
- Reforçar a relevância da legislação como base normativa já aplicável às práticas institucionais;
- Promover a conscientização sobre a obrigatoriedade do cumprimento da lei no contexto atual.

**Objetivo:**

- Garantir a adequação às exigências legais, por meio da implementação de políticas internas, termos de consentimento, controles de acesso e procedimentos de tratamento de dados;
- Fomentar a capacitação contínua dos colaboradores, garantindo a compreensão sobre dados pessoais e sensíveis, bases legais de tratamento e responsabilidades individuais e institucionais;
- Prevenir incidentes e mitigar riscos jurídicos, reduzindo a ocorrência de vazamentos, uso indevido de informações e aplicação de sanções.

**Alternativas:**

- A) 2018
- B) 2019
- C) **2020**
- D) 2021

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	62,8%
<b>ÍNDICE DE ERRO (em percentual)</b>	37,2%

## 4) A LGPD se aplica apenas a empresas privadas?

**Finalidade:**

- Assegurar a proteção dos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, independentemente da natureza jurídica da instituição.

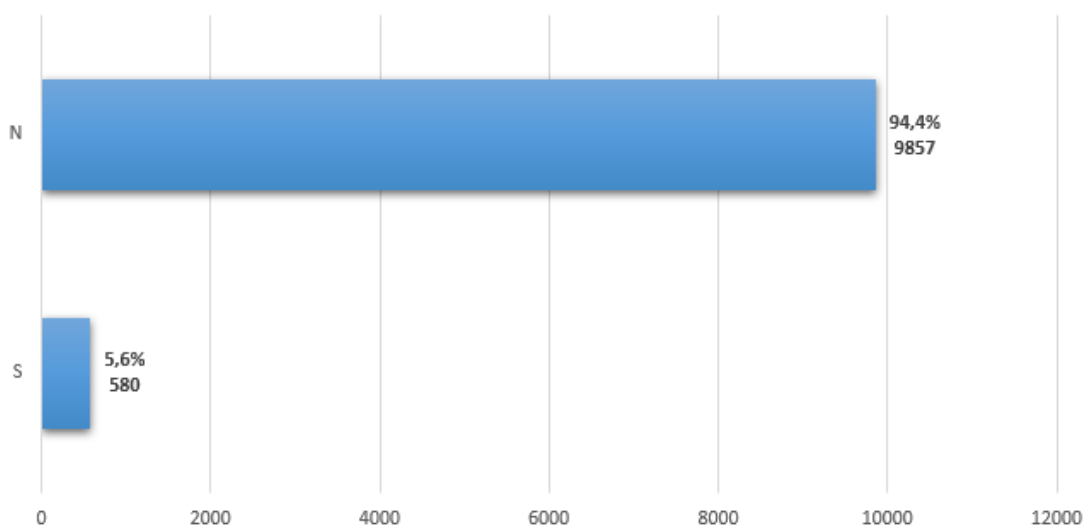
**Objetivo:**

- Conformidade Legal, a fim de adequar os processos internos às exigências da LGPD, evitando sanções e responsabilizações.
- Capacitar os colaboradores, visando promover treinamentos para que todos compreendam suas responsabilidades no tratamento de dados pessoais.
- Garantir clareza no uso dos dados e fortalecer a confiança institucional.

**Alternativas:**

Opção: Sim

Opção: Não

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>INDICE DE ACERTO (em percentual)</b>	94,4%
<b>INDICE DE ERRO (em percentual)</b>	5,6%

## 5) Quais dados são considerados pessoais pela LGPD?

**Finalidade:**

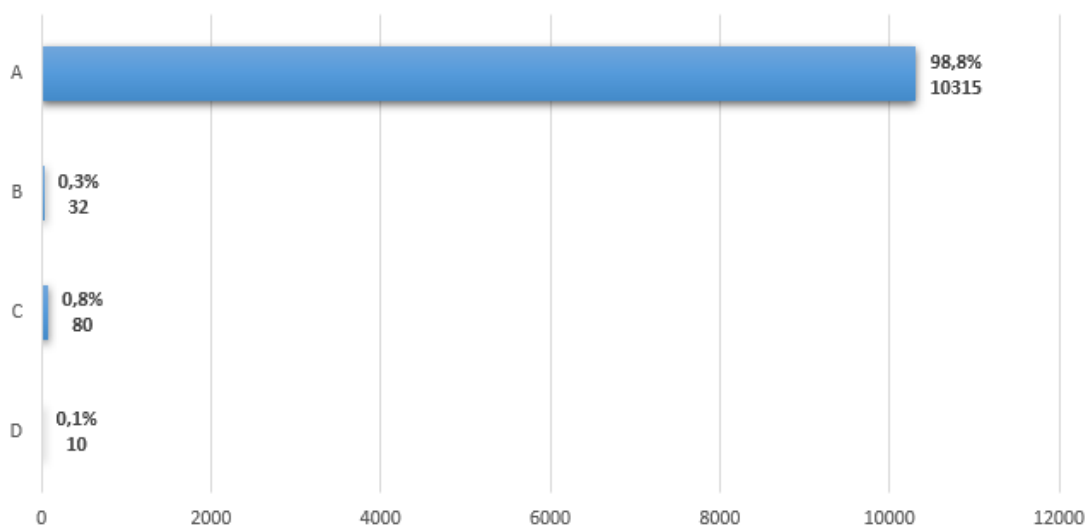
- Zelar para que informações capazes de identificar pessoas físicas sejam tratadas com segurança, responsabilidade e em conformidade com a base legal aplicável.

**Objetivo:**

- Capacitar os colaboradores para reconhecer quais informações estão protegidas pela LGPD.
- Definir bases legais, controlar o acesso e limitar o uso dessas informações.
- Prevenir o uso indevido e o vazamento de dados, incluindo o estabelecimento de medidas técnicas e administrativas de segurança.

**Alternativas:**

- A) **RG, CPF, endereço e e-mail**  
 A) CNPJ  
 B) Razão Social da empresa  
 C) Telefone Comercial

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>INDICE DE ACERTO (em percentual)</b>	98,8%
<b>INDICE DE ERRO (em percentual)</b>	1,2%

## 6) Quais dados são considerados sensíveis pela LGPD?

**Finalidade:**

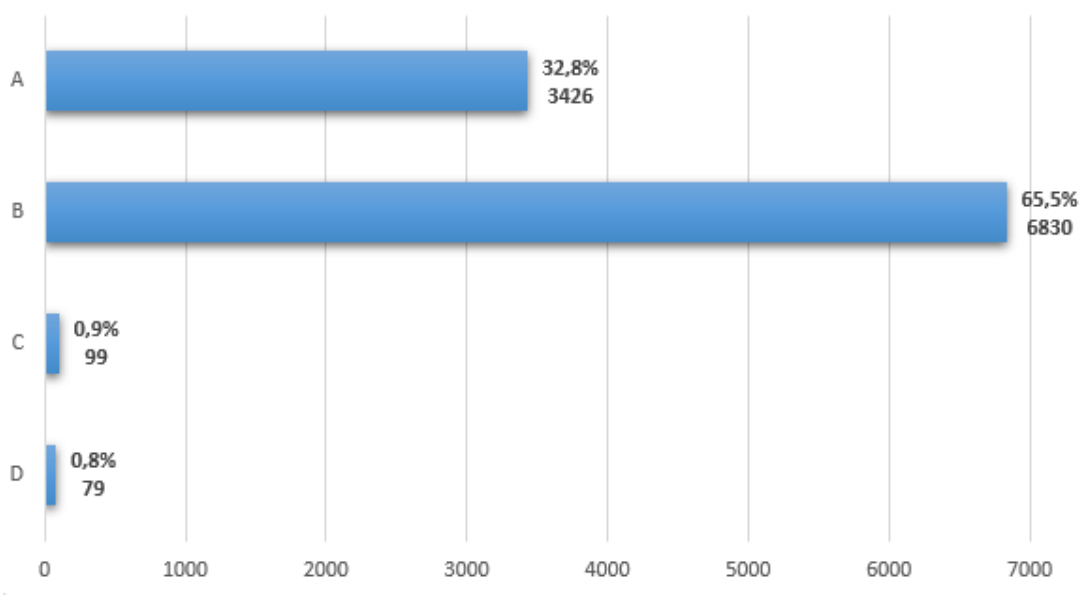
- Proteger os dados que possam expor o titular a discriminação, preconceito ou riscos significativos, garantindo sua proteção reforçada.

**Objetivo:**

- Reforço nas medidas de segurança, incluindo a aplicação de controles mais restritos de acesso e armazenamento.
- Capacitação contínua, a fim de treinar os colaboradores para reconhecer dados sensíveis e saber como tratá-los adequadamente.
- Evitar o uso inadequado que possa gerar prejuízos morais, sociais ou legais.

**Alternativas:**

- A) CPF e RG
- B) **Origem racial, convicções religiosas ou políticas**
- C) Endereço Eletrônico (E-mail)
- D) Endereço Residencial

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>INDICE DE ACERTO (em percentual)</b>	65,5%
<b>INDICE DE ERRO (em percentual)</b>	34,5%

## 7) Qual órgão é responsável pela fiscalização da LGPD?

**Finalidade:**

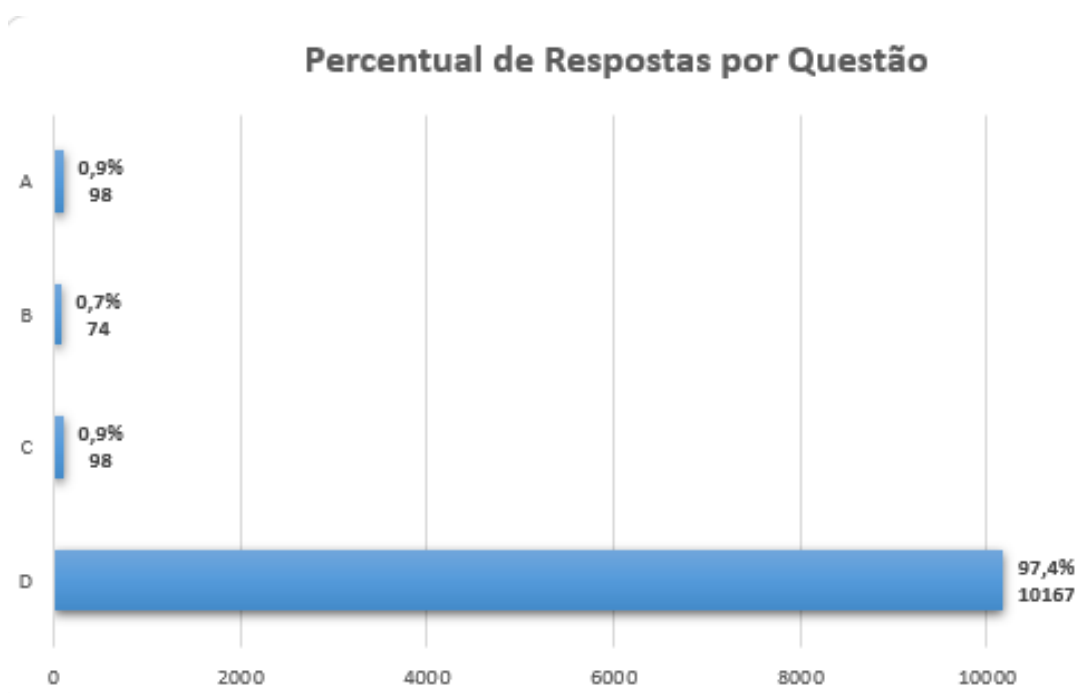
- Avaliar se os colaboradores compreendem a estrutura de governança e fiscalização da Lei Geral de Proteção de Dados (LGPD).
- Reforçar a importância de conhecer os órgãos reguladores.

**Objetivo:**

- Capacitação contínua dos colaboradores, a fim de preparar as equipes para compreender as obrigações legais e as Boas Práticas de Proteção de Dados.
- Fortalecimento da governança e do compliance, por meio da criação de mecanismos internos de controle, auditoria e monitoramento de dados.
- Promoção da cultura de proteção de dados, estabelecendo a responsabilidade institucional e a transparência nas atividades que envolvam dados pessoais.

**Alternativas:**

- A) Agência Nacional de Telecomunicações (ANATEL)
- B) Polícia Federal
- C) Tribunal de Justiça
- D) Agência Nacional de Proteção de Dados (ANPD)



Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	97,4 %
<b>ÍNDICE DE ERRO (em percentual)</b>	2,6%

8) Quais direitos a LGPD prevê para o Titular de Dados?

**Finalidade:**

- Verificar o nível de compreensão dos colaboradores acerca dos direitos dos titulares de dados pessoais, incluindo acesso, correção, eliminação, portabilidade e revogação de consentimento.

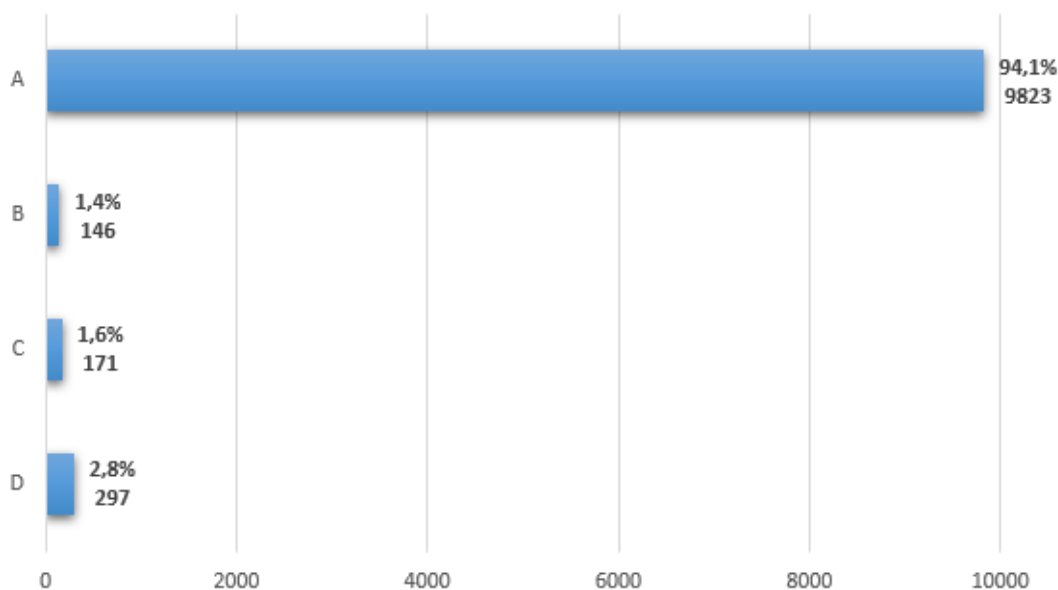
**Objetivo:**

- Garantir que os colaboradores saibam identificar e respeitar esses direitos no dia a dia, promovendo práticas de proteção de dados coerentes com a legislação.
- Reforçar a importância de tratar os Titulares de Dados com transparência e segurança.

**Alternativas:**

- A) **Confirmação da existência de tratamento e acesso aos dados.**
- B) Direito de acesso ao e-mail sem restrições.
- C) Direito a receber benefícios, exemplo: descontos em planos de saúde, em serviços online.
- D) Direito de contestar compras feitas na internet.

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

<b>INDICE DE ACERTO (em percentual)</b>	94,1%
<b>INDICE DE ERRO (em percentual)</b>	5,9%

9) A LGPD prevê sobre a transferência internacional de dados?

**Finalidade:**

- Avaliar se os colaboradores compreendem as regras e condições estabelecidas pela lei para o compartilhamento de dados pessoais com outros países.

**Objetivo:**

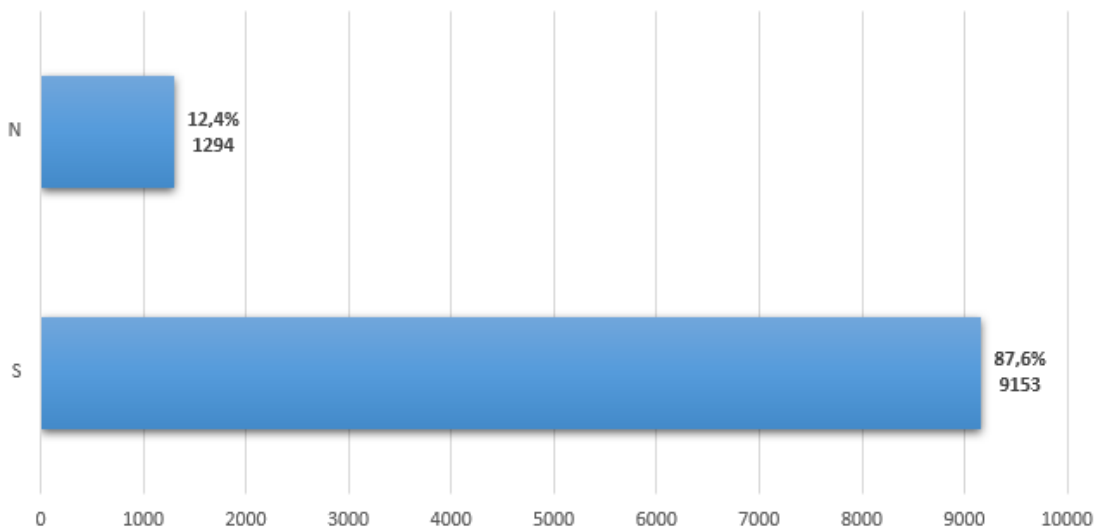
- Identificar situações que exigem atenção especial, como a necessidade de consentimento, a verificação do nível de proteção do país destinatário ou a adoção de garantias específicas, a fim de contribuir com a conformidade legal, a segurança dos dados e a proteção dos direitos dos titulares.

**Alternativas:**

Opção: Sim

Opção: Não

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	87,6%
<b>ÍNDICE DE ERRO (em percentual)</b>	12,4%

10) A LGPD protege os dados de crianças e adolescentes?

**Finalidade:**

- Certificar-se de que os colaboradores compreendem que a lei estabelece regras específicas e mais rigorosas para o tratamento de dados pessoais de crianças e adolescentes, garantindo proteção adicional e a necessidade de consentimento específico dos pais ou responsáveis.

**Objetivo:**

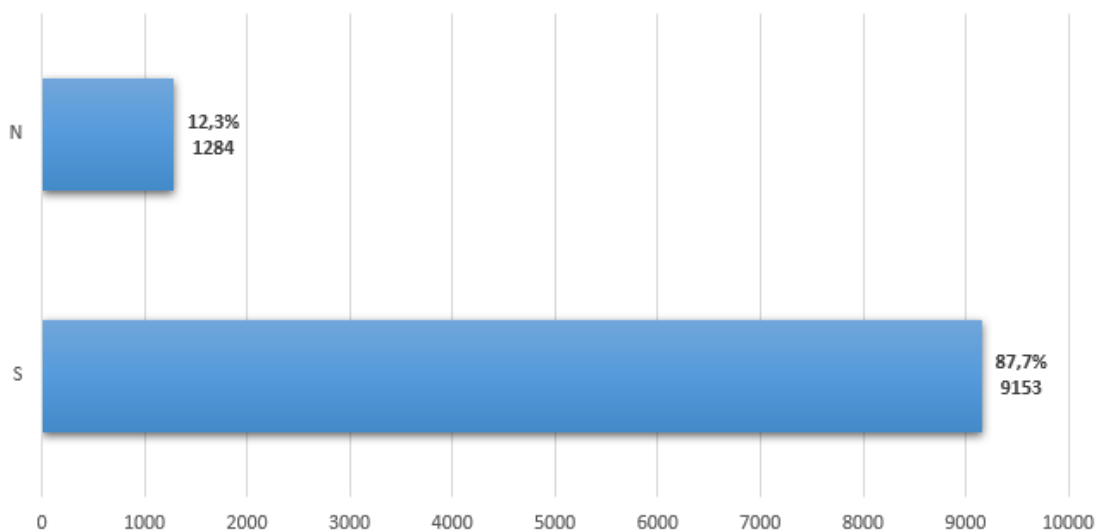
- Reforçar a importância de identificar e tratar dados de pessoas menores de idade com atenção especial, respeitando os direitos dos titulares e promovendo a conformidade legal e a segurança das informações.

**Alternativas:**

Opção: Sim

Opção: Não

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

<b>INDICE DE ACERTO (em percentual)</b>	87,7%
<b>INDICE DE ERRO (em percentual)</b>	12,3%

11) É permitido compartilhar dados de pacientes com outros profissionais sem consentimento?

**Finalidade:**

- Avaliar se os colaboradores compreendem regras da LGPD e as Boas Práticas de Proteção de Dados Sensíveis, especialmente no que se refere a informações de saúde, que possuem proteção reforçada.

**Objetivo:**

- Assegurar que os profissionais saibam quando o compartilhamento é permitido, prevenindo o uso indevido de informações e garantindo a proteção da privacidade dos titulares.

**Alternativas:**

Opção: Sim

Opção: Não



Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	95,2%
<b>ÍNDICE DE ERRO (em percentual)</b>	4,8%

12) Um dos princípios da LGPD é a necessidade?

**Finalidade:**

- Verificar se os colaboradores compreendem que a LGPD estabelece o princípio da necessidade, que determina que o tratamento de dados pessoais deve se limitar ao mínimo necessário para atingir a finalidade prevista.

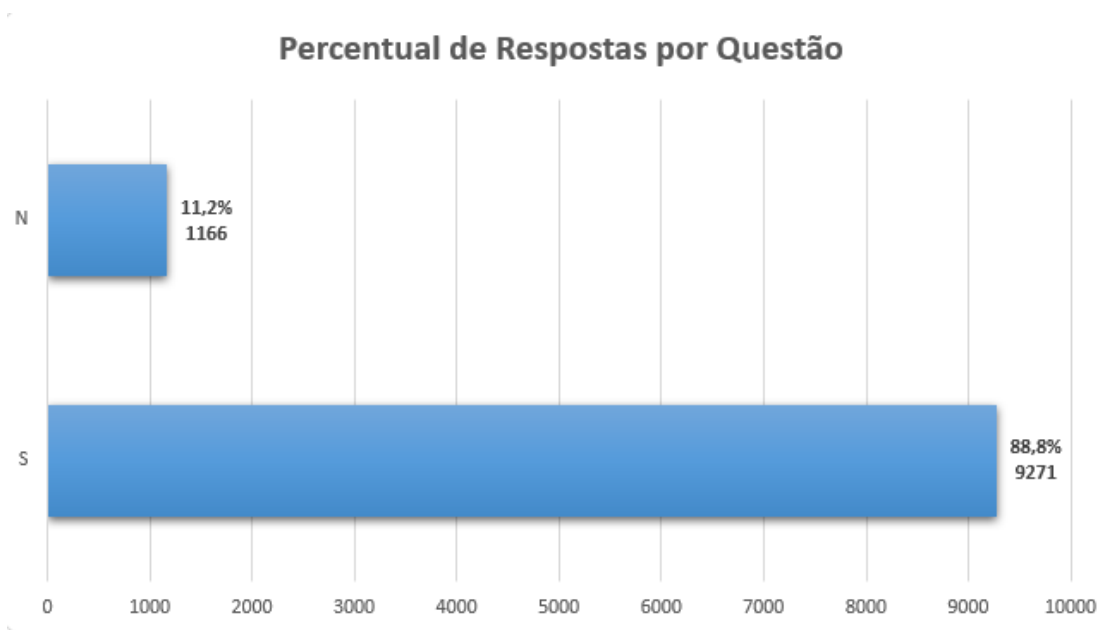
**Objetivo:**

- Garantir que os colaboradores apliquem o princípio da necessidade na prática, evitando coleta, armazenamento ou uso excessivo de dados e contribuindo para a **conformidade legal e a proteção dos direitos dos titulares.**

**Alternativas:**

Opção: **Sim**

Opção: **Não**



Fonte: Coleta de Dados 2025-2026

<b>INDICE DE ACERTO (em percentual)</b>	88,8%
<b>INDICE DE ERRO (em percentual)</b>	11,2%

## 13) Segundo a LGPD, quem é o Encarregado de Dados/DPO?

**Finalidade:**

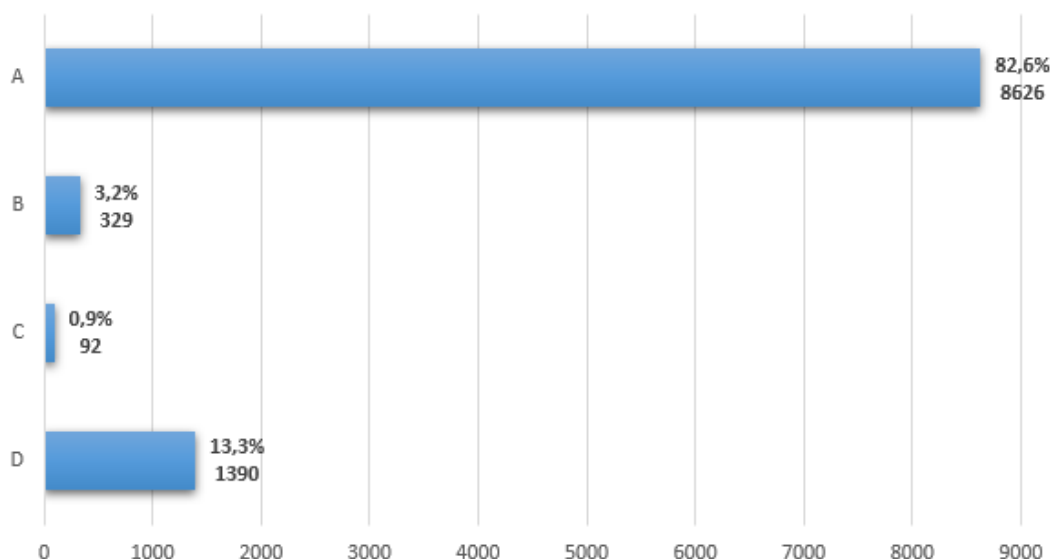
- Identificar se os colaboradores compreendem o papel e as responsabilidades do Encarregado de Dados/DPO, conforme definido pela LGPD, especialmente no que se refere à função de canal de comunicação entre a instituição, os titulares de dados e a ANPD.

**Objetivo:**

- Promover que os colaboradores consigam identificar corretamente a figura do DPO, reconhecendo sua importância na proteção de dados pessoais, na orientação interna sobre boas práticas e na cooperação com a Agência Nacional de Proteção de Dados, prevenindo falhas de conformidade e fortalecendo a governança de dados na instituição.

**Alternativas:**

- Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre a Instituição, os titulares de Dados e a Agência Nacional de Proteção de Dados (ANPD).**
- Pessoa responsável pela análise de todos os dados.
- Pessoa responsável pela supervisão e eliminação dos dados.
- Pessoa responsável por manter os registros dos dados nos sistemas da Instituição.

**Percentual de Respostas por Questão**

Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	82,6%
<b>ÍNDICE DE ERRO (em percentual)</b>	17,4%

14) Como deve ser realizado o tratamento de dados pessoais sensíveis?

**Finalidade:**

- Identificar se os colaboradores compreendem as regras específicas da LGPD para o tratamento de dados sensíveis, reconhecendo a necessidade de consentimento expresso do titular ou de seu responsável legal, salvo exceções previstas em lei.

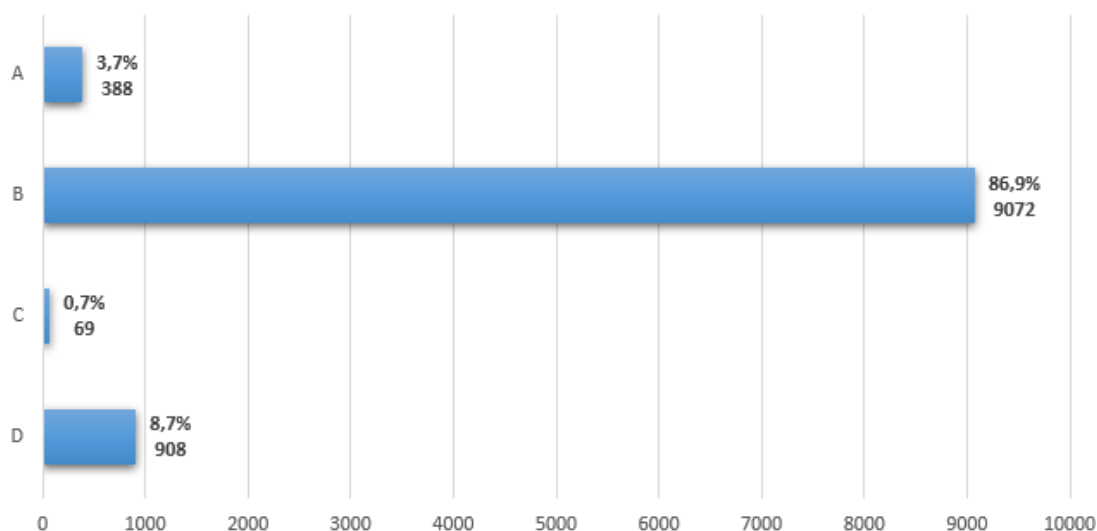
**Objetivo:**

- Assegurar que os colaboradores saibam aplicar corretamente os procedimentos legais ao tratar dados pessoais sensíveis, prevenindo uso indevido, vazamentos ou violação de direitos dos titulares, reforçando a conformidade legal e a proteção de dados dentro da SMS.

**Alternativas:**

- A) Pode ser realizado sem o consentimento expresso do titular de dados.  
 B) **Pode ser realizado mediante consentimento do titular dos dados ou seu responsável legal.**  
 C) Pode ser realizado sem consentimento nos casos de menores.  
 D) Nenhuma das alternativas elencadas acima.

**Percentual de Respostas por Questão**



Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	86,9%
<b>ÍNDICE DE ERRO (em percentual)</b>	13,1%

15) Como deve ser o consentimento do titular, à luz da LGPD?

**Finalidade:**

- Verificar se os colaboradores compreendem os requisitos legais para obtenção do consentimento, garantindo que ele seja livre, informado, inequívoco e específico para finalidades previamente determinadas.

**Objetivo:**

- Orientar os colaboradores a aplicarem corretamente os princípios da LGPD ao solicitar o consentimento dos titulares, evitando o tratamento indevido de dados, promovendo a transparência e garantindo a proteção dos direitos dos titulares de dados pessoais.

**Alternativas:**

- A) **Livre, informado, inequívoco e específico para finalidades previamente determinadas.**
- B) De forma verbal e opcional.
- C) De forma vaga e temporária.
- D) Apenas verbal e sem especificar a finalidade.



Fonte: Coleta de Dados 2025-2026

<b>ÍNDICE DE ACERTO (em percentual)</b>	91,8%
<b>ÍNDICE DE ERRO (em percentual)</b>	8,2%

16) Você já recebeu treinamento sobre LGPD na Instituição? (Pergunta de pesquisa — sem gabarito)

**Finalidade:**

- Identificar o histórico de capacitação dos colaboradores e mapear quem já possui conhecimento prévio sobre a LGPD.

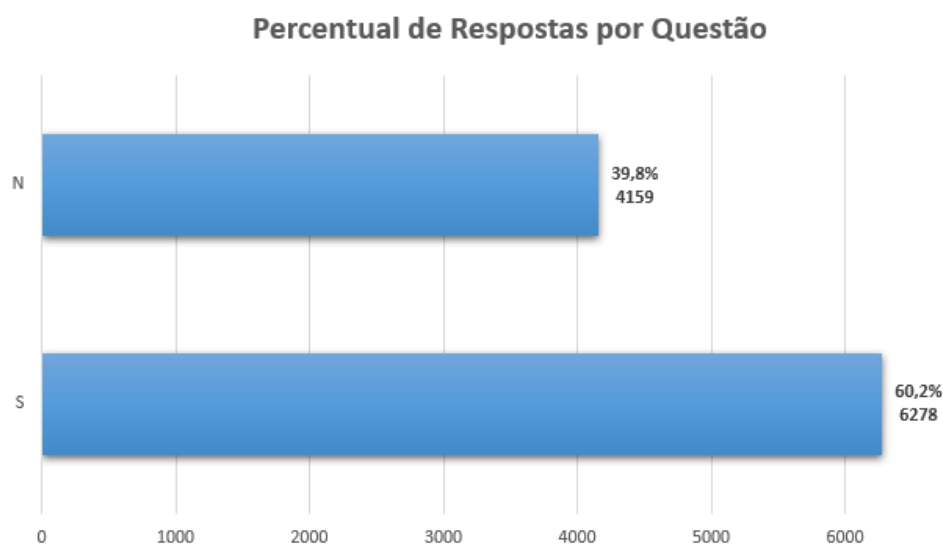
**Objetivo:**

- Avaliar a necessidade de ações de treinamento adicionais, detectar possíveis lacunas de conhecimento e planejar estratégias de conscientização e capacitação contínua sobre proteção de dados pessoais na Instituição.

**Alternativas:**

Opção: Sim

Opção: Não



Fonte: Coleta de Dados 2025-2026

<b>INDICE DE ACERTO (em percentual)</b>	60,2%
<b>INDICE DE ERRO (em percentual)</b>	39,8%

17) Ao receber uma ligação a colaboradora acolhe um pedido de envio de parte do prontuário do paciente por e-mail. O solicitante não justifica a finalidade nem a necessidade. Além disso, sabe-se que o funcionário é da área administrativa. Nesse caso:

#### Finalidade:

- Verificar se os colaboradores compreendem a forma correta de tratar dados sensíveis, reconhecendo a importância do consentimento do titular e da verificação da necessidade e finalidade do compartilhamento antes de fornecer qualquer informação.

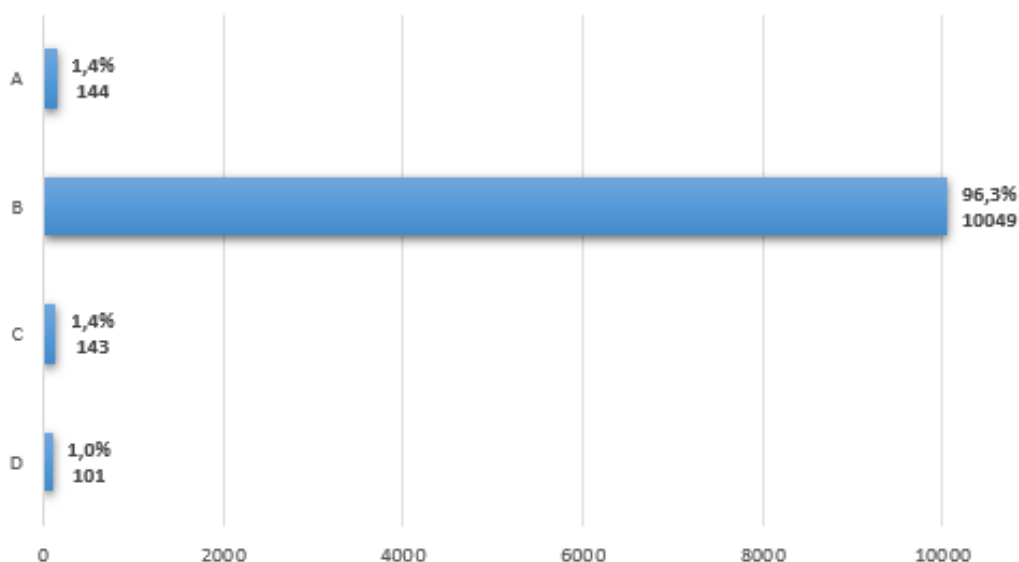
#### Objetivo:

- Orientar os colaboradores a agirem com cautela ao lidar com dados pessoais sensíveis, garantindo que não ocorram compartilhamentos indevidos, reforçando a proteção da privacidade dos titulares e a conformidade com a LGPD, além de incentivar a consulta a Gestores ou responsáveis em casos de dúvida.

#### Alternativas:

- A) Você fornece o prontuário todo e não somente a parte solicitada.  
 B) **Você não fornece, pois trata-se de dado sensível sujeito a consentimento.**  
 C) Você repassa ao solicitante apenas o requerido sem questionamentos.  
 D) Você, no caso de dúvida, não consulta o Gestor do Serviço e ainda assim, envia.

#### Percentual de Respostas por Questão



Fonte: Coleta de Dados 2025-2026

ÍNDICE DE ACERTO (em percentual)	96,3%
ÍNDICE DE ERRO (em percentual)	3,7%

### 4.3 GOVERNANÇA

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

No âmbito institucional, foi constituído um time multidisciplinar, contando com a colaboração entre as áreas de tecnologia, processos de negócios e jurídico, governança da privacidade, processos orientados a dados e transparência, permitindo, assim, o equilíbrio de competências e habilidades para o desenvolvimento das atividades do comitê.

Com o objetivo de reforçar as ações e o mapeamento da abrangência da LGPD na Instituição, foi criado um ambiente on-line para que o Comitê possa se apropriar e discutir a Lei Geral de Proteção de Dados, bem como estabelecer diretrizes institucionais e estratégias, a fim de garantir sua efetiva implantação e cumprimento. Esse ambiente constitui-se como um espaço colaborativo voltado à construção e à apropriação de conhecimentos, bem como à aproximação dos participantes em torno desse objetivo comum.

O processo de governança em LGPD é fundamental para garantir que as operações institucionais sejam conduzidas de forma ética, transparente e responsável no tratamento de dados pessoais, promovendo a confiança dos titulares de dados e assegurando o cumprimento das exigências legais.

#### 4.3.1 METODOLOGIA

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

A metodologia desenvolvida para a criação de um ambiente de sustentação da LGPD na SMS consistiu em um conjunto de ferramentas e aplicações que permitiram realizar um mapeamento amplo do momento inicial da instituição e apoiaram sua evolução até o padrão atualmente alcançado.

Para a aplicação da LGPD (Lei Geral de Proteção de Dados) de forma eficaz, adotou-se uma metodologia estruturada, observando alguns preceitos fundamentais da LGPD, conforme descrito abaixo:

1. **Conscientização e Treinamento:** Inicia-se com a conscientização sobre a LGPD em toda a instituição, desde a alta administração até os colaboradores que atuam na linha de frente, oferecendo-se 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:** Realiza-se um inventário completo dos dados pessoais que a instituição coleta, armazena, processa e compartilha, incluindo-se a identificação da origem dos dados, da finalidade do processamento, dos meios de armazenamento e das partes envolvidas no processamento.
3. **Análise de Riscos e Impacto à Privacidade:** Realiza-se uma avaliação detalhada dos riscos associados ao tratamento de dados pessoais, identificando-se possíveis ameaças à segurança dos dados, como vazamentos, acessos não autorizados ou violações de privacidade, bem como avaliando-se 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, são desenvolvidas políticas e procedimentos claros para governar o tratamento de dados pessoais, incluindo-se políticas de privacidade, consentimento, segurança da informação, retenção de dados e resposta a incidentes de segurança.
5. **Implementação de Medidas Técnicas e Organizacionais:** São implementadas medidas técnicas e organizacionais para garantir a segurança dos dados pessoais e o cumprimento dos requisitos da LGPD, incluindo controle de acesso, pseudonimização, anonimização, minimização de dados e auditoria de segurança.
6. **Monitoramento e Revisão Contínua:** Estabelece-se um programa de monitoramento contínuo para garantir que as políticas e procedimentos de proteção de dados sejam devidamente seguidos, realizando-se auditorias periódicas para avaliar o cumprimento da LGPD e promovendo-se ajustes sempre que necessário.
7. **Resposta a Incidentes:** Prevê-se o desenvolvimento de 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 seguir essa metodologia, busca-se 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 estruturada por meio de reuniões realizadas sempre com a presença de um núcleo permanente, que permaneceu inalterado e se reuniu semanalmente, pelo período máximo de uma hora para a execução do planejamento.

Os demais participantes foram integrados conforme as ações e atividades, em momentos de concentração e dispersão, com as demandas e encomendas subsidiadas pela discussão dos assuntos.

Foi elaborado um cronograma a ser seguido, o qual foi aprovado pela Direção e amplamente divulgado, com a finalidade de garantir que as agendas se tornassem prioritárias para esses encontros, os quais passaram a ser secretariados, com produção de atas, formalizando a participação e as respectivas entregas.

Além disso, a Instituição elaborou o seu regulamento, visando disciplinar os aspectos gerais e as orientações relativas à Lei Geral de Proteção de Dados, com caráter geral para todas as unidades, serviços e áreas integrantes da Rede de Saúde Santa Marcelina.

Em 2025, foi lançada a nova versão do Manual Institucional de Diretrizes, Boas Práticas e Condutas Éticas – Política de Compliance, na qual são verificáveis atualizações relevantes, incluindo a incorporação de diretrizes relacionadas às partes interessadas que atuam com a Santa Marcelina Saúde, bem como o tema da Integridade – Governança, Sustentabilidade e Ética (Item V). Destaca-se que cada parte interessada é considerada copartícipe e corresponsável pelo compromisso da Santa Marcelina Saúde com a integridade e a conformidade, entre outros assuntos.

Como estratégia de disseminação de conteúdo, a Santa Marcelina Saúde utilizou, dentre outras medidas, o ambiente virtual da AAGAPE Santa Marcelina como repositório de conteúdos e fonte de consulta, além de ações específicas de treinamentos e capacitações presenciais, visando à uniformização de conceitos e práticas, os quais foram posteriormente convertidos em política institucional.

#### 4.3.3 INSTRUMENTOS UTILIZADOS

Como estratégia inicial de disseminação de conteúdo, a Santa Marcelina Saúde utilizou, 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, visando à uniformização de conceitos e práticas, os quais posteriormente foram convertidos em política institucional.

#### 4.3.4 MATERIAL DE APOIO ÁUDIO VISUAL

Foram criados vídeos institucionais, com o objetivo de orientar os colaboradores quanto ao consentimento e à cultura da LGPD na SMS, bem como de servir como instrumento orientador para o preenchimento dos formulários requisitados pelo Comitê LGPD aos representantes dos serviços e áreas.

**- Vídeo – Comunicado | Presidência | LGPD – 2025 – Santa Marcelina Saúde:**

Link de acesso: <https://santamarcelina.org/comunicado-presidencia-lgpd-2025/>

**- Vídeo – Comunicado | DPO | LGPD – 2025**

Link de acesso: <https://santamarcelina.org/comunicado-dpo-lgpd-2025/>

**- Vídeo – Orientações sobre o questionário | Gestor | LGPD – 2025**

Link de acesso: <https://santamarcelina.org/video-questionario-lgpd-gestores-2025/>

**- Vídeo – Orientações sobre o questionário | Não Gestor | LGPD – 2025**

Link de acesso: <https://santamarcelina.org/video-questionario-lgpd-2025/>

**- Treinamento LGPD 2025 – Capacitação, utilização, aplicação, revisão de conceito e casos práticos envolvendo a LGPD no âmbito da Santa Marcelina Saúde:**

Link de acesso: <https://santamarcelina.org/video-lei-geral-protecao-dados-2025/>

## **5 – ANÁLISE DE NECESSIDADE E PROPORCIONALIDADE**

Todos os dados coletados nas operações cotidianas da SMS são criteriosamente selecionados, com o intuito de atender à real necessidade de utilização dos dados, levando em consideração sua finalidade e proporcionalidade, de forma que não haja coleta de informações excessivas ou que não sejam necessárias e essenciais para o atendimento do serviço proposto, respeitando, assim, o princípio da minimização de dados.

Isso significa que os dados coletados devem limitar-se ao mínimo necessário para o atingimento da finalidade proposta, sendo pertinentes, proporcionais e não excessivos.

Ainda, são realizados esforços para garantir a qualidade dos dados, assegurando sua exatidão, clareza, relevância e atualização, em conformidade com os direitos dos titulares, atendendo ao previsto no artigo 18 da LGPD.

A medida mostra-se proporcional ao risco crítico da atividade assistencial. Ao utilizar cenários do cotidiano de cada cargo específico — desde a recepção até a equipe clínica —, o questionário equilibra a teoria da norma com a prática operacional.

O benefício de mitigar acessos indevidos e vazamentos de informações de saúde justifica a adoção da medida, assegurando que cada profissional compreenda sua responsabilidade direta na proteção da dignidade do titular.

Assim, a Instituição cumpre seu dever de zelo sem sobrecarregar os processos, garantindo que a segurança da informação caminhe junto ao cuidado com o paciente.

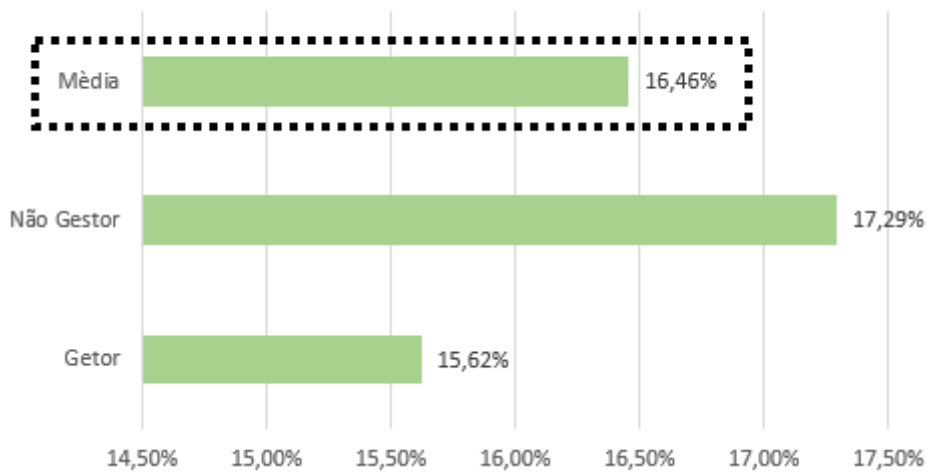
## **6 – METODOLOGIA ADOTADA PARA IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS**

Com a finalidade de manter a conformidade com a legislação e assegurar a proteção dos dados pessoais dos titulares, foi conduzido um processo detalhado para realizar essa identificação e avaliação das operações de tratamento e armazenamento dos dados pessoais.

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

Como parte da metodologia de aplicação da Matriz de Risco, a definição do nível de exposição fundamentou-se na utilização direta dos resultados obtidos nos questionários aplicados aos colaboradores (Gestores e Não Gestores). O total de não conformidades foi apurado a partir da média aritmética dos erros registrados em todas as questões de ambos os formulários, constituindo-se como indicador objetivo para a quantificação do risco. Este índice reflete o gap de conhecimento prático e operacional, permitindo que a probabilidade e o impacto sejam avaliados de forma fundamentada, com base nos dados coletados durante o diagnóstico situacional.

### LGPD - CLASSIFICAÇÃO DE RISCO



#### Resultado do Impacto:

Ao avaliar o índice médio de 16,46% de não conformidade, resultante da aplicação dos questionários aos Gestores e não Gestores, reputam-se a probabilidade e o impacto como muito baixos.

Probabilidade	90%	Média	Média	Alta	Alta	Alta
	70%	Baixa	Média	Média	Alta	Alta
	50%	Baixa	Baixa	Média	Alta	Alta
	30%	Baixa	Baixa	Média	Média	Alta
	10%	Baixa	Baixa	Baixa	Baixa	Média
		Muito Baixo	Baixo	Moderado	Alto	Muito Alto
Impacto						

## 7 – MEDIDAS PARA TRATAR OS RISCOS

Entende-se como primordiais algumas medidas a serem compartilhadas com os integrantes da SMS para o tratamento dos riscos, conforme os exemplos abaixo:

MEDIDA	DESCRIÇÃO
1	Atualização de momentos pedagógicos voltados à capacitação e à sensibilização sobre a LGPD junto aos Gestores e Colaboradores da SMS;
2	Revisão contínua das informações relativas às finalidades do tratamento de dados em todos os formulários de cadastro, consultas, processos e relatórios (físicos e digitais) da SMS;
3	Reforço das orientações aos colaboradores sobre as boas práticas de armazenamento e guarda de dados pessoais nos ambientes físico e digital, incluindo locais de retenção de documentos (gavetas, arquivos, depósitos etc.) e sistemas institucionais da SMS, com vistas à prevenção de acessos indevidos e à adequada proteção das informações;
4	Acompanhamento da adequada identificação no acesso aos setores internos por Gestores e Colaboradores, com vistas ao fortalecimento das Boas Práticas de Controle e Segurança das Informações;
5	Monitoramento da proteção lógica nos sistemas, incluindo atualizações de antivírus, gestão de senhas e demais controles de acesso;
6	Manutenção de registros de log (logs de acesso, alteração ou eliminação de dados, contendo identificador, data, hora e endereço IP);
7	Monitoramento do nível de segurança dos sites externos, incluindo a utilização do protocolo HTTPS e de TLS na comunicação por e-mail;
8	Monitoramento das salvaguardas de dados, incluindo backups diários, redundância e plano de disaster recovery em ambientes fisicamente distintos.

Prevê-se, ainda, a adoção de medidas de segurança técnicas e administrativas destinadas a proteger os dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

A Instituição não tem a obrigação de eliminar integralmente todos os riscos associados às atividades de tratamento de dados pessoais, devendo adotar medidas técnicas e administrativas adequadas e proporcionais para sua mitigação, de modo a reduzir os riscos a níveis aceitáveis. Tal abordagem observa os princípios da prevenção e da segurança previstos no art. 6º, bem como as obrigações de adoção de medidas de segurança estabelecidas no art. 46 e as diretrizes de boas práticas e governança previstas no art. 50 da Lei Geral de Proteção de Dados Pessoais.

## 8. RESUMO E O PLANO DE AÇÃO 2025-2026

O RIPD da Santa Marcelina Saúde consolida as atividades desenvolvidas pela Instituição, incluindo um Plano de Ação estruturado por etapas, com prazos, áreas responsáveis e metas definidas, que visam não apenas promover a maturidade dos processos institucionais vinculados ao tema, mas também

garantir o aperfeiçoamento das ferramentas tecnológicas utilizadas, em alinhamento com as normas e resoluções da ANPD.

O escopo do Plano de Ação 2025–2026 contempla a revisão dos documentos institucionais publicados no site institucional, a implementação de um Programa de Especialização em Dados voltado à Ciência e à Pesquisa, com workshops, treinamentos e vídeos educativos (pílulas), bem como a criação ou aprimoramento de sistemas, a fim de assegurar a conformidade técnica exigida pelo Regulamento de Dosimetria e Aplicação de Sanções Administrativas da ANPD. Adicionalmente, inclui o monitoramento permanente das ações implementadas, bem como a revisão anual do inventário de dados e do Relatório de Impacto à Proteção de Dados (RIPD).

As ações também se encontram atreladas à transformação da ANPD em autarquia de natureza especial, responsável pela regulação e fiscalização da proteção de dados pessoais no Brasil, incluindo a tutela dos dados de crianças e adolescentes no ambiente digital, em conformidade com o disposto no art. 14 da Lei Geral de Proteção de Dados Pessoais e com as diretrizes associadas ao chamado “ECA Digital”, o que amplia de forma significativa o seu papel institucional.

Além disso, prevê-se o fortalecimento da cultura de reporte e de resposta a incidentes, com a otimização do fluxo de acionamento do Encarregado pelo Tratamento de Dados Pessoais (DPO) e o incentivo à identificação proativa de eventuais falhas envolvendo terceiros e áreas institucionais, incluindo marketing, sob a premissa da “não punição”, orientada à melhoria contínua dos processos. Tal iniciativa possui caráter estratégico para a mitigação de riscos reputacionais e de eventuais sanções administrativas, contribuindo para consolidar a conformidade em proteção de dados como pilar da governança institucional.

Nesse contexto, o Comitê LGPD realizará o monitoramento contínuo das normas e orientações expedidas pela Agência Nacional de Proteção de Dados, bem como promoverá auditorias periódicas de vulnerabilidade, com periodicidade semestral, com o objetivo de identificar e tratar previamente eventuais lacunas de segurança antes que se convertam em incidentes passíveis de fiscalização ou sanção.

Tal medida encontra respaldo nos princípios da prevenção e da segurança previstos no art. 6º, bem como nas obrigações de adoção de medidas técnicas e administrativas de proteção estabelecidas no art. 46 da Lei Geral de Proteção de Dados Pessoais, além das diretrizes de boas práticas e governança previstas no art. 50 da mesma lei, em consonância com o Regulamento de Dosimetria e Aplicação de Sanções Administrativas da ANPD.

Prevê-se a renovação dos momentos pedagógicos destinados aos Gestores e Colaboradores do grupo Santa Marcelina Saúde, bem como a elaboração e a aplicação de novos questionários direcionados aos prestadores de serviços, com o objetivo de avaliar o nível atual de maturidade institucional e a cultura organizacional em relação à LGPD.

A medida visa fortalecer a observância das boas práticas de proteção de dados e assegurar a adequada conformidade com a legislação vigente no âmbito das relações com terceiros.

## 9. PRINCIPAIS AVANÇOS EM RELAÇÃO À 2ª FASE LGPD SMS (RIPD 23/24)

Em relação a experiência obtida na 1ª e 2ª 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, 22 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.
- 7. Mensuração da maturidade institucional:** A aplicação do questionário específico permitiu diagnosticar o nível de aculturação e maturidade dos colaboradores em relação à LGPD. Essa coleta de dados transformou percepções subjetivas em indicadores concretos, permitindo identificar gargalos de conhecimento e direcionar treinamentos de forma mais assertiva, garantindo que a conformidade não seja apenas documental, mas praticada no cotidiano operacional.

## 10 – SEGURANÇA DA INFORMAÇÃO

Sob o aspecto da segurança da informação, a Instituição estabelece um conjunto de boas práticas previstas em sua cartilha de uso interno, elaborada no âmbito do Comitê de Privacidade e Proteção de Dados da Santa Marcelina Saúde. O documento tem como finalidade orientar os colaboradores e Gestores quanto aos princípios e diretrizes de segurança da informação, além de simplificar o entendimento sobre o tema, apresentando conceitos fundamentais, identificando os principais

agentes envolvidos no tratamento de dados pessoais e descrevendo as práticas institucionais adotadas para a adequada proteção das informações.

Nesse contexto, reconhece-se que os riscos relacionados à Segurança da Informação tendem a ampliar-se e, em determinadas circunstâncias, materializar-se, especialmente do aumento das ameaças cibernéticas e de vazamento de dados pessoais. A ação consolida o fortalecimento da cultura de segurança da informação, promovendo a construção de comportamentos, valores e práticas compartilhadas que orientam a forma como a segurança é compreendida e disseminada na Instituição.

Diante desse cenário, foi realizado um teste de phishing direcionado às áreas administrativas da Santa Marcelina Saúde, com o objetivo de avaliar a capacidade de Gestores e Colaboradores para identificar e reportar possíveis ameaças à área de Tecnologia da Informação (TI), contribuindo para a disseminação da Cultura de Privacidade, sendo ela um reflexo da forma como uma organização enxerga e valoriza a proteção de seus colaboradores, processos e ativos, criando um ambiente em que todos, desde a liderança até os colaboradores da base, têm consciência do seu papel na prevenção de incidentes.

## 11 – CONCLUSÃO

Com base nas diretrizes do Relatório de Impacto à Proteção de Dados Pessoais (RIPD 2025-2026) do Santa Marcelina Saúde, o conteúdo produzido tem o condão de evidenciar a maturidade dos processos e os resultados alcançados, adiante detalhado:

Em continuidade ao Programa Anual de Conformidade, a terceira fase da estratégia de governança (RIPD 2025-2026) consolida o amadurecimento institucional alcançado por meio de ciclos sucessivos de melhoria, fundamentando-se nos resultados de uma abrangente pesquisa de conscientização realizada entre dezembro de 2025 e janeiro de 2026. Este diagnóstico, aplicado a uma amostra significativa que incluiu desde Gestores de serviços com 100% de participação até o quadro geral de colaboradores, evidenciou um índice de conformidade superior a 83%, o que permite classificar a probabilidade e o impacto de riscos residuais como muito baixos.

A estrutura de governança que sustenta esses números é composta por um Comitê LGPD permanente que realiza reuniões semanais para execução do planejamento e monitoramento das normas da ANPD. Esse trabalho resultou na criação de instrumentos públicos de transparência, como o canal direto com o DPO, a Diretiva de Proteção de Dados e políticas de privacidade integradas ao Programa de Integridade e Compliance da instituição. Tais medidas asseguram que o tratamento de dados, focado primordialmente nos fluxos de pacientes, familiares e gestão de pessoas, ocorra sob salvaguardas rigorosas.

Como resultado final, a instituição logrou êxito ao transformar a conformidade legal em uma cultura organizacional de ética digital e proteção proativa. Entre as atividades positivas realizadas, destaca-se a implementação de estratégias de educação corporativa baseadas em "pílulas" audiovisuais e estudos de caso reais, além do fortalecimento de uma cultura de "não-punição" que incentiva o reporte espontâneo de incidentes. Para o futuro próximo, o Santa Marcelina Saúde priorizará a realização de auditorias de vulnerabilidade semestrais e o desenvolvimento de um Programa de Especialização em

## RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

MEMBROS DO COMITÊ LGPD / DPO SMS

Dados para Ciência e Pesquisa, garantindo que a segurança da informação evolua no mesmo ritmo da assistência à saúde.

**12 – 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 organização, 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	
<hr/> Charles Neris dos Santos	<hr/> Fernanda Oliveira
ENCARREGADO	REPRESENTANTE DO COMITÊ LGPD SMS
<hr/> Carlos da Silva	<hr/> Eliza Yukie Inakake  <hr/> Gustavo Oliveira
REPRESENTANTE LEGAL DO CONTROLADOR	
<hr/> Ir Rosane Ghedin	

São Paulo, 26 de março de 2026

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

