Gama Imagem

Política de Segurança da Informação

Histórico de revisões

Versão	Data	Alteração
1	20/05/2024	Marcelly Batista e Cecília Barros
2	14/06/2024	Marcelly Batista e Cecília Barros

1. Sobre a Política de Segurança da Informação (PSI)

A Política de Segurança da Informação (PSI) é o documento que orienta e estabelece as diretrizes corporativas da Gama Imagem para a proteção dos ativos de informação e a prevenção da responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

2. Conceitos importantes

A gestão da segurança da informação inicia-se com a definição de políticas, procedimentos, guias e padrões.

A princípio, a segurança da informação abrange três pilares básicos, que são:

- **Integridade:** É um aspecto que garante que a informação não perca sua originalidade desde a sua criação;
- **Disponibilidade:** É um aspecto que garante que a informação esteja sempre disponível.
- **Confidencialidade:** É um aspecto que garante que a informação seja acessada, somente por usuários autorizados.

Nesse sentido, é fundamental o conhecimento dos seguintes conceitos:

- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- **Dados Pessoais:** informação relacionada a pessoa natural/física identificada ou identificável.
- **Dados Pessoais Sensíveis:** dado pessoal sobre origem racial, ou étnica, convicção religiosa, opinião política, filiação à sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- **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.

3. Objetivos da Política de Segurança da Informação

- Estabelecer diretrizes e normas que permitam aos funcionários, prestadores de serviços, estagiários e afins da Gama Imagem seguir padrões de comportamento desejáveis e aceitáveis, de acordo com a legalidade e as boas práticas mundiais, a fim de mitigar riscos técnicos e jurídicos;
- Nortear a definição de procedimentos específicos de Segurança da Informação e a implementação de controles e processos para o atendimento de seus requisitos;
- Preservar a confidencialidade, a integridade e a disponibilidade das informações da Gama Imagem;
- Prevenir possíveis incidentes e responsabilidade legal da instituição e de seus funcionários, prestadores de serviços, estagiários e afins;
- Garantir a normalidade e a continuidade das atividades da Gama Imagem, protegendo os processos críticos contra falhas ou desastres significativos;
- Atender aos requisitos legais, regulamentares e contratuais pertinentes à atividade da Gama Imagem;
- Minimizar os riscos de danos, perdas financeiras, participação no mercado, confiança de clientes e de parceiros ou qualquer outro impacto negativo nas atividades da Gama Imagem resultante de uma falha de segurança;
- Assegurar o treinamento contínuo e atualizado das políticas e dos procedimentos de Segurança da Informação, enfatizando as obrigações das pessoas em relação à respectiva segurança;
- Garantir que todas as responsabilidades da Segurança da Informação sejam claramente definidas e preservadas.

4. Aplicação da Política de Segurança da Informação

Todas as normas aqui estabelecidas devem ser aplicadas por toda a rede e seguidas por todos os funcionários, prestadores de serviços, estagiários e afins para a proteção da informação e para o uso de recursos tecnológicos.

Esta PSI compromete e responsabiliza cada usuário a manter-se atualizado sobre este documento e as normas relacionadas, buscando orientação da direção sempre que não estiver absolutamente seguro quanto à aquisição e/ou ao descarte de informações.

5. Princípios da Política de Segurança da Informação

Esta PSI se rege pelos princípios de segurança e privacidade do cliente. Os equipamentos devem ser utilizados apenas para a realização de atividades profissionais, com senso de responsabilidade e ética.

Esta política se rege pelos princípios da Lei Geral de Proteção de Dados, quais sejam:

- **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- **Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- **Livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- **Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A Gama Imagem reserva-se o direito de monitorar e registrar todo e qualquer uso das informações geradas, armazenadas ou veiculadas na instituição. Para tanto, são criados e implantados controles apropriados em todos os pontos e sistemas que a Gama Imagem julgar necessário para reduzir os riscos, pautando-se na legalidade.

6. Requisitos da Política de Segurança da Informação

A PSI deve ser comunicada a todos os funcionários, prestadores de serviços, estagiários e afins, visando à efetividade e à real cultura de uso ético e legal dos recursos tecnológicos, bem como a Segurança da Informação da Gama Imagem.

A PSI e as Normas serão revisadas e atualizadas com periodicidade mínima de um ano ou sempre que houver um fato novo e relevante, conforme análise e decisão do Comitê de Privacidade.

Todos os contratos da Gama Imagem devem constar de anexo ou a cláusula de confidencialidade para garantir o acesso aos ativos de informação.

O uso de sistemas da clínica só é permitido para usuários que formalizarem a ciência sobre a PSI.

A responsabilidade em relação à Segurança da Informação deve ser atribuída na fase de contratação, de forma a ser incluída nos contratos e monitorada durante a sua vigência.

Para funcionários, prestadores de serviços, estagiários e afins, contratados em período anterior à publicação desta política, e que não tenham assinado os respectivos documentos, deverá ser entregue um Termo de Ciência e Responsabilidade da PSI para a respectiva assinatura de forma física ou eletrônica.

Todos os funcionários, prestadores de serviços, estagiários e afins que tenham acesso a informações da Gama Imagem, devem passar por treinamento e conscientização sobre os procedimentos de segurança e o uso correto dos ativos oferecidos pela instituição. A finalidade é minimizar possíveis riscos de segurança, explicitar as responsabilidades e comunicar os procedimentos para a notificação de incidentes.

Os dados pessoais devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas aos riscos identificados, além de ter o acesso controlado, registrado e monitorado.

Todo dado pessoal deve ser protegido de divulgação, modificação, furto ou roubo por meio da aplicação de controles.

Devem ser estabelecidas e comunicadas normas e responsabilidades pela propriedade e custódia dos dados pessoais, bem como estabelecidos procedimentos e responsabilidades específicos para o uso e o gerenciamento dos respectivos dados oferecidos pela Gama Imagem, quando estiverem fora das instalações da instituição.

O uso de dispositivos móveis, assim como comunicadores instantâneos, devem ser devidamente regrados em normativos próprios, atendendo sempre aos princípios da privacidade, respeito ao usuário e à necessidade da coleta de autorização, quando aplicável, devendo ser informadas, na Política de Privacidade, informações sobre as condições de tratamento.

A Gama Imagem se exonera de toda e qualquer responsabilidade decorrente do uso indevido, negligente e/ou imprudente dos recursos e serviços concedidos aos usuários, reservando-se o direito de tomar as medidas administrativas e judiciais cabíveis contra os infratores, bem como analisar dados e evidências para a obtenção de provas a serem usadas em processos investigatórios e judiciais.

Todo incidente que afete a Segurança da Informação deverá ser comunicado inicialmente à direção, que, se julgar necessário, deverá encaminhá-lo posteriormente ao Comitê de Privacidade para análise. Toda e qualquer atividade que não esteja tratada nesta política ou normativos específicos deve ser realizada apenas após consulta e autorização do gestor da área.

O não cumprimento dos requisitos previstos nesta PSI e nas Normas de Segurança da Informação acarretará violação às regras internas da instituição, e o usuário estará sujeito às medidas administrativas e legais

cabíveis.

7. Monitoramento e Auditoria

Para garantir as regras mencionadas nesta PSI, bem como para fins de segurança e prevenção à fraude, a Gama Imagem reserva-se o direito de:

- Implantar sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônico, navegação, internet, dispositivos móveis ou wireless, entre outros componentes da rede. A informação gerada por esses sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;
- Inspecionar qualquer arquivo que esteja em rede, no disco local da estação ou em qualquer outro ambiente para assegurar o rígido cumprimento desta PSI;
- Instalar sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso;
- Instalar câmeras em suas dependências.

Os funcionários, prestadores de serviços, estagiários e afins tomam ciência de que ambientes, recursos tecnológicos, telefones, sistemas, computadores, dispositivos móveis e redes da instituição estão sujeitos a monitoramento e a gravação, atendendo à conformidade legal.

O colaborador ou prestador de serviços toma ciência, neste ato, de que, ao aceitar ou optar pelo uso de dispositivos pessoais para fins corporativos, a Gama Imagem poderá auditar e inspecionar os recursos de tecnologia da informação que estiverem em suas dependências ou que interajam com seus ambientes, sempre que considerar necessário, atentando-se à não discriminação e à proporcionalidade devida, respeitando a razoabilidade e privacidade.

8. Responsabilidades Específicas

8.1. Dos Usuários em geral

Funcionários, prestadores de serviços, estagiários e afins da Gama Imagem, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis por cumprir e zelar pela materialização e realização eficaz das normas e princípios da segurança da informação, em atenção especial ao compromisso com os critérios legais e éticos que envolvam a instituição.

É de inteira responsabilidade do usuário qualquer prejuízo ou dano sofrido ou causado à clínica e/ou a terceiros, em decorrência da não obediência às diretrizes e às normas aqui referidas.

Cabe a todos os usuários adotar as seguintes práticas:

• Cumprir fielmente políticas, normas e procedimentos de Segurança da Informação, incluindo regras estabelecidas neste documento;

• Buscar orientação do superior quando houver dúvidas relacionadas à Segurança da Informação;

• Assinar o Termo de Responsabilidade, formalizando a ciência da PSI e das Normas de Segurança da Informação, bem como assumindo a responsabilidade pelo seu cumprimento;

• Proteger as informações contra o acesso, a modificação, a divulgação ou a destruição não autorizada pela Gama Imagem;

• Assegurar que os recursos tecnológicos sejam utilizados apenas para fins profissionais aprovados e de interesse da instituição;

• Prezar pela segurança das informações confidenciais, incluindo todos e quaisquer dados pessoais a que tiverem acesso;

• Atender à Lei Geral de Proteção de Dados Pessoais, protegendo os dados a que tiver acesso ou que venha a manusear, sempre em conformidade com as regras da clínica;

• Comunicar imediatamente à direção sobre qualquer descumprimento ou violação da PSI; além disso, quando se tratar de infrações administrativas causadas por funcionários, prestadores de serviços, estagiários e afins; além de outras áreas, quando for necessário.

8.1.1. Política de Senhas

Os colaboradores, terceiros e passantes assumem inteiramente a responsabilidade pelo usuário (credencial) fornecido para acesso à rede, aplicações internas, externas, aplicativos móveis, internet e sistemas de forma individual e intransferível.

A Gama Imagem sempre adotará, quando disponível, pelo lado das aplicações, plataformas com validação de dois fatores via aplicativo, e-mail ou SMS. A verificação em duas etapas ajuda o uso das contas com mais segurança, porque as senhas podem ser esquecidas, roubadas ou comprometidas. Esta verificação usa uma segunda etapa para dificultar a entrada de outras pessoas em sua conta.

O uso de senha segura é obrigatório para os sistemas, serviços e dispositivos, que devem ser configurados conforme o padrão definido pela clínica, sendo obrigatória a alteração da senha conforme periodicidade e recomendações de segurança determinadas pela instituição.

- Para se obter uma senha de acesso forte, que ofereça mais segurança aos colaboradores, deve-se considerar as seguintes condições:
  - Tamanho mínimo de 8 caracteres;
  - Conter pelo menos uma letra maiúscula e uma minúscula;
  - Conter números;
  - Conter símbolos, incluindo: !@#$%^&*-_+=[]{}|\‘,.?/ ~“<>().
    - Exemplo: Um novo dia de Sol = Umn0v0d14d35@L
- Não repetir senhas anteriores (últimas 3 senhas).
- Mandatório alterar a senha a cada 90 dias.
- Evitar a utilização de:
  - Nomes, sobrenomes, dados de família, números de documentos, telefone, placas de carros, palavras de uso comum, bordões, nomes de times, filmes, séries, músicas, produtos, sequência númericas, de teclado (ex.: 09876543 / poiuy876) ou datas comemorativas;

Caso o usuário erre a senha após cinco tentativas, ocorrerá o bloqueio de sua credencial. A conta permanecerá bloqueada por 30 minutos; após esse periodo, a conta é automaticamente desbloqueada. Caso o bloqueio persista, será necessário solicitar a abertura de chamado. Da mesma forma, para casos de dúvidas ou outras questões.

Todo acesso deve ser identificado de forma individual, seja ele interno ou externo, sendo proibido o compartilhamento de credencial e uso de usuários genéricos.

É proibido compartilhar senhas com outras pessoas, sejam quais forem, assim como anotá-las em post-its, agendas, telefones pessoais ou quaisquer locais de fácil acesso.

8.1.2. Condutas

Os equipamentos disponibilizados para uso dos colaboradores devem permanecer disponíveis durante o maior tempo possível para que eles não tenham suas atividades laborais prejudicadas. Assim, algumas regras e medidas de segurança devem ser adotadas. São elas:

a. O colaborador deve zelar pelo seu equipamento de trabalho, mantendo-o sempre em boas condições de uso e limpeza.
b. A instalação de softwares só poderá ser realizada pela equipe do setor de Tecnologia da Informação;
c. Sempre que o colaborador se ausentar da sua estação de trabalho, deverá bloquear seu computador para evitar que terceiros tenham acesso à sua estação de trabalho;
d. As estações de trabalho só estarão acessíveis aos colaboradores através de contas de seu usuário;
e. Os documentos e arquivos relativos à atividade desempenhada pelo colaborador é de interesse da organização e deverão ser armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;
f. É proibido instalação de software sem autorização do setor de Tecnologia da Informação;
g. Bloquear tela do equipamento ao sair da mesa;
h. Cumprir a política da mesa limpa, evitando manter documentos expostos em cima da mesa, principalmente ao se ausentar do posto de trabalho;
i. É proibido desinstalar ou desativar medidas de segurança, como antivírus, bloqueios de acesso ou qualquer barreira de proteção instalada nos computadores.

8.2. Dos Gestores/Gerentes

Cabe ao(s) gerente(s) e gestor(es) de área:

- Manter postura em relação à Segurança da Informação e servir de modelo de conduta para os funcionários, prestadores de serviços, estagiários e afins sob a sua gestão;
- Orientar subordinados acerca da necessidade de cumprir com a presente PSI; oferecer feedback e orientação em casos de comportamentos que não estejam de acordo com os valores aqui estabelecidos ou, em casos de graves violações ou reincidência na conduta, aplicar as penalidades devidas, em conformidade com a legislação trabalhista;
- Cumprir esta política, as normas e os procedimentos de Segurança da Informação;
- Garantir acesso e conhecimento a esta política, bem como às normas e aos procedimentos aqui estabelecidos;
- Adaptar as normas, processos, procedimentos e sistemas sob sua responsabilidade para atender à PSI;
- Observar e zelar pela aplicação das regras e legislação de Proteção de Dados Pessoais;
- Comunicar imediatamente à direção toda e qualquer violação de Segurança da Informação, incluindo violação de dados pessoais, que deverá informar acerca da ocorrência de infrações provenientes de

funcionários, bem como informar às demais áreas, quando houver necessidades específicas;
- Garantir a implementação de mecanismos necessários para o descarte seguro das informações;

8.3. Da Direção

Cabe à direção:

• Adotar postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os demais colaboradores e parceiros;

• Elaborar, para toda informação sob a sua responsabilidade, matriz que relaciona cargos e funções da Gama Imagem às autorizações de acesso concedidas;

• Manter registro e controle atualizados de todas as autorizações de acessos concedidas, determinando, sempre que necessário, a pronta suspensão do acesso ou a alteração da autorização concedida;

• Reavaliar as autorizações de acesso, sempre que necessário ou solicitado, cancelando aquelas que não se fizerem mais necessárias;

• Planejar a expansão e o desenvolvimento do negócio, considerando as diretrizes de proteção de dados e da privacidade desde a estruturação da ideia;

• Observar e zelar pela aplicação das regras e legislação de Proteção de Dados Pessoais na organização.

8.4. Do setor de Tecnologia da Informação

O setor de TI será responsável pela gestão do uso de tecnologias necessárias ao bom andamento dos negócios da clínica e de ações preventivas. Cabe a ele:

- Apresentar as atualizações da PSI e das Normas de Segurança da Informação ao Comitê de Privacidade para aprovação e posterior publicação;
- Propor as metodologias e processos específicos para a Segurança da Informação, como a avaliação de risco;
- Apoiar a avaliação e a adequação dos controles específicos da Segurança da Informação para novos sistemas ou serviços;
- Promover adequação dos recursos técnicos e de infraestrutura necessários para atender à Lei de Proteção de Dados Pessoais;
- Analisar criticamente incidentes com o Comitê de Privacidade;
- Manter a comunicação efetiva com o Comitê de Privacidade para mantê-lo informado sobre assuntos relacionados ao tema e que afetem ou tenham potencial para afetar a clínica;
- Atuar de forma preventiva, adotando as medidas que julgar necessário para evitar incidentes de violação à proteção dos dados tratados pela organização.

8.5. Da Gestão de Recursos Humanos

Cabe à Gestão de Recursos Humanos:

- Atribuir, na fase de contratação dos funcionários, prestadores de serviços, estagiários e afins, e formalizar nos contratos individuais de trabalho, a responsabilidade quanto ao cumprimento da PSI e sua responsabilidade para com a Proteção de Dados Pessoais;

- Colher e arquivar a assinatura do Termo de Responsabilidade e ciência da Política e Normas de Segurança da Informação dos profissionais já contratados;
- Comunicar formalmente e imediatamente à direção toda e qualquer alteração no quadro funcional da instituição, contratações, demissões, alterações de cargos, funções, entre outros, no prazo mínimo de 24 horas, e de imediato em casos específicos, a fim de evitar acessos não autorizados e/ou desnecessários;
- Receber da gerência informações sobre violações da Política e Normas e promover as tratativas e a instauração de processo disciplinar, quando cabível;
- Apoiar e promover ações de conscientização e de capacitação em Segurança da Informação e Proteção de Dados Pessoais, para todos os profissionais da clínica;
- Zelar e promover a devida proteção de dados pessoais, em conformidade com as normas internas e legislação pertinentes.

8.6. Do Comitê de Privacidade

O Comitê de Privacidade deve ter um perfil multidisciplinar e contar com a participação de gestores de diferentes áreas da Gama Imagem. Deve ser formado por um representante das principais instâncias da instituição. Pode, ainda, utilizar especialistas internos ou externos para apoiarem nos assuntos que exijam conhecimento técnico específico.

O Comitê de Privacidade deve reunir-se formalmente, no mínimo, uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar algum incidente grave ou definição relevante para a clínica.

São atribuições do Comitê de Privacidade:

- Propor investimentos relacionados à Segurança da Informação com o objetivo de maximizar a redução de riscos;
- Propor alterações nas versões da PSI e a inclusão, eliminação ou alteração de normas complementares;
- Discutir e propor iniciativas para aprimorar, melhorar e dar continuidade à segurança das informações;
- Avaliar os incidentes de segurança e propor ações corretivas;
- Discutir e propor medidas cabíveis no processo disciplinar para os casos de descumprimento da PSI;
- Deliberar sobre questões relacionadas à Proteção de Dados Pessoais.

9. Da Proteção de Dados Pessoais

A Gama Imagem, em atendimento e respeito à Lei Geral de Proteção de Dados Pessoais, deverá garantir a disponibilidade, integridade e confidencialidade dos dados pessoais em todo seu ciclo de vida, sendo tratados de forma permanente como dados confidenciais.

Todo tratamento de dados pessoais deverá estar atrelado a uma finalidade específica, informada ao titular e devidamente atrelada a uma ou mais bases legais previstas nos artigos 7º e 11 da Lei Geral de Proteção de Dados Pessoais, atentando-se aos princípios da necessidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e prestação de contas.

O detalhamento dos requisitos e regras para tratamento de dados pessoais serão disponibilizados na Política de Privacidade, sendo necessário que todos os colaboradores e prestadores de serviços tomem ciência e sejam sensibilizados sobre o tema e a respectiva política.

Toda e qualquer alteração ou criação de sistemas, serviços ou produtos que envolvam tratamento de dados pessoais deverão aplicar o “Privacy by Design/Privacidade desde a concepção”.

Todos os ativos de informação da Gama Imagem que suportem o armazenamento de dados precisam ser verificados antes da entrega para eventual venda, remanejamento ou reutilização, com intuito de assegurar que todos os dados pessoais, informações sigilosas, softwares tenham sobregravados com segurança por meio de técnicas e softwares que tornem as informações originais irrecuperáveis (sanitização) em vez de usarem apenas as funções padrão de formatação.

É necessário praticar uma correta política de uso de backup. O backup é uma cópia de segurança de todos os dados e informações, e assegura que setor de tecnologia da informação esteja preparado para restaurar (recuperar) todos os dados contidos na máquina. Assim, em caso de incidente, todos os dados serão restaurados de forma íntegra. São regras da política de backup:

- Qualquer sistema, dado ou informação relevante para a organização deve possuir uma cópia de segurança, para eventuais incidentes, permitindo a recuperação para minimizar os impactos no negócio;
- Backups de arquivos armazenados em rede interna devem ser realizados de forma automática, a fim de garantir a segurança dos arquivos ali armazenados;
- As mídias de backup devem ser armazenas em local seco, limpo e climatizado, longe da luz solar, identificados com data e hora da realização do backup;
- Backups automatizados devem ser realizados fora do horário comercial.

Além dos princípios mencionados, a clínica deverá elaborar um plano de resposta à violação de dados pessoais, elaborar o Relatório de Impacto sempre que necessário, utilizar processos de anonimização e pseudonimização sempre que necessário, fazer registro das operações de tratamento de dados pessoais, utilizar protocolos de criptografia na transmissão e armazenamento de dados pessoais, bem como implementar um sistema de gestão de dados pessoais.

10. Das Disposições Finais

As infrações a esta PSI e às Normas de Segurança da Informação serão passíveis de processo disciplinar, podendo resultar de mera advertência até demissão por justa causa.

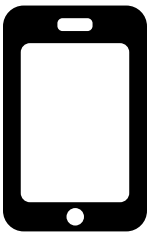
O uso de qualquer recurso da Gama Imagem para atividades ilegais é motivo de demissão por justa causa e a instituição vai cooperar ativamente com as autoridades. A PSI da clínica será complementada por Normas de Segurança da Informação que tratem assuntos relacionados ao uso de correio eletrônico, rede corporativa, internet, Proteção de Dados Pessoais, entre outros, que serão consideradas partes integrantes desta PSI.

Esta PSI e as Normas de Segurança da Informação estarão disponíveis em documentos internos, em local de fácil localização e acesso restrito. Normas específicas relacionadas a questões técnicas e confidenciais, e que requeiram acesso por equipes e pessoas específicas, devem ser colocadas à disposição apenas a pessoas autorizadas.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Gama Imagem.

11. Em caso de dúvidas

Em caso de dúvida sobre a presente Política de Segurança da Informação, é possível o esclarecimento das disposições pelo Comitê de Privacidade e Proteção de Dados da Gama Imagem, através de e-mail endereçado ao endereço “lgpd@gamaimagem.com.br”.



Documento elaborado em serviço de consultoria jurídica pelas advogadas Marcelly Batista (OAB/PB nº 27.360) e Cecília Barros (OAB/PB nº 33.139)