Política de Segurança da Informação

1. Objetivo

Estabelecer, implementar, manter e melhorar o Sistema de Gestão de Segurança da Informação da Mitri Consultoria e Gestão Médica, protegendo informações institucionais, administrativas, assistenciais e pessoais contra acesso, uso, divulgação, alteração, perda, destruição ou indisponibilidade não autorizados.

Esta Política define a abordagem da Mitri para gestão de ativos, riscos, objetivos, controles, responsabilidades e nível de proteção necessário, assegurando confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, privacidade e continuidade dos processos críticos.

2. Escopo e abrangência

Aplica-se a todos os setores administrativos e assistenciais da Mitri, às unidades e serviços sob sua responsabilidade ou gestão, e a todas as pessoas que acessem informações ou recursos institucionais, incluindo:

- Diretores, gestores, colaboradores, corpo clínico, profissionais de saúde, estagiários e aprendizes.
- Prestadores, fornecedores, consultores, parceiros, clientes e demais terceiros.
- Informações em papel, meio eletrônico, áudio, vídeo, imagem, comunicação verbal e qualquer outra forma de registro.
- Sistemas, redes, equipamentos, dispositivos móveis, mídias removíveis, serviços em nuvem, repositórios, prontuários e ambientes físicos.
- Atividades presenciais, remotas, externas e realizadas em instalações de terceiros.

3. Referencias e requisitos aplicáveis

A implementação desta Política observará a legislação, os contratos e os referenciais aplicáveis ao escopo da Mitri, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD), normas dos conselhos profissionais, obrigações relativas a prontuários e a edição licenciada e vigente dos Padrões Internacionais de Acreditação AACI contratados pela organização.

Esta Política foi estruturada para atender especialmente ao Padrão 30 – Gestão de Segurança da Informação da AACI, mantendo interface com os requisitos de controle de informação documentada, gerenciamento de riscos, privacidade, confidencialidade e prontuários.

4. Definições

Termo	Definição
Ativo de informação	Pessoa, processo, informação, sistema, equipamento, serviço, ambiente ou recurso que possua valor para a Mitri.
Confidencialidade	Garantia de acesso e divulgação somente por pessoas, processos ou entidades autorizadas.
Integridade	Garantia de exatidão, completude e proteção contra alteração ou destruição não autorizada.
Disponibilidade	Garantia de acesso à informação e aos recursos por usuários autorizados quando necessário.
Autenticidade	Garantia de identidade, autoria e origem verificáveis.
Rastreabilidade	Capacidade de identificar ações, acessos, alterações, autoria, data e hora.
Incidente de segurança	Evento confirmado ou suspeito que comprometa ou possa comprometer informações, ativos, serviços ou titulares.
SGSI/ISM	Sistema de Gestão de Segurança da Informação: conjunto coordenado de políticas, processos, pessoas, tecnologias, controles e evidências.
Risco	Efeito da incerteza sobre os objetivos, avaliado por probabilidade, consequência e eficácia dos controles.
Risco residual	Risco remanescente após a aplicação de controles.
RTO	Tempo máximo definido para restaurar um processo ou serviço após interrupção.
RPO	Quantidade máxima tolerável de perda de dados medida no tempo.
BIA	Análise de Impacto no Negócio utilizada para identificar processos críticos, dependências e impactos de interrupção.
Proprietário do ativo	Responsável por classificar, autorizar acesso e assegurar proteção adequada ao ativo.
Equipamento autônomo/endpoint	Computador, notebook, celular, tablet ou outro dispositivo capaz de processar ou armazenar informação.
Terceiro operador	Pessoa ou organização que trata informações ou executa serviços em nome da Mitri conforme contrato e instruções documentadas.

5. Princípios

- Necessidade de saber e privilégio mínimo.
- Defesa em profundidade e controles proporcionais ao risco.
- Segregação de funções e responsabilização individual.
- Privacidade e segurança desde a concepção e por padrão.
- Uso de informações apenas para finalidades legítimas, autorizadas e compatíveis.
- Tomada de decisão baseada em evidências e melhoria contínua.
- Comunicação de boa-fé, sem retaliação, de suspeitas, fragilidades e incidentes.

6. Governança e Responsabilidades

6.1 Diretoria

- Aprovar esta Política, os riscos residuais de sua alçada e os recursos necessários.
- Assegurar que o SGSI esteja alinhado ao contexto, à estratégia e às obrigações da Mitri.
- Receber e analisar, no mínimo anualmente, resultados de riscos, incidentes, auditorias, continuidade, terceiros, indicadores e planos de ação.

6.2 Tecnologia da Informação e Segurança da Informação

- Manter o SGSI, os padrões técnicos, os controles, a documentação e as evidências.
- Gerenciar identidades, acessos, ativos, configurações, vulnerabilidades, logs, backups, incidentes e recuperação.
- Monitorar a conformidade, reportar desempenho e orientar áreas, usuários e terceiros.
- Avaliar mudanças, projetos, aquisições, integrações e exceções sob a perspectiva de risco.

6.3 Encarregado de Dados, Jurídico, Qualidade, RH e Contratos

- O Encarregado de Dados orienta o tratamento de dados pessoais, direitos dos titulares e comunicação regulatória.
- O Jurídico valida requisitos legais, comunicações, contratos e medidas decorrentes de incidentes.
- A Qualidade controla documentos, auditorias, não conformidades, ações corretivas e análise de eficácia.
- O RH integra segurança à admissão, movimentação, desligamento, termos, capacitação e medidas disciplinares.
- Contratos assegura avaliação e cláusulas de segurança, privacidade e continuidade para terceiros.

6.4 Gestores, proprietários de ativos, usuários e terceiros.

- Gestores e proprietários definem necessidade de acesso, classificação, criticidade, retenção e controles dos ativos sob sua responsabilidade.
- Usuários e terceiros utilizam recursos apenas para fins autorizados, protegem credenciais, respeitam classificações e comunicam imediatamente suspeitas ou incidentes.
- O dever de confidencialidade permanece durante e após o encerramento do vínculo.

7. Gestão de riscos de segurança da informação

A Mitri manterá processo documentado e contínuo para identificar, analisar, avaliar, priorizar, tratar, monitorar e comunicar riscos aos ativos, pessoas, pacientes, titulares, processos, finanças, reputação e continuidade.

A avaliação considerará, no mínimo, probabilidade, natureza e magnitude das consequências, conectividade, fatores temporais, vulnerabilidades e eficácia dos controles existentes. Cada risco deverá possuir proprietário, classificação, decisão de tratamento, prazo, recurso, medida de desempenho e risco residual.

- Eliminar, reduzir, compartilhar/transferir ou aceitar o risco conforme critérios e alçadas aprovados.
- Manter Registro de Riscos atualizado como informação documentada.
- Revisar riscos continuamente, no mínimo anualmente, e após mudanças, incidentes ou novos serviços.
- Reportar riscos altos e críticos à Diretoria e acompanhar a eficácia dos planos de tratamento.

8. Classificação e tratamento da informação

Toda informação e ativo associado deverá ser classificado pelo proprietário conforme valor, sensibilidade, criticidade, obrigações e impacto potencial.

Classificação	Tratamento geral
Pública	Divulgação autorizada; não produz impacto relevante se conhecida externamente.
Interna	Uso institucional; compartilhamento limitado a públicos relacionados à atividade.
Confidencial	Acesso restrito por necessidade; inclui informações comerciais, contratuais, pessoais e operacionais sensíveis.
Restrita	Maior criticidade; inclui dados de saúde, prontuários, credenciais, chaves, investigações e informações cujo acesso indevido possa causar dano grave.

- Aplicar controles compatíveis de acesso, rotulagem, armazenamento, transmissão, cópia, impressão, retenção, compartilhamento e descarte.
- Reavaliar a classificação quando houver mudança de finalidade, contexto, sensibilidade, obrigação ou uso.
- Utilizar somente repositórios, e-mails, mensageria e canais homologados; é vedado tratar informação institucional em contas pessoais não autorizadas

9. Gestão de acessos e identidades

A concessão, alteração, revisão e revogação de acessos físicos e lógicos seguirá processo formal, rastreável e baseado em função, vínculo, necessidade de saber, privilégio mínimo e segregação de funções.

- Cada usuário terá identificação individual. Contas compartilhadas ou genéricas somente serão permitidas mediante justificativa, controle compensatório, aprovação e rastreabilidade.
- Admissões, movimentações e desligamentos deverão gerar solicitação, aprovação, execução e validação nos prazos definidos.
- Acessos privilegiados serão individualizados, restritos, registrados, monitorados e revisados periodicamente.
- A recertificação dos acessos críticos ocorrerá, no mínimo, trimestralmente; os demais acessos serão revisados conforme risco e ao menos anualmente.
- Contas inativas, órfãs, expiradas ou incompatíveis serão bloqueadas ou removidas tempestivamente.
- Acesso emergencial deverá ser aprovado, limitado no tempo, monitorado e revisado após o uso.

10. Credenciais, senhas e autenticação

- Credenciais são pessoais, sigilosas e intransferíveis; seu compartilhamento é proibido.
- Senhas iniciais serão temporárias, transmitidas por meio seguro e alteradas no primeiro acesso.
- Redefinições exigirão autenticação proporcional ao risco; senhas não serão enviadas ou armazenadas em texto desprotegido.
- Senhas devem ter complexidade e comprimento definidos tecnicamente, não conter informações facilmente dedutíveis e não ser reutilizadas de forma indevida.
- Sistemas aplicarão bloqueio por tentativas, proteção de armazenamento, expiração ou rotação quando indicada pelo risco e histórico de reutilização conforme capacidade técnica.
- Autenticação multifator será obrigatória para acessos remotos, privilegiados, sistemas críticos e demais cenários definidos por risco.
- Suspeita de comprometimento deverá ser comunicada imediatamente e resultar em bloqueio ou troca da credencial.

11. Segurança de equipamentos, dispositivos e mídias

11.1 Localização e proteção

- Equipamentos serão inventariados, identificados, atribuídos a responsáveis e posicionados para reduzir acesso não autorizado e ameaças ambientais, incluindo incêndio, água, energia, temperatura, poeira, furto e dano.
- Áreas técnicas, racks, arquivos e equipamentos críticos terão acesso físico restrito e controles compatíveis com o risco.

11.2 Uso externo, remoto e dispositivos móveis

- Uso fora das instalações dependerá de autorização, termo de responsabilidade e configuração homologada.
- Dispositivos deverão utilizar bloqueio automático, criptografia quando aplicável, antimalware, firewall, atualizações, VPN ou canal seguro e gerenciamento central quando disponível.
- Perda, furto, dano ou suspeita de acesso indevido deverá ser comunicada imediatamente.
- É proibido armazenar dados institucionais em dispositivo pessoal sem autorização e controles formais.

11.3 Sanitização, reutilização e descarte

- Informações serão apagadas por método aprovado antes da reutilização, devolução, doação, manutenção externa ou descarte de equipamento e mídia.
- O descarte será rastreável e, quando terceirizado, acompanhado de cadeia de custódia e certificado de destruição ou sanitização.
- A área responsável validará a remoção de dados antes da baixa patrimonial ou transferência do ativo.

12. Mesa limpa, tela limpa e impressão segura

- Documentos confidenciais ou restritos não permanecerão expostos em mesas, salas, veículos, impressoras ou áreas compartilhadas.
- Telas serão bloqueadas sempre que o usuário se afastar e automaticamente após período de inatividade definido.
- Senhas, chaves, códigos e informações sensíveis não poderão ser deixados em papéis, quadros ou locais visíveis.
- Impressões sensíveis serão retiradas imediatamente e descartadas em recipiente/processo confidencial.
- Ao final da jornada, documentos e mídias serão guardados em local protegido; auditorias ambientais poderão verificar a conformidade.

13. Uso aceitável de recursos e comunicações

- Recursos corporativos destinam-se prioritariamente às atividades autorizadas da Mitri e devem ser utilizados com ética, legalidade e respeito.
- É proibido usar recursos para assédio, discriminação, ameaça, fraude, violação de direitos, instalação não autorizada, ataque, evasão de controle ou divulgação indevida.
- Links, anexos e solicitações suspeitas não deverão ser abertos ou atendidos; a ocorrência deverá ser comunicada pelo canal institucional.
- Informações serão compartilhadas somente com destinatários autorizados, na extensão necessária e por canal homologado.
- A Mitri poderá monitorar seus recursos de forma proporcional, transparente, autorizada e compatível com a legislação e as finalidades de segurança e continuidade.

14. Segurança do Prontuários e informações assistenciais

Prontuários em papel, meio eletrônico, áudio, vídeo, imagem, laudos, exames e informações mantidas em áreas assistenciais ou de apoio serão protegidos contra perda, furto, destruição, alteração, reprodução, divulgação e acesso não autorizados.

- O acesso será individual, restrito à necessidade assistencial, administrativa ou legal e compatível com o perfil autorizado.
- Cada entrada deverá preservar autoria, data, hora, integridade e autenticidade; correções ocorrerão por adendo ou mecanismo rastreável, sem apagamento indevido.
- Após autenticação, alterações deverão ser impedidas ou registradas em trilha de auditoria.
- Liberação de informações ou cópias ocorrerá somente a pessoas autorizadas, conforme procedimento, legislação, ordem válida e verificação de identidade.
- Prontuários deverão permanecer acessíveis aos profissionais autorizados, ser retidos pelo prazo aplicável e protegidos em todos os locais, inclusive áreas clínicas, arquivos, laboratórios, radiologia e ambientes de contingência.
- A presença, localização e informações pessoais ou de saúde do paciente não serão divulgadas sem fundamento e autorização aplicáveis

15. Gestão de terceiros e serviços terceirizados

A terceirização de processamento, hospedagem, suporte, armazenamento ou qualquer atividade com acesso a informações não transfere a responsabilidade da Mitri pela segurança.

- Terceiros serão avaliados antes da contratação e periodicamente, conforme criticidade e risco.
- Contratos definirão confidencialidade, finalidade, instruções, acesso, controles, logs, subcontratação, continuidade, auditoria, incidentes, privacidade, retenção, devolução, eliminação e encerramento do acesso.

- Mudanças relevantes, incidentes ou desempenho inadequado poderão gerar reavaliação extraordinária.
- Ao término do vínculo, acessos serão revogados e informações serão devolvidas, transferidas ou eliminadas conforme instrução e evidência.

16. Aquisição, desenvolvimento, mudanças e vulnerabilidades

- Sistemas, integrações, projetos, equipamentos e serviços novos ou alterados passarão por avaliação de segurança e privacidade antes da implantação.
- Requisitos de segurança serão definidos desde a concepção, incluindo acesso, logs, backup, continuidade, retenção, testes e tratamento de vulnerabilidades.
- Mudanças terão solicitação, avaliação de impacto, aprovação, teste, plano de retorno e evidência de implantação.
- Vulnerabilidades e correções serão priorizadas conforme risco; exceções dependerão de controle compensatório e aceite formal.

17. Backup, recuperação e retenção

- Sistemas, dados e informações relevantes serão armazenados em repositórios corporativos homologados e incluídos em escopo de backup compatível com sua criticidade.
- Backups serão protegidos contra acesso, alteração e destruição, segregados quando necessário e monitorados quanto ao sucesso e falhas.
- Retenção, frequência, RPO e RTO serão definidos com os proprietários dos processos e aprovados conforme criticidade.
- Falhas serão registradas, tratadas e escaladas; testes de restauração serão realizados periodicamente e documentados.
- Dados não deverão ser mantidos somente em equipamento local ou pessoal.

18. Gestão de continuidade de negócios

A Mitri manterá processo gerenciado de continuidade para reduzir interrupções e restaurar operações críticas em prazo aceitável após desastre, falha de segurança, indisponibilidade, perda de serviço, acidente ou ação deliberada.

- Realizar BIA e avaliação de riscos para identificar processos críticos, dependências, impactos e prioridades.
- Definir estratégias preventivas e de recuperação, responsáveis, recursos, contatos, comunicação, RTO, RPO e critérios de acionamento.
- Manter planos de contingência operacional, continuidade e recuperação de desastres para processos e serviços críticos.
- Realizar testes e simulações em periodicidade baseada no risco e, no mínimo, anualmente para cenários críticos.

- Registrar resultados, falhas, lições aprendidas, ações corretivas, aprovação e atualização dos planos.
- Em contingência assistencial, preservar segurança, confidencialidade, autoria e posterior reconciliação dos registros.

19. Capacitação e conscientização

- Todos os públicos abrangidos receberão orientação na admissão e reciclagem anual, com conteúdo proporcional ao papel e ao risco.
- Públicos críticos receberão capacitação específica sobre prontuário, dados de saúde, acessos privilegiados, incidentes, phishing, continuidade e responsabilidades.
- A eficácia será avaliada por teste, simulação, observação, auditoria ou indicador, e não somente por presença.
- A meta institucional é 100% do público obrigatório capacitado no prazo; atrasos exigirão regularização e escalonamento ao gestor.

20. Exceções, descumprimento e não retaliação

- Exceções dependerão de justificativa, prazo, análise de risco, controle compensatório, proprietário e aprovação na alçada competente.
- O descumprimento poderá resultar em medidas educativas, corretivas, disciplinares, contratuais, civis ou penais, respeitados os procedimentos aplicáveis.
- A comunicação de boa-fé de fragilidades, suspeitas ou incidentes é estimulada e não deverá gerar retaliação.

21. Controle de documentos e evidências

- Esta Política e seus documentos complementares deverão possuir identificação, versão, autor, proprietário, aprovação, vigência e histórico.
- Distribuição, acesso, recuperação, armazenamento, preservação, legibilidade, mudança, retenção e descarte serão controlados.
- Documentos externos necessários à operação serão identificados e mantidos atualizados.
- Versões obsoletas serão retiradas de uso ou claramente identificadas para impedir aplicação indevida.
- Evidências de conformidade serão protegidas contra alteração, perda e acesso não autorizado.

22. Vigência e revisão

Esta Política entra em vigor após aprovação e publicação no repositório oficial. Será revisada a cada 12 meses ou antes quando ocorrer alteração legal, regulatória, contratual, tecnológica ou organizacional relevante; mudança de serviço; incidente significativo; resultado de auditoria; alteração de risco; ou determinação da Diretoria.

Qualquer alteração deverá ser analisada, aprovada e registrada antes de entrar em vigor.

23. Referências bibliográficas

1. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 26 ago. 2026.

2. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Texto compilado. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 26 ago. 2026.

3. BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709/2018 para dispor sobre a proteção de dados pessoais e criar a Autoridade Nacional de Proteção de Dados. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 26 ago. 2026.

4. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Resolução CD/ANPD nº 19, de 23 de agosto de 2024. Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/assuntos-internacionais/transferencia-internacional-de-dados. Acesso em: 26 ago. 2026

Elaborado: André Trindade Neri de Mendonça Agosto/2026

Validado: Ingrid Uroz Silva COREN- SP: 604075 Agosto/2026

Validade Julho/2028