SSI-MAN001 MANUAL DO SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO (SGSI)

Copy of version 4.0 (approved and current)

Last Approval or Periodic Review Completed 19/03/2024

Next Periodic Review Needed On or Before 19/03/2025

Effective Date 19/03/2024

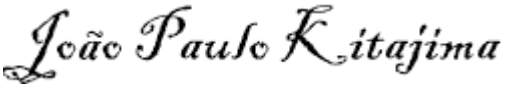
Controlled Copy ID 491097

Location Website corporativo

Organization MENDELICS ANALISE GENOMICA

Comments for version 4.0
Declaração de aplicabilidade passou para v3.0

Approval and Periodic Review Signatures

Type	Description	Date	Version	Performed By	Notes
Approval	Aprovação (2)	19/03/2024	4.0	Joao Paulo Kitajima	v3.0 da Declaração de Aplicabilidade
Approval	Aprovação (2)	13/03/2024	3.0	Joao Paulo Kitajima	Melhorias no manual considerando norma ISO 27001:2022
Approval	Aprovação (1)	13/03/2024	3.0	Bruno Felfoldi	
Approval	Aprovação (2)	12/02/2024	2.0	 Joao Paulo Kitajima	
Approval	Aprovação (1)	12/02/2024	2.0	Bruno Felfoldi	
Approval	Lab Director	30/10/2023	1.0	Fernando Kok MD	
Approval	Aprovação (2)	30/10/2023	1.0	Joao Paulo Kitajima	
Approval	Aprovação (1)	30/10/2023	1.0	Bruno Felfoldi	

Version History

Version	Status	Type	Date Added	Date Effective	Date Retired
4.0	Approved and Current	Major revision	19/03/2024	19/03/2024	Indefinite
3.0	Retired	Major revision	13/03/2024	13/03/2024	19/03/2024
2.0	Retired	Major revision	12/02/2024	12/02/2024	13/03/2024
1.1	Retired	Minor revision	16/11/2023	16/11/2023	12/02/2024
1.0	Retired	Initial version	30/10/2023	30/10/2023	16/11/2023

MANUAL DO SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO (SGSI)

1. Introdução

Este documento tem por objetivo apresentar a política e os requisitos referentes à gestão da Segurança da Informação (SI), formalizado como o Sistema de Gestão da Segurança da Informação (SGSI) da Mendelics. Serve de base para os outros documentos que implementam os procedimentos operacionais que atendem a estes requisitos e que estão alinhados com a política corporativa. A Mendelics adota como referência a norma ISO 27001:2022 ("*Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos*" / ano 2022) e a norma ISO 27002:2022 ("*Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação*" / ano 2022).

A adoção de um SGSI é uma decisão estratégica pois a Mendelics:

- processa dados e informações sensíveis;
- existe dentro de um mundo interconectado digitalmente; e
- está sujeita a uma legislação local e global relativa à preservação da privacidade de dados e informações.

Este manual não aborda um Sistema de Gestão da Privacidade da Informação (SGPI), normatizado pela ISO 27701 e que estende a norma ISO 27001.

2. Conceitos

Usamos como referência a base de conhecimento da IEC (*International Electrotechnical Commission*) para definir informação e dado:

- Informação: conhecimento sobre objetos, como fatos, eventos, coisas, processos ou ideias (incluindo conceitos) que, dentro de um determinado contexto, tem um significado particular;
- Dado: representação concreta de informações de maneira formalizada e adequada para processamento humano ou automático.

De uma maneira geral, serão usados estes dois conceitos juntos ou de maneira intercambiável, pois é objetivo alcançar o melhor nível de segurança para as informações e para os dados manipulados pela Mendelics. Além disto, ainda que predominantemente digitais, este documento deve contemplar também a segurança de dados e informações em outros meios físicos (por exemplo, papel).

Segundo a norma ISO 27001, a segurança dos dados e da informação depende de três propriedades que devem ser preservadas ao máximo (através dos requisitos apresentados neste documento):

- *Confidencialidade*: é uma propriedade a qual um dado confidencial e sua informação representada só podem ser *acessadas por entidades autorizadas*. A privacidade é um direito de uma entidade (normalmente uma pessoa ou uma organização), agindo em seu próprio nome, em determinar qual o grau da confidencialidade de suas informações privadas;
- *Integridade*: propriedade de dados e das informações representadas que *não devem ser alterados ou destruídos de maneira não detectada e não rastreável. Garante a precisão da informação/dado e evita que o dado seja corrompido.* A Mendelics inclui nesta propriedade a exatidão das informações e dados que representam fidedignamente uma realidade; e
- *Disponibilidade*: propriedade de um dado e sua informação representada *serem prontamente acessíveis e utilizáveis sob demanda por uma entidade autorizada*.

0 SGSI deve preservar a confidencialidade, a integridade e a disponibilidade da informação pela aplicação de um processo de ***gestão de riscos***, bem como fornecer

confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

3. Expectativas, Escopo e Política

3.1 A Mendelics

A Mendelics é um laboratório clínico privado brasileiro, de *site* único, com clientes no Brasil e no exterior, focado em testagem genômica (testagem genética baseada na identificação de parte ou de toda a sequência de DNA). Atende pessoas físicas, pessoas jurídicas e entes públicos. Serve de laboratório de apoio para outros provedores de saúde e envia parte de seus testes oferecidos para outros laboratórios de apoio.

Contexto:

- *A testagem genômica é uma atividade nova e de mercado promissor e global*, baseada em tecnologias de sequenciamento de DNA inovadoras e de ponta. O mercado da genômica está em ascensão e engloba tanto os grandes laboratórios clínicos bem estabelecidos que oferecem outros testes bioquímicos tradicionais bem como laboratórios de nicho, como a Mendelics;
- *Não existe uma regulamentação abrangente e unificada* que rege este tipo de atividade. Existe apenas uma regulamentação específica para laboratórios clínicos em geral (ANVISA RDC 786/2023) e uma lei específica para privacidade de dados, a Lei Geral de Proteção de Dados Pessoais (LGPD) nº 13.709/2018. Mesmo em países centrais, a testagem genômica não é uma atividade consolidada no âmbito regulatório;
- *Os dados manipulados pela Mendelics são sensíveis*, pois são dados de saúde de pacientes;
- A classe médica, de uma maneira geral, não conhece de forma aprofundada as tecnologias genômicas, seus benefícios e suas limitações. Este fenômeno também é de ordem global. Existe uma pressão de mercado a fim de formar mais especialistas nesta área: o advento da Medicina Personalizada ou de Precisão, que depende de profissionais proficientes em genômica. A sociedade como um todo também não está familiarizada com a tecnologia genômica, seus objetivos e limitações. *A oferta de mão-de-obra especializada, necessária para o diagnóstico molecular, é limitada*;

- Dada a crescente demanda em volume e qualidade, *a genômica tem exigido processos escaláveis de diagnóstico*, através da automação de seus processos, bem como do emprego de técnicas baseadas em Inteligência Artificial (IA). Os testes genômicos envolvem, para cada exame, a geração de uma quantidade excepcional de dados ("*big data*"). A oferta de testes genômicos somente foi possível também com os avanços da Bioinformática e da computação distribuída (por exemplo, através das tecnologias de nuvem). A alta escala resulta em uma redução significativa do custo, da complexidade e do tamanho dos equipamentos e dos insumos necessários para a realização de testes genômicos. O resultado é um teste acessível para o paciente;
- *A tecnologia laboratorial para a implementação de testes genômicos é importada dos países centrais*. Alguns insumos podem ser fabricados em solo nacional, mas a tecnologia embarcada foi desenvolvida em solo estrangeiro. Por outro lado, existe competência nacional de alta qualidade na área de desenvolvimento de software bioinformático e análise de dados clínicos;
- *Aumento da criminalidade digital*, exemplificada pelas invasões a sistemas corporativos de informação, acessos não autorizados, assunção criminal de identidade de terceiros, solicitação de resgate de dados através de chantagem e outras ações que ferem intencionalmente a confidencialidade, a integridade e a disponibilidade dos dados e informações.

Como uma corporação e, dado o contexto acima, a Mendelics se apresenta como uma empresa inovadora, baseada em processos eficientes, com foco na acessibilidade dos testes genéticos (custos suportáveis para os clientes e uma coleta simplificada de amostra). A Mendelics tem como missão "Tornar o diagnóstico genético rápido, preciso e acessível para todos que precisam", como visão "ser uma das principais referências mundiais em diagnóstico e interpretação genômica" e como valores: ética, seriedade, honestidade, confiabilidade, comprometimento, dedicação, acessibilidade, precisão, eficiência e inovação. A cultura organizacional está focada em comunicação, disponibilidade e foco na resolução de problemas. Conta com uma estrutura hierárquica enxuta, baseada no processo central laboratorial e nas atividades de suporte (ex. administrativo).

É importante ressaltar que a Mendelics, por ser um estabelecimento de saúde humana, faz parte do ecossistema da tutela da saúde. A tutela da saúde é um Direito Fundamental previsto pela Constituição Federal de 1988. Assim, quando for necessária a realização de um procedimento a fim de proteger a saúde de um indivíduo, poderão ser utilizados os dados dele mediante essa justificativa.

3.2 Necessidades e Expectativas das Partes Interessadas

As partes interessadas (relevantes) abordadas pelo SGSI e sua política são:

- Os clientes da Mendelics, sejam pessoas físicas ou jurídicas, incluindo empresas parceiras. Requisitos relevantes ao SGSI: confidencialidade, disponibilidade e integridade;
- Todos os colaboradores, sejam contratados ou autônomos, presenciais ou remotos, ou colaboradores de empresas terceirizadas atuando internamente na Mendelics. Requisitos relevantes ao SGSI: confidencialidade, disponibilidade e integridade;
- Familiares dos colaboradores e terceirizados residentes. Requisitos relevantes ao SGSI: confidencialidade;
- Os acionistas e membros do Conselho de Administração. Requisitos relevantes ao SGSI: confidencialidade;
- Os fornecedores terceirizados de insumos e de serviços. Requisitos relevantes ao SGSI: confidencialidade;
- Os que visitam esporadicamente a Mendelics, como convidados, ou regularmente, como os auditores. Requisitos relevantes ao SGSI: confidencialidade;
- Os entes reguladores, certificadores, acreditadores e governamentais que têm relação formal com a Mendelics ou que a Mendelics possua dependência regulatória direta. Requisitos relevantes ao SGSI: confidencialidade, disponibilidade e integridade;
- A mídia. Requisitos relevantes ao SGSI: confidencialidade e integridade;
- Serviços de emergência (por exemplo, Corpo de Bombeiros, Polícia, SAMU). Requisitos relevantes ao SGSI: confidencialidade, disponibilidade e integridade;
- Qualquer indivíduo que contacte a Mendelics por alguma razão específica (a população em geral). Requisitos relevantes ao SGSI: confidencialidade e integridade.

Quem manipula legalmente alguma informação ou dado da ou sobre a Mendelics é parte interessada do SGSI.

A expectativa do SGSI é que a manipulação de qualquer dado ou informação pela parte interessada seja realizada respeitando os requisitos necessários de confidencialidade,

integridade e disponibilidade. Esta expectativa é igualmente compartilhada pela parte interessada.

3.3 Escopo

O escopo do SGSI são as instalações físicas da organização, bem como os ativos de informação, incluindo equipamentos, software, dados e outros recursos relativos à tecnologia de informação. Conforme SSI-FOR002 Declaração de Aplicabilidade v3.0.

São considerados relevantes neste escopo:

- A parte interessada como definida anteriormente;
- Todos os processos que envolvem uma manipulação de dados ou de informações;
- Dados e informações digitais ou em qualquer outro meio manipulados pela Mendelics;
- A propriedade intelectual gerada pela Mendelics e que inclui software, marcas e processos;
- Os meios de comunicação proprietários utilizados pela Mendelics, em especial as redes digitais;
- As instalações físicas da organização, bem como os ativos privados (próprios) de informação, incluindo equipamentos e quaisquer outros recursos relativos à tecnologia de informação.

O escopo do SGSI se alinha com o escopo de negócio e operacional da Mendelics. Todos os departamentos e áreas fazem parte do escopo do SGSI, bem como o único *site* no qual a Mendelics opera.

Estão excluídos do escopo, pela impossibilidade de controle direto, mas sujeitos ao monitoramento e auditoria, quando possível:

- A Internet;
- Os dispositivos privados não proprietários da Mendelics que os colaboradores usam remotamente;
- A infra-estrutura física (por exemplo, servidores e redes) dos provedores de tecnologia em nuvem (*cloud*).

Os elementos relevantes não cobertos pelo escopo do SGSI devem ser, todavia, adequadamente identificados e considerados na gestão de riscos do SGSI.

Como a Mendelics utiliza serviços de tecnologia da informação baseados em nuvem (*cloud*), é importante caracterizar o *uso* desta nuvem para avaliar o escopo do SGSI. A Mendelics utiliza provedores na nuvem segundo dois modelos:

- *Platform as a Service (PaaS)*: além da infra-estrutura e serviços associados (por exemplo, *backup*), o provedor oferece ambientes de desenvolvimento para os desenvolvedores internos da Mendelics (por exemplo, sistemas operacionais, ambientes de programação para diversas linguagens, sistemas de gestão de banco de dados, etc.). Os exemplos de provedores de nuvem para a Mendelics que se enquadram neste modelo são a Google e a Amazon;
- *Software as a Service (SaaS)*: o provedor oferece a solução completa de software, hardware e gestão de dados. O exemplo de provedor de nuvem para a Mendelics e que se enquadra neste modelo é a Totvs (aplicativo Protheus).

Em ambos os modelos, os dados processados e armazenados sempre fazem parte do escopo do SGSI. Para os casos dentro do modelo PaaS, os aplicativos desenvolvidos também fazem parte do escopo do SGSI. Por outro lado, como elencado anteriormente, os equipamentos na nuvem não fazem parte do escopo do SGSI da Mendelics.

3.4 Política

A organização deve estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão da Segurança da Informação (SGSI), através de processos com compliance e alinhados com as melhores práticas. As informações e dados (principalmente os sensíveis) devem ser tratados com o grau devido de confidencialidade, de integridade e de disponibilidade exigido legalmente. A privacidade dos dados de pacientes deve ser integralmente respeitada, assim como toda informação estratégica da companhia.

A política da segurança da informação deve:

- estar disponível como informação documentada;
- ser comunicada dentro da organização;
- estar disponível para a parte interessada, conforme apropriado;

- possuir um guardião que garanta a sua revisão.

Uma declaração da alta administração deve ser emitida como forma de endossar a política definida e adotada pela Mendelics. A mesma também deve estar disponível como informação documentada, ser comunicada dentro da organização, estar disponível para a parte interessada, conforme apropriado e possuir um guardião que garanta a sua revisão. O guardião da política é o responsável corrente pelo SGSI especificado no formulário SSI-FOR001.

4. Liderança

O envolvimento direto e constante da liderança é fator fundamental para o sucesso do SGSI.

4.1 Liderança e Comprometimento

A Alta Direção deve demonstrar sua liderança e comprometimento em relação ao SGSI pelos seguintes meios:

- assegurando que a política de segurança da informação e os objetivos da segurança da informação estejam estabelecidos e sejam compatíveis com a direção estratégica da organização;
- assegurando a integração dos requisitos do SGSI nos processos da organização;
- assegurando que os recursos necessários para o SGSI estejam disponíveis;
- comunicando a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do SGSI;
- assegurando que o SGSI alcance seus resultados pretendidos;
- orientando e apoiando os envolvidos a contribuir para a eficácia do SGSI;
- promovendo a melhoria contínua; e
- apoiando outros papéis relevantes da gestão para evidenciar como sua liderança se aplica às áreas sob sua responsabilidade.

A declaração a ser emitida pela alta gestão reforça o compromisso da alta gestão com estas ações.

4.2 Papéis, Responsabilidades e Autoridades

- Responsável legal oficial: CEO (Diretor Presidente);
- Encarregado pelo tratamento de dados pessoais: CEO (Diretor Presidente);
- Responsável pelo SGSI: Diretor da Área da Qualidade;
- Equipe de desenvolvimento, implementação e manutenção do SGSI com responsabilidades e autoridades operacionais (Equipe Operacional):
    - Responsável pela área da Tecnologia da Informação;

- Responsável pela área da Infra-estrutura;
- Responsável pela área da Qualidade;
- Responsável pela área de Recursos Humanos.

O responsável pelo SGSI tem como responsabilidade assegurar que o mesmo esteja em conformidade com os requisitos deste documento bem como relatar sobre o desempenho do SGSI para a Alta Direção.

Papéis, responsabilidades e autoridades devem ser divulgados, pelo menos uma vez por ano, para a equipe através dos canais digitais internos de comunicação.

5. Planejamento

5.1 Objetivos do Planejamento

O SGSI deve alcançar os seguintes objetivos:

- Garantir a devida confidencialidade dos dados manipulados;
- Garantir a devida integridade dos dados manipulados;
- Garantir a devida disponibilidade dos dados manipulados.

Ao realizar o planejamento do SGSI a fim de atingir estes objetivos e estar alinhado com a política estabelecida, a Mendelics deve:

- Assegurar que o SGSI alcance os objetivos pretendidos;
- Prevenir ou reduzir os efeitos indesejados;
- Alcançar a melhoria contínua;
- Planejar as ações para abordar riscos e oportunidades; e
- Avaliar a eficácia destas ações.

O planejamento eficaz de um SGSI passa obrigatoriamente por uma *gestão de riscos*, conforme discutido na norma ISO 27001 e pelo pleno atendimento aos requisitos desta norma.

5.2 Avaliação e Tratamento dos Riscos de Segurança da Informação

Um SGSI adequado depende de uma correta avaliação e procedimentos de tratamento dos riscos. Os riscos devem ser identificados e devidamente gerenciados.

Considera-se um risco, dentro do que foi definido como objetivos, quando:

- quebra-se o compromisso de garantir o direito à privacidade ou se divulga informação confidencial;
- compromete a fidelidade/fidedignidade dos dados e das informações;
- interfere negativamente na disponibilidade dos dados e informações.

Uma análise crítica dos riscos de segurança da informação deverá ser realizada anualmente, documentada em separado ou em conjunto com a análise crítica feita pela diretoria. Deve ser realizada pela equipe operacional do SGSI (vide item 4.2) e validada pela alta direção. Deve ainda manter uma coerência dos resultados apresentados (sendo comparáveis, válidos e consistentes - sempre que possível, quantitativos). Deve fazer parte do processo de gestão de riscos da Mendelics, processo este gerenciado pela área da Qualidade.

5.3 Metodologia

A metodologia utilizada pela Mendelics para alcançar os objetivos listados anteriormente deve levar em conta:

- consistência com a política do SGSI;
- mensurabilidade;
- os requisitos aplicáveis, avaliação e tratamento dos riscos;
- o monitoramento dos objetivos;
- a comunicação dos objetivos;
- a atualização dos mesmos;
- a documentação;
- os recursos disponíveis;
- os responsáveis;
- os prazos;
- a avaliação da eficácia.

O documento central interno do SGSI é o SSI-FOR001 que contém:

- *link* para a lista de riscos, avaliação e tratamento (plano) (SSI-FOR003), alinhada com as ferramentas disponíveis para a gestão de risco da Mendelics;
- a lista de requisitos (ou controles) aplicáveis;
- *link* para a declaração de aplicabilidade que deve conter informações sobre os controles como status do controle e justificativas de inclusão/exclusão de controles (SSI-FOR002);
- a formalização das informações instanciadas da política como nome de responsáveis, detalhes do escopo e formas de contato com a equipe responsável pelo SGSI;
- a lista de indicadores usados para mensurar os objetivos e as metas esperadas;
- interações possíveis dentro da parte interessada;

- política de classificação de dados e informações;
- registro de ações de melhoria.

Os documentos da gestão de risco devem também ser assinados digitalmente de modo que os proprietários dos riscos aprovem o plano de tratamento de riscos da SI e aceitem os riscos residuais, se porventura existirem.

O documento SSI-FOR003 é de uso interno ao SGSI, mas o documento final oficial para a gestão de riscos na Mendelics, inclusive riscos de SI, é o REG-DOC002 Mapa de Processos e Gestão de Riscos. A gestão de riscos de SI adota os mesmos processos do SGQ (Sistema de Gestão da Qualidade) especificados no REG-MAN009 Manual da Gestão de Riscos.

O SGSI trabalha junto com o SGQ em relação aos seguintes processos:

- Gestão de riscos;
- Não conformidades;
- Melhoria contínua;
- Indicadores de qualidade; e
- Auditoria Interna e Análise Crítica.

O SGSI segue os mesmos procedimentos corporativos gerais para os processos acima.

5.4 Vulnerabilidades e Monitoramento Automatizado

Vulnerabilidades são fraquezas de um ativo ou de um controle que pode ser explorado por uma ou mais ameaças. Está diretamente associado a um conjunto de riscos e portanto deve ser gerenciado dentro da mesma sistemática adotada para a gestão corporativa de riscos.

Mitigar as vulnerabilidades depende de ferramentas automatizadas para o monitoramento de atividades e tráfego digital. As ferramentas mais eficazes são oferecidas por terceiros. A política atual da Mendelics é não adotar ferramentas sem antes avaliar detalhadamente os riscos envolvidos. O tratamento de uma vulnerabilidade pode gerar um problema ao invés de resolvê-lo, ao delegar para terceiros atividades de alto risco para a segurança da informação.

Ambientes, ferramentas e programas de gestão da vulnerabilidade precisam ser analisados caso a caso. Um relatório final precisa ser redigido e aprovado pela Diretoria.

5.5 Planejamento de Mudanças

Quando a organização determinar as necessidades para as mudanças do SGSI, estas mudanças devem ser conduzidas de uma forma planejada. O Responsável pelo SGSI deve preparar uma proposta e aprovar com os demais envolvidos.

6. Recursos e Competência

6.1 Recursos

Os recursos necessários para estabelecer, implementar, manter e melhorar continuamente o SGSI devem ser determinados anualmente na orçamentação realizada no último trimestre do ano fiscal. Deve ser documentada em planilha, negociada e aprovada em Diretoria como todos os outros itens orçamentários.

6.2 Competências

O SGSI, em colaboração com a área de Recursos Humanos, deve identificar, para cada cargo existente na Mendelics, as competências necessárias que os colaboradores devem possuir e que afetem o desempenho do SGSI.

Estas competências estão associadas às áreas gestoras do SGSI, a saber:

- Tecnologia da Informação;
- Infraestrutura;
- Qualidade & Regulatório;
- Direito Jurídico.

A certificação documentada destas competências é baseada em:

- Currículo;
- Avaliação do treinamento de pessoal;
- Avaliação do desempenho de pessoal;
- Resultados alcançados.

Treinamentos complementares devem ser regularmente realizados e, quando possível, uma análise crítica da equipe de operação do SGSI deve ser realizada anualmente para, entre outros pontos, avaliar a eficácia das ações tomadas e dos treinamentos realizados.

A gestão da avaliação da competência deve ser um processo contínuo e documentado pela área de Recursos Humanos e Qualidade.

6.3 Conscientização e Comunicação

Todo o corpo de colaboradores deve conhecer a política do SGSI definida neste documento, sua contribuição para a eficácia do SGSI e o impacto das não conformidades associadas ao SGSI. A conscientização ocorre:

- no momento da contratação do colaborador;
- em ações regulares promovidas pela equipe do SGSI;
- em mensagens de efeito nos canais de comunicação digitais.

Em relação à comunicação, a equipe do SGSI deve definir, interna e externamente, o que comunicar, quando comunicar, com quem comunicar e como se comunicar.

A planilha SSI-FOR001 deve conter abas que registrem as ações e eventos de conscientização e comunicação.

O staff deve ser treinado em Segurança da Informação e Privacidade no mínimo uma vez por ano.

6.4 Informação Documentada

O planejamento e registros do SGSI devem ser documentados na planilha SSI-FOR001. Os documentos gerados seguem as regras estabelecidas para a gestão de documentos na Mendelics. Outros documentos adicionais podem ser criados para complementar as informações presentes no SSI-FOR001.

6.5 Contatos com Grupos de Interesse Específico em SI

Para uma atualização periódica e *on-line* sobre SI e assegurar que ocorra o fluxo adequado de informações relacionadas a segurança da informação, o processo atual na Mendelics é o cadastramento voluntário dos colaboradores nas listas news@securityweek.com (internacional) e contato@cisoadvisor.com.br (nacional). É sugerido também seguir o Instagram da ANPD (Autoridade Nacional de Proteção de Dados) do Governo Brasileiro (gov.br).

7. Operação

A operação do SGSI deve ser realizada pela equipe operacional descrita neste documento. Deve colocar em prática os pontos levantados anteriormente:

- realizar o planejamento segundo especificado;
- avaliar e tratar os riscos envolvidos na SI;
- planejar e avaliar os recursos e competências envolvidas;
- conscientizar, comunicar e documentar.

O documento central desta operação é o SSI-FOR001.

A gestão de toda exceção relativa aos procedimentos ou políticas do SGSI devem envolver toda ou parte da diretoria. O procedimento desta gestão depende da exceção e, independente da mesma, a documentação escrita deve ser gerada para registro e acompanhamento.

8. Avaliação de Desempenho

8.1 Monitoramento, Medição, Análise e Avaliação

A organização deve documentar na planilha REG-FOR002:

a) o que precisa ser monitorado e medido, incluindo controles e processos da SI;
b) os métodos para monitoramento, medição, análise e avaliação, conforme aplicável, para assegurar resultados válidos;
c) quando o monitoramento e a medição devem ser realizados;
d) quem deve monitorar e medir;
e) quando os resultados do monitoramento e da medição devem ser analisados e avaliados;
f) quem deve analisar e avaliar estes resultados.

A planilha REG-FOR002 é gerenciada pelo SGQ. Algumas informações sobre o monitoramento também se encontra no formulário SSI-FOR001.

8.2 Auditoria Interna

A organização deve conduzir auditorias internas no mínimo anualmente para prover informações sobre se o SGSI:

a) está em conformidade com a política e objetivos organizacionais e com os requisitos apresentados neste documento;
b) está efetivamente implementado e mantido.

A programação e o planejamento da auditoria interna devem ser realizados dentro da programação e do planejamento da auditoria interna realizada pela equipe da garantia da Qualidade na Mendelics. Os requisitos são os mesmos das auditorias internas de outras áreas da organização:

a) definir os critérios e o escopo da auditoria, para cada auditoria;
b) selecionar auditores e conduzir auditorias que assegurem objetividade e imparcialidade do processo de auditoria;

c) assegurar que os resultados das auditorias sejam relatados para a gestão pertinente.

A alta direção deve analisar criticamente o SGSI da organização no mínimo anualmente, para assegurar a sua contínua adequação, pertinência e eficácia. Esta análise crítica deve incluir considerações em relação a:

a) situação das ações de análises críticas anteriores;
b) mudanças nas questões internas e externas que sejam relevantes para o SGSI;
c) mudanças nas necessidades e expectativas das partes interessadas que sejam relevantes para o SGSI;
d) *feedback* sobre o desempenho do SGSI, incluindo tendências para não conformidades e ações corretivas, resultados da medição e monitoramento, resultados de auditorias e cumprimento dos objetivos do SGSI;
e) *feedback* das partes interessadas;
f) resultados da avaliação dos riscos e situação do plano de tratamento de riscos;
g) oportunidades para a melhoria contínua.

Os resultados da análise crítica pela Direção devem incluir decisões relativas às oportunidades para melhoria contínua e quaisquer necessidades de mudanças do SGSI. A informação documentada (SSI-FOR001) deve ser disponibilizada como evidência dos resultados das análises críticas pela Direção.

9. Melhoria Contínua e Não Conformidade

A organização deve melhorar continuamente o seu SGSI em sua integralidade em todos os pontos abordados neste documento. Quando a não conformidade ocorre, a organização deve:

a) reagir a não conformidade e, conforme apropriado tomar ações para controlá-la e corrigi-la e lidar com as consequências;
b) avaliar a necessidade de ações para eliminar as causas de não conformidade e evitar sua repetição ou ocorrência em outro lugar, através de uma análise crítica;
c) implementar quaisquer ações necessárias;
d) analisar criticamente a eficácia de quaisquer ações corretivas tomadas;
e) realizar mudanças no SGSI, quando necessário.

As ações corretivas devem estar alinhadas aos efeitos das não conformidades encontradas. Documentação deve estar disponível como evidência da natureza das não conformidades e quaisquer ações subsequentes tomadas e com os resultados de qualquer ação corretiva.

10. Requisitos Legais, Estatutários, Regulamentares e Contratuais

A Mendelics deve atender a todos os requisitos legais, estatutários, regulamentares e contratuais, independentes se pertinentes ou não à segurança da informação. A lista destes requisitos, sua documentação e manutenção é apresentada no SSI-FOR001. O objetivo é assegurar *compliance*, evitando interrupção do negócio, passivos jurídicos, problemas de imagem e o funcionamento inadequado da corporação.

11. Considerações Finais e Documentos Correlatos

Este documento está alinhado com os requisitos da norma ISO 27001:2022. Qualquer observação ou dúvida sobre o mesmo, entrar em contato através dos seguintes endereços eletrônicos: contato@mendelics.com.br, dados@mendelics.com.br e infosec@mendelics.com.br ou pelo canal interno Slack #infosec. A área de Recursos Humanos pode ser acionada também, por exemplo, se o colaborador necessitar de confidencialidade no contacto.