

## Sistema de Gestão de Segurança da Informação

# Checklist do projeto de implementação de um SGSI

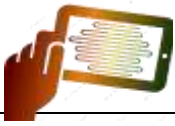
### Orientação prática para implementar um SGSI conforme a ISO/IEC 27001

#### Definição, justificativa, delimitação de escopo e planejamento do projeto

- Estude as normas em profundidade: faça um treinamento de implementador líder (lead implementer), se possível.
  - Estude o negócio em profundidade para entender seus objetivos, estratégias, cultura, governança, a gestão de riscos de informação e de segurança já existente, *etc.*
- Se a organização tiver uma abordagem definida e estruturada para esta fase, use-a!
- Elabore um business case que identifique e promova os benefícios de negócio do SGSI.
  - Olhe além de “segurança” e “conformidade” *por exemplo*: ajudar a gestão a administrar riscos do negócio, apoiar/viabilizar outras iniciativas e estratégias empresariais.
  - Identifique, explore e detalhe um conjunto amplo de objetivos de negócio relacionados a: gestão de riscos e segurança da informação; controles de segurança da informação, cibernéticos, manuais e automatizados; conformidade e validação; resiliência; boas práticas, maturidade; eficiência, custo-efetividade *etc.*
  - Esclareça as prioridades relativas desses objetivos *por exemplo* classificando todos ou agrupando-os em categorias como “essencial”, “importante”, “bom ter” e talvez “a evitar”.
  - Seja honesto sobre as mudanças organizacionais/de governança que virão, incluindo a potencial disrupção, os custos e os prazos.
- Seja realista quanto a recursos, prioridades e capacidades.
- Inclua mais do que folga/contingência suficiente para lidar com dificuldades imprevistas.
  - Apresente um “modelo” de opção de não fazer nada (straw man) e alternativas, conforme apropriado *por exemplo*: diferencie objetivos essenciais, importantes e opcionais; compare custos e benefícios de diferentes escopos de ISMS.

#### Aprovação do projeto

- Não espere que o business case se venda sozinho, por mais empolgante e positivo que pareça.
  - “Venda” a ideia à gestão: socialize o material, colete feedback e ajuste a proposta.
- Identifique, explore e trate preocupações reais, especialmente impedimentos (blockers).
- Busque oportunidades de alinhamento com estratégias corporativas e outras iniciativas.



- Refine os objetivos e a proposta do projeto, adicionando detalhes explícitos quando isso trazer (ou exigir) clareza *por exemplo*: métricas.
- Enquanto aguarda a aprovação, continue trabalhando no planejamento e, idealmente, avançando nos aspectos essenciais, como a avaliação de riscos de informação.
- Seja absolutamente claro sobre o que é essencial e só negocie em outras áreas, mesmo que isso signifique que o projeto seja recusado ou adiado.

### Atividades de implementação

- Mire baixo, acerte alto: foque intensamente no que é essencial e avance em outros objetivos com menor prioridade/urgência, se houver recursos.
- Sempre que possível, reutilize conteúdo, políticas, procedimentos e controles já existentes, *etc.*, adaptando conforme necessário.
- Colabore de perto com equipes/funções/organizações/indivíduos relacionados.
- Trabalhe para desenvolver (up-skill) a equipe central por meio de treinamento, mentoria e experiência no trabalho.
  - Comece a operar elementos do SGSI assim que for praticável, praticando e refinando-os e, idealmente, contabilizando os benefícios obtidos (financeiros ou não).
  - Busque vitórias rápidas e divulgue-as: feedback positivo é inestimável para motivação e energia.

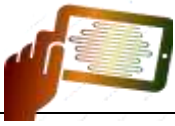
### Gestão do projeto, supervisão, reporte de progresso e gestão de riscos do projeto

Se a organização tiver um método/abordagem de gestão de projetos, use-o!

- Trabalhe com gerentes experientes de programas e projetos.
  - Estabeleça arranjos de governança adequados (*por exemplo*: estrutura, reportes, métricas, aprovações) para o projeto, pois isso evoluirá para a governança do SGSI no devido tempo.
  - “Dê um passo para frente e dois para trás”: identifique e trate riscos/problemas/retrocessos, aproveitando e promovendo oportunidades para avançar.
  - Acompanhe o caminho crítico e tudo o que consome (ou pode consumir) suas contingências, com muita atenção.
  - Cuidado com estresse e burnout: não ultrapasse cargas de trabalho razoáveis por longos períodos, incluindo a sua.
  - Invista em comunicações claras e relacionamentos eficazes: isso vai durar além da fase de implementação.

### Certificação e outras atividades de asseguarção

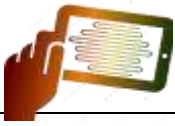
- Encare a certificação como uma oportunidade de melhoria, mais do que como um obstáculo a superar.



- Reserve tempo para esclarecer objetivos, identificar fornecedores e contratar organismos certificadores.
  - Especifique auditores de certificação experientes e competentes, prevendo menos desgaste e mais valor agregado.
  - Organize os pré-requisitos da certificação, como documentação do SGSI concluída, registros de atividades, auditorias internas do SGSI *etc.*
  - Prepare a gestão para entender o propósito e o valor da garantia relacionada ao SGSI, à gestão de riscos e segurança da informação, à conformidade *etc.*
  - Prepare o marketing para divulgar a certificação, fortalecendo marcas corporativas, abrindo novas oportunidades de negócios *etc.*
  - Coordene de perto a comunicação entre a equipe, a gestão e o organismo certificador no período que antecede a certificação, mantendo alinhamento e expectativas.
- Olhe além do certificado em si: sempre há mais a fazer e mais planejamento necessário *por exemplo*: integração com outros sistemas de gestão.

#### **Transição para a operação normal (business-as-usual)**

- Planeje uma construção e implementação do SGSI gradual, sequencial/em partes, em vez de um “big bang”.
- Comece a *usar* essas políticas, procedimentos, métricas, relatórios *etc.* assim que estiverem disponíveis: inevitavelmente leva tempo para descobrir e “alinhar” as arestas e integrar tudo em um sistema de gestão coerente e autossustentável; portanto, isso constitui “oportunidades de melhoria”.
- Mantenha a comunicação dentro e fora da equipe, extraíndo mais valor das métricas por meio de feedback motivacional, direcionamento e repriorização.
- Torne-se cada vez mais focado no negócio e no ambiente externo à medida que o SGSI entra na rotina, sem negligenciar a equipe e as necessidades individuais.



## Direitos autorais



Este trabalho está protegido por direitos autorais © 2024, IsecT Limited, com alguns direitos reservados. Ele está licenciado sob a licença [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 License](https://creativecommons.org/licenses/by-nc-sa/4.0/). Você pode reproduzir, circular, utilizar e criar obras derivadas a partir deste material, desde que: (a) ele não seja vendido nem incorporado a um produto comercial; (b) a devida atribuição seja feita à SecAware ([www.SecAware.com](http://www.SecAware.com)), e (c) caso seja compartilhado, as obras derivadas sejam compartilhadas sob os mesmos termos deste material.

## Isenção de responsabilidade

Este é um checklist genérico de exemplo. Ele não foi concebido para atender a todas as organizações e circunstâncias. Seu conteúdo tem caráter apenas orientativo. Acesse [www.SecAware.com](http://www.SecAware.com) para o texto completo de 39 páginas [Pragmatic ISMS implementation guideline](#), que explica e detalha, cláusula por cláusula, a ISO/IEC 27001 — em essência, nossa versão da [ISO/IEC 27003](#).