ISO 27001 – Estrutura e Escopo

1. Estrutura e Escopo da ISO 27001

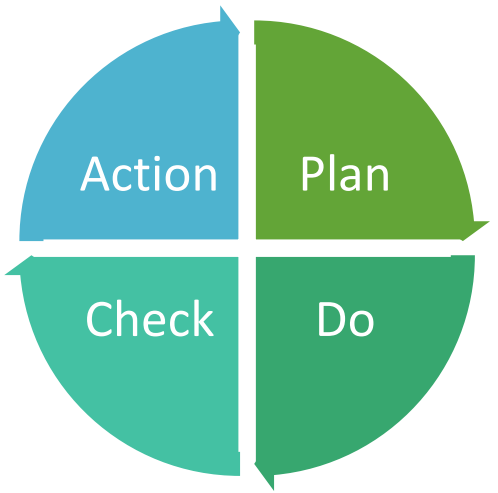
A ISO/IEC 27001 é a principal norma internacional de Segurança da Informação, responsável por estabelecer requisitos para criar, implementar, manter e melhorar continuamente um Sistema de Gestão da Segurança da Informação (SGSI).

Ela garante que as organizações tenham processos estruturados para proteger seus ativos de informação contra ameaças internas e externas, sempre buscando melhoria contínua.

Estrutura da ISO 27001

A norma é organizada em torno do ciclo de melhoria contínua PDCA (Plan – Do – Check – Act), também utilizado em normas como a ISO 9001 (Qualidade) e a ISO 14001 (Meio Ambiente).

Importante: o SGSI não é algo estático. O ambiente de ameaças evolui (novos ataques, novas tecnologias) e a empresa precisa ajustar constantemente suas práticas.



Estrutura da ISO 27001

Plan (Planejar)

- Definir políticas e objetivos de segurança da informação.
- Mapear ativos e identificar riscos (ameaças e vulnerabilidades).
- Estabelecer quais controles de segurança devem ser aplicados.

Do (Executar)

- Colocar em prática os controles, processos e políticas definidos.
- Exemplo: implantar políticas de acesso, criar planos de backup, treinar colaboradores.

Check (Verificar)

- Monitorar, medir e revisar o desempenho do SGSI.
- Realizar auditorias internas para avaliar se os controles funcionam corretamente.

Act (Agir / Melhorar)

- Corrigir falhas encontradas e atualizar controles.
- Garantir a melhoria contínua do sistema.

Escopo da ISO 27001

O escopo é um dos primeiros passos na implementação da norma. Ele define até onde o SGSI vai atuar dentro da organização.

O que o escopo determina:

- Quais áreas, processos e unidades organizacionais serão cobertos.
- Quais ativos de informação estão protegidos (documentos, sistemas, banco de dados, infraestrutura, etc.).
- Limites físicos e lógicos do SGSI.

Características do escopo:

- Deve ser claro, documentado e justificado.
- Deve considerar as necessidades do negócio e as exigências legais, regulatórias e contratuais.
- Pode ser restrito (focado em uma área ou processo) ou abrangente (cobrindo toda a organização).

Escopo da ISO 27001

Exemplos práticos de escopo:

- 1. Uma clínica médica define o escopo como: “Proteção dos registros eletrônicos de pacientes e sistemas de gestão hospitalar”.
- 2. Um banco define o escopo como: “Infraestrutura de datacenter e sistemas de internet banking”.
- 3. Uma universidade pode restringir o escopo ao “Departamento de TI responsável pelo sistema acadêmico online”.

2. Termos Fundamentais

Ao estudar a ISO/IEC 27001 é essencial compreender alguns conceitos básicos que sustentam todo o processo de gestão da segurança da informação. Esses termos são usados constantemente na norma e na prática de gestão de riscos.

Ativo de informação

- Um ativo de informação é tudo aquilo que possui valor para a organização e que precisa ser protegido. Não se limita a dados em formato digital, mas inclui também documentos em papel, equipamentos, infraestrutura tecnológica, softwares, processos, reputação da empresa e até mesmo o conhecimento e a experiência das pessoas. Se a perda, alteração ou divulgação indevida desse ativo puder causar prejuízo ao negócio, ele deve ser tratado como ativo de informação.

Ameaça

- Ameaça é qualquer causa potencial capaz de provocar um incidente indesejado contra um ativo. As ameaças podem ser naturais (enchentes, incêndios), acidentais (falhas humanas, erro de configuração) ou intencionais (ataques cibernéticos, espionagem). Uma ameaça não garante que o incidente ocorrerá, mas representa a possibilidade de ocorrência.

2. Termos Fundamentais

Vulnerabilidade

- Vulnerabilidade é uma fragilidade ou falha que pode ser explorada por uma ameaça para causar dano a um ativo. Pode estar presente em sistemas (como softwares desatualizados), em processos (como falta de políticas claras), em pessoas (como ausência de treinamento) ou em aspectos físicos (como portas destrancadas em áreas críticas).

Risco

- O risco surge da combinação entre uma ameaça e uma vulnerabilidade. Representa a probabilidade de que um incidente ocorra e o impacto que isso pode gerar para a organização. Assim, mesmo uma ameaça séria pode não representar alto risco se não houver vulnerabilidades associadas, enquanto uma vulnerabilidade grave pode ser menos preocupante se não houver ameaça que a explore. A gestão de riscos busca avaliar essa relação e priorizar o tratamento adequado.

Controles

- Controles são medidas adotadas para reduzir os riscos a níveis aceitáveis para a organização. Eles podem ser administrativos (políticas, normas internas), técnicos (firewalls, antivírus, criptografia) ou físicos (travas, câmeras de vigilância, barreiras de acesso). A escolha dos controles deve estar alinhada aos riscos identificados e ao nível de proteção exigido para os ativos de informação.

3. Sistema de Gestão da Segurança da Informação (SGSI)

O Sistema de Gestão da Segurança da Informação (SGSI) é o conjunto de políticas, processos, procedimentos e controles implementados em uma organização para garantir que os ativos de informação estejam protegidos de forma sistemática e contínua. Ele é o núcleo da ISO/IEC 27001 e estabelece como a empresa organiza suas práticas de segurança da informação.

Um SGSI não se limita à área de tecnologia. Ele envolve pessoas, processos e tecnologia, funcionando como uma estrutura de governança que assegura a confidencialidade, a integridade e a disponibilidade das informações.

Estrutura do SGSI

A ISO/IEC 27001 propõe que o SGSI seja construído com base no ****ciclo PDCA (Plan – Do – Check – Act)****, que promove a melhoria contínua. O SGSI segue o ciclo PDCA da norma. Enquanto na seção anterior vimos o conceito geral, aqui destacamos como cada etapa se traduz em ações práticas dentro da gestão da segurança

Estrutura do SGSI

Plan (Planejar)

- Definir o escopo do SGSI e as necessidades de segurança da organização.
- Estabelecer a política de segurança da informação.
- Identificar ativos, ameaças, vulnerabilidades e riscos associados.
- Determinar os controles a serem implementados e os objetivos de segurança.

Do (Executar)

- Implementar os controles e processos planejados.
- Colocar em prática políticas, planos de resposta a incidentes e medidas de proteção.
- Garantir que os colaboradores sejam treinados e cientes de suas responsabilidades.

Estrutura do SGSI

Check (Verificar)

- Monitorar e medir os resultados obtidos em relação aos objetivos de segurança definidos.
- Realizar auditorias internas para verificar a eficácia dos controles.
- Avaliar incidentes e não conformidades que possam ter ocorrido.

Act (Agir ou Melhorar)

- Corrigir falhas identificadas no monitoramento ou nas auditorias.
- Revisar políticas, objetivos e controles, adequando-os a novas ameaças ou mudanças no ambiente da organização.
- Implementar ações de melhoria contínua para fortalecer o SGSI.

Importância do SGSI

Permite que a organização tenha um processo estruturado de gestão de riscos.

Cria uma cultura de segurança que envolve todos os colaboradores.

Garante conformidade com requisitos legais, regulatórios e contratuais.

Reforça a confiança de clientes e parceiros, mostrando que a empresa protege adequadamente suas informações.

Elementos Fundamentais do SGSI

Para funcionar de forma eficiente, o SGSI deve contar com:

- Política de Segurança da Informação: documento que expressa o compromisso da organização com a proteção da informação.
- Processos de Gestão de Riscos: identificação, análise, avaliação e tratamento dos riscos relacionados aos ativos de informação.
- Controles de Segurança: medidas práticas para reduzir riscos (administrativos, técnicos e físicos).
- Auditorias e Monitoramento: mecanismos para verificar se as práticas estão sendo seguidas e se continuam eficazes.
- Melhoria Contínua: revisão periódica para garantir que o SGSI evolua junto com as necessidades da organização.

Benefícios de um SGSI bem implementado

Garante a confidencialidade, integridade e disponibilidade das informações.

Reduz a probabilidade de incidentes e o impacto de falhas.

Demonstra comprometimento com a segurança diante de clientes, parceiros e órgãos reguladores.

Cria uma cultura de segurança na organização, envolvendo todos os colaboradores.

4. Gestão de Recursos no SGSI

A gestão de recursos é um dos pilares para o funcionamento eficaz de um Sistema de Gestão da Segurança da Informação (SGSI). Mesmo que a organização possua políticas bem estruturadas e controles definidos, sem a alocação adequada de recursos humanos, tecnológicos e financeiros, o SGSI não alcançará seus objetivos.

A ISO/IEC 27001 enfatiza que a direção da organização deve garantir os recursos necessários para:

- Estabelecer, implementar e manter o SGSI.
- Apoiar a melhoria contínua.
- Assegurar que os colaboradores compreendam suas responsabilidades na proteção da informação.

Tipos de Recursos no SGSI

1. Recursos Humanos
   - Envolvem todas as pessoas que interagem com ativos de informação.
   - Incluem colaboradores diretos, terceirizados e prestadores de serviços.
   - Exigem definição clara de responsabilidades relacionadas à segurança.
   - Necessitam de treinamento e conscientização para reduzir falhas humanas e riscos de engenharia social.
   - Exemplo: treinamentos periódicos sobre phishing, boas práticas de senha, uso seguro de dispositivos móveis.

Tipos de Recursos no SGSI

2. Recursos Tecnológicos
   - Dizem respeito à infraestrutura necessária para sustentar o SGSI.
   - Incluem hardware, softwares, redes de comunicação, sistemas de backup e ferramentas de monitoramento.
   - Devem estar atualizados e configurados de forma segura, evitando vulnerabilidades exploráveis.
   - Exemplo: uso de sistemas de criptografia, firewall, autenticação multifator.

Tipos de Recursos no SGSI

3. Recursos Financeiros e Organizacionais
   - Refletem o compromisso da alta gestão em disponibilizar orçamento para segurança da informação.
   - Permitem contratar especialistas, realizar auditorias, adquirir ferramentas e manter planos de continuidade de negócios.
   - Sem apoio financeiro, a segurança pode ficar restrita a soluções improvisadas e ineficazes.
   - Exemplo: investimento em auditoria externa para avaliar a maturidade do SGSI.

Importância da Gestão de Recursos

Garante que a segurança da informação seja sustentável a longo prazo.

Evita que o SGSI se torne apenas um “documento formal” sem aplicação prática.

Permite equilibrar custos e nível de proteção, alinhando investimentos de segurança às prioridades do negócio.

Reforça a ideia de que a segurança da informação é responsabilidade de toda a organização, não apenas da área de TI.

Exemplos Práticos de Alocação de Recursos

1. Uma empresa que sofre com falta de pessoal treinado decide priorizar conscientização de usuários antes de investir em novas ferramentas tecnológicas.
2. Uma organização com orçamento limitado opta por controles administrativos e de processo, como políticas internas e auditorias manuais, enquanto planeja investimentos futuros em soluções técnicas.
3. Uma instituição financeira, por lidar com dados sensíveis, direciona maior parte de seu orçamento para tecnologias avançadas de proteção, como monitoramento em tempo real e detecção de intrusões.

Exercícios em Grupo

Atividade 1 – Definindo o Escopo

1. Formem grupos.

2. Cada grupo será uma empresa fictícia (exemplos: hospital, escola, banco, startup de software).

3. Escrevam em papel o escopo do SGSI para essa empresa, definindo quais áreas, processos e ativos estarão incluídos.

4. Justifiquem por que escolheram esses elementos para compor o escopo.

Atividade 2 – Identificação de Ativos, Ameaças e Vulnerabilidades

1. Considerem a lista de ativos genéricos: pessoas, documentos, servidores, sistemas de pagamento.

2. Para cada ativo, indiquem:

Uma ameaça (exemplos: incêndio, invasão, erro humano).

Uma vulnerabilidade (exemplos: ausência de backup, falta de treinamento).

3. Proponham um controle prático para reduzir o risco relacionado a cada ativo.

Atividade 3 – Dinâmica de Recursos

1. Cada grupo receberá um cenário:
   - Pouco orçamento.
   - Falta de pessoal treinado.
   - Infraestrutura defasada.

2. Com base no cenário, decidam como priorizar os recursos disponíveis para manter o SGSI funcionando.

3. Registrem as decisões do grupo.

4. Ao final, comparem suas escolhas com as de outros grupos e discutam as diferentes estratégias adotadas.

A – Pouco orçamento

A empresa está em fase inicial e não possui verba suficiente para adquirir novas ferramentas tecnológicas. Quase todo o orçamento disponível já está comprometido com despesas operacionais.

Desafio: como manter um SGSI mínimo sem gastar muito? Quais controles administrativos ou organizacionais podem ser priorizados?

B – Falta de pessoal treinado

A organização possui infraestrutura razoável, mas a equipe não tem experiência em segurança da informação. Há poucos profissionais capacitados e não há programas de treinamento em andamento.

Desafio: como reduzir riscos com uma equipe que não domina boas práticas de segurança?

C – Infraestrutura defasada

Os sistemas e equipamentos são antigos, alguns softwares estão desatualizados e não há plano de substituição a curto prazo. Apesar disso, a empresa depende desses sistemas para continuar funcionando.

Desafio: como lidar com vulnerabilidades tecnológicas sem poder trocar toda a infraestrutura de imediato?

E – Alta dependência de terceiros

Grande parte dos serviços de TI é terceirizada, incluindo hospedagem de sistemas e manutenção de servidores. A empresa não tem controle total sobre os provedores contratados.

Desafio: como garantir a segurança da informação mesmo dependendo de fornecedores externos?

Cenário A – Pouco orçamento

A empresa está em fase inicial e não possui verba suficiente para adquirir novas ferramentas tecnológicas. Quase todo o orçamento disponível já está comprometido com despesas operacionais.

Desafio: como manter um SGSI mínimo sem gastar muito? Quais controles administrativos ou organizacionais podem ser priorizados?

Cenário B – Falta de pessoal treinado

A organização possui infraestrutura razoável, mas a equipe não tem experiência em segurança da informação. Há poucos profissionais capacitados e não há programas de treinamento em andamento.

Desafio: como reduzir riscos com uma equipe que não domina boas práticas de segurança?

Cenário C – Infraestrutura defasada

Os sistemas e equipamentos são antigos, alguns softwares estão desatualizados e não há plano de substituição a curto prazo. Apesar disso, a empresa depende desses sistemas para continuar funcionando.

Desafio: como lidar com vulnerabilidades tecnológicas sem poder trocar toda a infraestrutura de imediato?

Cenário D – Crescimento acelerado

A empresa está expandindo rapidamente, contratando novos funcionários e abrindo novas unidades. Entretanto, o SGSI não acompanhou esse crescimento e não há padronização das práticas de segurança.

Desafio: como estabelecer controles de segurança enquanto a empresa cresce de forma desorganizada?

Cenário E – Alta dependência de terceiros

Grande parte dos serviços de TI é terceirizada, incluindo hospedagem de sistemas e manutenção de servidores. A empresa não tem controle total sobre os provedores contratados.

Desafio: como garantir a segurança da informação mesmo dependendo de fornecedores externos?

Cenário F – Ambiente regulado

A empresa atua em um setor altamente regulamentado (por exemplo, banco, hospital ou operadora de telecomunicações) e precisa cumprir normas legais rígidas, mas ainda não estruturou um SGSI formal.

Desafio: como priorizar recursos para atender rapidamente às exigências regulatórias sem comprometer toda a operação?