

Anexo 3 – Checklist de auditoria interna para o ISO 27001 e ISO 22301**1. Checklist de auditoria interna para o ISO 27001**

Cláusula	Requisito da norma	Conformidade Sim/Não	Evidência
4.2	A organização determinou quais são as partes interessadas?		
4.2	A lista de requisitos de todas as partes interessadas existe?		
4.2	A organização determina os requisitos de segurança da informação?		
4.2	A organização determina os requisitos de continuidade de negócios?		
5.1	A direção assegura que o SGSI atinge seus objetivos?		
5.1	A direção assegura que o SGSI atinge seus objetivos de segurança da informação?		
5.1	A direção assegura que o SGSI atinge seus objetivos de continuidade de negócios?		
5.3	As papéis e responsabilidades para a segurança da informação são atribuídas e comunicadas?		
5.3.1	A organização estabelece e comunica os papéis e responsabilidades para a segurança da informação?		
5.3.2	A organização estabelece e comunica os papéis e responsabilidades para a continuidade de negócios?		
6.1.3	O processo de avaliação de riscos está documentado, incluindo as opções de tratamento do riscos?		
6.1.3.1	Os riscos de segurança da informação são avaliados e tratados de acordo com o plano de segurança da informação?		
6.1.3.2	Os riscos de continuidade de negócios são avaliados e tratados de acordo com o plano de continuidade de negócios?		

Commented [AES1]: Se você precisar de ajuda para realizar a

Commented [AES2]: Para saber mais sobre este tema:

- leia este artigo: Como fazer uma Lista de Verificação para Auditoria Interna da ISO 27001 / ISO 22301
<https://advisera.com/27001academy/pt-br/knowledgebase/como-fazer-uma-lista-de-verificacao-para-auditoria-interna-da-iso-27001-iso-22301/>

Commented [AES3]: Estes são os requisitos da norma ISO

Commented [AES5]: A ser preenchido durante a auditoria -

Commented [AES4]: A ser preenchido durante a auditoria -

6.1.3, 8.3	Existe o Plano de tratamento de riscos e está aprovado pelos proprietários do risco?		
6.2	O Plano de tratamento de riscos define quem é responsável pela implementação de qual controle, com quais recursos, quais são os prazos e qual é o método de avaliação?		
7.1	Existem procedimentos de tratamento de riscos aprovados e implementados?		
7.2	Existem procedimentos de tratamento de riscos aprovados e implementados, incluindo a avaliação de riscos?		
7.3	O pessoal está ciente da Política de segurança da informação, de sua função, e da consequência em não estar em conformidade com as regras?		
7.4	Existe o processo para comunicar as informações relativas à segurança, incluindo as responsabilidades e o que comunicar?		
7.5	Existem procedimentos de gestão de documentos e registros, incluindo a política de controle e acesso a documentos, e a implementação de políticas, procedimentos e controles?		
7.6	Os documentos de gestão de risco são atualizados?		
8.1	Os processos contratados são identificados e controlados?		
9.1	Está definido o que precisa ser mensurado, por qualquer método, quem é responsável, quem irá analisar e avaliar os resultados?		
9.2	Os resultados de mensuração dos documentos e registros são analisados e avaliados?		
9.3	Existem programas de auditoria que definem a escopo, responsabilidades, métodos, critérios e meios de auditoria?		
9.2	As auditorias internas são executadas de acordo com o programa de auditoria, os resultados são reportados através do Relatório de auditoria interna e as ações corretivas relevantes propostas?		

9.3	A revisão gerencial é regularmente executada e os resultados são documentados na ata da reunião?		
9.3	A organização mantém registros de todas as reuniões de revisão gerencial?		
9.3	A organização mantém registros de todas as reuniões de revisão gerencial?		
10.1	A organização considera eliminar a causa da não conformidade e onde apropriado toma ações corretivas?		
10.1	Todas as não conformidades são registradas junto com as ações corretivas?		
10.1	Todas as não conformidades de segurança da informação são registradas junto com as ações corretivas?		
10.1	Todas as não conformidades de segurança da informação são registradas junto com as ações corretivas?		
A.5.2	Todas as responsabilidades quanto à segurança da informação são claramente definidas em um ou diversos documentos?		
A.5.3	As obrigações e responsabilidades são definidas de forma a evitar conflito de interesse, principalmente quando informações e sistemas de alto risco estão envolvidas?		
A.5.3	A organização mantém registros de conformidade com as obrigações e responsabilidades definidas de forma a evitar conflito de interesse?		
A.5.3	A organização mantém registros de conformidade com as obrigações e responsabilidades definidas de forma a evitar conflito de interesse?		
A.5.6	Está claramente definido quem deveria estar em contato com grupos de interesses especiais ou com associações profissionais?		
A.5.7	As ameaças à segurança da informação são coletadas e analisadas para produzir inteligência sobre ameaças?		
A.5.7	Os registros de segurança da informação são coletados e analisados para produzir inteligência sobre ameaças?		
A.5.7	Os registros de segurança da informação são coletados e analisados para produzir inteligência sobre ameaças?		

A.5.9	É elaborado um Inventário de ativos?		
A.5.9	Cada ativo no Inventário de ativos tem um proprietário designado?		
A.5.10	Os dados são armazenados em locais físicos e lógicos seguros?		
A.5.10	Existem procedimentos em vigor para lidar com informações sensíveis?		
A.5.11	Todos os funcionários e contratados devolveram todos os ativos da organização quando o contrato foi rescindido?		
A.5.12	A informação é classificada de acordo com critérios especificados?		
A.5.12	A informação classificada está sob controle de acesso por parte dos funcionários autorizados?		
A.5.12	A informação classificada está sob controle de acesso por parte dos fornecedores autorizados?		
A.5.14	Existem acordos com terceiros que regulem a segurança da transferência de informações?		
A.5.14	As mensagens trocadas pelas redes estão devidamente protegidas?		
A.5.14	Existem procedimentos de controle de acesso por parte dos usuários de registros e registros para controle de acesso?		
A.5.14	Os usuários têm acesso apenas às informações necessárias para o trabalho?		
A.5.16	Os direitos de acesso são fornecidos por meio de um processo de registro formal?		
A.5.17	As senhas iniciais e outras informações de autenticação secreta são fornecidas de forma segura?		
A.5.17	Existem regras para o uso de senhas fortes e para a troca regular de senhas?		
A.5.17	Os usuários são obrigados a usar uma senha forte e a trocá-la regularmente?		
A.5.18	Existe um sistema formal de controle de acesso ao fazer login nos sistemas de informação?		

A.5.18	Os proprietários de ativos verificam periodicamente todos os direitos de acesso privilegiado?		
A.5.18	Os direitos de acesso de todos os funcionários e colaboradores foram revogados após a saída de cada um deles?		
A.5.18	As listas de controle de acesso foram atualizadas e aprovadas a parir de uma revisão periódica?		
A.5.20	Todos os requisitos de segurança relevantes estão incluídos nos acordos com os fornecedores e parceiros?		
A.5.21	Os acordos com provedores de nuvem e outros fornecedores incluem requisitos de segurança para garantir a entrega confiável de serviços?		
A.5.21	Os fornecedores de tecnologia regularmente avaliam a conformidade com os requisitos de segurança e qualidade de serviços?		
A.5.21	Os fornecedores de tecnologia são avaliados em conformidade com os requisitos de segurança, de forma a assegurar a entrega de serviços confiáveis?		
A.5.23	Os processos de aquisição, uso, gerenciamento e saída de serviços em nuvem estão em conformidade com os requisitos de segurança identificados?		
A.5.24	Os procedimentos e responsabilidades para o gestão de incidentes estão claramente definidos?		
A.5.24	Os procedimentos de resposta de incidentes são atualizados?		
A.5.24	Os procedimentos de resposta de incidentes incluem uma revisão periódica?		
A.5.27	Os incidentes de segurança são analisados de forma a obter conhecimento sobre como preveni-los?		
A.5.28	Existem procedimentos que definem como coletar evidências de incidentes que serão aceitáveis durante o processo legal?		
A.5.28	Os incidentes são analisados de forma a obter conhecimento sobre como preveni-los?		

A.5.28	Existem procedimentos para garantir a continuidade de operações de emergência durante uma crise de segurança?		
A.5.29	O exercício e o teste são realizados para garantir uma resposta eficaz?		
A.5.30	A prontidão de TIC é planejada, implementada, mantida e testada com base nos requisitos de continuidade de negócios e TIC?		
A.5.31	Existem procedimentos de resposta a incidentes, segurança, continuidade e recuperação de desastres?		
A.5.32	Existem procedimentos para garantir a continuidade de serviços de emergência durante uma crise de segurança?		
A.5.33	Todos os registros estão protegidos de acordo com os requisitos regulamentares, contratuais e outros requisitos identificados?		
A.5.34	As informações de identificação pessoal são protegidas conforme exigido por leis e regulamentos?		
A.5.35	Os registros de informação e dados pessoais são protegidos?		
A.5.36	Os sistemas de informação são revisados regularmente para verificar sua conformidade com as políticas e normas de segurança da informação?		
A.5.37	Os procedimentos operacionais dos processos de TI foram documentados?		
A.5.38	As informações de confidencialidade de segurança são protegidas e controladas?		
A.5.39	Os sistemas de informação são protegidos de acordo com os requisitos regulamentares, contratuais e outros requisitos identificados?		

A.6.3	Todos os funcionários e contratados relevantes estão sendo treinados para desempenhar suas funções de segurança e existem programas de conscientização?		
A.6.4	Todos os funcionários que cometeram uma violação de segurança foram submetidos a um processo disciplinar formal?		
A.6.5	Os procedimentos de segurança de terceiros são gerenciados adequadamente e os fornecedores de serviços terceirizados são avaliados regularmente?		
A.6.6	Os procedimentos de segurança de terceiros são gerenciados adequadamente e os fornecedores de serviços terceirizados são avaliados regularmente?		
A.6.7	Existem regras que definem como as informações da organização são protegidas durante o trabalho remoto?		
A.6.8	Os funcionários e contratados estão relatando falhas e eventos de segurança?		
A.6.9	Os procedimentos de segurança de terceiros são gerenciados adequadamente e os fornecedores de serviços terceirizados são avaliados regularmente?		
A.6.10	Os procedimentos de segurança de terceiros são gerenciados adequadamente e os fornecedores de serviços terceirizados são avaliados regularmente?		
A.7.2	As áreas de entrega e carregamento são controladas de forma que pessoas não autorizadas não possam entrar nas dependências da organização?		
A.7.3	As áreas seguras estão localizadas de forma que não sejam visíveis para pessoas de fora e não sejam facilmente alcançadas de fora?		
A.7.4	Os procedimentos de segurança de terceiros são gerenciados adequadamente e os fornecedores de serviços terceirizados são avaliados regularmente?		
A.7.5	Os procedimentos de segurança de terceiros são gerenciados adequadamente e os fornecedores de serviços terceirizados são avaliados regularmente?		
A.7.6	Os procedimentos de trabalho para áreas seguras são definidos e cumpridos?		
A.7.7	Existe uma regra que obrigue os usuários a remover papéis e mídia quando não estiverem presentes e bloquear suas telas?		

A.7.8	Existem procedimentos para remoção de arquivos protegidos de acesso de computadores de terceiros (externos)?		
A.7.9	Os níveis de segurança estão adequadamente protegidos contra os níveis associados ao armazenamento de informação?		
A.7.10	Os procedimentos que definem como lidar com mídias removíveis estão de acordo com as regras de classificação?		
A.7.10	Existem procedimentos formais para descartar a mídia?		
A.7.11	Existem procedimentos para teste de integridade de dados?		
A.7.12	Os níveis de segurança de sistemas operacionais estão adequadamente protegidos?		
A.7.13	O equipamento é mantido regularmente de acordo com as especificações e boas práticas dos fabricantes?		
A.7.14	Todos os dados confidenciais e software licenciado são removidos da mídia ou equipamentos quando descartados?		
A.8.1	Os dados pessoais armazenados seguem as diretrizes legais?		
A.8.2	Os direitos de acesso e integridade de procedimentos são controlados adequadamente?		
A.8.3	O acesso a informações, softwares e sistemas é restrito conforme Política de controle de acesso?		
A.8.4	O acesso ao código-fonte é restrito a pessoas autorizadas?		
A.8.5	Existem procedimentos para controle de acesso de sistemas de acesso com a Política de controle de acesso?		
A.8.6	Existem procedimentos para controle de acesso de sistemas de acesso com a Política de controle de acesso?		
A.8.7	O software antivírus e outros softwares para proteção contra malware estão instalados e atualizados?		

A.8.8	Existe alguém encarregado de coletar informações sobre vulnerabilidades e essas vulnerabilidades são prontamente resolvidas?		
A.8.9	Os controles de segurança de terceiros implementados para avaliar sua confiabilidade com as atividades críticas de negócios de informação?		
A.8.10	As informações de terceiros, clientes, parceiros e outros de fornecedores, fornecedores, fornecedores, fornecedores e outros?		
A.8.10	As informações armazenadas em sistemas, dispositivos e mídia são excluídas quando não são mais necessárias?		
A.8.11	Os dados são mascarados de acordo com as políticas aplicáveis e requisitos comerciais e legais?		
A.8.12	Os controles de segurança de terceiros de todos os serviços de terceiros que recebem, armazenam ou processam informações confidenciais?		
A.8.13	A política de retenção de registros é desenvolvida de acordo com requisitos de controle de acesso aos registros?		
A.8.14	A infraestrutura de TI é implementada com redundância para atender às expectativas durante os desastres?		
A.8.15	Todas as atividades do usuário, falhas e outros eventos dos sistemas de TI são registrados e alguém as verifica?		
A.8.16	Os logs de eventos de segurança de todos os dispositivos de terceiros que processam informações de negócios de informação?		
A.8.17	Os relógios em todos os sistemas de TI são sincronizados com uma única fonte de tempo correto?		

A.8.18	O uso de ferramentas utilitárias, que possam sobrepor os controles de segurança de aplicativos e sistemas, é estritamente controlado e limitado a um pequeno círculo de funcionários?		
A.8.19	As ferramentas de software e hardware utilizadas estão devidamente controladas e limitadas a um pequeno círculo de funcionários?		
A.8.20	Os dados de segurança de serviços críticos e informações de serviços críticos?		
A.8.21	Os requisitos de segurança para serviços de rede interna e externa estão definidos e incluídos nos contratos?		
A.8.22	Os grupos de usuários, serviços e sistemas estão segregados em diferentes redes?		
A.8.23	Os dados de segurança de serviços críticos e informações de serviços críticos?		
A.8.23	Os dados de segurança de serviços críticos e informações de serviços críticos?		
A.8.24	As chaves de criptografia são adequadamente protegidas?		
A.8.25	Há regras definidas para o desenvolvimento seguro de software e sistemas?		
A.8.26	Os requisitos de segurança de serviços críticos e informações de serviços críticos?		
A.8.27	Os requisitos de segurança de serviços críticos e informações de serviços críticos?		
A.8.28	Os princípios de codificação segura são aplicados no desenvolvimento de software?		
A.8.29	O teste para verificar se os requisitos de segurança foram implementados são executados durante o desenvolvimento de software?		
A.8.30	Os requisitos de segurança de serviços críticos e informações de serviços críticos?		
A.8.31	Os requisitos de segurança de serviços críticos e informações de serviços críticos?		

A.8.31	Os ambientes de desenvolvimento, teste e produção são estritamente separados?		
A.8.32	Todas as mudanças nos sistemas de TI, mas também em outros processos que possam afetar a segurança da informação, são rigorosamente controladas por meio de procedimentos de mudança?		
A.8.33	Os dados de teste são armazenados separadamente e protegidos?		
A.8.34	Os dados de teste são armazenados em ambientes de produção, desenvolvimento e testes de forma segura e não são acessíveis?		

2. Checklist de auditoria interna para o ISO 22301

Cláusula	Requisito da norma	Conformidade Sim/Não	Evidência
4.2.1	A organização determinou quais são as partes interessadas?		
4.2.1	A lista de requisitos de todas as partes interessadas existe?		
4.2.2	A organização determinou os requisitos para os produtos e serviços que fornece?		
4.2.3	A organização determinou os requisitos para os fornecedores e serviços que recebe?		
5.1	A alta direção suporta de forma ativa as atividades de continuidade de negócios?		
5.2	O SGCN é compatível com o propósito da organização?		
5.3	A alta direção realiza o comprometimento de fornecer recursos necessários e informações de continuidade de negócios?		
5.4	Existem uma Política de continuidade de negócios e uma Política de continuidade de negócios de negócios?		
5.2	A Política de continuidade de negócios é comunicada dentro da organização?		
5.3	A pessoa responsável pelo SGCN é designada e esta pessoa tem autoridade suficiente?		
5.4	As pessoas responsáveis pelo SGCN possuem autoridade suficiente para implementar o SGCN?		
5.5	A organização determina quais os riscos de continuidade de negócios?		
6.1	A organização planejou ações para endereçar os riscos e oportunidades identificados?		
6.2.1	Os objetivos de continuidade de negócios estão definidos e eles são comunicados para todos os funcionários relevantes?		
6.2.2	A organização determina os requisitos de continuidade de negócios para os fornecedores e serviços que recebe?		

Commented [AES6]: Estes são os requisitos da norma ISO

Commented [AES8]: A ser preenchido durante a auditoria -

Commented [AES7]: A ser preenchido durante a auditoria -

6.2.2	Existem procedimentos para aprovar as alterações necessárias no SGCN, incluindo quem faz a revisão e aprova os documentos, onde e como eles são publicados, armazenados e protegidos?		
6.3	As alterações necessárias no SGCN são realizadas de forma planejada?		
7.1	Recursos adequados são fornecidos para todos os elementos do SGCN?		
7.2	Existem procedimentos para aprovar as alterações necessárias no SGCN, incluindo quem faz a revisão e aprova os documentos, onde e como eles são publicados, armazenados e protegidos?		
7.3	Existem procedimentos para aprovar as alterações necessárias no SGCN, incluindo quem faz a revisão e aprova os documentos, onde e como eles são publicados, armazenados e protegidos?		
7.4	Existem procedimentos que definem o que comunicar relativo à continuidade de negócios, quando comunicá-la e para quem?		
7.5	Existe o processo de gestão de documentos e registros, incluindo quem faz a revisão e aprova os documentos, onde e como eles são publicados, armazenados e protegidos?		
7.6	Os documentos de registro estão bem organizados?		
8.1	Existem procedimentos para aprovar as alterações necessárias no SGCN, incluindo quem faz a revisão e aprova os documentos, onde e como eles são publicados, armazenados e protegidos?		
8.2.1	Os processos para a avaliação de riscos e a análise de impacto nos negócios estão definidos?		
8.2.2	A análise de impacto nos negócios é executada, incluindo todas as atividades e os impactos de não executar estas atividades são avaliados ao longo do tempo?		
8.3.1	Existem procedimentos para aprovar as alterações necessárias no SGCN, incluindo quem faz a revisão e aprova os documentos, onde e como eles são publicados, armazenados e protegidos?		
8.3.2	As estratégias e soluções de continuidade de negócios estão identificadas?		

8.3.3	As estratégias e soluções selecionadas, baseadas nos objetivos de tempo de recuperação são definidas para cada atividade?		
8.3.4	Existem procedimentos de continuidade de negócios para a recuperação das atividades críticas, informações, sistemas e tecnologia, equipamentos, ferramentas de comunicação, transporte, pessoal e fornecedores?		
8.3.5	Os procedimentos de continuidade de negócios para a recuperação de negócios são atualizados com base nas mudanças de requisitos para todos os tipos de condições de negócios e são baseadas para garantir a continuidade, eficiência e a capacidade de recuperação?		
8.4.2	Existem procedimentos de resposta a incidentes com a iniciação de limites e procedimentos de respostas?		
8.4.3	Existe o procedimento para comunicar com as partes interessadas, e que define como os meios de comunicação estarão disponíveis?		
8.4.4	Existem planos de continuidade de negócios que incluem a gestão e a manutenção de meios alternativos para a recuperação de negócios?		
8.4.5	Os procedimentos de continuidade de negócios incluem a recuperação de negócios?		
8.5	Exercícios e testes regulares são executados e eles têm base em cenários e, relatórios de testes pós-exercício são produzidos?		
8.6	São realizadas revisões periódicas da documentação e avaliado o cumprimento de todos os requisitos?		
8.6	Os procedimentos de continuidade de negócios incluem a recuperação de negócios e a gestão dos procedimentos de continuidade de negócios?		
8.6	Os procedimentos de continuidade de negócios incluem a recuperação de negócios e a gestão dos procedimentos de continuidade de negócios?		
9.1.1	Está definido o que precisa ser mensurado, por qualquer método, quem é responsável, quem irá analisar e avaliar os resultados?		

9.1.1	Os resultados da mensuração e monitoramento são documentados e reportados para as pessoas responsáveis?		
9.2	Existem programas de auditoria que diferenciam áreas, departamentos, unidades, setores e níveis de auditoria?		
9.2	As auditorias internas são realizadas de acordo com o programa de auditoria, de modo que os resultados sejam de benefício de auditoria interna e sejam corretos, completos e precisos?		
9.3	A revisão gerencial é regularmente executada e os resultados são documentados na ata da reunião?		
9.3	A direção decidiu sobre as questões críticas importantes para o êxito do SGCN?		
9.3	A organização trata a cada não conformidade?		
9.3	A organização considera a cada não conformidade e cada ação corretiva como ações críticas?		
10.1	Todas as não conformidades são registradas junto com as ações corretivas?		