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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
5.1	A direção assegura que o SGSI atinge seus objetivos?		
[illegible]	[illegible]		
[illegible]	[illegible]		
5.3	As papéis e responsabilidades para a segurança da informação são atribuídas e comunicadas?		
[illegible]	[illegible]		
[illegible]	[illegible]		
6.1.3	O processo de avaliação de riscos está documentado, incluindo as opções de tratamento do riscos?		
[illegible]	[illegible]		
[illegible]	[illegible]		

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

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/

[illegible]

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

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

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

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	[illegible]		
7.2	[illegible]		
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	[illegible]		
7.6	[illegible]		
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?		
9.1	[illegible]		
9.2	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		

A.5.9	É elaborado um Inventário de ativos?		
A.5.9	Cada ativo no Inventário de ativos tem um proprietário designado?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		

[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		

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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		

[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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 equipamento quando descartados?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
A.8.17	Os relógios em todos os sistemas de TI estão 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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
A.8.24	As chaves de criptografia são adequadamente protegidas?		
A.8.25	Há regras definidas para o desenvolvimento seguro de software e sistemas?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		

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?		
[illegible]	[illegible]		
[illegible]	[illegible]		

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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		

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

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

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

[illegible]	[illegible]		
6.3	As alterações necessárias no SGCN são realizadas de forma planejada?		
7.1	Recursos adequados são fornecidos para todos os elementos do SGCN?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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 executas, incluindo todas as atividades e os impactos de não executar estas atividades são avaliados ao longo do tempo?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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?		
[illegible]	[illegible]		
[illegible]	[illegible]		
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	[illegible]		
9.2	[illegible]		
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?		
10.1	[illegible]		
10.1	[illegible]		
10.1	Todas as não conformidades são registradas junto com as ações corretivas?		