## 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?		
40	I necessaria descriptoria de l'ellera merimo in erroria dell'edaci		
10	So regarding group de 100 de projection com a finação acressigan?		
5.1	A direção assegura que o SGSI atinge seus objetivos?		
	Scote a Militios de regunerça de Montaglio con algebras de la estration per deller su digeliose.		
N.E.	a fallico de agurargo de referenção a propriada de tres de agencação?		
5.3	As papéis e responsabilidades para a segurança da informação são atribuídas e comunicadas?		
	Common & solida & los ones Accommoda, solida & common & ante & los ones common ante		
N = 3, N 2	On Trace wide block pales, it seek propriets to, probabilishes, smoothebilis in a risk de form, soon marketin wide documentation		
6.1.3	O processo de avaliação de riscos está documentado, incluindo as opções de tratamento do riscos?		
	Calle or Care Care Care Calle		
MAC P	E fectoração de apricatifidade E producida em publicativas o debus pero cada conscion		

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?	
10	Nouvez altiquate de foracillo pro- tallo a correcto de 100°	
	Table as competitivos acido dell'india, nonumentos associados e mantidos al agueros de competitivosos?	
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?	
	Notate e processor de aporido de decumentos e rapismos, horunido quam No e minido e aprinos in decumentos, ende e como encudo publicados, ende e como encudo publicados,	
100	To discommission de origine autorise de commission?	
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?	
	To resultable de mercunaçõe de desumentable o reportable pero se proses reportable?	
Mar.	Total v pragrams de suditorio que deline el presió, responsabilidades, readinos, priorite e escape de auditorio <sup>a</sup>	
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?	
10	A Altraglio decidir, sotto es apacidito cilitoso reportantes para o dello de 1000	
80	A regardingly reagon a solit rite sorter regards?	
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?	
833	Yellor as partition de regularique de other regular reconstrise des apreciatios para directos a partitionidas?	
8.5.5	Todas as participa de exporceça de electrosphe de reconde e acustosales?	
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?	
811.8	A directio cotto cognedo atriumento que reales as funcionarios o contratados cumoram as regimo de segurança de referençatori	
8.53	Sale comments dell'inde queri deserte sale en contain con qual submittale?	
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?	
8.58	As region the experiency do informação mobile recordos em codo proposi-	
**	Service de apropriée de la Production de	

A.5.9	É elaborado um Inventário de ativos?	
A.5.9	Cada ativo no Inventário de ativos tem um proprietário designado?	
K 1: (0)	No region para o l'internerità altrapado di reformação o artino estilo discovernados?	
110	tottor proofmento que Miliani orio. Se ser récregões cooficates?	
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?	
8.5	I demake better at mode in some an a prosidence at the	
8.5.08	A principle de handrifecto de observações à regularismentale em particas a procedimento formació	
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?	
8.3.0	Some area fiction do commit de annos are define reportes de regione e apprecia per commit de annos?	
***	In contrast the same speed in which is more and a same side.	
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?	
8.5.07	Scotor regres force percent auditors who were prologor perform within other region de automospher	
83.07	processor and the second section of the section of	
A.5.18	Existe um sistema formal de controle de acesso ao fazer login nos sistemas de informação?	

Anexo 3 – Checklist de auditoria interna

ver [versão] da [data]

Página 4 de 15

A.5.18	Os proprietários de ativos verificam periodicamente todos os direitos de acesso privilegiado?	
N. 1. 100	So d'intro de acoso de radio os Successirios e com assalos finam- ernacidos auto o tilminos de acos com assal	
N.3.10	A participa de como motor do mosos empresados o formaciodente e participa ante decumentados	
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?	
	To formacidano de montroles regularmento quanto i conformidade con as requistro de esporanço e subfisido, se porquindo?	
N. S. 200	No floor afteragilies are accretion a contrator, con formacodicino e perceiros, se fiscas e processos accidentes de resolto en concelerações	
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?	
41.0	Nation as exercise de regularique de exclusión e riscolification?	
11.00	Supressiff medical substruction of the supervision of the alternation of the department of the supervision	
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?	
41.00	To requirite para profruidade da regurerajo do reformação acido definidad?	

Anexo 3 – Checklist de auditoria interna

ver [versão] da [data]

Página 5 de 15

	1	
N.S. (88)	bosser prooffinents aar gestern i perincidade de oppronje de internaçõe decente pris cine su un disperior?	
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?	
	Traditio an exploration de exploration regisserione, exploratione, contratourio e matrice actifer traditio e descurrenteador?	
0.3180	Scotter procedimento, que gerenten y acinação dos ilhertos de propriedade resentual, returnidos uso de pilhases transcado?	
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?	
83.80	A segundo de riformação e notada regularmente por un auditor redupandonari	
11.00	Dispersion recording to the expersion of the particular or property control for expersion of the expersion of the particular control of the expersion of the control of	
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?	
883	As on Trapho & emocidente de mercula, en ordinario o empregano percunados?	
No.	Os acondiscom funcionários a contraballo: superificam as responsabilidades de repurespo do reformação?	

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?	
	No responsabilidades de esponergo de riberresplo que servenecem el ribe spila el encrea de encues empregatico seda del reduce se comunici.	
100	I regerosphi titto tede or thoute & perfeccióliste que protur cresse en periodo con troprosi.	
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?	
6.73	Scotor Eros reguns que prinque do regilos corridore que	
10.70	A colorado spres desper seguras il protegodo con spreticion que per ritori aggiren il colorado de persona autorizados?	
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?	
6.74	la reconsider de recritorale pera entre de saturale?	
M.75	Studentos, protegilo spetry hobistic e matria cottorna solito nationalisi.	
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?	

	T	
10	I regularmento cotti tecnimalibi de forma a proteggi to de accesso vide autorimale o de proteggi criticottori	
6.79	To attino de reporceçõe estile altrapationeres protegitos questo do acido nosticados no dispredirecto de especiaçõe?	
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?	
10	Empoyensette pessa Tento de plinoresigido contenuado/	
	the cation de energie e de sonormunicaçãos estás estrapadormenta promption?	
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?	
	No region para a transporte argum de Republicas relativi	
4.63	to diretto de acosa protigosto de generados nos cultude especial	
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?	
885	Engles against Engles (Branch Steine A Steine Arabis and Anthro Arabis A Service Brasson)	
10.00	Egyptic reprises a parity response proof a specified a parity re-	
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?	
***	On commande reformaçõe do recisados regulamente para aprilirar sua portermidade com as políticas e remas de regunaçõe de récimaçõe?	
	As configuração de fundaces, cofficies, amigos e sobre de contencióles, decomensales, representado, mentendos e seriados?	
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?	
8810	To commiss de presenção de assumente de dedis de eplicados escribos que presessor, princersor su resorrigen informações confidencias?	
8.8100	a Martico de objiso de esporenço é deservacios de se objiso de esporenço de escriados de acerdo com esporenço de	
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?	
M-91-70	To regar Trescordo regar do administrador ; do acologidos de Norrea que pessoas ede autorizadas do assuare abestinos.	
	No redito, commune a spiriutivan olik repritorialita, com aplika spropriedas terrasiko pero austra populari recidentes de segurança de riformação?	
A.8.17	Os relógios em todos os sistemas de TI estão sincronizados com uma única fonte de tempo correto?	

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 recongle de colhezes i conformente controvalle, acciono precodimentes para paga final	
As redacido con routa de ferros o protegor a referrações do comos o principar	
Os requisitos de segurança para serviços de rede interna e externa estão definidos e incluídos nos contratos?	
Os grupos de usuários, serviços e sistemas estão segregados em diferentes redes?	
E acceso a citino accorrego il generolistico perio reducir a respecialite a riscosi	
botto a politica que regula a celificação e autros com nos de crongrafio	
As chaves de criptografia são adequadamente protegidas?	
Há regras definidas para o desenvolvimento seguro de software e sistemas?	
Os especiales de esperança de informação da definida e sprincada no desenvarionmento no especiação de aplicativas	
Di principio pero citerras de engelhera espera esido discorrestados e impermentados!	
Os princípios de codificação segura são aplicados no desenvolvimento de software?	
O teste para verificar se os requisitos de segurança foram implementados são executados durante o desenvolvimento de software?	
boster orderes dell'inde persionite es connect	
E desenvolvemente renetitisado de cotomo e reprisonado?	
	possam sobrepor os controles de segurança de aplicativos e sistemas, é estritamente controlado e limitado a um pequeno círculo de funcionários?  Os requisitos de segurança para serviços de rede interna e externa estão definidos e incluídos nos contratos?  Os grupos de usuários, serviços e sistemas estão segregados em diferentes redes?  As chaves de criptografia são adequadamente protegidas?  Há regras definidas para o desenvolvimento seguro de software e sistemas?  Os princípios de codificação segura são aplicados no desenvolvimento de software?  O teste para verificar se os requisitos de segurança foram implementados são executados durante o desenvolvimento de

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?	
16.00	To dialitie de recess des publishes mentes principales e protogolies?	
11.00	No codificación des comercias de produçãos de prompados e seas abadas de forma a econoxia a risco de riber applicir	

## 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?		
100	I regardação determina proposa pero Vider per se requisitos apricipario a regularizaci.		
111	l'escape anti Mourrentado, Millordo ques produtto e arrogo estilo reculto e a motudos estilo equitados!		
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?		
	I alto direglio montra i comprometimento an formazio radio di recursio i comunicari a reportinco de controctado de registros?		
16.00	Scote uma Million de controcidade de regione e no define e estruturo pero si deliniçõe de algenises.		
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?		
	As populs or responsabilitàtules para a continuolable de regiones de difficultant comunicables.		
111	Longerough difference, talks in format participated		
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?		
Marin.	To object use de continuidade de regiónico de mensurbeiro e de montrosido e esuricados?		

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 -

			1
	too definite is que precise de filles pers etirge se répéties, quen é rependent, que de la precise e que recurso de terrestració		
6.3	As alterações necessárias no SGCN são realizadas de forma planejada?		
7.1	Recursos adequados são fornecidos para todos os elementos do SGCN?		
10	Table as competitivos estilo dell'india, non amendo essociado e repristo es regiones de competitivoso?		
111	Coperand with corns & Publica & portractibate de registros, de cue forção, e dos consequêncios em discostre em portermidade com as registro.		
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?		
100	To discurrent so de origen autoriso de serviciados?		
100	Surveyora communito de deministra e priminador		
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?		
Ker	No recognition representations per sollo de l'estable e les dependêncies entre le discribable e parties récressable estàble de l'étable.		
KIN	It auchtgebe de from it mercetele para teller er et rédele, processor e étien e er forr-public par procesor se translate de descriptions		
8.3.2	As estratégias e soluções de continuidade de negócios estão identificadas?		

Anexo 3 – Checklist de auditoria interna

ver [versão] da [data]

Página 13 de 15

8.3.3	As estratégias e soluções selecionadas, baseadas nos objetivos de tempo de recuperação são definidas para cada atividade?	
838	Table is recurse receptive persis expensable discribinative persiss, reterrapides, addition or reterrapides, esponenteets, fire conveyed dis- servanteets, fire conveyed, français, persisso or fire excellents.	
841	The proceed framework is a price of the control of	
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?	
-	Tocorer province de continuidade de registros apar trotagen as papallo e responsabilidades a eleptos despituados pero e recuperração de atrodades?	
8.63	Microsoffmento Boumentallo que definen y miscongle di atroduleo?	
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?	
88	To respect tion, Nation or recollect pills in the control of the responsible space or of resplict day proceed in proceedings the control of the latest space of the respect to the control of the respect to the control of the respect to the respect to the control of the respect to the respect	
***	to specificate the contraction the regions the formation operation the secondary	
9.1.1	Está definido o que precisa ser mensurado, por qualquer método, quem é responsável, quem irá analisar e avaliar os resultados?	

	Os resultados da mensuração e	
9.1.1	monitoramento são documentados e	
	reportados para as pessoas responsáveis?	
10.0	Total o programs de auditorio que delhe sa pressa, inquernatiridades, interina, critoria o scope de auditorio <sup>o</sup>	
	As auditorias internas alle sassuntados de acordo com o programo de auditoria, as	
8.0	municipality day reports allow at reads the	
	or street streets properly.	
0.3	A revisão gerencial é regularmente	
9.3	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?	
-	Langue Couglio-ringe a collection conformation?	
	A experiments mentiles element a passe for	
	agles on street	
10.1	Todas as não conformidades são registradas junto com as ações corretivas?	