[logotipo da organização]

[nome da organização]

PROCEDIMENTO DE AUDITORIA INTERNA

Código:	
Versão:	
Data da versão:	
Criado por:	
Aprovado por:	
Nível de confidencialidade:	

Commented [AES1]: Para aprender como preencher este documento, e ver exemplos reais do que você precisa escrever, veja este vídeo tutorial "How to Write ISO 27001/ISO 22301 Internal Audit Procedure and Audit Program".

Para acessar o tutorial: Em sua caixa de entrada, encontre o e-mail que você recebeu no momento da compra. Lá, você verá um link e uma senha que lhe permitirá acessar o vídeo tutorial.

Commented [AES2]: Todos os campos desde documento que aparecem entre colchetes devem ser preenchidos.

Commented [AES3]: Para aprender mais sobre este tópico, leia estes artigos:

- Dilemas com os auditores internos das normas ISO 27001 e BS 25999-2 https://advisera.com/27001academy/pt-br/blog/2010/12/16/dilemas-com-os-auditores-internos-das-normas-iso-27001-e-bs-25999-2/
- 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/

Considere fazer este treinamento online gratuito: ISO 27001 Internal Auditor Course https://advisera.com/training/iso-27001-internal-auditor-course/

Além disso, dê uma olhada neste livro: ISO Internal Audit: A Plain English Guide https://advisera.com/books/iso-internal-audit-plain-english-guide/

Commented [AES4]: Se você precisar de ajuda para realizar a auditoria interna da ISO 27001/ISO 22301 em sua organização, verifique este ISO Consultant Directory para encontrar o especialista adequado.

Commented [AES5]: O sistema de codificação do documento deve estar de acordo com o atual sistema de codificação de documentos da organização. Caso não haja um sistema desse tipo na organização, esta linha pode ser excluída.

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
	0.1	Advisera	Esboço básico do documento

Sumário

1. Finalidade, escopo e usuários

A finalidade deste Procedimento é descrever todas as atividades relacionadas à auditoria, como elaboração do programa de auditoria, seleção de um auditor, condução de auditorias individuais e geração de relatórios.

Este Procedimento aplica-se a todas as atividades realizadas no Sistema de Gestão da Segurança da Informação (SGSI) [Sistema de Gestão da Continuidade de Negócios (SGCN)].

Os usuários deste documento são [membros da alta direção] da [nome da organização], bem como os auditores internos.

Commented [AES6]: Este trecho deve ser inserido no lugar do SGSI caso o procedimento refira-se exclusivamente à gestão da continuidade de negócios.

Commented [AES7]: Organismos da alta direção no escopo do SGSI

Commented [AES8]: Inclua o nome da sua organização.

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas 9.2, A.5.30, A.5.35 e A.8.34
- Norma ISO 22301, cláusulas 9.2
- Política de segurança da informação
- Política de continuidade de negócios
- Procedimento de ação corretiva

Commented [AES9]: Exclua este item se o procedimento referir-se somente à gestão da continuidade de negócios.

Commented [AES10]: Exclua este item se o procedimento referir-se somente à segurança da informação.

Commented [AES11]: Você pode encontrar um modelo para este documento na pasta "05_Politicas_gerais" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES12]: Exclua este item se o procedimento referir-se somente à gestão da continuidade de negócios.

Commented [AES13]: Você pode encontrar um modelo para este documento na pasta "10_Documentos_principais_de_continuidade_de_negocios_da_ISO_22301" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES14]: Exclua este item se o procedimento referir-se somente à segurança da informação.

Commented [AES15]: Você pode encontrar um modelo para este documento na pasta "14_Acoes_corretivas" do Kit de documentação Premium da ISO 27001 e ISO 22301.

3. Auditoria interna

3.1. Finalidade da auditoria interna

A finalidade da auditoria interna é determinar se os procedimentos, controles, processos, acordos e outras atividades no SGSI [SGCN] estão de acordo com as normas ISO 27001 e ISO 22301, as regulamentações aplicáveis e a documentação interna da organização, se esses itens foram implementados e mantidos com eficácia e se atendem aos requisitos da política e aos objetivos estabelecidos.

Commented [AES16]: Trecho a ser excluído se o procedimento

Commented [AES17]: A ser excluído se você não for

Commented [AES18]: Exclua este parágrafo se o auditor

3.2. Planejamento de auditoria interna

O [cargo] aprova um programa anual para auditorias internas, que é elaborado conforme o formulário do Anexo 1 Programa anual de auditoria interna.

Commented [AES19]: Ex.: gerente de continuidade de

O Programa anual de auditoria interna deve conter as seguintes informações sobre cada uma das auditorias internas:

- período da auditoria (especifique as datas ou o mês para o qual a auditoria está planejada)
- escopo da auditoria (departamentos, processos, cláusulas da norma, etc.)
- critérios da auditoria (normas, legislação e regulamentações, documentação interna, normas corporativas e/ou obrigações contratuais)
- [blurred]
- [blurred]

Os auditores internos nomeados devem registrar as auditorias realizadas no Programa anual de auditoria interna.

3.3. Indicação de auditores internos

O [cargo] deve indicar auditores internos.

Um auditor interno pode ser alguém da organização ou não. Os critérios para indicação de auditores internos são:

- conhecimento das normas ISO/IEC 27001 e ISO 22301
- [blurred]
- [blurred]

O [cargo] deve selecionar os auditores internos de forma a garantir a objetividade e imparcialidade, isto é, para evitar conflitos de interesses, pois os auditores não devem auditar seu próprio trabalho.

[blurred]

3.4. Condução de auditorias internas

Os responsáveis pelas auditorias internas são identificados no Programa anual de auditoria interna.
[blurred]

Os seguintes fatores devem ser levados em consideração durante uma auditoria interna:

- critérios estabelecidos no Programa anual de auditoria interna
- resultados das auditorias internas ou externas anteriores
- [blurred]
- [blurred]

Os seguintes aspectos e a verificação delas devem ser documentados como resultados de auditoria interna:

- Relatório de auditoria interna – deve ser enviado para [cargo]

Commented [AES20]: Estes são todos obrigatórios; não exclua

Commented [AES21]: Por exemplo, gerente de segurança,

Commented [AES22]: Estes são critérios recomendados para a nomeação de auditores internos e estão em conformidade com a cláusula 7.2 da norma ISO.

Commented [AES23]: Trecho a ser excluído se o procedimento

Commented [AES24]: A ser excluído se você não for

Commented [AES25]: Ex.: gerente de segurança, gerente de

Commented [AES26]: Ou ISO 22301.

Commented [AES27]: Para obter dicas sobre como realizar auditorias eficazes, leia este artigo:

Commented [AES28]: Ex.: gerente de continuidade de

- [illegible]

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*	[illegible]	[illegible]	[illegible]
Programa anual de auditoria interna (em formato eletrônico)	Computador de [cargo]	[illegible]	[illegible]	[illegible]
Relatório de auditoria interna (em formato eletrônico)	Computador do auditor interno e do [cargo]	[illegible]	[illegible]	[illegible]
Checklist de auditoria interna (formulário preenchidoi durante a auditoria interna)	Computador do auditor interno	[illegible]	[illegible]	[illegible]

Somente o [cargo] pode conceder aos outros funcionários o direito de acessar o Programa anual de [illegible]

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

[illegible]

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade de ações corretivas identificadas durante a auditoria
- quantidade de ações corretivas identificadas durantes a auditoria de certificação realizada após a auditoria interna
- [illegible]

Commented [AES29]: Você pode encontrar um modelo para [illegible]

Commented [AES30]: Adapte o período desta coluna às suas [illegible]

Commented [AES31]: Geralmente a pessoa que aprovou o [illegible]

Commented [AES32]: Geralmente em formato PDF.

Commented [AES33]: Geralmente em formato PDF.

Commented [AES34]: Ex.: gerente de continuidade de [illegible]

Commented [AES35]: Isso é apenas uma recomendação; [illegible]

6. Anexos

- Anexo 1 – Programa anual de auditoria interna
- Anexo 2 – Relatório de auditoria interna
- [illegible]

[cargo]
[nome]

_____
[assinatura]

Commented [AES36]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.