[logotipo da organização]

[nome da organização]

DECLARAÇÃO DE APLICABILIDADE

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 Statement of Applicability"

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 com o escrever a Declaração de aplicabilidade, leia este artigo:

A importância da Declaração de aplicabilidade da ISO 27001 https://advisera.com/27001academy/pt-br/knowledgebase/a-importancia-da-declaracao-de-aplicabilidade-da-iso-27001/

Commented [AES4]: 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 documento é definir quais controles são adequados para implementação na [nome da organização], quais são os objetivos desses controles e como eles são implementados, além de aprovar riscos residuais e aprovar formalmente a implementação desses controles.

Este documento inclui todos os controles relacionados no Anexo A da norma ISO 27001. Os controles são aplicáveis a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI).

Os usuários deste documento são funcionários da [nome da organização] que trabalham no objetivo da SGSI.

2. Documentos de referência

- Norma ISO/IEC 27001, cláusula 6.1.3.d)
- Política de segurança da informação
- Metodologia de avaliação e tratamento de riscos
- Relatório de avaliação e tratamento de riscos

3. Aplicabilidade dos controles

Os seguintes controles do Anexo A da ISO 27001 são aplicáveis:

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.5.1	Políticas de segurança da informação				Todas as políticas referidas abaixo nesta coluna; cada política tem um proprietário designado, que deve rever o documento nos intervalos planejados.	

Commented [AES5]: Inclua o nome da sua organização.

Commented [AES6]: Inclua o nome da sua organização.

Commented [AES7]: 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 [AES8]: Você pode encontrar um modelo para este documento na pasta "06_Avaliacao_e_tratamento_de_riscos" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES9]: Você pode encontrar um modelo para este documento na pasta "06_Avaliacao_e_tratamento_de_riscos" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES10]: Para saber mais sobre os controles do Anexo A da ISO 27001, dê uma olhada neste livro:

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.5.2	Papéis e responsabilidades pela segurança da informação				As papéis e responsabilidades para a segurança da informação são listadas em diversos documentos do SGSI. Se necessário, o [cargo] define outras papéis e responsabilidades.	
A.5.3	Segregação de funções				Qualquer atividade que inclua informações sensíveis é aprovada por uma pessoa e implementada por outra.	
A.5.4	[redacted]				[redacted]	
A.5.5	[redacted]				[redacted]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

[redacted]

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

[redacted]

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

[redacted]

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

[redacted]

Commented [AES11]: Com base nos resultados de avaliação [redacted]

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.5.6	Contato com grupos de interesse especial				O [cargo] é responsável por monitorar [liste os nomes de grupos de interesse e de fóruns de segurança].	
A.5.7	Inteligência de ameaças				[Política de segurança do fornecedor], [Procedimento de gestão de incidentes], [Procedimentos de segurança para o departamento de TI]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

Commented [AES16]: Diferentes grupos de interesse podem

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.5.10	Uso aceitável de informações e outros ativos associados				[Política de segurança de TI], [Política de classificação da informação]	
A.5.11	Devolução de ativos				[Política de segurança de TI], [Política de segurança do fornecedor]	
A.5.12	Classificação das informações				[Política de classificação da informação]	
A.5.13	Rotulagem de informações				[Política de classificação da informação]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.5.18	Direitos de acesso				[Política de controle de acesso], [Política de senhas]	
A.5.19	Segurança da informação nas relações com fornecedores				[Política de segurança do fornecedor]	
A.5.20	Abordagem da segurança da informação nos contratos de fornecedores				[Política de segurança do fornecedor], cláusulas de segurança selecionadas do documento [Cláusulas de segurança para fornecedores e parceiros]	
A.5.21	Gestão da segurança da informação na cadeia de fornecimento de TIC				[Política de segurança do fornecedor]	
A.5.22	[redacted]				[redacted]	
A.5.23	[redacted]				[redacted]	
A.5.24	[redacted]				[redacted]	
A.5.25	[redacted]				[redacted]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

[redacted]

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

[redacted]

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

[redacted]

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

[redacted]

Commented [AES11]: Com base nos resultados de avaliação [redacted]

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.5.26	Resposta a incidentes de segurança da informação				[Procedimento de gestão de incidentes], [Plano de resposta a incidentes]	
A.5.27	Aprendizado com incidentes de segurança da informação				[Procedimento de gestão de incidentes], [Procedimento de ação corretiva], [Formulário de revisão de pós-incidentes]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

Commented [AES17]: Faça isso apenas se a gestão de

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.5.30	Prontidão de TIC para continuidade de negócios				[Plano de recuperação de desastre], [Procedimento de auditoria interna]	
A.5.31	Requisitos legais, estatutários, regulamentares e contratuais				[Procedimento para identificação de requisitos], [Lista de requisitos legais, regulatórios, contratuais e outros], [Política para uso de controles criptográficos]	
A.5.32	Direitos de propriedade intelectual				[Política de segurança de TI]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

[illegible]

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

[illegible]

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

[illegible]

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

[illegible]

Commented [AES11]: Com base nos resultados de avaliação [illegible]

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.5.36	Conformidade com políticas, regras e normas para segurança da informação				Todos os proprietários de ativos de informações, bem como a direção, fazem a revisão regular da implementação dos controles de segurança; o [cargo] é responsável pela verificação da conformidade técnica dos sistemas de informação com os requisitos de segurança.	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

Commented [AES18]: Por exemplo: por currículo, contato com

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.6.3	Conscientização, educação e treinamento de segurança da informação				[Política de segurança da informação], [Plano de treinamento e conscientização], [Treinamento de conscientização em segurança da Advisera], [Política de segurança do fornecedor]	
A.6.4	Processo disciplinar				[Procedimento de gestão de incidentes]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

Commented [AES19]: Veja a lista de vídeos gratuitos de

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.6.7	Trabalho remote				[Política de Segurança de TI] / [Política de dispositivo móvel, teletrabalho e trabalho em home office], [Política traga seu próprio dispositivo (BYOD)]	
A.6.8	Relato de eventos de segurança da informação				[Procedimento de gestão de incidentes]	
A.7.1	Perímetros de segurança física				As áreas seguras são [defina quais] e são protegidas [descreva como].	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

Commented [AES20]: Por exemplo, escritórios, arquivos,

Commented [AES21]: Por exemplo, com paredes, sistemas de

Commented [AES22]: Por exemplo, cartões de acesso, guardas

Commented [AES23]: Por exemplo, com paredes, sistemas de

Commented [AES24]: Por exemplo, porta dos fundos do seu

Commented [AES25]: Por exemplo, com paredes, sistemas de

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.7.4	Monitoramento de segurança física				[Procedimentos para trabalho em áreas seguras]; áreas seguras são monitoradas [descreva como].	
A.7.5	Proteção contra ameaças físicas e ambientais				Um sistema de alarme está instalado e conectado ao [descreva a quem]; câmeras de vigilância estão instaladas; a proteção contra incêndios está implementada [descreva como]; a proteção contra enchentes está implementada [descreva como].	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

Commented [AES26]: Ex.: com monitoramento por vídeo, vigilante.

Commented [AES27]: Ex.: central de monitoramento de

Commented [AES28]: Ex.: sala do servido.

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.7.9	Segurança de ativos fora das instalações da organização				[Política de segurança de TI] / [Política de dispositivo móvel, teletrabalho e trabalho em home office]	
A.7.10	Mídia de armazenamento				[Política de classificação da informação], [Política de segurança de TI], [Procedimentos de segurança para o departamento de TI] / [Política de descarte e destruição]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

Commented [AES29]: Ex.: UPS, gerador, etc.

Commented [AES30]: Por exemplo, protetores de cabos, orifícios e passagens de segurança, tubos de proteção, etc.

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.7.13	Manutenção de equipamentos				O [cargo] deve manter um registro de manutenção para todos os equipamentos de acordo com as instruções do fabricante e garantir a manutenção adequada no momento adequado.	
A.7.14	Descarte seguro ou reutilização de equipamentos				[Procedimentos de segurança para o departamento de TI] / [Política de descarte e destruição]	
A.8.1	Dispositivos endpoint do usuário				[Política de segurança de TI] / [Política de dispositivo móvel, teletrabalho e trabalho em home office] / [Política de mesa limpa e tela limpa], [Política traga seu próprio dispositivo (BYOD)]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.8.5	Autenticação segura				[Política de controle de acesso], [Política de classificação da informação]	
A.8.6	Gestão de capacidade				[Procedimentos de segurança para o departamento de TI]	
A.8.7	Proteção contra malware				[Procedimentos de segurança para o departamento de TI], [Política de segurança de TI]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.8.12	Prevenção de vazamento de dados				[Política de classificação da informação], [Política de segurança de TI], [Procedimentos de segurança para o departamento de TI]	
A.8.13	Cópias de segurança da informação				[Procedimentos de segurança para o departamento de TI] / [Política de cópias de segurança], [Política de segurança de TI]	
A.8.14	Redundância de instalações de tratamento de informações				[Plano de recuperação de desastre]	
A.8.15	Log				[Procedimentos de segurança para o departamento de TI]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

[illegible]

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

[illegible]

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

[illegible]

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

[illegible]

Commented [AES11]: Com base nos resultados de avaliação [illegible]

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.8.20	Segurança de redes				[Procedimentos de segurança para o departamento de TI]	
A.8.21	Segurança dos serviços de rede				[Procedimentos de segurança para o departamento de TI]	
A.8.22	Segregação de redes				[Procedimentos de segurança para o departamento de TI]	
A.8.23	Filtragem da Web				[Política de segurança em TI], [Procedimentos de segurança para o departamento de TI]	
A.8.24	Uso de criptografia				[Política sobre o uso de criptografia]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

[illegible]

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

[illegible]

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

[illegible]

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

[illegible]

Commented [AES11]: Com base nos resultados de avaliação [illegible]

ID	Controles de acordo com a norma ISO/IEC 27001	Aplicabilidade (SIM/NÃO)	Justificativa para a seleção/não seleção	Objetivos do controle	Método de implementação	Status
A.8.30	Desenvolvimento terceirizado				[Política de segurança do fornecedor], [Política de desenvolvimento seguro]	
A.8.31	Separação dos ambientes de desenvolvimento, teste e produção				[Procedimentos de segurança para o departamento de TI], [Política de desenvolvimento seguro]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [AES15]: Indique o status da implementação - por exemplo, "Planejado", "Parcialmente implementado", "Totalmente implementado".

Commented [AES14]: Método de implementação - especifique o documento, controle técnico ou descreva o processo. Deixe em branco caso o controle esteja marcado como não aplicável.

A tabela lista os documentos deste Kit relevantes para cada controle; se não houver documentos relevantes para o controle, uma descrição sugerida do processo é fornecida.

Commented [AES12]: Para aprender mais sobre objetivos de controle, leia este artigo:

Commented [AES13]: Isso deveria ser definido pare cada um de seus controles, e se possível, tornados mensuráveis; no entanto, você também pode copiar os objetivos listados nas categorias de cláusula no Anexo A.

Commented [AES11]: Com base nos resultados de avaliação

4. Aceitação de riscos residuais

Commented [AES31]: A aceitação de riscos residuais deve

Como nem todos os riscos podem ser reduzidos no processo de gestão de riscos, todos os riscos residuais descritos aqui são aceitos:

1. todos os riscos com o valor 0, 1 ou 2
2. [illegible]

Commented [AES32]: Exclua este texto e a tabela se não

[Preencha a tabela com os dados sobre todos os riscos individuais que não são aceitáveis; use a [illegible]

Num.	Nome do ativo	Proprietário do ativo	Ameaça	[illegible]	[illegible]	[illegible]	[illegible]

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

[illegible] **Commented [AES33]:** Isso é apenas uma recomendação; [illegible]

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

- quantidade de não conformidades em função de um método de implementação de controles individuais mal definidos
- [illegible]
- [illegible]

[cargo] **Commented [AES34]:** A Declaração de aplicabilidade precisa [illegible]

[nome]

_____

[assinatura] **Commented [AES35]:** Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.