Tabela de tratamento de riscos

implementado de [data] a [data]

Ativos/ameaças/vulnerabilidades						*Valores antes do tratamento*		
Núm.	**Nome do ativo**	**Proprietário do ativo**	**Ameaça**	**Vulnerabilidade**	**Proprietário do risco**	**Consequência**	**Probabilidade**	**Risco**
1	*software aplicativo*	*gerente de TI*	*erros de aplicações*	falta de controle de dados de entrada e saída	gerente de TI	*2*	*1*	*3*
2	*links de comunicação*	*gerente de TI*	*quebra de relações contratuais*	falta de implementação ou implementação ineficiente de auditoria interna	gerente de TI	*2*	*1*	*3*
3	*software aplicativo*	*gerente de TI*	*erros de aplicações*	conexões de rede pública não protegidas	gerente de TI	*2*	*1*	*3*
4	*escritórios*	*gerente de instalações*	*interrupção no fornecimento de energia*	local sensível a desastres naturais	gerente de instalações	*2*	*1*	*3*
5	*links de comunicação*	*gerente de TI*	*falha nos equipamentos*	local sensível a vazamento de água	gerente de TI	*2*	*1*	*3*

Tratamento do risco		*Valores após tratamento*		
Seleção de opções	**Meios de implementação**	**Consequência**	**Probabilidade**	**Risco**
2. Transferência de riscos para terceir	A.5.20 Abordar a segurança da informaçã	2	0	2
1. Seleção de controles	A.5.22 Monitoramento, revisão e gerenci	2	0	2
2. Transferência de riscos para terceir	A.5.20 Abordar a segurança da informaçã	2	0	2
1. Seleção de controles	A.7.5 Proteção contra ameaças físicas e	2	0	2
1. Seleção de controles	A.7.8 Localização e proteção do equipam	1	0	1
				0
				0
				0
				0
				0
				0
				0
				0

Opções de tratamento de riscos

1. Seleção de controles
2. Transferência de riscos para terceiros
3. Contenção de riscos
4. Aceitação de riscos

Controles de acordo com o Anexo A da norma ISO/IEC 27001

A.5.1 Políticas de segurança da informação
A.5.2 Papéis e responsabilidades pela segurança da informação
A.5.3 Segregação de funções
A.5.4 Responsabilidades da direção
A.5.5 Contato com autoridades
A.5.6 Contato com grupos de interesse especial
A.5.7 Inteligência de ameaças
A.5.8 Segurança da informação no gerenciamento de projetos
A.5.9 Inventário de informações e outros ativos associados
A.5.10 Uso aceitável de informações e outros ativos associados
A.5.11 Devolução de ativos
A.5.12 Classificação das informações
A.5.13 Rotulagem de informações
A.5.14 Transferência de informações
A.5.15 Controle de acesso
A.5.16 Gestão de identidade
A.5.17 Informações de autenticação
A.5.18 Direitos de acesso
A.5.19 Segurança da informação nas relações com fornecedores
A.5.20 Abordagem da segurança da informação nos contratos de fornecedores
A.5.21 Gestão da segurança da informação na cadeia de fornecimento de TIC
A.5.22 Monitoramento, revisão e gestão de mudanças dos serviços de fornecedores
A.5.23 Segurança da informação para uso de serviços em nuvem
A.5.24 Planejamento e preparação da gestão de incidentes de segurança da informação
A.5.25 Avaliação e decisão sobre eventos de segurança da informação
A.5.26 Resposta a incidentes de segurança da informação
A.5.27 Aprendizado com incidentes de segurança da informação
A.5.28 Coleta de evidências
A.5.29 Segurança da informação durante a disrupção
A.5.30 Prontidão de TIC para continuidade de negócios
A.5.31 Requisitos legais, estatutários, regulamentares e contratuais
A.5.32 Direitos de propriedade intelectual
A.5.33 Proteção de registros
A.5.34 Privacidade e proteção de IIP
A.5.35 Análise crítica independente da segurança da informação
A.5.36 Conformidade com políticas, regras e normas para segurança da informação
A.5.37 Procedimentos operacionais documentados
A.6.1 Seleção
A.6.2 Termos e condições de contratação
A.6.3 Conscientização, educação e treinamento em segurança da informação
A.6.4 Processo disciplinar
A.6.5 Responsabilidades após encerramento ou mudança da contratação
A.6.6 Acordos de confidencialidade ou não divulgação
A.6.7 Trabalho remoto
A.6.8 Relato de eventos de segurança da informação
A.7.1 Perímetros de segurança física
A.7.2 Entrada física
A.7.3 Segurança de escritórios, salas e instalações

A.7.4 Monitoramento de segurança física
A.7.5 Proteção contra ameaças físicas e ambientais
A.7.6 Trabalhando em áreas seguras
A.7.7 Mesa limpa e tela limpa
A.7.8 Localização e proteção de equipamentos
A.7.9 Segurança de ativos fora das instalações da organização
A.7.10 Mídia de armazenamento
A.7.11 Serviços de infraestrutura
A.7.12 Segurança do cabeamento
A.7.13 Manutenção de equipamentos
A.7.14 Descarte seguro ou reutilização de equipamentos
A.8.1 Dispositivos endpoint do usuário
A.8.2 Direitos de acessos privilegiados
A.8.3 Restrição de acesso à informação
A.8.4 Acesso ao código fonte
A.8.5 Autenticação segura
A.8.6 Gestão da capacidade
A.8.7 Proteção contra malware
A.8.8 Gestão de vulnerabilidades técnicas
A.8.9 Gestão de configuração
A.8.10 Exclusão de informações
A.8.11 Mascaramento de dados
A.8.12 Prevenção de vazamento de dados
A.8.13 Cópias de segurança da informação
A.8.14 Redundância de instalações de tratamento de informações
A.8.15 Log
A.8.16 Atividades de monitoramento
A.8.17 Sincronização do relógio
A.8.18 Uso de programas utilitários privilegiados
A.8.19 Instalação de software em sistemas operacionais
A.8.20 Segurança de redes
A.8.21 Segurança dos serviços de rede
A.8.22 Segregação de redes
A.8.23 Filtragem da Web
A.8.24 Uso de criptografia
A.8.25 Ciclo de vida de desenvolvimento seguro
A.8.26 Requisitos de segurança da aplicação
A.8.27 Princípios de arquitetura e engenharia de sistemas seguros
A.8.28 Codificação segura
A.8.29 Teste de segurança em desenvolvimento e aceitação
A.8.30 Desenvolvimento terceirizado
A.8.31 Separação dos ambientes de desenvolvimento, teste e produção
A.8.32 Gestão de mudanças
A.8.33 Informações de teste
A.8.34 Proteção de sistemas de informação durante os testes de auditoria