EXEMPLO DE MODELO DE LISTA DE VERIFICAÇÃO PARA AVALIAÇÃO DE RISCOS NA SEGURANÇA CIBERNÉTICA

CONTROLE CONFORME A ISO 27001	FASES DE IMPLEMENTAÇÃO	TAREFAS	EM CONFORMIDADE?	NOTAS
5	***Políticas de segurança da informação***			
5.1	**Orientação do gerenciamento para segurança da informação**			
5.1.1	Políticas de segurança da informação	Há políticas de segurança?	☐	
		Todas as políticas são aprovadas pelo gerenciamento?	☐	
		Evidência de conformidade?	☐	
6	***Organização de segurança da informação***			
6.1	**Funções e responsabilidades da segurança da informação**			
6.1.1	Funções e responsabilidades da segurança	Funções e responsabilidades definidas?	☐	
6.1.2	Segregação de tarefas	Segregação de tarefas definidas?	☐	
6.1.3	Contato com autoridades	Órgão/autoridade de verificação contatada para verificação da conformidade?	☐	
6.1.4	Contato com grupos de interesse especial	Contato estabelecido com grupos de interesse especial relacionados à conformidade?	☐	
6.1.5	Segurança da informação no gerenciamento de projetos	Evidência de segurança da informação no gerenciamento de projeto?	☐	
6.2	**Dispositivos móveis e teletrabalho**			
6.2.1	Política de dispositivos móveis	Política definida para dispositivos móveis?	☐	
6.2.2	Teletrabalho	Política definida para trabalhar remotamente?	☐	
7	***Segurança dos recursos humanos***			
7.1	**Antes da contratação**			
7.1.1	Triagem	Política definida para seleção de funcionários antes da contratação?	☐	
7.1.2	Termos e condições do emprego	Política definida para os termos e condições do RH para contratação?	☐	
7.2	**Durante a contratação**			
7.2.1	Responsabilidades de gerenciamento	Política definida para as responsabilidades do gerenciamento?	☐	
7.2.2	Conscientização, educação e treinamento em segurança da informação	Política definida para conscientização, educação e treinamento em segurança da informação?	☐	
7.2.3	Processo disciplinar	Política definida para processo disciplinar com relação à segurança da informação?	☐	

7.3	**Rescisão e mudança de emprego**			
7.3.1	Responsabilidades de rescisão ou mudança de emprego	Política definida para rescisão do RH ou para mudança de emprego com relação à segurança da informação?	☐	
8	***Gerenciamento de ativos***			
8.1	**Responsabilidades pelos ativos**			
8.1.1	Inventário de ativos	Lista completa de inventário de ativos?	☐	
8.1.2	Propriedade dos ativos	Lista completa de propriedade de ativos	☐	
8.1.3	Uso aceitável dos ativos	Definição de "uso aceitável" da política de ativos	☐	
8.1.4	Retorno dos ativos	Política definida de devolução de ativos?	☐	
8.2	**Classificação da informação**			
8.2.1	Classificação da informação	Política definida para classificação da informação?	☐	
8.2.2	Rotulagem das informações	Política definida para informações de rotulagem?	☐	
8.2.3	Manipulação de ativos	Política definida para manipulação de ativos?	☐	
8.3	**Tratamento da mídia**			
8.3.1	Gerenciamento de mídia removível	Política definida para gerenciamento de mídia removível?	☐	
8.3.2	Descarte de mídia	Política definida para descarte de mídia?	☐	
8.3.3.	Transferência de mídia física	Política definida para transferência de mídia física?	☐	
9	***Controle de acesso***			
9.1	**Responsabilidades pelos ativos**			
9.1.1	Controle da política de acesso	Política definida para controle de acesso?	☐	
9.1.2	Acesso às redes e serviços de redes	Política definida para acesso a redes e serviços de rede?	☐	
9.2	**Responsabilidades pelos ativos**			
9.2.1	Cadastro e cancelamento de cadastro de usuários	Política definida para registro e cancelamento de registro de ativos de usuário?	☐	
9.2.2	Provisionamento de acesso a usuários	Política definida para provisionamento de acesso ao usuário?	☐	
9.2.3	Gerenciamento de direitos de acesso privilegiados	Política definida para gerenciamento de direitos de acesso privilegiado?	☐	

9.2.4	Gerenciamento de informações de autenticação secreta de usuários	Política definida para gerenciamento de informações de autenticação secreta de usuários.	☐	
9.2.5	Análise dos direitos de acesso do usuário	Política definida para revisão dos direitos de acesso de usuário?	☐	
9.2.6	Remoção ou ajuste dos direitos de acesso	Política definida para remoção ou ajuste de direitos de acesso?	☐	
9.3	**Responsabilidades do usuário**			
9.3.1	Uso das informações de autenticação secreta	Política definida para uso de informações de autenticação secreta?	☐	
9.4	**Controle de acesso ao sistema e ao aplicativo**			
9.4.1	Restrições de acesso às informações	Política definida para restrições de acesso às informações?	☐	
9.4.2	Procedimentos seguros de login	Política definida para procedimentos de login seguro?	☐	
9.4.3	Sistema de gerenciamento de senhas	Política definida para sistemas de gerenciamento de senhas?	☐	
9.4.4	Uso de programas utilitários privilegiados	Política definida para uso de programas utilitários privilegiados?	☐	
9.4.5	Controle de acesso a código-fonte de programa	Política definida para controle de acesso a código-fonte de programa?	☐	
10	***Criptografia***			
10.1	**Controles criptográficos**			
10.1.1	Política sobre o uso de controles criptográficos	Política definida para uso de controles criptográficos?	☐	
10.1.2	Gerenciamento de chaves	Política definida para gerenciamento de chaves?	☐	
11	***Segurança física e ambiental***			
11.1	**Áreas seguras**			
11.1.1	Perímetro de segurança física	Política definida para perímetro de segurança física?	☐	
11.1.2	Controles de entrada física	Política definida para controles de entrada física?	☐	
11.1.3	Proteção de escritórios, salas e instalações	A política foi definida para proteção de escritórios, salas e instalações?	☐	
11.1.4	Proteção contra ameaças externas e ambientais	Política definida para proteção contra ameaças externas e ambientais?	☐	
11.1.5	Trabalhando em áreas seguras	Política definida para trabalhar em áreas seguras?	☐	
11.1.6	Áreas de carga e descarga	Política definida para áreas de carga e descarga?	☐	

11.2	**Equipamentos**			
11.2.1	Localização e proteção de equipamentos	Política definida para localização e proteção de equipamentos?	☐	
11.2.2	Utilitários de suporte	Política definida para utilitários de suporte?	☐	
11.2.3	Segurança do cabeamento	Política definida para segurança do cabeamento?	☐	
11.2.4	Manutenção de equipamentos	Política definida para manutenção de equipamentos?	☐	
11.2.5	Remoção de ativos	Política definida para remoção de ativos?	☐	
11.2.6	Segurança de equipamento e ativos fora das instalações	A política foi definida para segurança de equipamentos e ativos fora das instalações?	☐	
11.2.7	Descarte seguro ou reutilização de equipamentos	Descarte seguro ou reutilização de equipamentos?	☐	
11.2.8	Equipamento de usuário sem supervisão	Política definida para equipamento do usuário sem supervisão?	☐	
11.2.9	Política para escrivaninha e tela limpas	Política definida para escrivaninha e tela limpas?	☐	
12	***Segurança das operações***			
12.1	**Procedimentos e responsabilidades operacionais**			
12.1.1	Procedimentos de operação documentados	Política definida para procedimentos de operação documentados?	☐	
12.1.2	Gerenciamento de mudanças	Política definida para gerenciamento de mudanças?	☐	
12.1.3	Gerenciamento da capacidade	Política definida para gerenciamento de capacidade?	☐	
12.1.4	Separação de ambientes de desenvolvimento, testes e operações	A política foi definida para separação de ambientes de desenvolvimento, testes e operações?	☐	
12.2	**Proteção contra malware**			
12.2.1	Controles contra malware	Política definida para controles contra malware?	☐	
12.3	**Backup do sistema**			
12.3.1	Backup	Política definida para backup de sistemas?	☐	
12.3.2	Backup de informações	Política definida para backup de informações?	☐	
12.4	**Registro e monitoramento**			
12.4.1	Registro de eventos	Política definida para registro de eventos?	☐	

12.4.2	Proteção das informações de registros	Política definida para proteção de informações de registros?	☐	
12.4.3	Registro do administrador e operador	Política definida para registro do administrador e do operador?	☐	
12.4.4	Sincronização do relógio	Política definida para sincronização de relógios?	☐	
12.5	**Controle de software operacional**			
12.5.1	Instalação de software em sistemas operacionais	Política definida para instalação de software em sistemas operacionais?	☐	
12.6	**Gerenciamento de vulnerabilidade técnica**			
12.6.1	Gerenciamento de vulnerabilidades técnicas	Política definida para gerenciamento de vulnerabilidades técnicas?	☐	
12.6.2	Restrição à instalação de software	Política definida para restrição à instalação de software?	☐	
12.7	**Considerações sobre auditoria de sistemas de informação**			
12.7.1	Controle de auditoria de sistemas da informação	Política definida para controle de auditoria de sistemas da informação?	☐	
13	***Segurança das comunicações***			
13.1	**Gerenciamento de segurança da rede**			
13.1.1	Controles de rede	Política definida para controles de rede?	☐	
13.1.2	Segurança dos serviços da rede	Política definida para segurança dos serviços da rede?	☐	
13.1.3	Separação em redes	Política definida para segregação em redes?	☐	
13.2	**Transferência de informações**			
13.2.1	Políticas e procedimentos de transferência de informações	Política definida para procedimentos e políticas de transferência de informações?	☐	
13.2.2	Contratos sobre transferência de informações	Política definida para contratos de transferência de informações?	☐	
13.2.3	Mensagens eletrônicas	Política definida para mensagens eletrônicas?	☐	
13.2.4	Contratos de confidencialidade ou não divulgação	Política definida para contratos de confidencialidade ou não divulgação?	☐	
13.2.5	Aquisição, desenvolvimento e manutenção do sistema	A política foi definida para aquisição, desenvolvimento e manutenção de sistemas?	☐	
14	***Aquisição, desenvolvimento e manutenção do sistema***			
14.1	**Requisitos de segurança dos sistemas de informação**			
14.1.1	Análise e especificação de requisitos de segurança da informação	Política definida para análise e especificação de requisitos de segurança da informação?	☐	

14.1.2	Proteção aos serviços de aplicativos em redes públicas	Política definida para proteção de serviços de aplicativos em redes públicas?	☐	
14.1.3	Proteção de transações de serviço de aplicativo	Política definida para proteção de transações de serviço de aplicativo?	☐	
14.2	**Segurança nos processos de desenvolvimento e suporte**			
14.2.1	Desenvolvimento interno	Política definida para desenvolvimento interno?	☐	
15	***Relacionamentos com fornecedores***			
15.1.1	Relacionamentos com fornecedores	Política definida para relacionamentos com fornecedores?	☐	
16	***Gerenciamento de incidentes de segurança da informação***			
16.1.1	Gerenciamento de segurança da informação	Política definida para gerenciamento de segurança da informação?	☐	
17	***Aspectos de segurança da informação no gerenciamento da continuidade dos negócios***			
17.1	**Continuidade da segurança da informação**			
17.1.1	Continuidade da segurança da informação	Política definida para continuidade da segurança da informação?	☐	
17.2	**Redundâncias**			
17.2.1	Redundâncias	Política definida para redundâncias?	☐	
18	***Conformidade***			
18.1	**Conformidade com requisitos legais e contratuais**			
18.1.1	Identificação dos requisitos legais e contratuais aplicáveis	Política definida para identificação dos requisitos legais e contratuais aplicáveis?	☐	
18.1.2	Direitos de propriedade intelectual	Política definida para direitos de propriedade intelectual?	☐	
18.1.3	Proteção de registros	Política definida para proteção de registros?	☐	
18.1.4	Privacidade e proteção de dados pessoais identificáveis	Política definida para privacidade e proteção de dados pessoais identificáveis?	☐	
18.1.5	Regulamentação de controle criptográfico	Política definida para regulamentação do controle criptográfico?	☐	
18.1	**Revisão independente da segurança da informação**			
18.1.1	Conformidade com as políticas e normas de segurança	Política definida para conformidade com as políticas e normas de segurança?	☐	
18.1.2	Revisão da conformidade técnica	Política definida para revisão da conformidade técnica?	☐	

AVISO DE ISENÇÃO DE RESPONSABILIDADE

Qualquer artigo, modelo ou informação fornecidos pela Smartsheet no site são apenas para referência. Embora nos esforcemos para manter as informações atualizadas e corretas, não fornecemos garantia de qualquer natureza, seja explícita ou implícita, a respeito da integridade, precisão, confiabilidade, adequação ou disponibilidade do site ou das informações, artigos, modelos ou gráficos contidos no site. Portanto, toda confiança que você depositar nessas informações será estritamente por sua própria conta e risco.

Este modelo é fornecido apenas como amostra. Este modelo não é, de forma alguma, conselho jurídico ou de conformidade. Os usuários deste modelo devem determinar quais informações são necessárias para alcançar seus objetivos.