**Lista de verificação para projeto de implementação da ISO 27001**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Fases da implementação*** | ***Tarefas*** | ***Documentos do kit a serem usados*** | ***Feito*** |
| *Obter apoio da direção* | Pesquisar quais benefícios da ISO 27001 seriam aplicáveis a sua organização | - |  |
| Apresentar os benefícios para a gestão e obter o comprometimento deles | - |  |
| Obter aprovação formal para iniciar o planejamento do projeto | - |  |
|  |  |  |
| *Preparar para o seu projeto* | Escrever o procedimento para controle de documentos | 01 – Procedimento de controle de documentos e registros |  |
| Educar seu equipe de projeto | - |  |
| Escrever o plano do projeto, incluindo a definição do gerente do projeto, equipe do projeto, patrocinador do projeto, recursos necessários e marcos | 02 – Plano do projeto |  |
| Definir quais partes interessadas precisam ser informadas sobre cada etapa do projeto | - |  |
| Organizar a reunião de abertura | - |  |
|  |  |  |
| *Identificar requisitos* | Definir procedimento para identificar partes interessadas | 03 – Procedimento para identificação de requisitos |  |
| Identificar os requisitos das partes interessadas | 03.1 – Lista de obrigações legais, regulamentares, contratuais e outras |  |
|  |  |  |
| *Definir o escopo, intenção e responsabilidades da direção* | Escrever o documento do escopo do SGSI | 04 – Documento sobre o escopo do SGSI |  |
| Escrever a Política de segurança da informação | 05 – Política de segurança da informação |  |
| Decidir sobre os objetivos de segurança da informação | 05 – Política de segurança da informação |  |
|  |  |  |
| *Realizar a gestão de riscos* | Desenvolver a metodologia de avaliação e tratamento de riscos | 06 – Metodologia de avaliação e tratamento de riscos |  |
| Realizar a avaliação de riscos | 06.1 – Tabela de avaliação de riscos |  |
| Realizar o tratamento de riscos | 06.2 – Tabela de tratamento de riscos |  |
| Escrever o relatório de avaliação de riscos | 06.3 – Relatório de avaliação e tratamento de riscos |  |
|  |  |  |
| *Desenvolver o perfil de segurança da sua organização e plano de ação sobre como atingi-lo* | Desenvolver a Declaração de aplicabilidade | 07 – Declaração de aplicabilidade |  |
| Aceitar os riscos residuais | 07 – Declaração de aplicabilidade |  |
| Desenvolver o Plano de tratamento de riscos | 08 – Plano de tratamento de riscos |  |
|  |  |  |
| *Implementar os controles* | Implementar todos os controles definidos no Plano de tratamento de riscos | Documentos na pasta 09\_Anexo\_A\_Controles\_de\_seguranca |  |
| Manter registros de implementação | Para documentos do SGSI isto é visível através do histórico de versões de um documento; para software isto pode ser algum log sobre teste e liberação. |  |
|  |  |  |
| *Realizar programas de treinamentos e conscientização* | Realizar treinamento para todos os empregados que não possuem as habilidades necessárias | 10 – Plano de treinamento e conscientização |  |
| Realizar programas de conscientização para todos os empregados e terceiros que tem um papel em seu SGSI | 10 – Plano de treinamento e conscientização |  |
|  |  |  |
| *Implementar procedimentos de gestão* | Escrever o procedimento para auditoria interna | 11 – Procedimento de auditoria interna |  |
| Desenvolver o programa de auditoria | 11.1 – Programa anual de auditoria interna |  |
| Definir quais medições a serem realizadas, relacionadas aos objetivos do SGSI e controles | 12.1 – Relatório de medição |  |
| Identificar fontes de informação a serem usadas para a análise crítica pela gestão | 12.2 – Minutas da análise crítica pela direção |  |
| Escrever o procedimento para ações corretivas | 13 – Procedimento de ação corretiva |  |
|  |  |  |
| *Operar o SGSI* | Manter todos os registros requeridos pelas suas políticas e procedimentos | Vários registros e logs que são criados devido a documentos do SGSI – ex.: log de cópias de segurança (do software de cópias de segurança), Lista de obrigações legais, regulamentares, contratuais e outras preenchida, etc. |  |
| Realizar ações corretivas conforme necessário como consequência de melhorias necessárias para a operação do SGSI | 13.1 – Formulário de ação corretiva |  |
|  |  |  |
| *Monitorar e medir o SGSI* | Assegurar o monitoramento de todos os seus sistemas | Registros de monitoramento definidos em cada documento implementado, ex.: número de incidentes, número de erros em um sistema em particular, etc. |  |
| Medir se os objetivos para o SGSI e para os controles foram atingidos | 12.1 – Relatório de medição |  |
|  |  |  |
| *Realizar auditoria interna* | Realizar auditoria(s) interna | 11.3 – Checklist de auditoria interna |  |
| Escrever um relatório de auditoria interna | 11.2 – Relatório de auditoria interna |  |
| Realizar ações corretivas como consequência de não conformidades encontradas durante a auditoria interna | 13.1 – Formulário de ação corretiva |  |
|  |  |  |
| *Realizar análise crítica pela direção* | Realizar a análise crítica pela direção | - |  |
| Manter registros da análise crítica pela direção | 12.2 – Minutas da análise crítica pela direção |  |
| Realizar ações corretivas como consequência de melhorias identificadas durante a análise crítica pela direção | 13.1 – Formulário de ação corretiva |  |
|  |  |  |
| *Auditoria de certificação* | Obter propostas de vários organismos de certificação | - |  |
| Selecionar o organismo de certificação | - |  |
| Estágio 1 da auditoria de certificação | - |  |
| Estágio 2 da auditoria de certificação | - |  |
| Visitas de supervisão | - |  |
|  |  |  |