ADEQUAÇÃO À NORMA ABNT NBR ISO 27001 – GESTÃO DE SEGURANÇA DA INFORMAÇÃO

1. Tema

Produção e Qualidade

2. Subtema

Gestão da Qualidade

3. Categoria de serviço

Acesso a Serviços de Terceiros

4. Tipo de serviço / instrumento

Consultoria Tecnológica / Acesso a Serviço Tecnológico

5. Modalidade

Presencial

6. Público alvo

Me e EPP

7. Setor indicado

Agronegócio, Comércio, Indústria e Serviços

8. Macrossegmento

-

9. Descrição

ETAPA 01 | ALINHAMENTO DA PROPOSTA

Realizar reunião de abertura junto à empresa demandante, para nivelamento do escopo do trabalho e validação do planejamento de execução dos serviços, composto de cronograma resumido com os principais eventos, agendas de reuniões e definição dos responsáveis pelo acompanhamento dos serviços por parte da empresa

demandante. Ferramentas como entrevista com o cliente são importantes como forma de obter informações necessárias para fundamentar a entrega proposta.

ENTREGA ETAPA 01: Documento contendo os responsáveis pela prestação do serviço, o escopo do serviço, o plano de ação com o cronograma das atividades e outros aspectos acordados entre as partes, assinado pela empresa demandante.

ETAPA 02 | DIAGNÓSTICO E PLANO DE AÇÃO

Diagnóstico da empresa em relação aos seguintes itens, quando aplicáveis:

- Processos de planejamento e gestão ligados à liderança;
- Processos de suporte;
- Processos de operação da empresa;
- Processos de avaliação de desempenho e melhoria.

ENTREGA ETAPA 02: Relatório do diagnóstico, com o plano de desenvolvimento das ações.

ETAPA 03 | SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO E AUDITORIA INTERNA

Com base no(s) diagnóstico(s) realizado(s) na etapa anterior, deve-se organizar as informações e orientar a empresa para o processo de implantação do Sistema de Gestão da Segurança da Informação ABNT NBR ISO 27001, como recomendado:

- Propor estratégias e política de segurança da informação;
- Definir e organizar os processos de trabalho da empresa;
- Levantar os riscos e oportunidades, avaliação e tratamento do risco;
- Criar procedimentos e normas internas;
- Criar indicadores de desempenho;
- Capacitar os empregados da empresa na ABNT NBR ISO 27001;
- Orientar e acompanhar a realização de auditoria interna;
- Orientar no tratamento das não-conformidades/oportunidades de melhoria identificadas na auditoria interna.

ENTREGAS ETAPA 03:

- Relatório técnico final contendo bases e premissas utilizadas, tarefas executadas, resultados obtidos (inclusive com registros fotográficos), oportunidades de melhoria a partir da auditoria interna, pontos auditados, recomendações, conclusões e, se for o caso, as não conformidades identificadas, orientando a empresa na implementação das ações corretivas necessárias; assinado pela empresa demandante.
- Declaração, assinada pela empresa demandante, atestando o recebimento da(s) entrega(s) realizadas pela prestadora de serviço e que a prestadora de serviço explicou à empresa demandante o conteúdo da(s) entrega(s) efetivadas.
- Comprovação da capacitação dos empregados da empresa, abrangendo o conteúdo da ABNT NBR ISO 27001.

10. Benefícios e resultados esperados

A norma ISO 27001 é uma referência internacional para a gestão da segurança da informação. A norma tem como princípio geral a adopção pela organização de um conjunto de requisitos, processos e controles com o objetivo de mitigarem e gerirem adequadamente o risco.
A adoção da norma ISO 27001 serve para que as organizações implantem um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um Sistema de Gestão de Segurança de Informação. Isso permite que proteja todos os dados financeiros e confidenciais de maneira mais eficiente, minimizando a probabilidade de serem acessados ilegalmente ou sem permissão.

11. Estrutura e materiais necessários

-

12. Responsabilidade da empresa demandante

1. Aprovar a proposta do Sebrae, valores e condições de pagamento.
2. Conhecer e validar a proposta de trabalho, o escopo das etapas e as entregas da prestadora de serviço.
3. Disponibilizar agenda prévia para visitas, reuniões e atividades propostas pela prestadora de serviço.
4. Fornecer informações técnicas sobre os processos, produtos ou serviços à prestadora de serviço para o desenvolvimento do trabalho.
5. Acompanhar a prestadora de serviço em visita(s) técnica(s) aos espaços físicos, se previsto no escopo do trabalho.
6. Avaliar o serviço prestado.

13. Responsabilidade da prestadora de serviço

1. Realizar reunião para alinhamento e apresentação das atividades previstas.
2. Analisar a demanda e as informações fornecidas pela empresa.
3. Elaborar proposta, escopo de trabalho, cronograma das etapas do trabalho, agenda de reuniões e atividades, sendo necessário validar com a empresa demandante.
4. Fornecer as entregas previstas, validadas pela empresa demandante, ao Sebrae.
5. Cumprir com as obrigações previstas no Regulamento do Sebraetec.

14. Perfil desejado da prestadora de serviço

Corpo técnico com experiência comprovada de pelo menos 3 (três) anos na implementação de sistemas de gestão de segurança da informação.

15. Pré-diagnóstico

Faz-se necessário o levantamento das seguintes informações, quando do recebimento da demanda:

1. A empresa já tem esta certificação? Qual foi o organismo certificador?
2. A organização contratou serviços de consultoria para auxílio na implantação do sistema de gestão?
3. Quais unidades/filiais devem ser certificadas?
4. Quais serão os processos abrangidos pelo sistema de gestão de segurança da informação?
5. Qual a quantidade de empregados envolvidos nos processos a serem abrangidos pelo sistema de gestão da qualidade?
6. Quantos setores/unidades/células serão envolvidos pelo sistema de gestão de segurança da informação?
7. A empresa tem uma política de qualidade conhecida pelos seus empregados e clientes?
8. A empresa dispõe de um representante da direção?
9. A empresa dispõe de rotinas e procedimentos descritos para os seus principais processos?
10. A empresa utiliza indicadores para monitorar os seus processos?
11. Há uma demanda externa, regulamentar ou de mercado, para a certificação do sistema de gestão de segurança da informação da empresa?

16. Observações

1. Na impossibilidade desta ficha técnica ser aplicada presencialmente, ela poderá ser aplicada de forma remota (ferramentas de videoconferência, ligações telefônicas, aplicativos de mensagens e/ou e-mails). No momento da contratação a empresa demandante deverá ser comunicada que parte do serviço ou a integralidade dele, quando aplicável, acontecerá de forma remota. Além disso, o alinhamento do formato do atendimento deve ser feito na Etapa 01 entre a empresa demandante e a prestadora de serviço tecnológico;
2. Na impossibilidade de as entregas serem assinadas fisicamente pela empresa demandante, elas poderão ser validadas via assinatura digital, aceite eletrônico ou e-mail, em que a empresa demandante deverá manifestar o aceite e encaminhar para a prestadora de serviço tecnológico, e esta deverá incluir o comprovante de validação da empresa demandante nas entregas para o registro do atendimento;
3. Os valores dos honorários apresentados pela prestadora de serviço devem incluir todas as despesas com impostos e encargos sociais, conforme legislação tributária em vigor, que possa incidir sobre o objeto da proposta;
4. Despesas adicionais com terceiros (direitos autorais, fotografias, hospedagem, imagens, registro de domínio, revisões, textos, conteúdo dinâmico, entre outros) ficam a cargo exclusivo da empresa demandante e devem ser previamente autorizadas por ela durante a validação da proposta de trabalho;
5. É de responsabilidade da prestadora de serviço todo o trabalho, da concepção à aprovação da empresa demandante.

6. A prestadora de serviço não pode ser responsabilizada por erros de terceiros contratados pela empresa demandante.

HISTÓRICO DE ALTERAÇÕES			
Versão	Data	Link	Responsável
1	27/08/2019	https://datasebrae.com.br/wp-content/uploads/2019/08/Adequação-à-norma-ABNT-NBR-ISO-27001-Gestão-de-Segurança-da-Informação-GQ13054-1.pdf	Eduardo Cardoso Garrido
2	15/04/2020	https://datasebrae.com.br/wp-content/uploads/2020/04/Adequação-à-norma-ABNT-NBR-ISO-27001-Gestão-de-Segurança-da-Informação-GQ13054-2.pdf	Coordenação Sebraetec