

TERMO DE REFERÊNCIA PARA CONTRATAÇÃO DE SERVIÇOS DE AUDITORIA EXTERNA DE PRIMEIRA SUPERVISÃO DA ISO 27001:2013, MIGRAÇÃO PARA ISO 27001:2022 E CERTIFICAÇÃO DOS SISTEMAS DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DA PRODAM NA ISO 27701

1. JUSTIFICATIVA DA CONTRATAÇÃO

A PRODAM conquistou a certificação ISO 27001:2013 para seu Sistema de Gestão da Segurança da Informação (SGSI) em 2023. Buscando manter a conformidade com as normas vigentes, planeja realizar a auditoria de primeira supervisão da ISO 27001:2013 e migrar para a certificação ISO 27001:2022 em 2024. Reconhecendo a importância da privacidade das informações pessoais, a PRODAM também almeja a certificação ISO 27701 para seu Sistema de Gerenciamento de Informações de Privacidade (SGIP). Portanto, a contratação de uma auditoria externa se faz necessária para avaliar e assegurar a adequação do SGSI à nova versão da norma e certificar o SGIP.

2. OBJETO

Contratação dos serviços para realizar a auditoria externa de primeira supervisão da ISO 27001:2013, a migração do SGSI da PRODAM da ISO 27001:2013 para a ISO 27001:2022, e a certificação do SGIP conforme a ISO 27701. As auditorias serão realizadas de acordo com as datas acordadas entre a Contratada e a PRODAM, preferencialmente no 2º semestre de 2024, com o prazo máximo até 31 de outubro de 2024, coincidindo com a auditoria de recertificação do Sistema de Gestão da Qualidade da PRODAM na ISO 9001:2015.

3. DESCRIÇÃO DETALHADA DOS SERVIÇOS

3.1. Auditoria de Primeira Supervisão da ISO 27001:2013:

- Realizar a auditoria de primeira supervisão do SGSI da PRODAM na ISO 27001:2013.
- Escopo: "Hospedagem em Data Center, Projeto e Desenvolvimento de sistemas e execução de soluções em Tecnologia da Informação e Comunicação para os processos de negócio, incluindo Sistemas de trânsito, educação e administrativos do setor público, conforme a Declaração de Aplicabilidade versão 08.3."

3.2. Auditoria de Migração (ISO 27001:2022):

- Realizar a auditoria de migração do SGSI da PRODAM, assegurando a conformidade com as normas ISO 27001:2022.

- Escopo: "Hospedagem em Data Center, Projeto e Desenvolvimento de sistemas e execução de soluções em Tecnologia da Informação e Comunicação para os processos de negócio, incluindo Sistemas de trânsito, educação e administrativos do setor público, conforme a Declaração de Aplicabilidade versão 08.3."

3.3. Auditoria de Certificação (ISO 27701:2019):

- Realizar a auditoria de certificação do SGIP da PRODAM, garantindo a conformidade com os requisitos da norma ISO 27701:2019.

4. ABRANGÊNCIA DOS SERVIÇOS

As auditorias abrangerão todos os documentos e processos relacionados aos Sistemas de Gestão da Segurança da Informação e de Gerenciamento de Informações de Privacidade da PRODAM, incluindo, mas não se limitando aos seguintes documentos:

- **Atas de Análise Crítica do SGSI;**
- **Documentação Externa Aplicável;**
- **Planejamento Estratégico**

- **SI10**-Política de Privacidade - Externa;
- **SI11**-Política de Privacidade - Interna;
- **SI12** - Política de Cookie;
- **SI13-LGPD** - Minuta com Regras de Proteção de Dados Pessoais para Contrato de Clientes;
- **SI14** - Política para exercício de direitos pelo titular de dados pessoais;
- **SI15** - LGPD - Termo de Consentimento (Obtenção e Revogação);
- **SI16** - LGPD - Guia de Elaboração do Relatório de Impacto de Proteção de Dados Pessoais;
- **SI17** - LGPD - Mapeamento e Registro das Atividades de Tratamento;
- **SI2**-Política da Segurança da Informação;
- **SI3**-Termo de responsabilidade e confidencialidade para colaboradores;
- **SI4**-Manual do Sistema de Gestão da Segurança da Informação;
- **SI5**-Plano de continuidade de negócios;
- **SI6**-Termo de Responsabilidade para Fornecedores e Parceiros - Processamento;
- **SI7** - Termo de Responsabilidade para Fornecedores e Parceiros - Desenvolvimento;
- **SI8**-Objetivos da Segurança da Informação e Monitoramento Operacional;
- **SI9**-Termo de Responsabilidade e Confidencialidade para Colaborador de Prestador de Serviços;
- **Estorganiz2** - Regimento Interno e Organograma Oficial;
- **NOR4**- Norma de classificação da informação;
- **NOR4**-Norma de classificação da informação;
- **NOR1**-Uso seguro de redes sociais;
- **NOR10**-Norma de Desenvolvimento Seguro;
- **NOR11**-Norma de Estações de Trabalho;
- **NOR2**-Norma de acesso à internet e serviços específicos;
- **NOR3**-Norma de backup e recuperação de arquivos;
- **NOR5**-Norma de uso de dispositivos móveis;
- **NOR6**-Norma de gestão de ativos;
- **NOR7**-Norma de gestão de logs;
- **NOR8**-Norma de Gestão de Acesso Lógico;
- **NOR9**-Norma de controles criptográficos;
- **Proced9**-Auditoria Interna do SGSI.

5. VÍNCULO EMPREGATÍCIO

O(a) contratado(a) prestará serviços como profissional autônomo, sem qualquer vínculo empregatício com a PRODAM.

6. EXIGÊNCIAS PARA CONTRATAÇÃO

6.1. A empresa contratada deve apresentar declaração de aptidão e experiência em auditorias de primeira supervisão da ISO 27001, migração de SGSI para a versão 2022 e certificação ISO 27701:2019 em empresas do porte da PRODAM, com atestados fornecidos por entidades idôneas, comprovando a execução de serviços de auditoria em ISO 27001 e ISO 27701 em empresas com requisitos semelhantes.

6.2. Deve ser apresentada uma relação das empresas certificadas em ISO 27001: 2013, ISO 27001:2022 e ISO 27701:2019 no Brasil onde a contratada atuou.

6.3. A contratada deve comprovar seu credenciamento junto a órgãos acreditadores nacionais e internacionais para realizar auditorias de certificação.

7. ACOMPANHAMENTO DO SERVIÇO

A Supervisão da Qualidade da PRODAM será responsável pelo controle, acompanhamento e relacionamento direto com a contratada para garantir a execução dos serviços conforme especificado.

8. RESPONSABILIDADES DA CONTRATADA

8.1. A contratada será responsável por todas as despesas de transporte, alimentação e estadia de sua equipe para os eventos necessários à execução do contrato, realizados nas instalações da PRODAM em Manaus-AM.

8.2. Deve entregar o relatório de cada auditoria em até 5 dias úteis após a realização da auditoria.

8.3. A contratada fornecerá um questionário de avaliação de seus auditores, a ser preenchido e devolvido pela contratante.

9. RESPONSABILIDADES DA CONTRATANTE

9.1. A contratante fornecerá à contratada todas as informações e condições necessárias ao cumprimento do objeto em tempo hábil.

9.2. Realizará o pagamento pelos serviços prestados conforme descrito no documento, com a possibilidade de reajuste nos valores do contrato de acordo com o índice de inflação.

10. CLÁUSULA DE SIGILO E CONFIDENCIALIDADE

A contratada se compromete a seguir as diretrizes da Política de Segurança da Informação da PRODAM e a assinar o Termo de Responsabilidade e Sigilo fornecido pela contratante.

11. PAGAMENTO DA CONTRATADA

11.1. Após a conclusão satisfatória de cada auditoria, a contratada receberá o valor correspondente. O mesmo procedimento será seguido em futuros anos, se necessário, com a possibilidade de reajuste dos valores de acordo com o índice de inflação.

12. Matriz de Riscos

LEVANTAMENTO DE RISCOS

IDENTIFICAÇÃO DO RISCO	PROBABILIDADE	IMPACTO	IMPORTÂNCIA
R.1. Possíveis desafios na implementação dos controles e práticas recomendadas pelas normas ISO/IEC 27001:22 e ISO/IEC 27701:19	2	2	4
R.2. Resistência interna à adoção de novas práticas e controles por parte dos colaboradores.	2	2	4
R.3. Possíveis conflitos ou desalinhamentos com os processos e práticas já estabelecidos na PRODAM.	1	2	2
R.4. Problemas técnicos durante a implementação ou auditoria, como falhas em sistemas de segurança da informação.	1	3	3
R.5. Potenciais ameaças à segurança da informação durante a transição e implementação.	2	3	6
R.6. Possíveis atrasos na implementação e conclusão do processo de certificação.	2	2	4
R.7. Desafios relacionados a não conformidades com requisitos legais e regulatórios.	1	3	3
R.8. Dificuldades na manutenção dos requisitos após a certificação.	2	2	4

	PROBABILIDADE	ALTA = 3	MÉDIA = 2	BAIXA = 1	IMPORTÂNCIA
IMPACTO	ALTO = 3	9	6	3	ALTA

Nível de Classificação
Público

Grupo de acesso
PRODAM

	MÉDIO = 2	6	4	2	MÉDIA
	BAIXO = 1	3	2	1	BAIXA

Solicitante:

Leomax Paulino de Azevedo

Supervisor da Qualidade

Manaus – AM, 23 de janeiro de 2024