



## Curso Lead Implementer para a Gestão da Privacidade da Informação (Baseado na NBR ISO 27701)

### PROGRAMA DETALHADO

**DIA :13/04/2020**

**Instrutor:** Carlos Alberto Iglesia Bernardo

**Carga Horária:**4h (8:30/12:30)

**Módulo I:** A Norma ISO 29100: Tecnologia da informação-Técnicas de segurança: Estrutura de Privacidade.

- Escopo
- Termos e definições relacionados com privacidade
- Elementos básicos da estrutura de privacidade
- Visão geral da estrutura de privacidade
- Atores e papéis
- Interações
- Reconhecendo DP
- Requisitos de salvaguarda de privacidade
- Políticas de privacidade
- Controles de privacidade
- Os princípios de privacidade
- Correspondência entre conceitos da ISO 29100 e conceitos da ISO 27000



**Instrutor:** Ariosto Farias Jr

**Carga Horária:** 4h (13:30/17:30)

**Módulo II:** A Norma NBR ISO 27701:2019-Técnicas de segurança-Extensão da NBR ISO 27001 e NBR ISO 27002 para gestão da privacidade da informação -Requisitos e diretrizes

- Histórico e evolução das normas ISO 27001, ISO 27002 e ISO 27701.
- Termos e definições relacionados com Sistemas de Gestão, Riscos e Segurança da informação.
- Motivos para adotar a ISO 27701

=====

**DIA :14/04/2020**

**Instrutor:** Ariosto Farias Jr

**Carga Horária:** 8h (8:30/17:30)

**Módulo II:** A Norma NBR ISO 27701:2019-Técnicas de segurança-Extensão da NBR ISO 27001 e NBR ISO 27002 para gestão da privacidade da informação -Requisitos e diretrizes:

- Requisitos específicos de um Sistema de Gestão da Privacidade da Informação-SGPI apropriados para uma organização que atue como um **Controlador de DP** ou como um **Operador de DP**
- Controles e objetivos de controles da ISO 27001
- Controles e objetivos de controles específicos de um SGPI para uma organização que atue como um **Controlador de DP**
- Controles e objetivos de controles específicos de um SGPI para uma organização que atue como um **Operador de DP**
- Diretrizes específicas de um SGPI relacionadas com a ISO 27002
- Diretrizes adicionais da ISO 27002 para **Controladores** de Dados Pessoais-DP
- Diretrizes adicionais da ISO 27002 para **Operadores** de Dados Pessoais-DP
- Mapeamento dos controles da ISO 27701 com o Regulamento da União Europeia sobre a Proteção de Dados.
- Mapeamento da ISO 27701 com o a LGPD-Lei Geral de Proteção de Dados.
- As normas da família ISO 27000 que apoiam a ISO 27701 (ISO 27000, ISO 27003, ISO 27004, ISO 27007 e ISO 27018)

=====



**DIA: 15/04/2020**

**Instrutor:** Rafael Batista

**Carga Horária:** 4h (8:30/12:30)

**MÓDULO III : A Norma ISO 29134:Security techniques – Guidelines for Privacy Impact Assessment (PIA)**

- Preparação: O que é, Por que fazer (benefícios), Objetivos, Papéis e responsabilidades
- Diretrizes: Definição da equipe de trabalho, planejamento e recursos necessários (humanos e financeiros), Definição do escopo e Identificação e envolvimento das partes interessadas
- Execução: Fluxo de dados pessoais, Como são coletados, Porque são coletados, Quem são os responsáveis pelos dados, Tipo de processamento realizado, Diretrizes para proteção de privacidade, Descrição dos controles de segurança da informação e privacidade existentes e necessários baseado na ISO 29100
- Avaliação dos riscos de segurança da informação e privacidade: Identificação, Análise, Tratamento dos riscos, Opções de tratamento e Definição dos controles
- Controles estabelecidos na legislação e controles exigidos por procedimentos internos ou externos
- Tópicos do PIA que serão levados a conhecimento das partes interessadas pertinentes

**Instrutor:** Nilton S. Moreira

**Carga Horária:** 4h (13:30/17:30)

**Módulo IV : NBR ISO 27005: 2019 - Gestão de riscos de segurança da informação, alinhada e orientada para a gestão da privacidade da informação**

- Gestão de Riscos – Visão Geral
- Estabelecimento do contexto
- Avaliação dos riscos de segurança da informação e privacidade
- Identificação, Análise e Avaliação de Riscos
- Tratamento de Riscos: Estabelecimento de um Plano de Tratamento de Riscos de Segurança da Informação e privacidade da informação
- Comunicação e Consulta
- Monitoramento e Análise crítica

=====



**DIA:16/04/2020**

**Instrutor:** Uelinton Santos

**Carga horária:**4h (8:30/12:30)

**MÓDULO V :** A ISO 29151:2020 Tecnologia da informação – Técnicas de segurança – Código de prática para proteção de dados pessoais

- Escopo
- Termos e definições
- Aspectos Gerais (Objetivo, requisitos, controles, seleção de controles, diretrizes da organização, ciclo de vida, estrutura da norma)
- Diretrizes adicionais de implementação e outras informações para determinados controles existentes relevantes descritos na ISO / IEC 27002
- Conjunto estendido de controles para proteção de DP

**Instrutor:** Willian Bitencourt

**Carga horária:**2h (13:30/15:30)

**Módulo VI:**A Norma ISO 27035- Gestão de incidentes de segurança da informação Parte 3: Diretrizes para operações de respostas a incidentes de TIC, alinhada e orientada para a gestão da privacidade da informação

- O que é Incidente de Segurança da Informação e Privacidade da Informação-SIPI
- Monitorando, detectando e notificando um Incidente de SIPI
- Notificando e classificando um Incidente de SIPI
- Evento versus Incidente, Tipos e classificações de SIPI
- Procedimentos de Resposta e Tratamento de Incidentes de SIPI
- Políticas, procedimentos e Planos de Tratamento
- Contenção, Recuperação e Erradicação
- Processo Disciplinar
- Coleta de Evidências, Produção de Laudos ou Relatórios
- Aprendendo com os Incidentes de SIPI
- Análise de Causa Raiz
- Conscientização
- Indicadores e melhoria contínua.



ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS  
FORO NACIONAL DE NORMALIZAÇÃO  
CERTIFICADORA DE PRODUTOS E SISTEMAS

**Instrutor:** Bruno Basso

**Carga horária:** 2h (15:30/17:30)

**Módulo VII :** Benchmarking da NBR ISO 27701 com as regulamentações do GDPR e de outras legislações aplicáveis à proteção de Dados Pessoais

- A importância do *General Data Protection Regulation* (Regulamento Geral de Proteção de Dados da União Europeia) para o SGPI
- A Lei Geral de Proteção de Dados Pessoais no contexto do SGPI

**DIA:**17/04 (Manhã)

**Exame:** 9:00/12:00