Segurança Cibernética com base na Resolução CNJ 396/2021

Instrutora: Eduardo Chaves Ferreira

Graduado em Engenharia da Computação pelo Instituto Militar de Engenharia (IME). Doutorado em modelagem matemática computacional – ênfase em análise de dados – pelo Laboratório Nacional de Computação Científica (LNCC). Bacharel em Direito pelo IESB. Auditor Federal de Controle Externo (AFCE-TCU) - Diretor da área de segurança e infraestrutura de dados.

Apresentação

Tendo em vista o aumento de ameaças cibernéticas, conforme demonstrado por recentes incidentes de segurança em órgãos e empresas do setor público brasileiro, torna-se necessária a criação de Programas de Segurança Cibernética, com vistas a implantar sistemas adequados de proteção.

Com essa finalidade, o Conselho Nacional de Justiça (CNJ) instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ – Resolução CNJ 396/2021), que traz diretrizes para que órgãos do Poder Judiciário implantem seus Programas Internos de Segurança da Informação.

A Estratégia traz recomendações para: avaliar a situação dos órgãos (assessment interno); realizar análise de risco e validação de objetivos a serem alcançados; implantar mecanismos de proteção cibernética; validar a implantação do sistema de gestão de segurança; atender a determinações do controle interno e externo; estabelecer bases normativas internas; estruturar equipes e responsabilidades; promover a mudança cultural; desenvolver processo de comunicação de incidentes de segurança da informação e criar a governança necessária para manter todas as atividades citadas.

A complexidade dessa estratégia faz com que muitos órgãos enfrentem dificuldades na sua concepção, implantação e acompanhamento; tornando demorada a tomada de decisão e a execução de ações para enfrentamento de ameaças. Tal demora torna organizações vulneráveis à ocorrência de incidentes e as sujeitam a sanções previstas na legislação e por órgãos de controle.

O curso tem por objetivo apresentar o passo-a-passo para a implantação da Estratégia de Segurança Cibernética, conforme previsto na Resolução CNJ 396/2021, com abordagem prática e visão dos requisitos essenciais para o programa, bem como capacitar gestores a desenhar, implantar e acompanhar o Programa de Segurança Cibernética do órgão, em conformidade com a Resolução, indicando práticas, técnicas e ferramentas a serem utilizadas.

Programa:

1. **Principais Riscos e Vulnerabilidades**
   a. Classes de ataques cibernéticos e Vulnerabilidades dos sistemas de informação
2. **Resolução CNJ 396/2021 – Comparação com padrões internacionais e normas internas de órgãos brasileiros**
   a. Estrutura da resolução: PSEC-PJ, ENSEC-PJ e PCESC-PJ e Comparação com padrões internacionais: ISO 27000, OWASP, NIST e CIS
   b. Normas Poder Executivo: PNSIC, PNSI, E-Ciber, ENSIC, PLANSIC e GSI INs 01, 03 e 05
3. **Avaliação interna (assessment) da segurança da informação no órgão**
   a. Avaliação de sistemas de informação *on-premises*
   b. Impactos da adoção de nuvem pública, de serviço IaaS, PaaS e SaaS e do trabalho remoto
   c. Modelo CIS V8 para assessment interno (análise dos 18 controles)
4. **Análise dos riscos para priorização de ações**
   a. Análise de risco em TI, entendendo probabilidade e impacto, e seleção de controles baseada em risco
   b. CIS Risk Assessment Method - RAM
5. **Estruturação do Programa de Segurança Cibernética**
   a. Sistema de Gestão da Segurança da Informação e Programa de Segurança da Informação
   b. Política Corporativa de Segurança da Informação e Treinamento, Estrutura Organizacional, Auditoria e Orçamento
6. **Equipe, estrutura interna e governança para suporte à segurança**
   a. Comitê de Governança de Segurança da Informação e Encarregado pelo tratamento de dados (LGPD)
   b. Gestor de segurança da informação e Gestor de conformidade
   c. Gestor de riscos de Segurança da Informação e Gestor de riscos de Continuidade de Negócios
   d. Equipes de Tratamento de Incidentes
7. **Impactos no planejamento institucional, na cultura e em treinamentos**
   a. Compromisso alta gestão, PET, Plano de Gestão, Estratégia Digital e PDTI
   b. Mudança cultural e treinamentos especializados
8. **Política de Segurança Cibernética**
   a. Escopo, Conceitos, Princípios, Diretrizes, Competências, Penalidades e Atualização
   b. Normativos requeridos pelas ISO 27002 – 5, pelas IN 01 e IN 05 – GSI e na Portaria CNJ 162/2021
9. **Acompanhamento da execução do Programa e questões de auditoria**
   a. Gestão ágil do plano e engajamento de equipes e Questões de auditoria com base no CIS
10. **Portaria CNJ 162/2021 - Resposta a incidentes: Prevenção, Gerenciamento, Investigação e ETIR**
    a. Protocolo de Prevenção de Incidentes Cibernéticos, Protocolo de Gerenciamento de Crises Cibernéticas e Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário

Público-alvo: gestores e técnicos de órgãos do Poder Judiciário, nos níveis estratégico e tático. Gestores e equipes das áreas de Auditoria Interna, Gestão de Riscos e *Compliance*.

Benefícios para os Participantes: o treinamento capacita o participante a avaliar, planejar, implantar e acompanhar a execução de um programa interno de segurança cibernética.

Ao término do curso o participante receberá certificado emitido pelo Instituto Brasileiro de Governança Pública (IBGP).

Carga Horária: 20 horas

Solicite uma Proposta para Cursos *In Company*
Para mais informações, acesse:

[Curso Segurança Cibernética com base na Resolução CNJ 396/2021]