Treinamento

Certificação Digital + Criptografia

O Treinamento de Certificação Digital e Criptografia da e-Sec é focado nas equipes das organizações e abrange fundamentos, operação, administração e desenvolvimento de soluções que utilizem certificação digital e/ou criptografia. Os treinamentos são elaborados de acordo com as demandas específicas de cada organização, adaptando-se conforme as necessidades dos clientes.

Programação em Certificação Digital - Java

Esta modalidade do curso abordará o suporte à Criptografia e Certificação Digital disponibilizado pela Plataforma JAVA. O objetivo é permitir que um desenvolvedor Java integre, em suas aplicações, serviços como sigilo, integridade e autenticidade utilizando somente as funcionalidades nativas da Plataforma Java.

Pré-requisitos: Fundamentos em Certificação Digital – Módulo Básico

Carga horária: 40h

- Suporte à Segurança na Plataforma Java
  - Segurança na Linguagem
  - Suporte à Criptografia
  - Controles de Acesso e Autenticação
  - Comunicação Segurança
  - Infraestrutura de Chaves Públicas (PKI)
- Introdução à JCA/JCE
  - Princípios
  - Providers
  - Engines
- Criptografia Simétrica
- Geração de Chaves Secretas
- Criptografia Assimétrica
- Geração de Par de Chaves
- Funções de Hash
- MAC
- Assinatura Digital
- Certificação Digital
  - Leitura de Certificados
  - Campos do Certificado Digital

- Verificação da situação de Revogação
  - Leitura de CRL
- Cadeias de Certificação
  - Certificados Confiáveis
  - Montagem de uma cadeia de certificados
  - Verificação de uma cadeia de certificados
  - Habilitando suporte à OCSP
- Repositório de Chaves e Certificados
  - Acessando KeyStores
  - Repositórios PKCS#12
- Dispositivos Criptográficos
  - Padrão PKCS#11
  - Uso do Provider SunPKCS11
  - Assinatura digital usando hardware
  - Acessando o Repositório de Chaves do Windows
- Comunicação Segura em Java
  - Framework JSSE
  - O protocolo TLS
  - Sockets Seguros
  - Acessando URLs Seguras (HTTPS)
  - Integração com Dispositivos Criptográficos
- Padrões de Assinatura Digital
  - Padrão PKCS#7
  - Padrão XMLDSig
    - Assinatura Digital de documentos XML
    - Verificação de Assinatura Digital XML