UNIVERSIDAD NACIONAL DEL LITORAL
FACULTAD DE INGENIERÍA Y CIENCIAS HÍDRICAS

Curso de extensión

Firma digital aplicada a los procesos administrativos

1. Objetivos

General

Que el alumno logre conocer los conceptos básicos asociados a la firma digital y las posibles formas de utilización en los procesos de la administración electrónica

Específicos

Que el alumno logre:

- Utilizar documentos electrónicos en el proceso de transformación de la administración tradicional hacia la administración digital.
- Conocer el rol y la interrelación de los aspectos legales, administrativos y tecnológicos, necesarios para la validez de los documentos electrónicos.
- Analizar estrategias para la implementación de firma en diferentes procesos administrativos.
- Conocer tecnologías asociadas y/o de soporte para el proceso de firma y para su almacenamiento a largo plazo.
- Adquirir una visión integral de la temática y sus implicancias locales, nacionales e internacionales.

2. Destinatarios

- Estudiantes y graduados de carreras de informáticas.
- Público en general con conocimientos en administración y manejo de PC que necesiten conocimientos precisos sobre la tecnología de Firma Digital.

3. Docentes responsables

Mg. Graciela Brusa.

Ing. Miguel Ángel Robledo.

4. Contenidos mínimos

Módulo N° 1: Administración Digital: Definición, características y problemáticas.

El rol de la administración en las organizaciones. El proceso de despapelización. El documento electrónico: características, soporte, tipos, formatos, valor probatorio. Propiedades de autoría, confidencialidad, integridad y no repudio de los documentos. Actos administrativos utilizando medios electrónicos. Clasificación, archivo y conservación a largo plazo de la documentación digital. La gestión documental en una organización. Aspectos legales asociados.

Módulo N° 2: Criptografía de llave privada o criptosistemas simétricos.

Criptografía Simétrica. Criptografía de llaves públicas o criptosistema asimétrico. Generación de claves personales pública y privada. Intercambio de claves. Cifrado de documentos. Utilización de la clave pública de un usuario para encriptar.

Módulo N° 3: Firma Digital: Conceptos tecnológicos y marco normativo.

Funciones unidireccionales de uso criptográfico (hash ó funciones resúmenes). Certificados digitales X.509. Marco Normativo Nacional. Esquema de confianza: Autoridades Certificantes, Ente Licenciante y Autoridades de Registro. Ciclo de vida de un certificado digital. Infraestructura de Clave Pública (PKI). Almacenes de certificados: navegadores, dispositivos criptográficos, dispositivos criptográficos biométricos. Estándares aplicables. Políticas de certificación. Políticas de uso de firma digital. Estándares aplicables. Diferencia entre la firma electrónica y la firma digital. Estado de situación local, nacional e internacional.

Módulo N° 4: Proceso de firma y comprobación de la validez de una firma.

Solicitud, renovación y revocación de certificados. Listas de certificados revocados (CRLs y protocolo OCSP). Aplicación de firma digital en correo electrónico. Firmas digital pdf incrustada. Tipos de firmas digitales. Múltiples firmas: Co-firma y Firma jerárquica. Sellado digital de fecha y hora (TS-TimeStamping): definición, Autoridad de Certificación de TS, aplicación con firma digital. Firma digital XAdES. Firma longeva: Utilización del estándar XAdES. Circuitos administrativos candidatos para aplicación de firma digital.

Módulo N° 5: Aplicación práctica de firma digital en circuitos administrativos

Rediseño de procesos tradicionales con la incorporación de firma digitales.

5- Bibliografía

Raina, K., *PKI Security Solutions for the Enterprise: Solving HIPAA, E-Paper Act, and Other Compliance Issues* (2003). Wiley, ISBN-13: 978-0471314292

Schneier B., Applied cryptography (2nd ed.): protocols, algorithms, and source code in C, (1995). John Wiley & Sons, Inc., New York, NY

Ellison, C. y Schneier, B., Ten Risks of PKI (2000). Computer Security Journal, Vol. XVI, No. 1

Kasinath, G, and Armstrong, L. (2007). Analysis of PKI as a means of securing ODF documents. 5th Australian Information Security Management Conference, Edith Cowan University, 4 December, 2007

Lioy, A.; Marian, M.; Moltchanova, N.; Pala, M.: PKI past, present and future (2006), International Journal of Information Security, Springer, Vol.5, Nr. 1, S.18-29.

A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. (1997). Series on Discrete Mathematics and its Applications. CRC Press.

6- Duración, carga horaria y horario

El curso consiste en cinco módulos con contenidos teóricos y prácticos.

Duración (en meses): dos meses (agosto/setiembre 2014).

Duración (en horas): 40 horas.

Modalidad: A distancia (Plataforma e-learning).

7- Sistema de evaluación y promoción

Certificados de Cursado: requiere entrega y aprobación (nota igual o mayor a 70%) de los prácticos de los módulos 1 al 4.

Certificados de Aprobación: requiere entrega y aprobación (nota igual o mayor a 70%) del trabajo práctico integrador de todos los módulos (1 al 5).

8- Conocimientos previos requeridos a los asistentes

Conocimientos básicos del uso de paquetes de oficina y navegación por Internet

9- Matrícula

1000$ Graduados, 700$ Estudiantes, 600$ Socios ACOFICH.