Descripción del Curso en Línea sobre el Sistema de Firma Electrónica Web Murachí

Realizado por: Luz Mairet Chourio, Pedro Buitrago
Revisado por:
Versión 1.0
Fecha de elaboración: 08-04-2020

Justificación del Curso

El sistema Murachí es un servicio web que permite que desde otros sistemas web se puedan consumir recursos para verificar y firmar documentos digitales con certificados de la Infraestructura Nacional de Certificación Electrónica de la República Bolivariana de Venezuela. El sistema Murachí comenzó a desarrollarse en el año 2015 y nace considerando los siguientes problemas y necesidades:

Problemas

- Desconocimiento de la mayoría de la población y usuarios de tecnologías de información y comunicación de la legislación existente en materia de firmas electrónicas y delitos informáticos.
- Desconocimiento de la mayoría de usuarios de la tecnología de certificación electrónica y firmas electrónicas. Todavía se desconoce la existencia de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) y la Infraestructura Nacional de Certificación Electrónica de la República Bolivariana de Venezuela.
- A pesar de que existen instituciones de la Administración Pública Nacional (APN) que utilizan documentos firmados electrónicamente aún existe una percepción de desconfianza en usuarios que reciben estos documentos.
- La Ley de Infogobierno, promulgada en la Gaceta Oficial N° 40.274 del 10 de Octubre de 2013, establece en su artículo 24 “El Poder Público de garantizar la integridad, confidencialidad, autenticidad y disponibilidad de la información, a través del uso de certificados y firma electrónica emitidas dentro de la cadena de confianza de certificación electrónica del Estado venezolano, de conformidad con el ordenamiento jurídico venezolano y la legislación que rige la materia”.

Esto implica que se debe resolver el problema de la adecuación de las instituciones para soportar estos trámites y servicios.

- No se conocen herramientas o aplicaciones de verificación de documentos firmados electrónicamente en línea dentro de la APN.

Necesidades

- Consolidar la promoción y uso de los certificados electrónicos de la Infraestructura Nacional de Certificación Electrónica de la República Bolivariana de Venezuela.
- Brindar a los usuarios y ciudadanos herramientas sencillas para verificar documentos firmados electrónicamente que garanticen la integridad y la autoría de los documentos.
- Proveer herramientas que permitan la integración sencilla de firma electrónica y verificación en sistemas informáticos existentes y de nuevo desarrollo.

Los problemas y necesidades planteadas anteriormente determinan el contexto a partir del cual se propone el desarrollo de un servicio web para la verificación y firma electrónica de documentos denominado Murachí. Ahora bien, para fomentar la apropiación y el despliegue del servicio web Murachí es necesario diseñar, desarrollar e implementar un curso en línea que presente las nociones básicas de los conceptos que involucra el servicio web Murachí, que muestre su funcionamiento y el consumo de los servicios para que los participantes pueden desarrollar destrezas en la materia.

Objetivos del Curso

- **Objetivo General:** Mostrar el servicio web Murachí desde la parte teórica que involucra el uso de tecnologías criptográficas hasta el uso de la interfaz de programación para el consumo de los servicios de verificación y firma electrónica, en aras de apoyar el proceso de apropiación y despliegue del servicio web Murachí.

- **Objetivos específicos:**
  - Entender conceptos sobre seguridad informática.

- Identificar la relaciones entre los conceptos de vulnerabilidad, riesgo, ataque, amenaza y control.
- Revisar conceptos básicos asociados a la tecnología de servicios web.
- Conocer las características del servicio web Murachí de firma electrónica y verificación.
- Realizar ejercicios prácticos usando el API del Sistema Murachí para consumir los servicios de verificación y firma electrónica.
- Usar la aplicación PortableSigner para realizar la firma electrónica usando certificado en formato PKCS#12.

Contenidos del Curso

El presente curso se ha estructurado en cinco lecciones, a saber:

- **1. Nociones Básicas de la Seguridad Informática:** inicia con la exploración de los aspectos teóricos sobre la seguridad informática, ello implica revisar y entender los conceptos asociados, así como comprender las relaciones que existen entre diversos incidentes de seguridad.
  - Contenido 1: Introducción a la seguridad Informática
  - Contenido 2: Introducción a la Gestión de Activos de Información
- **2. Tecnologías web y su aplicación en la verificación y firma electrónica:** busca que los participantes obtengan conocimientos sobre los conceptos básicos de la tecnología de servicios web y su aplicación concreta en un servicio de firma electrónica y verificación de documentos, y conocer las características del servicio web Murachí de firma electrónica y verificación.
  - Contenido 1: Introducción básica a servicios web
  - Contenido 2: Introducción al servicio web Murachí
- **3. Configuración del ambiente de desarrollo**: esta lección contempla los pasos prácticos necesarios para instalar los insumos requeridos para el uso del complemento de firma electrónica web y la instalación de los dispositivos criptográficos.
  - Contenido 1: Instalar el Complemento de Firma Electrónica

- Contenido 2: Instalar y Configurar el Dispositivo Criptográfico

- **4. Gestión de firma electrónica y verificación usando Murachí:** en esta lección se realizan ejercicios prácticos para realizar una página básica en HTML donde se procesa la verificación y firma electrónica usando el servicio del sistema Murachí .
  - Contenido 1: Versión del API de Murachí
  - Contenido 2: Firmar Electrónica de Documento PDF
  - Contenido 3. Verificar Firma Electrónica
- **5. Gestión de firma electrónica usando PKCS#12:** en esta lección se realizan ejercicios prácticos para generar certificados autofirmados en formato PKCS#12 y realizar una página básica en HTML donde se procesa la firma electrónica usando la aplicación PortableSigner.
  - Contenido 1: Certificado electrónico autofirmado en formato PKCS#12
  - Contenido 2: Firma electrónica de documento PDF usando la aplicación PORTABLESIGNER

Cronograma y evaluaciones del curso

En la tabla que se presenta a continuación se indican las actividades a realizar en cada Unidad, así como la evaluación para cada una de éstas y la fecha en la que deben ser realizadas. El curso inicia el 20 de abril y culminará el 8 de mayo de 2020.

Lección	Actividad a realizar	Porcentaje de evaluación	Fecha de realización
Conociendo la plataforma	Revisión de la descripción del curso	5%	20 al 22 de abril
	Actualización del perfil y participación en el foro de bienvenida	5%	
Nociones básicas de la Seguridad Informática	Revisión de contenido	5%	20 al 24 de abril
	Evaluación (aprende)	10%	
Tecnologías web y su aplicación en la verificación y firma electrónica	Revisión de contenido	5%	27 de abril a21l 01 de mayo
	Evaluación (aprende)	10%	
Configuración del ambiente de desarrollo	Revisión de contenido	10%	
	Evaluación (aprende)	10%	

Gestión de firma electrónica y verificación usando Murachí	Revisión de contenido	10%	04 al 08 de mayo
	Evaluación (aprende)	10%	
Gestión de firma electrónica usando PKCS#12	Revisión de contenido	10%	
	Evaluación (aprende)	10%	

Facilitadores del Curso

Ya se actualizó.

Orientaciones

- **Dedicación semanal de horas:** Las actividades pueden realizarlas a tu ritmo, siempre y cuando te ajustes al *cronograma* propuesto. El cronograma del curso está planteado desde el 20 de abril al 08 de mayo de 2020 y está planificado para realizarse en un lapso estimado de 20 horas académicas. Se les recomienda agendar el tiempo semanal de dedicación para la revisión de los recursos y la realización de las actividades previstas.
- **Canales de comunicación:** Recuerden que tienen disponibles varios espacios para la interacción con lxs facilitadores y participantes del curso. En particular, la plataforma cuenta con una opción para redactar tu mensaje en “Perfil”, que se encuentra en el panel izquierdo del aula. En caso de que se presente algún inconveniente técnico con la plataforma del aula virtual, puedes plantear tu situación a través del foro de “Preguntas”. Adicionalmente, para cualquier sugerencia o comentario puedes escribir a lxs facilitadores al siguiente correo ejemplo@cenditel.gob.ve.
- **Tutoría:** Lxs facilitadorxs estarán atentxs a su participación dentro del aula y se dará respuesta a sus mensajes e inquietudes en un lapso no mayor de 24 horas, de lunes a viernes.