

ÍTEM VII - CAPACITACIÓN



7. PLAN DE CAPACITACIÓN PARA IMPRESORAS

7.1 ENTRENAMIENTOS

El consorcio Cedula 4.0 RD ha diseñado un plan de entrenamiento sin costo que inicia durante la fase de implementación con un entrenamiento general de todas las funciones de la solución de impresión y acompañamiento directo del fabricante durante el proceso. El entrenamiento será dividido en 2 fases un entrenamiento básico de operación para el personal que replicará esta capacitación en los centros de atención que incluye:

- Guía básica de operación de la solución
- mantenimiento preventivo
- validación de calidad de impresión
- resolución de incidencias básicas

Adicional a esto se entregará una guía de referencia rápida para uso básico de la solución y un video interactivo con material que apoya y guía al usuario en como operar la solución esta guía se recomienda que sea realizado en conjunto con la JCE con la solución final aprobada.

De igual forma se realizará un *entrenamiento* más especializado para el *personal técnico de la JCE* a fin de asegurar su conocimiento sobre las *características* técnicas de los equipos, *configuraciones*, y demás aspectos técnicos y operativos de la solución instalada. Dicho entrenamiento será realizado en las mismas instalaciones de la JCE por el personal directo del fabricante del hardware.

7.2 TÓPICOS DE ENTRENAMIENTO:

PREPARACIÓN DEL EQUIPO Y CONFIGURACIÓN INICIAL

Instalación del software: Asegúrate de tener instalado el software adecuado para el modelo de impresora láser. Verifica que los controladores sean los más recientes.

Calibración de la impresora: calibración inicial para asegurarse de que el láser y los componentes mecánicos estén correctamente alineados.

Configuración de la calidad de impresión: Ajusta los parámetros de resolución, velocidad de impresión, y otros aspectos técnicos a las necesidades del proyecto.





7.11 PLAN DE CAPACITACION PARA PKI

7.11.1 CONTENIDO

Los cursos que se describen a continuación ofrecidos y organizados por nuestros formadores para la solución de PKI, GET Trust.

- PKI Basics: formación sobre conceptos básicos de PKI e introducción
- CMS: formación sobre el Sistema de Gestión de Credenciales (CMS): En conjunto con ID PKI
- ID PKI: formación sobre software de ID PKI, incluyendo ID CA
- ID CA: formación sobre software de ID CA
- Instalación de ID PKI: formación sobre instalación de software de ID PKI, incluyendo instalación de ID CA
- Instalación de ID CA: formación sobre instalación de software de ID CA
- ID RA para Operadores: Introducción a PKI + uso de ID RA y EE para operadores. Gestión del ciclo de vida de los certificados
- BAC: formación sobre el módulo BAC
- Firmado electrónico: formación sobre el software de firma electrónica IDnomic Sign

Además de estas formaciones estándar, se puede establecer un programa específico con el cliente para cubrir necesidades específicas, como una formación en profundidad para un grupo específico de usuarios.

7.11.2 METODOLOGÍA

Nuestros formadores son profesionales de la formación, especializados en nuestro campo de especialización. Ponemos énfasis en los intercambios interactivos y el desarrollo de habilidades a través de la implementación operativa de nuestras soluciones. Como tal, cada sesión incluye conferencias, sesiones de preguntas y respuestas y trabajos prácticos para poner en práctica los conceptos presentados.

7.11.3 DESCRIPCIÓN

Referencia	PKI Basics
Objetivo	• Descubra los certificados y su ciclo de vida • Comprenda las tecnologías y las normas criptográficas • Comprenda la organización de PKI
Audiencia	Cualquier persona involucrada o interesada en implementar una solución PKI (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Este curso de capacitación proporciona los conocimientos mínimos necesarios para comprender completamente los demás módulos de capacitación impartidos.
Prerequisitos	Formación universitaria básica o ingeniero informático o equivalente mediante experiencia.
Plan	- Fundamentos de criptografía - Implementación de la criptografía

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

25 febrero 2025



	- Introducción a los conceptos de PKI - PKI y organización - La estructura de la PKI - Jerarquía de autoridad - Autoridad de certificación - Marco legal y regulatorio
Duración	4 horas

Referencia	Sistema de Gestión de Credenciales (CMS)
Objetivo	- Comprender los certificados y las tarjetas inteligentes. - Cómo utilizar tarjetas inteligentes en una infraestructura de gestión de certificados. - Implementar el CMS y sus módulos - Configurar y administrar el CMS - Comprender los componentes clave para utilizar el CMS con todos los demás componentes de PKI.
Audiencia	Cualquier persona involucrada o interesada en implementar una solución PKI (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Especialmente los futuros administradores de CMS o aquellos responsables de la solución.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	Día 1: - Introducción al CMS y sus componentes - Instalación e inicialización del software CMS - 1ª conexión en modo "Bootstrap" - Inicialización de la configuración - Inicialización de la seguridad (firma de certificados internos de módulos) - Configuración - Protección de datos, claves de almacenamiento (creación e implementación) - Conexión a directorios, creación de fuentes de datos, definición de perfiles de autenticación, aplicaciones (autenticación, firma de correo electrónico y cifrado) - Medios: políticas de PIN, personalización gráfica, fabricantes, gestión de secretos, creación de perfiles para tokens de entrenamiento - Tarjetas inteligentes: arquitectura y concepto, gestión de secretos - Creación de perfiles para tokens de entrenamiento - Presentación del cliente CMS - Generación de archivos XPI - Instalación del cliente CMS - Configuración del navegador para tokens



	- Creación de un perfil de gestión de tarjetas "SelfEnroll" para administradores, gestión de números de serie de confianza - Definición y uso de procesos / flujos de trabajo: - Solicitud de certificado de administrador designado - Control de acceso (zonas, grupos, gestión de derechos de zona y módulo) - Inicio de sesión con certificado de administrador designado - Preparar un Configuración de usuario final - Creación de perfil de Badge Office - Fuente de datos interna, creación y aprovisionamiento Día 2: - Creación de un perfil de gestión de tarjetas - Emisión por lotes, envío de correo - Creación de perfil, adición de derechos, creación de tokens, revocación, desbloqueo, seguimiento, desbloqueo de medios sin conexión... - Copia de seguridad/restauración - Administración funcional de CMS, gestión de registros
Duración	14 horas (2 días)

Referencia	Instalación
Objetivo	- Instalar manualmente el software de ID CA. - Conocer los componentes que conforman el producto, las arquitecturas típicas a implementar y las diferentes etapas de una instalación. - Identificar los prerrequisitos para la instalación. - Poner en marcha la solución y acceder a las interfaces de administración.
Audiencia	Cualquier persona involucrada o interesada en implementar una solución PKI (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Especialmente los futuros administradores de CMS o aquellos responsables de la solución.
Prerrequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	- Introducción a ID PKI y sus componentes técnicos - Arquitectura técnica de la solución - Requisitos previos - Instalación de ID CA - Ejercicios prácticos: - Verificar los requisitos previos - Instalar ID CA - Verificar la instalación correcta - Iniciar servicios y arrancar PKI - Analizar
Duración	7 horas

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D



Referencia	HSM Proteccio Training
Objetivo	- Presentación, preparación e integración de Proteccio HSM en el contexto de un proyecto PKI - Introducción a una ceremonia de entrega de llaves
Audiencia	Cualquier persona involucrada en la implementación de una solución PKI, incluido un HSM de Proteccio (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes), especialmente futuros administradores de PKI o gerentes de soluciones PKI involucrados en la Ceremonia de entrega de claves.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	- Descripción general de Proteccio HSM, arquitectura de hardware y funciones; - Presentación de los diferentes roles y funciones disponibles para cada uno; - Instalación de equipos y creación de tarjetas maestras SO y maestras de auditoría; - Configuración de red y TLS; - Administración local de equipos; - Instalación de la herramienta de administración en una estación de trabajo Windows y en una estación de trabajo Linux - Actualizaciones de software; - Creación de decks de instalación Shamir; - Creación, configuración y personalización de HSM virtuales; - Gestión de objetos de HSM virtuales; - Gestión de HSM virtuales; - Migraciones de tarjetas inteligentes; - Implementación del modo de balanceo de carga; - Guía de resolución de problemas, mantenimiento de rutina de Proteccio HSM; - Preguntas varias. - Ceremonia de llave con Keyseed - Objetivos de un KC - Procedimiento de KC - Procedimientos y herramientas - • Cierre de un KC
Duración	7 horas

Referencia	BAC Training
Objetivo	- Entender el pasaporte electrónico - Conocer los procesos de solicitud de certificados y su ciclo de vida. - Cómo utilizar tecnologías y estándares criptográficos - Cómo implementar/operar la solución BAC

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 40 R.D

25 febrero 2025



Audiencia	Cualquier persona involucrada en la implementación técnica de una solución PKI para pasaportes incluyendo el componente BAC (Gerentes de Seguridad, CISOs, Gerentes de Proyecto, Arquitectos, Administradores de Sistemas y Redes), y más particularmente futuros administradores de PKI o referentes de soluciones PKI.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	Día 1: - Introducción a la criptografía y PKI - Historia y evolución del pasaporte - Descripción del pasaporte electrónico - Presentación del producto BAC - Descripción general del producto CSCA - Configuración de CSCA - Ejercicios prácticos: - Creación de particiones - Creación de almacén de claves - Creación de CA - Gestión de CA de confianza - Creación y gestión de perfiles de certificados - Gestión de CRL - Renovación de CSCA Día 2: - Configuración del producto DS - Ejercicios prácticos: - Creación de un área de clientes - Creación de administradores DS - Declaración de usuario de cliente DS - Gestión de claves - Creación de DS - Firma de certificados por DS - o Gestión de estadísticas
Duración	14 horas (2 días)

Referencia	Firmado Digital
Objetivo	- Entender las firmas electrónicas - Conocer el proceso de verificación de firmas mediante certificados - Conocer los diferentes tipos de firma electrónica - Cómo utilizar tecnologías y estándares criptográficos - • Implementar y operar la solución.
Audiencia	Cualquier persona involucrada en la implementación técnica de una solución PKI para pasaportes incluyendo el componente BAC (Gerentes de Seguridad, CISOs, Gerentes de Proyecto, Arquitectos, Administradores de Sistemas y Redes), y más

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D.

25 febrero 2025



	particularmente futuros administradores de PKI o referentes de soluciones (integradores) PKI.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	- Descripción general del producto - Configuración - Ejercicios prácticos: - Parte de configuración - Conexión de HSM - Creación de clave maestra - Conexión a PKI - Configuración de CA de confianza - Configuración de importación y exportación - Configuración de la sección de gestión - Creación de usuarios - Creación de políticas de firma - Creación de claves y perfiles de firma - Configuración de firmas - Creación de visuales - Configuración de preferencias de firma - Gestión de auditorías
Duración	7 horas



7.12 PLAN DE CAPACITACION PARA TARJETA DIGITAL

7.12.1 CONTENIDO

Los cursos que se describen a continuación ofrecidos y organizados por nuestros formadores para la solución de tarjeta digital, GET mID.

- ISO 18013-5 Basics: formación sobre conceptos básicos de ISO 18013-5
- Formación de emisión de credenciales digitales ISO 18013-5.
- Instalación y Configuración de GET Mobile Administrator.
- Aplicación Móvil GET Mobile ID.
- Aplicación Móvil GET Mobile Verifier.

7.12.2 METODOLOGÍA

Nuestros formadores son profesionales de la formación, especializados en nuestro campo de especialización. Ponemos énfasis en los intercambios interactivos y el desarrollo de habilidades a través de la implementación operativa de nuestras soluciones. Como tal, cada sesión incluye conferencias, sesiones de preguntas y respuestas y trabajos prácticos para poner en práctica los conceptos presentados.

7.12.3 DESCRIPCIÓN

Referencia	ISO 18013-5 Basics
Objetivo	Descubra los conceptos básicos de ISO 18013-5 y como su implementación impacta la innovación digital y su ecosistema.
Audiencia	- Cualquier persona involucrada o interesada en implementar una solución ISO 18013-5 (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes, áreas funcionales de emisión de documentos, Planificación e innovación). - Este curso de capacitación proporciona los conocimientos mínimos necesarios para comprender completamente los demás módulos de capacitación impartidos.
Prerequisitos	Formación universitaria básica o ingeniero informático o equivalente mediante experiencia.
Plan	- Resumen ISO 18013-5 - Alcance del ISO 18013-5 - Avances innovadores en el mundo - Relación de la PKI con el ISO 18013-5 - Usos e innovaciones - Marco legal y regulatorio
Duración	4 horas

Referencia	Formación de emisión de credenciales digitales ISO 18013-5.
------------	---

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D.

25 febrero 2025



Objetivo	- Comprender los sistemas y procedimientos involucrados en la emisión de una credencial digital. - Cumplimiento del estándar ISO 18013-5 en su implementación.
Audiencia	Cualquier persona involucrada o interesada en implementar una solución ISO 18013-5 (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Especialmente los futuros administradores de GET Mobile ID o aquellos responsables de la solución.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Conocimientos generales de sistemas Android/iOS e infraestructura API o contenidos formativos. - Curso ISO 18013-5 Basics
Plan	- Flujo de emisión de credenciales. - Componentes e integraciones con sistemas CMS. - Integraciones e interacciones.
Duración	4 horas

Referencia	Instalación y Configuración de GET Mobile Administrator.
Objetivo	- Comprender el modelo de instalación, sus ubicaciones y demás configuraciones aplicadas al proyecto. - Operación de la solución. - Modelo de datos. - Integraciones disponibles.
Audiencia	Futuros administradores de CMS o aquellos responsables de la solución.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso ISO 18013-5 Basics - Formación de emisión de credenciales digitales ISO 18013-5.
Plan	- Arquitectura técnica de la solución - Requisitos previos - Instalación de los componentes en el proyecto. - Integraciones disponibles:
Duración	4 horas

Referencia	Aplicaciones Móviles GET
Objetivo	Aplicación de los conceptos adquiridos para el uso de las aplicaciones móviles finales.
Audiencia	Cualquier persona involucrada en la implementación de una solución ISO 18013-5 (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de



	sistemas y redes), especialmente futuros administradores de CMS o gerentes de soluciones CMS.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Conocimientos generales de sistemas Android/iOS e infraestructura API o contenidos formativos. - Curso ISO 18013-5 Basics
Plan	- Descripción general de las aplicaciones móviles. - Despliegue de soluciones móviles. - Funcionalidades posibles. - Taller Practico.
Duración	3 horas



Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D.