Resumen para la ejecución de aplicaciones para la validación de huellas criptográficas iniciales contra las huellas criptográficas de cada una de los 3 simulacros y la jornada electoral.

1. Primer paso: El Proveedor ejecutará la aplicación para crear las llaves pública y privada.
   Para ejecutar la aplicación es el siguiente comando:

   java -jar 2103Proveedor.jar generarLlaves Llavero/ Original.

   Donde ***java -jar 2103Proveedor.jar*** es el ejecutable creado para el Proveedor, ***generarLlaves*** indica la acción que el software debe realizar, ***Llavero/*** es la ruta donde se guardarán las dos llaves de forma local (para no comprometer la seguridad se sugiere crear esta carpeta) y **Original** es el nombre de la actividad que se está realizando.

   Nota: El software ***generarLlaves*** detecta si en la ruta ***Llavero*** ya existen las llaves. Si es el caso muestra un mensaje que ya existen las llaves y no se generan. Esto ocurre porque las llaves se deben de generar una sola vez.

2. Segundo paso: EL Proveedor realizará el inventario de los archivos de base de datos y aplicaciones utilizadas en el SIVEI.

3. Tercer paso: El Proveedor ejecutará la aplicación para las firmas criptográficas iniciales. Para ejecutar la aplicación es el siguiente comando:

   java -jar 2103Proveedor.jar firmarArchivos Inventario/ Llavero/LlavePrivada Original Ciudad

   Donde ***java -jar 1904Proveeor.jar*** es la aplicación de generación de huellas criptográficas y firmas digitales, ***Inventario/*** es la ruta donde se encuentran los archivos de las bases de datos y aplicaciones vacías e inicializadas, ***Llavero/LlavePrivada*** es la ruta donde se encuentra la llave privada (SK), ***Original*** es el nombre que se le da al lote de firmas iniciales y ***Ciudad*** es el nombre de la ciudad en la que fue realizada la generación de las firmas. Finalmente, el Proveedor enviará tanto la **LlavePublica** y el archivo **JSON** al Ente Auditor por medio de correo electrónico.

4. Cuarto paso: El Auditor generará la constancia de huellas criptográficas iniciales. Para ello se dirigirá a la siguiente URL http://auditoria.tamps.cinvestav.mx/Auditoria2023/generarConstancias/Huellas.php donde seleccionará el archivo **JSON** generado por la aplicación ***2103proveedor.jar.*** Para posteriormente hacer clic en el botón “generar constancia de huellas criptográficas” el cual desplegara un reporte con las huellas criptográficas iniciales.

5. Quinto paso: El Proveedor ejecutará la aplicación de firmas criptográficas, antes de cada uno de los simulacros y la jornada electoral. Para ejecutar la aplicación es el siguiente comando:

   java -jar 2103Proveedor.jar firmarArchivos Inventario/ Llavero/LlavePrivada S1-inicio CiudadVictoria.

   Donde ***java -jar 2103Proveedor.jar*** es la aplicación, ***Inventario/*** es la ruta donde se encuentra el inventario de archivos, ***Llavero/LlavePrivada*** es la ruta donde se encuentra la llave privada SK, ***S1-inicio*** indica al sistema que se está generando un lote de huellas criptográficas y firmas al inicio del Simulacro 1 y ***CiudadVictoria*** Indica que se está realizando en Ciudad Victoria. Para los siguientes eventos el único parámetro que se debe cambiar es el nombre del evento: por ejemplo: S2 para Simulacro 2, S3 para Simulacro 3 y JE para la Jornada Electoral.
   Finalmente, el Proveedor enviará el archivo **JSON** generado al Ente Auditor por medio de correo electrónico.

6. Sexto paso: El Auditor ejecutará la aplicación de validación de firmas criptográficas antes del inicio de la jornada electoral. Para ejecutar la aplicación es el siguiente comando:

   java -jar 2103INE.jar validar LIavero/LIavePublica Original Evento.

   Donde ***java -jar 2103INE.jar*** es la aplicación, ***validar*** es el nombre de la actividad que se está realizando, ***LIavero/LIavePublica*** es la ruta donde se encuentran la llave pública (n/a, si desea descargar la llave del servicio de almacenamiento), **Original** es el nombre del lote de firmas generadas inicialmente y ***Evento*** es el nombre del paquete de firmas que se quiere validar: Simulacro 1 (S1), Simulacro 2 (S2), Simulacro 3 (S3), Jornada Electoral (JE) o todos (ALL).

   Una vez finalizado la validación se podrá generar el reporte respectivo utilizando la siguiente URL: http://auditoria.tamps.cinvestav.mx/Auditoria2023/generarConstancias/Hechos.php donde seleccionará el archivo CSV Para corroborar la validación de los archivos, una vez seleccionado el archivo CSV presionará el botón “generar constancia de hechos” y se le desplegará un reporte con la validación de las firmas de los archivos generadas inicialmente y las firmas del evento a comparar.

Requisitos del sistema para la ejecución de las aplicaciones utilizadas para la validación de los documentos firmados inicialmente y los documentos firmados durante los simulacros y la jornada electoral.

- Contar con JAVA 8, si no se tiene instalado dirigirse a la página http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html, en la página encontrarán una lista de archivos para su instalación, el Proveedor debe de seleccionar el adecuado para su sistema operativo. Una vez obtenido el archivo para la instalación de JAVA es necesario seguir los pasos de instalación.
- El Proveedor deberá de respaldar la llave pública y compartirla por medio de correo electrónico al Ente Auditor.
- Contar con permisos de escritura y lectura del sistema de archivos dentro del equipo donde será ejecutada la aplicación o sobre las carpetas que serán utilizadas en el inventario.