HOSPITAL VÍCTOR LARCO HERRERA

OFICINA DE ESTADÍSTICA E INFORMÁTICA

UNIDAD FUNCIONAL DE INFORMATICA

DOCUMENTO NORMATIVO:

DIRECTIVA ADMINISTRATIVA N° 001 -2024-DG-OEI-HVLH/MINSA PARA LA IMPLEMENTACION Y GESTIÓN DEL USO DEL CERTIFICADO Y LA FIRMA DIGITAL EN PROCEDIMIENTOS ASISTENCIALES DEL HOSPITAL VICTOR LARCO HERRERA

DICIEMBRE 2024

INTRODUCCIÓN

El Hospital Víctor Larco Herrera, es una Institución Prestadora de Servicios de Salud de Tercer nivel especializado (III-E), que pertenece al Ministerio de Salud (MINSA).

El Hospital Víctor Larco Herrera, para el cumplimiento de su misión institucional y con el fin de garantizar adecuadas condiciones de prestación de salud mental a la población ha establecido la necesidad de implementar el uso de Tecnologías de Información, y también la sistematización de sus actividades. Para alcanzar la aplicación de estas formas de gestión se ha considerado el uso del certificado y la firma digital entre los diferentes clientes internos, con la finalidad de mejorar la interoperabilidad entre ellos, se requiere la digitalización de los procedimientos asistenciales, asegurando en ellos la identidad digital del remitente y facilitando la interoperabilidad, con esta identidad digital la persona podrá ejecutar acciones de comercio y gobierno electrónico con seguridad, confianza y pleno valor legal.

I. FINALIDAD

Establecer los procedimientos para el uso del Certificado y la Firma Digital en procedimientos asistenciales del Hospital Víctor Larco Herrera.

II. OBJETIVOS

2.1 OBJETIVO GENERAL

Disponer los lineamientos para que el Personal Asistencial del Hospital Víctor Larco Herrera utilicen el Certificado y la firma digital, para asegurar la adecuada gestión de la identidad digital, servicios digitales, interoperabilidad, seguridad digital.

2.2 OBJETIVO ESPECIFICO

Describir el cronograma que contenga las actividades necesarias para alcanzar la implementación y gestión de uso del Certificado y la firma digital como condición básica para garantizar una adecuada cobertura de prestaciones de salud de la población, en términos socialmente aceptables de seguridad, oportunidad y calidad.

III. AMBITO DE APLICACIÓN

El presente documento normativo es de aplicación obligatorio en el Hospital Víctor Larco Herrera, como medio para garantizar la gestión del uso del certificado y la firma digital.

IV. BASE LEGAL

- Ley N°26842, Ley General de Salud y sus modificatorias.
- Ley N° 27444, Ley de Procedimiento Administrativo General.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 30096, Ley de Delitos Informáticos.
- Ley N° 30171, Ley que modifica la Ley 30096, Ley de Delitos Informáticos.
- Decreto Legislativo 1155, que dicta Medidas destinadas a mejorar la Calidad del Servicio y declara de Interés Público el Mantenimiento de la Infraestructura y el Equipamiento en los Establecimientos de Salud a Nivel Nacional.
- Decreto Legislativo Nº 1554, que modifica la Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de Información. Técnicas de Seguridad. Sistemas

de Gestión de Seguridad de la Información. Requisitos.2° Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

- Resolución Ministerial N° 462-2023-MINSA, que aprueba la Directiva Administrativa N° 343-MINSA/OGTI-2023, "Directiva Administrativa que regula el uso de la firma electrónica y firma digital en los actos médicos y actos de salud".

V. DISPOSICIONES GENERALES

5.1 Glosario

AAC (Autoridad Administrativa Competente): Se encarga de administrar la IOFE, según el Reglamento de la Ley de Firmas y Certificados Digitales.

Área Usuaria: para efectos del presente documento, se considera como Área Usuaria del Certificado y Firma digital al Hospital Víctor Larco Herrera.

AST (Autoridad de Sellado de Tiempo): Es la que coloca y almacena el sello de tiempo al momento de firmar. Está debidamente acreditada por Indecopi.

Autenticación: Se refiere al procedimiento técnico de determinación de la Identificación de la persona que firma digitalmente.

Certificado Digital: Es como un DNI físico en el mundo de la Internet que te permite usarlo para firmar digitalmente documentos o contratos con el mismo valor legal que una firma manuscrita. Es generado y firmado digitalmente por una Entidad de Certificación y que permite identificar a la persona natural o jurídica que emitirá la firma digital.

Certificado Digital SSL (Secure Sockets Layers): Es el que demuestra que la identidad de una página en Internet es real, y protege la información privada.

Dispositivo Criptográfico: Elemento de Hardware, tal como un token criptográfico o tarjeta inteligente que permite almacenar de manera segura el Certificado digital y la clave privada del usuario.

Documento Electrónico: Es aquel documento administrativo en soporte electrónico que incorpora datos firmados electrónicamente mediante el certificado digital de un suscriptor y que cuenta con el mismo valor que los documentos administrativos firmados con firma manuscrita en un papel.

DPC (Declaración de Prácticas de Certificación): Es un documento que describe los servicios de certificación de la EC.

EC (Entidad de Certificación): Es la que emite los certificados digitales. Está debidamente acreditada por Indecopi.

ER (Entidad de Registro): Es la que registra y demuestra que la información del solicitante de un certificado digital es real. Está debidamente acreditada por Indecopi.

Firma Manuscrita: Es la firma que realiza una persona a puño y letra en un documento de papel.

Firma Digital: Es un mecanismo que permite a una persona firmar un documento electrónico de forma segura e inalterable, la cual reemplaza a la firma manuscrita y tiene el mismo valor legal según la Ley N°27269.

La firma digital es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios, incluso a distancia, que garantizan que éste mantiene bajo su control un elevado grado de confianza.

IOFE (Infraestructura Oficial de la Firma Electrónica): Se encarga de garantizar los procesos de certificación digital.

Persona Natural: Puede ser un ciudadano nacional o extranjero.

Persona Jurídica: Es una organización conformada por una o más personas.

Política de Privacidad: Es un documento que describe cómo la entidad maneja los datos personales de los ciudadanos.

Política de Seguridad: Es un documento que describe el plan de acción para afrontar los riesgos de seguridad.

Revocación: Es la finalización del certificado, y no es recuperable.
Sello de Tiempo: Es la fecha y hora acordada a nivel internacional para evitar una discusión debido a diferencias horarias para un documento firmado.
Token: es un dispositivo criptográfico que se basa en un microprocesador y ofrece autentificación en certificados digitales y solución de generación de firmas digitales con valor legal.

5.2 Validez Legal del Certificado y la Firma Digital

La Directiva Administrativa N° 343-MINSA/OGTI-2023, establece el uso de la firma electrónica y firma digital en los actos médicos y actos de salud, de cumplimiento obligatorio para las IPRESS públicas, privadas y mixtas, los profesionales de la salud, y las entidades autorizadas por el MINSA para proveer servicios de salud y que hagan uso o administren sistemas de información asistencial, que implementen la firma electrónica y la firma digital, así como de aplicación obligatoria para la DIRIS, DIRESA y GERESA siempre que actúen en calidad de administradores de usuarios de los sistemas de información asistencial o como entidades responsables de dichos sistemas; si y solo si: antes se ha efectuado el análisis de riesgo de la infraestructura tecnológica, y solo cuando el resultado haya sido de riesgo medio o bajo.

5.3 Conservación e Interoperabilidad de los Documentos Electrónicos

Los documentos electrónicos emitidos a través de la Herramienta Informática deben cumplir con las siguientes características:

- **Autenticidad:** Los documentos emitidos garantizan que han sido creados y enviados por los/las usuarios/as internos/as, autorizados y autenticados en la Herramienta Informática (HI), en la fecha y hora que se indica.
- **Confidencialidad:** La información contenida en los documentos emitidos por los órganos, unidades orgánicas, solo podrán ser de acceso para aquellos/as usuarios/as internos/as que cuenten con la respectiva autorización dentro de sus funciones encargadas. Asimismo, la HI cuenta con procesos automáticos de auditoría que registran todas las ocurrencias realizadas por los/las usuarios/as internos/as.
- **Disponibilidad:** Los documentos emitidos están disponibles para consultas de acuerdo al nivel de acceso autorizado para el/la usuario/a interno/a. La HI permite el registro de los metadatos que asocian a un documento emitido, facilitando de esta manera la fácil ubicación, disponibilidad, recuperación y trazabilidad de los mismos.
- **Fiabilidad:** Los documentos emitidos dan crédito de su contenido siendo la representación fidedigna de operaciones, actividades o hechos que estos afirman o ilustran, y que pueden ser susceptibles de ser utilizados para comprobar algo en el curso de las operaciones o actividades subsecuentes
- **Integridad:** Los documentos emitidos deben mantenerse completos e inalterables. De ser necesaria su impresión, estos no deben ser modificados

VI. DISPOSICIONES ESPECÍFICAS

6.1 Procedimiento para la Emisión del Certificado Digital

- La Dirección General del Hospital Víctor Larco Herrera designa al Administrador del Certificado Digital, quien posteriormente será el responsable de solicitar ante el ECEP. RENIEC los certificados que correspondan para cada uno de los servidores del Hospital que utilizarán la Firma Digital.
- La designación al administrador del Certificado Digital consiste en una delegación de facultades, y deberá ser comunicada a RENIEC.
- El Trámite para la emisión y gestión de certificados digitales para los signatarios se inicia después que se haya emitido el certificado digital a favor del Hospital Víctor Larco Herrera.
- El trámite para gestionar la obtención del certificado digital se genera por la necesidad de las UPSS para firmar digitalmente los documentos, para ello deberán hacerlo a través del Formato A – Solicitud para Uso de Firma Digital, ver anexo 02, el mismo que deberá ser

dirigido al Administrador del Certificado Digital
El Administrador del Certificado Digital deberá efectuar los siguientes procedimientos:

a) Registrar los Datos de los signatarios en el Formulario: "Autorización para la Emisión de Certificados Digitales a los Suscriptores" a través de su cuenta de usuario en el Portal de la ECEP-RENIEC
b) Generar el reporte "Lista de Autorizaciones Generadas". Este documento se firma en forma manuscrita y se envía en físico a la ECEP-RENIEC
c) El Administrador del certificado Digital deberá comunicar vía correo electrónico a los servidores a los que se les ha generado la Autorización. Se acerquen a la ECEP_RENIEC con su DNI vigente para recabar su certificado digital
d) Cuando el suscriptor/signatario se acerca a la EREP-RENIEC para recibir su certificado digital, pero no firma los formatos debido a que no se incluido información incorrecta o inexacta en el certificado digital, deberá comunicarse con el Administrador del Certificado Digital para que genere una solicitud a la ECEP –RENIEC.
e) El suscriptor recibirá una clave y la ruta para descargar el certificado digital emitido por la ECEP_RENIEC en un plazo máximo de cinco (5) días hábiles en su correo electrónico institucional. El suscriptor será responsable de revisar su correo tanto en la bandeja de entrada como en la bandeja de correo no deseado, la emisión de dicho certificado y sus instrucciones correspondientes.
f) Una vez recibido el correo electrónico del ECEP-RENIEC, el suscriptor deberá comunicarse con la UFI (Unidad Funcional de Informática) de la Oficina de Estadística e Informática del HVLH, para que procedan a la instalación del certificado digital en su equipo de cómputo. En el proceso de instalación del Certificado Digital se solicitará que el suscriptor ingrese una contraseña, la cual servirá para que pueda firmar a partir de ese momento los documentos electrónicos.
g) En caso que la Dirección General considere conveniente, determinará quién o quiénes podrán hacer uso de la instalación del certificado digital mediante un token u otro dispositivo de almacenamiento del certificado digital.

6.2 Uso del Certificado Digital por los Signatarios

- Los Jefes responsables de los Departamentos Asistenciales del Hospital Víctor Larco Herrera involucrados deberán garantizar la debida utilización de la firma digital.
- Para el uso y aplicación de la firma digital; el suscriptor deberá contar con el correspondiente Certificado Digital, y el dispositivo electrónico de seguridad de almacenamiento de la clave: Token y PC en el cual se deberá contar con el Software de Firma Digital.
- Los usuarios suscriptores de la firma digital harán uso de los certificados digitales para firmar digitalmente en los documentos electrónicos que correspondan a sus funciones. La facultad de uso de la firma digital, **la contraseña de su certificado digital es** intransferible; siendo responsabilidad y de ninguna manera podrá ser negada la firma digital presente en un documento electrónico en virtud a las seguridades establecidas para su uso, establecidas en la Ley N° 27269- Ley de Firmas y Certificados Digitales y su Reglamento y sus modificatorias.

6.3 Obtención y Gestión del Token Criptográfico

Un dispositivo criptográfico es un smartcard (con interfaz de contacto y/o proximidad) y/o token (con interfaz USB) con capacidad de realizar operaciones criptográficas. Un dispositivo criptográfico homologado, puede ser utilizado por la plataforma de generación de certificados digitales del RENIEC (en adelante la Plataforma), para generar certificados digitales de persona jurídica de clase III emitidos por la ECEP-RENIEC. Posterior a esta generación, el dispositivo criptográfico estará en la capacidad de realizar operaciones de firma digital con un software de generación de firma digital acreditado por la AAC en el marco de la IOFE.

- Solicitar al RENIEC, mediante la Ficha IV (de ECEP-RENIEC), la evaluación del dispositivo, adjuntando lo siguiente: Un (01) dispositivo criptográfico del modelo a homologar.
- El código o número de certificación de seguridad FIPS 140-2 y/o Common Criteria.

- El brochure técnico del dispositivo criptográfico emitido por el fabricante.
- El software (Middleware) del dispositivo criptográfico.
- La guía de usuario del dispositivo criptográfico Realizada la evaluación del dispositivo criptográfico, se entregará un reporte de cumplimiento de los requisitos técnicos/funcionales (Ficha III de ECEP-RENIEC).

6.4 Firmas Electrónicas en los Procedimientos Asistenciales

- Para aplicación y uso de la Firma Electrónica en el Hospital Víctor Larco Herrera contamos con el Sistema de Información SIHE donde se registra la atención digital de los pacientes. El sistema cumple con aspectos de seguridad, confidencialidad, disponibilidad, integridad y autenticidad, con el uso de la firma electrónica de los profesionales de la salud para el registro de los actos médicos y actos de salud que prestamos a nuestros usuarios, se podrá exonerar la impresión de múltiples formatos de atención y constituir integralmente la Historia Clínica Electrónica.
- El registro electrónico del acto médico y actos de salud deberán realizarse en el Sistema SIHE por el Profesional de la Salud en el momento que brinda la atención.
- El Hospital Víctor Larco Herrera garantiza que los profesionales de la salud que brindan atención, tienen que autenticar sus credenciales de acceso al sistema SIHE.
- En los actos médicos y de salud que utilizan el Sistema SIHE para el registro de atenciones, se usará la firma electrónica emitida por RENIEC, la cual se obtiene a través de un servicio web acreditado, para la continuidad del servicio de atención, posterior a ello se regulariza con la firma digital (criptografía asimétrica) del profesional de la salud.

6.5 Aplicación y Uso de la Firma Digital en los Sistemas Informáticos.

- Para la aplicación de la Firma Digital en los documentos electrónicos correspondientes a los actos médicos y de salud, nuestro sistema informático SIHE deberá integrar un módulo de firma digital que soporte el proceso.
- Para garantizar la autenticidad de los documentos electrónicos firmados digitalmente a través del SIHE, el Hospital Víctor Larco Herrera deberá validar el Módulo de Firma Digital.
- Para la implementación de la Firma y Certificado digital en el Hospital Víctor Larco Herrera se deberán efectuar una serie de procedimientos, los cuales se desarrollarán de manera progresiva, de acuerdo al cronograma; y siguiendo lo establecido en la presente directiva.

VII. RESPONSABILIDADES

7.1 Del Administrador del Certificado Digital

- Entregar información veraz durante la solicitud de emisión de certificados y demás procesos: Suspensión, Anulación, cancelación ante RENIEC.
- Cumplir permanentemente las condiciones establecidas por la entidad de Certificación.
- Solicitar la generación, renovación, actualización o cancelación de los certificados digitales ante la EREP-RENIEC
- Solicitar a la EREP-RENIEC la emisión y cancelación de los Certificados digitales del suscriptor, asumiendo las obligaciones del titular.

7.2 De la Oficina de Estadística e Informática

El Jefe/a de la Oficina está encargado de lograr que el Hospital provea la información estadística de salud y el soporte informático, mecanización e integración de los sistemas de información requeridos para los procesos organizacionales; depende de la Dirección General.

7.3 Unidad Funcional de Informática (UFI)

- Gestionar la provisión de servicios informáticos, sistemas de información, telecomunicaciones, informática y telemática en el ámbito institucional a través de las instancias pertinentes.
- Establecer y mantener la seguridad, integración y operatividad de las redes de información y bases de datos institucionales necesarias.

- Lograr y mantener ínter conectividad de las redes y bases de datos institucionales con las de nivel regional y nacional.
- Lograr que los usuarios internos y externos tengan la disponibilidad de asesoría y asistencia técnica disponible en el uso de aplicaciones informáticas, telecomunicaciones y nuevas tecnologías de información, como:
  - ✓ Brindar Capacitación y asistencia técnica en el uso del dispositivo de almacenamiento de certificado digital o token.
  - ✓ En caso de ser necesario, el Equipo de la UFI deberá atender las incidencias técnicas de los signatarios con respecto a la instalación de los certificados digitales y uso de las firmas digitales
  - ✓ Incorporar las medidas técnicas orientadas a mantener la integridad del documento electrónico con firma digital y que la información que contenga sea accesible para su posterior consulta.
- Implantar los proyectos de desarrollo de tecnología de información y telecomunicaciones que se programen a nivel sectorial.

VIII. ANEXOS

- Anexo 01: Cronograma para la Implementación de la Firma y Certificado Digital en el HVLH-2025
- Anexo 02 Formato A (Solicitud de uso de Firma Digital)

ANEXO 01. CRONOGRAMA PARA LA IMPLEMENTACIÓN DE LA FIRMA Y CERTIFICADO DIGITAL EN EL HVLH-2025

PROCESOS PARA LA IMPLEMENTACION DE FIRMA DIGITAL EN ACTOS MEDICOS Y DE SALUD	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SETIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
IMPLEMENTACION DE FIRMA DIGITAL EN RECETAS MEDICAS Y HOJAS DE EVOLUCION												
IMPLENTACION DE FIRMA DIGITAL ORDENES DE SERVICIO LABORATORIO, RX												
IMPLEMENTACION DE FIRMA DIGITAL EN FORMATOS FUA Y HOJAS DE REFERENCIA												
IMPLEMENTACION DE FIRMA DIGITAL EN FORMATOS FUA Y HOJAS DE REFERENCIA												

ANEXO 02 FORMATO A (SOLICITUD DE USO DE FIRMA DIGITAL)

SOLICITUD DE USO DE FIRMA DIGITAL		
Nombres:	**Apellidos:**	**N° de DNI :**
Cargo:	**Departamento:**	**Correo Institucional**
Observaciones:		
Firma del Jefe del Departamento **DNI N°** **Fecha:**		