

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de Ingeniería de Sistemas e Informática

Trabajo de Suficiencia Profesional

Enrolamiento de equipo al directorio activo e instalación del sistema de gestión documental y firma digital en la Red Asistencial de Salud Arequipa

Alejandro Steve Ayasta Yana

Para optar el Título Profesional de
Ingeniero de Sistemas e Informática

Arequipa, 2025

Repositorio Institucional Continental
Trabajo de suficiencia profesional



Esta obra está bajo una Licencia "Creative Commons Atribución 4.0 Internacional" .

INFORME DE CONFORMIDAD DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

A : Decano de la Facultad de Ingeniería
DE : Julio Cesar Alvarez Barreda
Asesor de trabajo de investigación
ASUNTO : Remito resultado de evaluación de originalidad de trabajo de investigación
FECHA : 17 de Enero de 2026

Con sumo agrado me dirijo a vuestro despacho para informar que, en mi condición de asesor del trabajo de investigación:

Título:

Enrolamiento de equipo al Directorio Activo e instalación del Sistema de Gestión Documental y Firma Digital en la Red Asistencial de Salud Arequipa

Autores:

1. Alejandro Steve Ayasta Yana – Carrera Profesional Ingeniería de Sistemas e Informática

Se procedió con la carga del documento a la plataforma "Turnitin" y se realizó la verificación completa de las coincidencias resaltadas por el software dando por resultado 16% de similitud sin encontrarse hallazgos relacionados a plagio. Se utilizaron los siguientes filtros:

- Filtro de exclusión de bibliografía SI NO
- Filtro de exclusión de grupos de palabras menores
Nº de palabras excluidas (PALABRAS): 10 palabras SI NO
- Exclusión de fuente por trabajo anterior del mismo estudiante SI NO

En consecuencia, se determina que el trabajo de investigación constituye un documento original al presentar similitud de otros autores (citas) por debajo del porcentaje establecido por la Universidad Continental.

Recae toda responsabilidad del contenido del trabajo de investigación sobre el autor y asesor, en concordancia a los principios expresados en el Reglamento del Registro Nacional de Trabajos conducentes a Grados y Títulos – RENATI y en la normativa de la Universidad Continental.

Atentamente,

La firma del asesor obra en el archivo original (no se muestra en
este documento por estar expuesto a publicación)

ASESOR

Mg. Julio César Alvarez Barreda

AGRADECIMIENTOS

Deseo expresar mi más profundo agradecimiento a mis padres, por su paciencia, apoyo incondicional y constante motivación durante todo mi proceso de formación profesional. Su ejemplo de esfuerzo y perseverancia ha sido la base que me ha permitido culminar esta etapa importante en mi vida.

Agradezco también a mi familia, especialmente a mis hijas, quienes con su ternura y alegría me brindaron la inspiración necesaria para seguir adelante y no rendirme ante las dificultades.

Extendiendo mi gratitud a la Red Asistencial de Salud de Arequipa, institución que me brindó la oportunidad de desarrollar este proyecto, confiando en mis capacidades para aportar a la mejora de su infraestructura tecnológica y a la modernización de sus procesos.

De igual manera, agradezco a mis docentes y a la Universidad Continental, por su guía académica y los conocimientos transmitidos que han sido fundamentales en mi crecimiento profesional y personal.

Un agradecimiento especial a mi asesor de suficiencia profesional, por su orientación, paciencia y valiosas recomendaciones durante el desarrollo de este informe, las cuales permitieron darle una mejor estructura y mayor solidez al trabajo realizado.

Finalmente, expreso mi reconocimiento a todos mi compañeros y colegas que, con su colaboración y apoyo, contribuyeron en el desarrollo exitoso de este trabajo de suficiencia profesional.

DEDICATORIA

A mis padres...

Quiero expresar mi más sincero agradecimiento por su paciencia, comprensión y, sobre todo, por el apoyo incondicional que me han brindado a lo largo de este camino académico. Su constante aliento y sacrificio han sido fundamentales para que hoy pueda culminar esta etapa tan importante de mi vida profesional.

Este informe de suficiencia profesional, con el que aspiro al título de Ingeniero de Sistemas e Informática, es también reflejo del esfuerzo y los valores que me inculcaron desde siempre.

Gracias por estar siempre conmigo.

ÍNDICE

ASESOR	ii
AGRADECIMIENTOS	iii
DEDICATORIA	iv
ÍNDICE	v
ÍNDICE DE TABLAS	viii
ÍNDICE DE FIGURAS.....	ix
RESUMEN EJECUTIVO	x
EXECUTE SUMMARY	xi
INTRODUCCIÓN	xii
CAPÍTULO I	1
ASPECTOS GENERALES DE LA EMPRESA	1
1.1 Datos generales de la institución.....	1
1.2 Actividades principales de la institución	1
1.3 Reseña histórica de la institución.....	2
1.4 Organigrama de la institución	3
1.5 Visión y misión	4
1.5.1 Visión.....	4
1.5.2 Misión	4
1.6 Bases Legales o Documentos Administrativos	4
1.7 Descripción del área donde realiza sus actividades profesionales	5
1.8 Descripción del cargo y de las responsabilidades del bachiller en la institución.....	6
1.8.1 Cargo.....	6
1.8.2 Descripción del cargo dentro del proyecto.....	6
1.8.3 Responsabilidades específicas	7
CAPÍTULO II	9
ASPECTOS GENERALES DE LAS ACTIVIDADES PROFESIONALES	9
2.1 Antecedentes o diagnóstico situacional	9

2.2	Identificación de oportunidad o necesidad en el área de actividad profesional	10
2.3	Objetivos de la actividad profesional.....	12
2.3.1	Objetivo general.....	12
2.3.2	Objetivos específicos	12
2.4	Justificación de la actividad profesional	12
2.5	Resultados esperados	14
CAPÍTULO III.....		16
MARCO TEÓRICO.....		16
3.1	Introducción	16
3.2	Fundamentos de la transformación digital en el sector salud	16
3.3	Infraestructura tecnológica y Directorio Activo	16
3.3.1	Componentes lógicos del Directorio Activo.....	17
3.3.2	Componentes físicos del Directorio Activo	18
3.4	Gestión documental electrónica.....	21
3.4.1	Características principales de un gestor documental eficaz.....	22
3.5	Seguridad informática en entornos institucionales	23
3.6	Metodologías de gestión de proyectos tecnológicos.....	23
3.7	Firma digital y su aplicación institucional	23
3.8	Certificado digital	24
3.9	Token criptográfico.....	24
3.10	Documento nacional de identidad electrónico	25
CAPÍTULO IV		26
DESCRIPCIÓN DE LAS ACTIVIDADES PROFESIONALES		26
4.1	Descripción de actividades profesionales	26
4.1.1	Enfoque de las actividades profesionales.....	31
4.1.2	Alcance de las actividades profesionales	34
4.1.3	Entregables de las actividades profesionales	35
4.2	Aspectos técnicos de la actividad profesional.....	37
4.2.1	Metodologías.....	37

4.2.2	Técnicas	38
4.2.3	Instrumentos.....	39
4.2.4	Equipos y materiales utilizados en el desarrollo de las actividades.....	39
4.3	Ejecución de las actividades profesionales	39
4.3.1	Cronograma de actividades realizadas	40
4.3.2	Proceso y secuencia operativa de las actividades profesionales	41
CAPÍTULO V.....		43
RESULTADOS		43
5.1	Resultados finales de las actividades realizadas	43
5.2	Logros alcanzados.....	44
5.3	Dificultades encontradas.....	46
5.4	Metodologías propuestas	47
5.4.1	Descripción de la implementación.....	49
5.5	Análisis	50
5.5.1	Comparación: situación inicial vs. situación final	51
5.5.2	Impacto de la actividad profesional	52
5.5.3	Evaluación de rol profesional	52
5.6	Aporte del bachiller en la institución	52
CONCLUSIONES		55
REFERENCIAS BIBLIOGRÁFICAS.....		56
REFERENCIAS BIBLIOGRÁFICAS.....		57
ANEXOS		59

ÍNDICE DE TABLAS

Tabla 1.	Cronograma de actividades realizadas.....	40
Tabla 2.	Logros alcanzados situación inicial VS situación final.....	46
Tabla 3.	Comparación situación inicial Vs situación final.....	51

ÍNDICE DE FIGURAS

Figura 1.	Organigrama Institucional de Red Asistencial Arequipa.....	3
Figura 2.	Componentes lógicos del Directorio Activo.....	18
Figura 3.	Autenticación de usuario.....	20
Figura 4.	Verificación con Segundo Factor.....	20
Figura 5.	Single Sign-On.....	21
Figura 6.	Respaldo de información de equipo.....	26
Figura 7.	Página de inicio Acronis 2015.....	27
Figura 8.	Imágenes de discos de equipos.....	27
Figura 9.	Activar/desactivar Secure Boot.....	28
Figura 10.	Nombre de equipo según nomenclatura.....	28
Figura 11.	Página inicio Sistema de Gestión Documental.....	29
Figura 12.	Software CryptoID.....	29
Figura 13.	Importación/Exportación de certificados digitales.....	30
Figura 14.	Capacitación SGD.....	33
Figura 15.	Manuales Firma Digital en repositorio institucional.....	33
Figura 16.	Avance a nivel Nacional, junio 2025.....	35
Figura 17.	Inicio de Sesión SGD.....	36

RESUMEN EJECUTIVO

El presente trabajo de suficiencia profesional tiene como objetivo principal documentar la participación en el proyecto de enrolamiento de equipos informáticos al Directorio Activo, así como la instalación e implementación del Sistema de Gestión Documental (SGD) y la Firma Digital en la Red Asistencial de Salud Arequipa, como parte del proceso institucional de modernización tecnológica y transformación digital.

Ante el crecimiento sostenido del parque informático y la necesidad de fortalecer la gestión de información en la red, se identificó la urgencia de implementar soluciones que permitieran administrar de forma centralizada los recursos tecnológicos, automatizar los procesos documentarios y garantizar la validez legal de los documentos electrónicos mediante la firma digital.

La ejecución del proyecto se desarrolló bajo una metodología técnico-operativa basada en buenas prácticas ITIL, que abarcó fases de diagnóstico, planificación, despliegue y evaluación. Se realizaron actividades de actualización y configuración de equipos, enrolamiento al dominio institucional, instalación del SGD y firma digital, así como capacitación a los usuarios finales y documentación de los procedimientos ejecutados.

Como resultado, se logró enrolar 1850 equipos al Directorio Activo, habilitar más de 1000 estaciones con el SGD y la Firma Digital, y capacitar a más de 800 usuarios en el uso seguro y eficiente de las nuevas herramientas. Estos resultados permitieron mejorar la trazabilidad de los procesos, reducir el uso de papel en un 60%, y acortar los tiempos de gestión documentaria de cinco a dos días hábiles.

El impacto institucional se refleja en una mayor eficiencia operativa, seguridad informática y madurez digital, posicionando a la Red Asistencial de Salud Arequipa como un referente en la implementación de soluciones tecnológicas sostenibles dentro del sector público de salud.

En el plano profesional, esta experiencia permitió aplicar conocimientos especializados en Infraestructura TI, gestión de servicios y seguridad digital, consolidando el rol del ingeniero de sistemas como agente estratégico en la innovación tecnológica y modernización del sector salud peruano.

Palabras claves: directorio activo, sistema de gestión documental, firma digital, transformación digital.

EXECUTE SUMMARY

The main objective of this professional proficiency assessment is to document the participation in the project to enroll IT equipment in the Active Directory, as well as the installation and implementation of the Document Management System (DMS) and Digital Signature in the Arequipa Health Care Network, as part of the institutional process of technological modernization and digital transformation.

Given the sustained growth of the IT infrastructure and the need to strengthen information management in the network, it was urgent to implement solutions that would allow for centralized management of technological resources, automate document processes, and guarantee the legal validity of electronic documents through digital signatures.

The project was executed using a technical and operational methodology based on ITIL best practices, which included diagnostic, planning, deployment, and evaluation phases. Activities included equipment upgrades and configuration, enrollment in the institutional domain, installation of the DMS and digital signature, as well as end-user training and documentation of the procedures executed.

As a result, 1,850 devices were enrolled in Active Directory, more than 1,000 stations were enabled with the SGD and Digital Signature, and more than 800 users were trained in the secure and efficient use of the new tools. These results led to improved process traceability, a 60% reduction in paper usage, and a reduction in document management times from five to two business days.

The institutional impact is reflected in greater operational efficiency, IT security, and digital maturity, positioning the Arequipa Health Care Network as a benchmark in the implementation of sustainable technological solutions within the public health sector.

On a professional level, this experience allowed the company to apply specialized knowledge in IT infrastructure, service management, and digital security, consolidating the role of the systems engineer as a strategic agent in technological innovation and modernization of the Peruvian health sector.

Keywords: active directory, document management system, digital signature, digital transformation.

INTRODUCCIÓN

El presente trabajo de suficiencia profesional tiene como objetivo principal documentar y sustentar el desarrollo de las actividades realizadas en el marco del proyecto de enrolamiento de equipos al Directorio Activo, instalación del Sistema de Gestión Documental y Firma Digital en la Red Asistencia de Salud Arequipa. Este proyecto responde a la necesidad de modernizar los procesos informáticos y garantizar la seguridad, confiabilidad y eficiencia en la gestión institucional, en un contexto de crecimiento exponencial del equipamiento tecnológico de la red.

En el capítulo 1 se presentan los aspectos generales del trabajo, incluyendo el planteamiento del problema, los objetivos planteados y la justificación que respalda la importancia de la implementación tecnológica en la institución.

En el capítulo 2 se expone el diagnóstico situacional de la Red Asistencial, destacando el incremento del equipamiento informático en más del 300%, lo que generó la necesidad de adoptar herramientas de administración centralizada, seguridad digital y gestión documental electrónica.

En el capítulo 3 se desarrolla el marco teórico, abordando los conceptos fundamentales del Directorio Activo, gestión documental y firma digital, así como las bases legales que regulan el uso de la firma digital en el Perú, sustentando el contexto normativo y técnico en el que se llevó a cabo el proyecto.

En el capítulo 4, se describen las actividades profesionales ejecutadas, detallando la planificación, metodologías empleadas, recursos utilizados y la secuencia operativa que permitió enrolar a los equipos al dominio institucional, habilitarlos con el sistema de gestión documental y los recursos para el proceso de firma digital, así como brindar soporte técnico y capacitación a los usuarios.

En el capítulo 5 se presentan los resultados obtenidos, los logros alcanzados, las dificultades encontradas y el planteamiento de mejoras, junto con el análisis y las recomendaciones finales. Asimismo, se expone el aporte del bachiller a la institución, resaltando cómo la experiencia profesional contribuyó al éxito del proyecto y fortaleció la gestión tecnológica en la red asistencial.

De manera general, las conclusiones principales señalan que la implementación permitió alcanzar un 95% de equipos enrolados al Directorio Activo, habilitados para el uso del SGD y

la firma digital, mejorando significativamente la seguridad informática y la eficiencia en la gestión de documentos electrónicos. Asimismo, se evidenció que la capacitación brindada a los usuarios fue clave para la adopción efectiva del sistema.

Los hallazgos más relevantes destacan la necesidad de contar con personal especializado en Ingeniería de Sistemas para garantizar la sostenibilidad de proyectos tecnológicos de gran escala, la importancia de una infraestructura estandarizada y la relevancia de la firma digital como herramienta estratégica en la transformación digital de los servicios de salud.

En este sentido, el presente informe no solo documenta el desarrollo de actividades profesionales específicas, sino que también evidencia el valor agregado del rol del ingeniero de Sistemas en procesos de innovación y modernización tecnológica dentro del sector salud.

CAPÍTULO I

ASPECTOS GENERALES DE LA EMPRESA

1.1 Datos generales de la institución

La institución donde se desarrolló la experiencia profesional corresponde a una entidad pública de alcance nacional, dedicada a la prestación de servicio de salud en sus diferentes niveles de atención. Su estructura organizativa contempla una red de establecimientos médicos distribuidos en diversas regiones del país, con el objetivo de brindar una atención integral, oportuna y de calidad a sus asegurados.

La red asistencial, en la cual se realizó la presente experiencia, se ubica en una de las principales ciudades del sur del país; cuenta con hospitales, policlínicos y centros médicos especializados. Esta red ha venido experimentando un importante crecimiento en cuanto a infraestructura tecnológica, modernización de procesos y fortalecimiento de capacidades humanas y técnicas, orientadas a mejorar la eficiencia de la atención médica y administrativa.

Dentro de su misión institucional se destaca el compromiso con la salud y bienestar de la población asegurada, mediante la provisión de servicios preventivos, curativos y de rehabilitación. Asimismo, promueve la innovación tecnológica y la transformación digital como ejes clave para optimizar su operatividad y garantizar una gestión eficiente y transparente.

1.2 Actividades principales de la institución

La institución tiene como eje central de sus labores la provisión de prestaciones de salud integrales, abarcando servicios de carácter preventivo, promocional, recuperativo y de rehabilitación, dirigidos a la población asegurada. Estas prestaciones se clasifican en tres grandes categorías:

- Prestaciones de prevención y promoción de la salud: incluyen campañas de vacunación, tamizaje, educación sanitaria, control de enfermedades crónicas y promoción de estilos de vida saludables. Estas acciones buscan fortalecer la conciencia colectiva en torno a la salud y anticiparse a la aparición de patologías, contribuyendo así a una sociedad más saludable y sostenible.
- Prestaciones asistenciales: comprenden la atención médica en los niveles primario, secundario y terciario, a través de consultas externas, emergencias, hospitalización, cirugía, atención especializada y procedimientos médicos de alta complejidad. Estas

acciones están orientadas no solo a resolver problemas clínicos, sino a garantizar la continuidad del cuidado, la seguridad del paciente y la calidez en el servicio, elementos intangibles que fortalecen la confianza del usuario en el sistema de salud.

- Prestaciones económicas y sociales: están orientadas al otorgamiento de subsidios por incapacidad temporal, maternidad, lactancia, sepelios y otras contingencias relacionadas con la pérdida o disminución de la capacidad económica y social de las familias, siendo un componente clave del enfoque integral del aseguramiento en salud.

A diario, la institución promueve valores intangibles fundamentales como la equidad en el acceso a los servicios, el respeto a la dignidad de las personas, y la eficiencia en el uso de los recursos públicos. Asimismo, trabaja continuamente en la mejora de la calidad percibida por el usuario, mediante la implementación de sistemas de gestión orientados a resultados y procesos de innovación tecnológica, como la digitalización de historia clínicas, la interoperabilidad de sistemas de información y el fortalecimiento de plataformas para la atención virtual.

De este modo, la institución no solo actúa como un proveedor de servicios médicos, sino también como un agente transformador del bienestar social, articulando su labor con otras entidades del Estado para garantizar un enfoque multisectorial en la atención de la salud y la protección del asegurado.

1.3 Reseña histórica de la institución

Inicios 1936 – 1947: durante el gobierno del Gral. Óscar Benavides, se implementaron políticas sociales para responder a las demandas populares. Se creó en Ministerio de Salud Pública, Trabajo y Previsión Social (1935) y el Seguro Social Obrero Obligatorio (1936), marcando el inicio de la seguridad social para los trabajadores

Crecimiento 1948 – 1973: bajo el régimen de Odría y luego Pedro Ugarteche, se amplió la cobertura con la creación del Seguro Social del Empleado (1948) y la construcción del Hospital del Empleado (1958), posteriormente llamado Hospital Edgardo Rebagliati.

Unificación 1973 – 1980: el gobierno de Juan Velasco Alvarado unificó los regímenes obreros y empleados con la creación del Seguro Social del Perú (1973), eliminando diferencias en los sistemas de pensiones, aunque aún con prestaciones de salud separadas.

Autonomía 1980 – 1997: con el regreso a la democracia, se crea el Instituto Peruano de Seguridad Social (IPSS 1980), con autonomía y cobertura ampliada. En los 90, bajo el gobierno de Fujimori, se crea la ONP (1992) y se refuerzan las funciones del IPSS.

Actualidad Modernización: en 1999 nace la Red Asistencial de Salud Arequipa, con autonomía administrativa y adscrito al Ministerio de Trabajo. Su gestión ha sido constantemente reformada para mejorar la atención a asegurados. Desde 2013 está en reorganización.

1.4 Organigrama de la institución

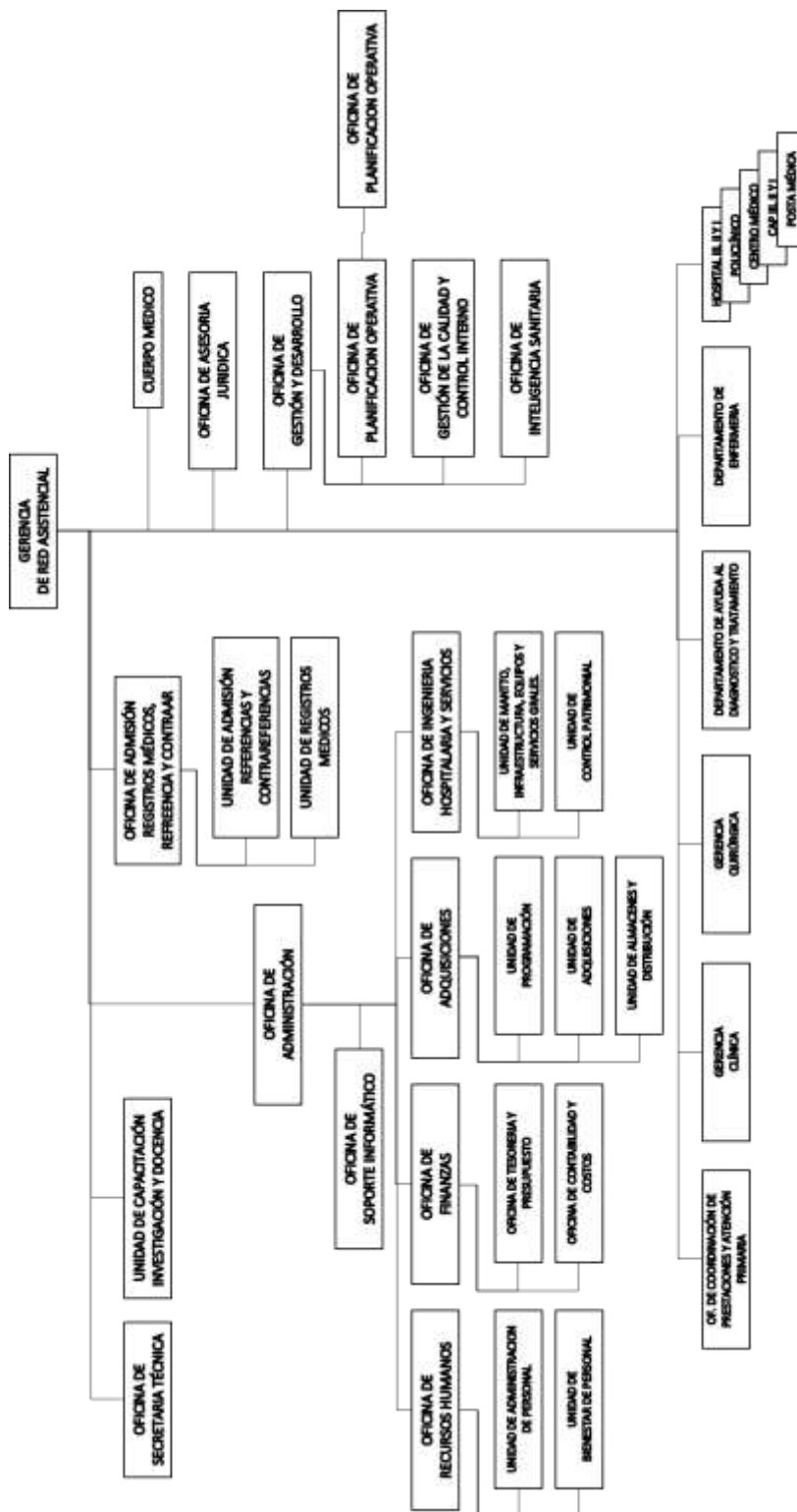


Figura 1. Organigrama Institucional de Red Asistencial Arequipa.

1.5 Visión y misión

1.5.1 Visión

Ser una institución moderna y en mejor continua, centrada en los asegurados, que garantiza el acceso a la seguridad social en salud con ética, oportunidad y calidad.

1.5.2 Misión

Brindamos prestaciones de salud, económicas y sociales a nuestros asegurados con una gestión eficiente e innovadora que garantiza la protección financiera de las prestaciones integrales.

1.6 Bases Legales o Documentos Administrativos

Las actividades desarrolladas durante la experiencia profesional se enmarcan dentro de la normativa vigente que regula el funcionamiento de las instituciones prestadoras de servicios de salud en el país, así como de las disposiciones internas emitidas por la propia entidad para garantizar una gestión eficiente, segura y transparente de sus procesos. Entre las principales bases legales y documentos administrativos que sustentan el trabajo realizado, se puede destacar:

- a) Ley N° 26790 – Ley de Modernización de la Seguridad Social en Salud:

Establece el marco legal para la organización y funcionamiento de los servicios de salud bajo un enfoque integral, solidario y eficiente, con énfasis en la protección del asegurado.

- b) Decreto Supremo N° 004-2019-SA-Reglamento del Sistema Nacional de Salud:

Define la estructura y funciones del sistema nacional de salud, promoviendo la interoperabilidad, el uso de tecnologías de información y la articulación de redes asistenciales.

- c) Ley N° 29733 – Ley de Protección de Datos Personales:

Norma de obligatorio cumplimiento en el tratamiento de información contenida en sistemas informáticos de gestión documental y firmas digitales, garantizando la confidencialidad, integridad y disponibilidad de los datos.

- d) Lineamientos para la Gestión Documental y Archivo en Entidades del Sector Público – Archivo General de la Nación:

Documento técnico que orienta la correcta implementación de sistemas de gestión documental digital, asegurando la autenticidad, fiabilidad y conservación de los documentos electrónicos.

e) Resoluciones de Gerencia Central y Gerencia de la Red Asistencial:

Instrucciones internas específicas que aprueban proyectos, planes operativos y lineamientos técnicos para la ejecución de iniciativas como la implementación de infraestructura tecnológica, enrolamiento al directorio activo, y despliegue de soluciones de firma digital.

f) Norma y Procedimientos Internos de la Oficina de Soporte Informático (OSI):

Documentos que regulan los protocolos de instalación de software, enrolamiento de equipos, control de inventarios, gestión de accesos y soporte técnico especializado.

g) Directivas y Manuales Técnicos del Sistema de Gestión Documental Electrónica (SGD):

Emitidos por la entidad o adoptados del marco regulador nacional, estos manuales establecen los criterios de uso, administración y operación de los sistemas digitales utilizados para la gestión de documentos.

Estas normativas y documentos administrativos han sido fundamentales para garantizar la legalidad, trazabilidad y alineamiento institucional del trabajo realizado, contribuyendo al fortalecimiento de la infraestructura tecnológica y de los procesos digitales de la entidad.

1.7 Descripción del área donde realiza sus actividades profesionales

La oficina de soporte informático forma parte del órgano de apoyo técnico de la Red Asistencial de Salud y tiene como responsabilidad principal garantizar el funcionamiento eficiente, seguro y continuo de la infraestructura tecnológica utilizada en los distintos servicios asistenciales y administrativos de la institución.

Esta oficina es un componente clave dentro de la estructura de la Oficina de Tecnología de la Información (OTI), actúa como el primer nivel de atención ante incidentes y requerimientos relacionados con los recursos informáticos, desempeñando un rol estratégico en la continuidad operativa, la calidad de servicio y la experiencia del usuario final.

Entre sus funciones principales se encuentran:

- Atención y resolución de incidencias técnicas: brinda soporte a usuarios ante fallas de hardware, software, redes y sistemas informáticos, asegurando la pronta solución para minimizar los tiempos de inactividad.
- Instalación, configuración y mantenimiento de equipos: realiza el formateo, configuración y puesta a punto de estaciones de trabajo, impresoras, periféricos y demás dispositivos, de acuerdo con las políticas institucionales.
- Enrolamiento y administración de equipos al Directorio Activo: asegura el registro, control de acceso y políticas de seguridad en los equipos de cómputo que forman parte de la red institucional.
- Implementación de software institucional: se encarga de instalar y verificar el funcionamiento de herramientas requeridas para la gestión documental, firma digital y otros sistemas de uso crítico en los procesos clínicos y administrativos.
- Gestión de usuarios y credenciales: apoya en la creación, modificación y eliminación de cuentas de usuario, respetando los protocolos de seguridad y trazabilidad.
- Documentación técnica y seguimientos de casos: Registra, actualiza y monitorea los tickets de soporte utilizando plataformas institucionales, lo que permite medir indicadores de atención y cumplimiento de niveles de servicio.
- Desde una perspectiva más amplia, la oficina de soporte informático no solo presta servicios operativos, sino que también aporta el fortalecimiento de la cultura digital institucional, promueve buenas prácticas en el uso de las tecnologías, y colabora en la adopción de soluciones innovadoras que contribuyen a la modernización del sistema de salud.
- Su labor es especialmente crítica en contextos de creciente demanda tecnológica, como la digitalización de expedientes clínicos, telemedicina, interoperabilidad de sistemas, seguridad informática y mejora continua de los procesos asistenciales mediante el uso de las TIC.

1.8 Descripción del cargo y de las responsabilidades del bachiller en la institución

1.8.1 Cargo

Ingeniero de Sistemas calificado para soporte informático para la Red Asistencial Arequipa.

1.8.2 Descripción del cargo dentro del proyecto

En el marco del proyecto de transformación digital en la red asistencial de salud, mi rol como Ingeniero de Sistemas estuvo enfocado en brindar soporte técnico especializado para la

preparación, configuración y alistamiento de equipos informáticos necesarios para el despliegue de las nuevas plataformas tecnológicas.

1.8.3 Responsabilidades específicas

- a) Actualización y configuración de estaciones de trabajo
 - Ejecución de actualización de la versión del sistema operativo Microsoft Windows a versiones compatibles con la infraestructura institucional (Windows 10 Pro 22H2).
 - Configuración de parámetros de red (dirección IP, DNS institucional, puerta de enlace predeterminad).
 - Asignación de nombre lógico de equipo siguiendo la nomenclatura establecida por el área de TI.
 - Activación de funciones del sistema como el cortafuego, escritorio remoto y actualizaciones automáticas.
 - Validación del estado del hardware mediante pruebas de funcionamiento de periféricos (puertos USB, tarjetas de red, adaptadores Wifi, audio y video).
 - Instalación y actualización de controladores (drivers) oficiales para garantizar la estabilidad del sistema.

- b) Enrolamiento de estaciones de trabajo al Directorio Activo (Active Directory):
 - Incorporación de cada equipo al dominio institucional mediante credenciales de administrador de dominio
 - Verificación de políticas de grupo (GPO) aplicadas al equipo y usuario, según las unidades organizativas (OU) asignadas.
 - Comprobación de replicación de políticas de seguridad y configuraciones de red a través del entorno de dominio
 - Configuración de perfiles de usuario bajo control de sesión mediante credenciales del dominio.
 - Pruebas funcionales de acceso a recursos compartidos en red (impresoras, carpetas compartidas, unidades mapeadas)
 - Registro del equipo en el inventario del dominio y documentación técnica asociada.

- c) Instalación y configuración de sistemas especializados (SGD y Firma Digital):
 - Despliegue del software cliente del Sistema de Gestión Documental (SGD) institucional, asegurando compatibilidad con el sistema operativo y el entorno de red.

- Instalación de certificados digitales personales e institucionales en el almacén de certificados del sistema operativo.
- Configuración del middleware criptográfico para correcta detección y uso del token USB o dispositivo criptográfico.
- Verificación de la conectividad con los servidores de autenticación y gestión documental mediante pruebas de acceso.
- Instalación de herramientas complementarias necesarias para la ejecución del SGD y firma digital (Java Runtime Environment, controladores del lector de tarjetas, complementos para navegadores web).
- Documentación del procedimiento de instalación para futuras réplicas o mantenimiento.

Estas tareas se ejecutaron siguiendo los lineamientos de la oficina de tecnología de la información (OTI), con un enfoque orientado a la estandarización, trazabilidad, seguridad informática y con continuidad operativa de los servicios digitales en la red asistencial.

CAPÍTULO II

ASPECTOS GENERALES DE LAS ACTIVIDADES PROFESIONALES

2.1 Antecedentes o diagnóstico situacional

En los últimos años, la red asistencial ha experimentado un crecimiento sostenido en cuanto a infraestructura tecnológica, impulsando por la necesidad de fortalecer los procesos asistenciales y administrativos mediante herramientas digitales. Este proceso de modernización ha permitido mejorar la calidad y oportunidad de los servicios ofrecidos a la población asegurada, en concordancia con los lineamientos estratégicos institucionales.

Un indicador clave de este crecimiento es el notable crecimiento del parque informático. A la fecha, la red cuenta con aproximadamente 1894 equipos de cómputo operativos, lo que representa un incremento superior al 300%, en comparación con años anteriores. Este aumento exponencial ha generado nuevas demandas técnicas y logísticas, relacionadas con la gestión, control y mantenimiento eficiente de los recursos informáticos distribuidos en los distintos establecimientos de salud.

Ante esta nueva realidad tecnológica, surgió la necesidad de implementar soluciones administrativas centralizadas, gestión documental electrónica y firma digital, con el fin de optimizar los flujos de trabajo, garantizar la seguridad de la información y cumplir con los estándares de interoperabilidad del sector público. En ese contexto, se aprobó la ejecución de un proyecto orientado a la implementación del Directorio Activo, el Sistema de Gestión Documental (SGD) y la plataforma de Firma Digital, tecnologías fundamentales para el avance hacia una administración digital segura, eficiente y escalable.

Como parte de este proyecto, se identificó la necesidad de contar con personal técnico especializado que pueda asumir tareas críticas relacionadas con la implementación, configuración y soporte de estas soluciones. Es en este marco que se sustenta la contratación de un ingeniero de sistemas, con competencias en redes, sistemas operativos, soporte informático y seguridad digital, para llevar a las actividades claves como:

- La preparación técnica de los equipos para su enrolamiento al dominio institucional.
- La incorporación ordenada de estaciones de trabajo al Directorio Activo.

- La instalación y configuración del software requerido por el Sistema de Gestión Documental y la Firma Digital.
- El soporte preventivo y correctivo durante las fases de despliegue, validación y estabilización del proyecto.

Este apoyo informático ha sido esencial para garantizar la continuidad operativa de los servicios, reducir tiempos de atención, estandarizar configuraciones, y fortalecer los pilares de la transformación digital en la red asistencial.

2.2 Identificación de oportunidad o necesidad en el área de actividad profesional

El incremento significativo del parque informático y la incorporación de nuevas herramientas tecnológicas en la red asistencial han generado un conjunto de necesidades específicas, cuyas oportunidades de mejora requieren ser atendidas mediante la participación de profesionales especializados. A continuación, se detallan las principales:

- a) Gestión centralizada del parque informático:
 - Necesidad de unificar y administrar los equipos de cómputo desde un entorno seguro y escalable
 - Implementación de políticas automatizadas de seguridad, actualización y acceso mediante el uso del Directorio Activo.
- b) Soporte informático especializado con enfoque en infraestructura TI:
 - Mayor demanda de personal capacitado en instalación, configuración y mantenimiento de hardware y software.
 - Atención eficiente a incidentes técnicos que afectan la productividad de áreas asistenciales y administrativas.
- c) Implementación y soporte de soluciones de gestión documental:
 - Requerimiento de soporte técnico para el despliegue de plataformas de gestión documental electrónica.
 - Acompañamiento a los usuarios finales en el uso correcto del sistema, garantizando la trazabilidad y legalidad de los documentos digitales.
- d) Adopción segura de la firma digital institucional:

- Necesidad de configurar certificados digitales, dispositivos criptográficos y middleware especializado.
 - Soporte en la validación de identidad digital y en la interoperabilidad de documentos firmados electrónicamente.
- e) Estandarización y documentación de procesos:
- Urgencia de establecer procedimientos operativos para tareas recurrentes: formateo, enrolamiento, instalación de software, etc.
 - Elaboración de manuales técnicos y guías de usuario para fortalecer la autonomía de las áreas usuarias.
- f) Control de inventario y trazabilidad de equipos:
- Desarrollo de mecanismos que permitan un control detallado del inventario informático, asociado al ciclo de vida de cada equipo.
 - Implementación de herramientas que permitan el monitoreo remoto y auditorías periódicas.
- g) Capacitación continua en tecnologías emergentes:
- Actualización constante del personal informático frente a nuevas herramientas institucionales.
 - Promoción de una cultura digital interna orientada a la innovación y el uso eficiente de los recursos informáticos.
- h) Fortalecimiento de la seguridad de la información:
- Necesidad de aplicar políticas de protección de datos personales, acceso restringido y respaldo seguro.
 - Implementación de medidas proactivas ante incidentes informáticos (antivirus, políticas de contraseña, cifrado)

Estas necesidades representan oportunidades claras para el desarrollo profesional de un ingeniero de Sistemas, cuya participación permite mejorar significativamente la eficiencia operativa, la seguridad digital y la calidad de los servicios prestados en la red asistencial de salud.

2.3 Objetivos de la actividad profesional

2.3.1 Objetivo general

Ejecutar tareas especializadas como ingeniero de sistemas en el proceso de implementación del Directorio Activo, el Sistema de Gestión Documental (SGD) y la plataforma de Firma Digital en la red asistencial de salud, contribuyendo al fortalecimiento de la infraestructura tecnológica, la automatización de procesos institucionales y la interoperabilidad segura de la información.

2.3.2 Objetivos específicos

- Se prepararon y optimizaron 1850 equipos de cómputo, actualizando sus sistemas operativos, configuraciones de red y recursos técnicos, asegurando condiciones óptimas para su integración al dominio institucional de la Red Asistencial de Salud.
- Se integraron con éxito las estaciones de trabajo al Directorio Activo (AD), aplicando políticas de grupo (GPO) y unidades organizativas (OU) según las áreas funcionales, logrando una administración centralizada, segura y estandarizada de usuarios y recursos.
- Se desplegó e integró en Sistema de Gestión Documental (SGD) y la plataforma de Firma Digital en más de 1000 estaciones de trabajo, configurando correctamente los certificados digitales y asegurando su interoperabilidad con los sistemas institucionales.
- Se implementaron buenas prácticas de soporte informático especializado, atendiendo más del 90% de los requerimientos técnicos y documentado los procedimientos de mantenimiento preventivo y correctivo, lo que permitió reducir los tiempos de inactividad y mejorar la continuidad operativa.
- Se capacitó a más de 800 usuarios administrativos y asistenciales en el uso del Sistema de Gestión Documental y Firma Digital, alcanzando un nivel de satisfacción superior al 85% según las evaluaciones posteriores a la formación.
- Se estandarizaron y documentaron los procedimientos técnicos ejecutados, generando cuatro manuales operativos y guías internas sobre enrolamiento, instalación de software, uso de certificados digitales y resolución de incidencias, fortaleciendo la trazabilidad y repetibilidad del proyecto.

2.4 Justificación de la actividad profesional

La actividad profesional desarrollada se enmarca en el proceso de transformación digital impulsado por la Red Asistencial de Salud Arequipa, en respuesta a la creciente demanda

tecnológica generada por el incremento del parque informático y la necesidad de fortalecer la eficiencia operativa y documental en los servicios de salud.

En este contexto, la participación del bachiller como Ingeniero de Sistemas tuvo un impacto significativo en la consolidación técnica del proyecto, al aplicar conocimientos especializados en infraestructura informática, redes, sistemas operativos, seguridad digital y gestión de servicios TIC, contribuyendo directamente a los resultados logrados en cada fase de implementación.

El aporte profesional individual se evidenció principalmente en los siguientes aspectos:

- Optimización técnica de la infraestructura: el bachiller ejecutó el aislamiento técnico de 1850 equipos de cómputo, asegurando compatibilidad, estabilidad y seguridad en la integración al dominio institucional, lo que permitió una gestión centralizada y eficiente de los recursos tecnológicos.
- Estandarización y documentación técnica: se desarrollaron manuales de instalación, procedimientos de enrolamiento y guías operativas, que actualmente sirven como referencia para futuras implementaciones y garantizan la continuidad operativa del proyecto.
- Fortalecimiento de la seguridad informática: mediante la correcta aplicación de políticas de grupo (GPO), control de accesos y configuración de certificados digitales, el bachiller contribuyó a elevar niveles de ciberseguridad y protección de la información sensible institucional.
- Capacitación y transferencia de conocimiento: la formación directa de más de 800 usuarios en el uso del Sistema de Gestión Documental y Firma Digital generó un impacto sostenible en las competencias digitales del personal administrativo y asistencial, reduciendo la dependencia del soporte técnico.
- Soporte técnico especializado y resolución de incidencias: se atendió y documentó más del 90% de los requerimientos técnicos, aplicando metodologías basadas en ITIL y buenas prácticas de soporte, lo que mejoró los indicadores de disponibilidad de servicios y satisfacción del usuario final.

La participación profesional del bachiller permitió articular la gestión técnica con los objetivos institucionales, asegurando que las soluciones tecnológicas implementadas fueran sostenibles, seguras y alineadas con los lineamientos de gobierno digital.

Por tanto, esta experiencia no solo representa la aplicación práctica de los conocimientos adquiridos durante la formación universitaria, sino también un aporte concreto y medible al

fortalecimiento de la infraestructura tecnológica institucional, consolidando el perfil de ingeniero de sistemas como un agente clave en la modernización del sector salud.

2.5 Resultados esperados

Previo al inicio de la ejecución del proyecto de implementación del Directorio Activo, Sistema de Gestión Documental (SGD) y Firma Digital en la red asistencial, se definieron los siguientes resultados esperados, formulados con indicadores cuantificables y alineados a los objetivos del fortalecimiento digital institucional.

a) Enrolamiento de estaciones de trabajo al Directorio Activo:

- Lograr el enrolamiento de al menos 1850 equipos de cómputo al dominio institucional, priorizando los equipos ubicados en áreas críticas (atención al usuario, consultorios, farmacia, archivo, etc.)
- Aplicar políticas de grupo estandarizadas en el 100% de los equipos enroladas, asegurando la correcta configuración de seguridad, control de acceso y recursos compartidos.

b) Soporte informático especializado:

- Atender y resolver más del 90% de los tickets de soporte generados durante el proceso de enrolamiento, instalación de software y configuración de servicios digitales, dentro de los plazos establecidos por la Oficinas de Tecnologías de la Información.
- Documentar procedimientos técnicos para al menos 4 actividades operativas clave (formateo, enrolamiento, instalación de SGD, configuración de firma digital), generando manuales internos de referencia.

c) Capacitación a usuarios finales:

- Capacitar a un mínimo de 800 usuarios institucionales en el uso del Sistema de Gestión Documental y la plataforma de Firma Digital, mediante sesiones grupales, asistencia personalizada y elaboración de guías de usuario.
- Alcanzar una tasa de satisfacción del 85% o superior en las encuestas aplicadas posterior a las capacitaciones, evaluando claridad, utilidad y aplicabilidad del contenido.

d) Habilitación de estaciones de trabajo con SGD y Firma Digital:

- Instalar y configurar correctamente el sistema SGD y los certificados digitales en al menos 1000 estaciones de trabajo, garantizando su operatividad con los sistemas institucionales.
- Verificar que el 100% de las estaciones habilitadas pueden generar, firmar digitalmente y enviar documentos electrónicos conforme a los flujos de trabajo establecidos por la administración.

Estos resultados esperados constituyen el marco de referencia para evaluar el avance y el impacto del proyecto, permitiendo además identificar puntos de mejor, asignar recursos con eficiencia y asegurar el cumplimiento de los objetivos estratégicos relacionados con la modernización tecnologías de la red asistencial.

CAPÍTULO III

MARCO TEÓRICO

3.1 Introducción

El presente capítulo desarrolla el marco teórico que sustenta la implementación del Directorio Activo, Sistema de Gestión Documental (SGD) y Firma Digital en la Red Asistencial de Salud Arequipa. Su objetivo es fundamentar los conceptos técnicos y de gestión involucrados en la transformación digital institucional, apoyándose en teorías, normas y estudios recientes relacionados con la administración de tecnologías de la información y la modernización de servicios públicos.

3.2 Fundamentos de la transformación digital en el sector salud

La transformación digital en el sector salud implica la integración de tecnologías de información para mejorar la eficiencia, la calidad y la accesibilidad de los servicios médicos. Según la Organización Mundial de la Salud (OMS, 2023), la digitalización de procesos permite una gestión más oportuna y segura de la información clínica y administrativa. En el contexto peruano, la Política Nacional de Transformación Digital (PCM, 2024) promueve la adopción de tecnologías que impulsen la interoperabilidad, la transparencia y la sostenibilidad institucional. La Red Asistencial de Salud Arequipa se enmarca en este proceso al implementar soluciones que fortalecen la gestión documental, la seguridad informática y la eficiencia administrativa.

3.3 Infraestructura tecnológica y Directorio Activo

El Directorio Activo (Active Directory) es una tecnología de Microsoft que permite la administración centralizada de usuarios, equipos y recursos dentro de una red. Su estructura jerárquica basada en dominios y políticas de grupo (GPO) facilita el control de accesos y la aplicación de configuraciones de seguridad (Microsoft, 2025). La implementación de un Directorio Activo en entornos institucionales como la Red Asistencial de Salud Arequipa mejora la eficiencia operativa y la seguridad de la infraestructura tecnológica.

Su arquitectura basada en dominios, arboles, Controladores de Dominio (DC), Unidades Organizativas (OUs), y la aplicación de política mediante Objetos de Políticas de Grupos (GPO).

Una característica del Directorio Activo es la capacidad para crear estructuras lógicas y jerárquicas de la información. Dicha estructura es fundamental para la organización de manera intuitiva y accesible de datos del directorio, esto permitirá que los administradores y usuarios utilizar de manera eficaz la información. El esquema que utiliza el Directorio Activo es un conjunto de reglas que definen clases y atributos de objetos, así como el formato en que esos datos son almacenados y compartidos.

El Directorio Activo incorpora funciones integrales de seguridad, además de gestionar información de usuarios y recursos. Dentro de las funciones se incluyen la autenticación de usuarios, antes de acceder a la red verifica la identidad del usuario, y el control de acceso, eso determina luego de la autenticación que recursos puede utilizar. Gracias a las políticas de seguridad son aplicables a nivel de usuario, grupo o recursos.

El catálogo global del Directorio Activo muestra una vista centralizada de datos de directorio, independientemente del dominio en que residan. Con que la búsqueda y acceso a la información a través de la red se simplifica, teniendo como resultado consultas y búsquedas eficientes por parte de usuarios y administradores.

Una característica importante del Directorio Activo es la replicación, asegurando que los controladores dentro de un dominio en específico contengan una copia actualizada y sincronizada de los datos del directorio. Garantizando consistencia y disponibilidad de información incluso con cambios y actualizaciones.

3.3.1 Componentes lógicos del Directorio Activo

Elementos que conforman la estructura y funcionamiento en un entorno de red del Directorio Activo. Los componentes lógicos son clave para el diseño, que se adaptaran a las necesidades de la organización (Microsoft, 2025).

Los componentes lógicos se organizan:

- a) Bosques: conjunto de dominio que tienen en común una estructura lógica. Al establecer relaciones de confianza entre dominios simplifica la administración, esto facilita la comunicación y colaboración dentro de la red.
- b) Dominio: es una división del bosque en unidades organizativas (OU), en la que se almacena información de usuarios y a su vez proporciona servicios de autenticación y autorización en la red empresarial. Permitiendo establecer relaciones de confianza, facilitando el acceso a recursos entre usuarios de áreas diferentes. Además de replicar

la información almacenada entre controladores de dominio garantizando la disponibilidad y consistencia de datos.

- c) Unidades Organizativas (OU): contenedores que agrupan objetos estableciendo jerarquías a nivel de dominio. Permitiendo gestionar eficazmente una mayor cantidad de objetos, el Directorio Activo admite la delegación de autoridad, esto permite la transferencia del control total administrativo o limitado sobre objetos a usuarios dentro del dominio.
- d) Objetos: recursos compartidos en red, tales como usuarios, equipos, impresoras, carpetas compartidas, etc. Estos tienen atributos definidos por propiedades y características.

Según lo conceptos recopilados anteriormente entendemos que bosques contienen dominios, y los dominios contienen unidades organizativas y a su vez contienen objetos.

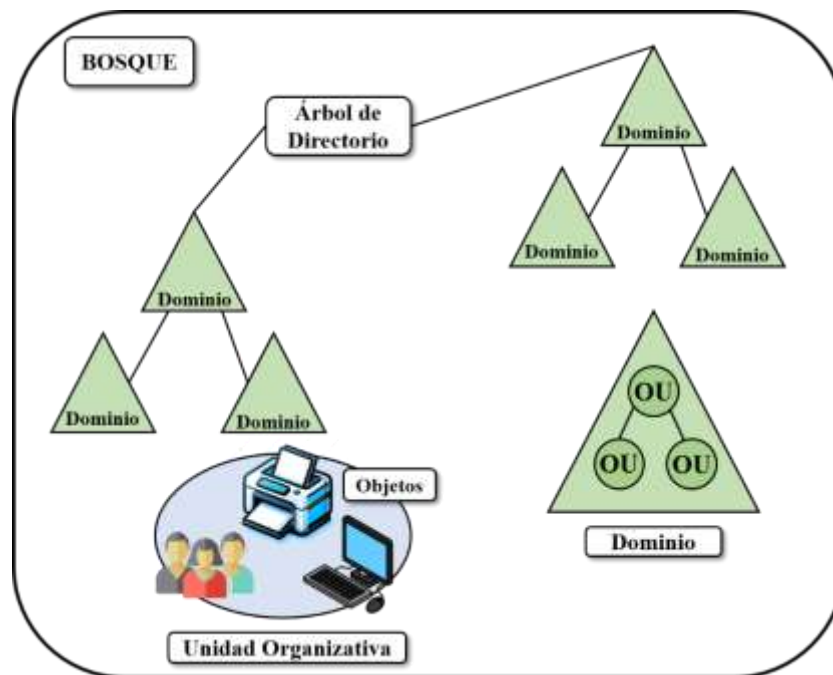


Figura 2. Componentes lógicos del Directorio Activo. Tomada de PCM (2017).

3.3.2 Componentes físicos del Directorio Activo

Hardware o elementos visibles que son parte de infraestructura del Directorio Activo. Que se organizan de la siguiente forma:

- a) Controlador de dominio: la copia de la base de datos el Directorio Activo es contenido del controlador de dominio. Encargado de procesar y replicar cambios entre los controladores de dominio que forman parte de un dominio o bosque.

- b) Sitio: los objetos específicos del Directorio Activo se encuentran en este contenedor, que se encuentra en un área geográfica que forma parte de la organización.
- c) Hardening de servidores: es el fortalecimiento de la seguridad, prácticas y procedimientos que reducen vulnerabilidades en Tecnologías de la Información (TI) y sistemas operativos. Buscando minimizar riesgos de seguridad informática, eliminar servicios no necesarios, ajustar configuraciones y aplicar controles, en entornos críticos como el Directorio Activo (Shrader, 2025).
- d) Importancia del Hardening en el Directorio Activo: utilizado para gestionar políticas de usuario y acceso a recursos compartidos en una red, en su mayor parte en entornos empresariales. Administrando credenciales y acceso de forma centralizada con la finalidad de proteger de ataques que comprometan la infraestructura de TI en una empresa.
- e) Principios básicos del Hardening: para una mejora continua en la seguridad, incluyen las siguientes prácticas:
 - Minimización: elimina servicios no esenciales con la finalidad de reducir los ataques.
 - Segmentación de seguridad: divide redes y sistemas para controlar un mejor acceso y reducir el riesgo de ataques en zonas seguras.
 - Gestión de configuraciones: implementa y estandariza políticas de seguridad, usando configuraciones seguras teniendo como base guías y estándares conocidos como NIST, CIST y DISA STIG.

El hardening del Directorio Activo contiene técnicas en varios aspectos del servicio:

- Políticas de Grupo (GPO): gestiona y aplica configuración de seguridad en todos los dispositivos de la red (Microsoft, 2025).
- Control de acceso a objetos: asegura que el acceso a información sensible solo a usuarios autorizados (Scarfone, Jansen y Tracy, 2008).
- Seguridad de autenticación: mediante el uso de políticas de seguridad como contraseñas fuertes, autenticación multifactor, restricción de acceso basadas en la necesidad de conocer y el principio de menor privilegio fortalece los procesos de autenticación (Microsoft, 2025).
- Monitoreo y auditoría: herramientas de monitoreo y auditoría para detectar cambios y actividades sospechosas dentro del Directorio Activo con el fin de garantizar el cumplimiento y la efectividad de las políticas de seguridad (Scarfone, Jansen y Tracy, 2008).

f) Autenticación: proceso crítico que determina si el usuario, es quien declara ser antes de conceder permiso para el acceso del sistema o plataformas digitales (Fernández, 2024). Proceso crucial de seguridad para cualquier sistema de información, utiliza diversos métodos:

- Algo que el usuario sabe: el método más común es una contraseña, vulnerable a diversos ataques, requiere ser fortalecido con otros métodos.
- Algo que el usuario posee: proporciona una segunda capa de seguridad el uso de token digitales o un código recibido por SMS, siendo este un factor de Autenticación Multifactor (MFA).
- Algo que el usuario es: nivel altamente confiable son los datos biométricos como huellas dactilares o reconocimiento facial.

Las evoluciones de los métodos de autenticación incorporan sistemas más robustos y eficientes como Autenticación Multifactor (MFA) y el Single Sign-On (SSO).



Figura 3. Autenticación de usuario.

g) Autenticación Multifactor (MFA): Fortalece el proceso de autenticación requiriendo diversas pruebas de identidad previo a conceder acceso, minimizando significativamente el riesgo de acceso no autorizados.



Figura 4. Verificación con Segundo Factor.

- h) Single Sign-On (SSO): el SSO permite el acceso a servicio y aplicaciones con un conjunto de credenciales, eso con la finalidad de simplificar la gestión de credenciales mejorando la experiencia de usuario; además de facilitar el acceso, también fortalece la seguridad al tener en controlado la autenticación del usuario (Onelogin, 2025).



Figura 5. *Single Sign-On.*

3.4 Gestión documental electrónica

El Sistema de Gestión Documental (SGD) es una herramienta que permite administrar, archivar y controlar el ciclo de vida de los documentos electrónicos. De acuerdo con la Secretaría de Gobierno y Transformación Digital (PCM, 2025), el Modelo de Gestión Documental (MGD) establece lineamientos para la estandarización de procesos documentarios en entidades públicas. En el sector salud, su adopción garantiza trazabilidad, reducción del uso del papel y mejora de la atención administrativa. Experiencias recientes del Instituto Nacional de Salud (INS, 2024) y del Instituto Nacional de Salud del Niño (INSN, 2024) demuestran el impacto positivo de los sistemas documentales en la gestión institucional.

El Sistema de Gestión Documental permite gestionar digitalmente documentos de una organización. Reemplazando los archivos físicos promoviendo así la digitalización de documentos, facilitando su acceso. Entre otras funciones como flujos de trabajo y colaboración en tiempo real y gestión de permisos de accesos a información sensible (Ayerdi, 2024).

Parte de transformación digital, un Sistema de Gestión Documental ayuda a los colaboradores organizar los documentos para:

- Garantizar la disponibilidad inmediata en tiempo real de documentos.
- Proteger documentación sensible mediante seguridad y confidencialidad con restricciones de acceso por usuario.
- Sustituir tareas repetitivas que se hacen de manera manual por flujos de trabajos automatizados.

- Reducir el uso de papel mediante la creación de procesos más sostenibles.

3.4.1 Características principales de un gestor documental eficaz

- a) Indexación para búsquedas eficientes: la indexación de documentos por parte del Sistema de Gestión Documental permite la búsqueda de rápida de documentos al tenerla clasificada. Ejemplos de posibles campos de índice son una fecha determinada, un numero de cliente o un tipo de documento en específico maximizando la capacidad de búsqueda.

El Sistema de Gestión Documental permite por palabras clave y texto completo (Ayerdi, 2024). Los Sistemas de Gestión Documental robustos automatizan la indexación de manera que los documentos no tengan que ser etiquetados manualmente. Para posterior los colaboradores podrán realizar consultas fáciles buscando con los términos relacionados en el índice.

- b) Flujo de trabajo automático: el flujo lógico de procesos creados por los flujos de trabajo digitales, aginan responsables de tareas y sustitutos en caso de no disponibilidad del colaborador. Las gestiones de flujo de trabajo especifican el proceso que inicia el flujo.

Los cambios de estado de un documento en el Sistema de Gestión Documental activa flujos de trabajo. Un sistema de gestión de flujos de trabajo permite que lo colaboradores y gestores puedan ver cada caso para ser controlados y supervisados. Los flujos que contiene varias tareas y pasos recurrentes son buenos candidatos para optimizar.

La gestión de expedientes de los colaboradores, tramites de facturación y contratos son un punto de partida para ser automatizadas traduciéndose en un gran aumento de productividad y ahorro de costos cuantificables.

Según la Presidencia del Consejo de Ministros de Perú, el Sistema de Gestión Documental permite un trámite de documentos electrónico promoviendo así el “Cero Papel” como política mediante el uso complementario de la Firma Digital y Certificados Digitales con valor legal, utilizando la Plataforma de Interoperabilidad del Estado para el cruce de documentación entre entidades públicas. A través de su Secretaría de Gobierno y Transformación Digital la Presidencia del Consejo de Ministros, no brindan los lineamientos y entrega de herramientas para la implementación del sistema en la administración pública (PCM, 2025).

Características del Sistema de Gestión Documental según la Presidencia del Consejo de Ministros:

- Documentación electrónica: permite el trámite y la difusión de documentos de forma digital.
- Firma digital: para la validez legal de los documentos electrónicos, el uso de firmas y certificados digitales hacen equivalentes a los documentos físicos.
- Política de “cero papel”: tiene como objetivo principal reducir el uso de papel en la administración pública, con el fin de optimizar procesos y ahorrando en insumos.
- Interoperabilidad: para compartir los documentos digitales se utiliza como conexión entre otras entidades públicas la Plataforma de Interoperabilidad del Estado.
- Enfoque en la transformación digital: pieza clave en la búsqueda de servicios digitales más eficientes y centrados en ciudadanía apoyando la implementación de la Ley de Gobierno Digital.

3.5 Seguridad informática en entornos institucionales

La seguridad informática se fundamenta en los principios de confidencialidad, integridad y disponibilidad de la información. Normas internacionales como la ISO/IEC 27001:2022 establecen los requisitos para implementar sistemas de gestión de seguridad de la información (SGSI). En el Perú, la Estrategia Nacional de Seguridad y Confianza Digital (PCM, 2024) refuerza la importancia de la ciberseguridad en instituciones públicas. La aplicación de políticas GPO y autenticación centralizada mediante Directorio Activo contribuye a mitigar riesgos y proteger los datos sensibles de la organización.

3.6 Metodologías de gestión de proyectos tecnológicos

El Project Management Body of Knowledge (PMBOK) es un estándar internacional que define las buenas prácticas para la gestión de proyectos. Su séptima edición (PMI, 2021) introduce un enfoque basado en principios que abarca la planificación, ejecución, seguimiento y cierre de proyecto. La aplicación del PMBOK en el presente proyecto permitió estructurar las fases de trabajo, identificar riesgos, controlar recursos y evaluar resultados. Complementariamente, las prácticas ITIL proporcionaron lineamientos para la gestión eficiente de servicios tecnológicos.

3.7 Firma digital y su aplicación institucional

La firma digital es un mecanismo criptográfico que garantiza la autenticidad, integridad y no repudio de los documentos electrónicos. Basada en la Infraestructura de Clave Pública (PKI), su aplicación en el Perú se regula por la Ley N° 27269 y su reglamento actualizado (PCM, 2023). El uso de certificados digitales emitidos por entidades acreditadas permite validar la identidad del firmante y fortalecer la seguridad jurídica de los documentos. En el contexto

institucional, la firma digital acelera procesos de aprobación, reduce costos operativos y contribuyente a la política de gobierno digital y cero papel.

Según la Presidencia del Consejo de Ministros de Perú, es un método criptográfico asimétrico que usa para garantizar la autenticidad, integridad y no repudio de los documentos digitales un par de claves. La Presidencia del Consejo de Ministros para el uso de firmas digitales en entidades públicas establece directivas y políticas, facilitando el uso de la firma digital mediante la emisión de certificados digitales y herramientas a través de la Plataforma del Estado Peruano y el servicio de Firma Perú (PCM, 2025).

La firma digital permite:

- Garantizar la identidad del ciudadano validando el documento firmado equivalente al documento físico.
- Garantizar la autoría, integridad y el no repudio del documento digital firmado.
- Apoya la política del “Cero Papel”.
- Disminuye tiempos optimizando procesos y costos ahorrando en insumos.
- Evita desplazamientos físicos, por siendo el proceso de firma digital se puede realizar desde un computador que tenga un software Firmador.
- Evita el envío y recepción de documentación física, ya que esta documentación firmada electrónicamente puede ser compartida a través de plataformas digitales.

3.8 Certificado digital

Documento emitido por una entidad de certificación, que vincula una clave pública y otra privada asegurando su identidad digital. Lo que permite ejecutar acciones de comercio y gobierno electrónico con valor legal (RENIEC, 2024).

3.9 Token criptográfico

Dispositivo en forma de una memoria de almacenamiento USB, que contiene un chip criptográfico en el que se almacena una clave privada para ejecución de la firma digital (RENIEC, 2024).

3.10 Documento nacional de identidad electrónico

El nuevo modelo del Documento Nacional de Identidad contiene un chip criptográfico integrado que permite efectuar la firma digital con ayuda de un periférico lector de DNIE y software requerido (RENIEC, 2024).

CAPÍTULO IV

DESCRIPCIÓN DE LAS ACTIVIDADES PROFESIONALES

4.1 Descripción de actividades profesionales

Durante la ejecución del proyecto, se llevaron a cabo actividades técnicas orientadas a garantizar la integración efectiva de las estaciones de trabajo al ecosistema digital institucional. Estas actividades se centraron en la preparación técnica de equipos, enrolamiento al Directorio Activo, instalación de los componentes del Sistemas de Gestión Documental (SGD), implementación de la plataforma de Firma Digital, soporte técnico, capacitación a usuarios y documentación de procesos.

Las tareas ejecutadas incluyeron:

- a) Actualización y configuración inicial de equipos de cómputo, asegurando compatibilidad con las políticas del dominio institucional.
- Realización de respaldo de información crítica previa la actualización del sistema operativo.

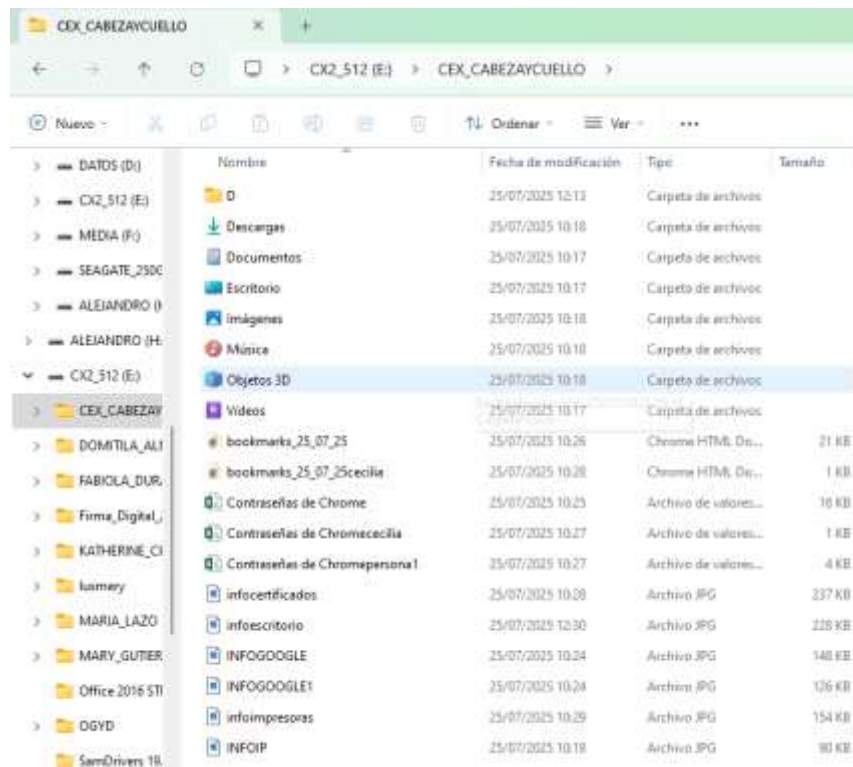


Figura 6. Respaldo de información de equipo.

- Aplicación de imágenes estándar mediante herramientas como Acronis 2015

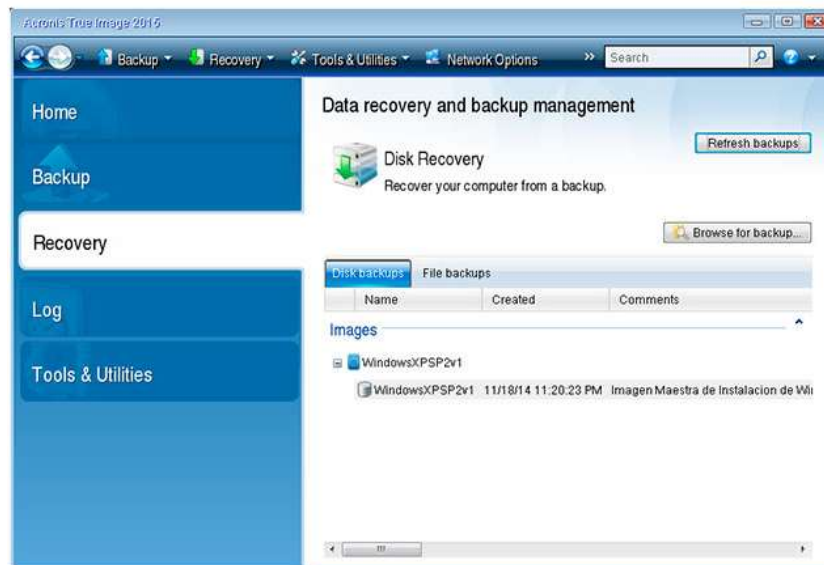


Figura 7. *Página de inicio Acronis 2015.*

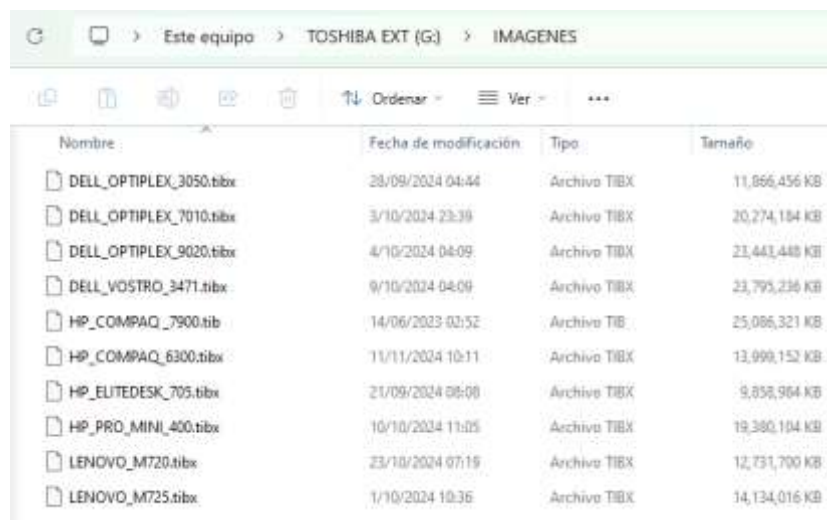


Figura 8. *Imágenes de discos de equipos.*

- Configuración de BIOS/UEFI para compatibilidad con sistemas operativos modernos y parámetros de seguridad (ejemplo deshabilitar arranque seguro de equipos antiguos).



Figura 9. Activar/desactivar Secure Boot.

- Instalación del sistema operativo institucional (Windows 10 Pro 22H2) desde medios autorizados.
 - Configuración de red local (Direcciones IP estáticas según la topología de red).
 - Establecimiento de parámetros regionales y de seguridad básica antes del enrolamiento.
- b) Enrolamiento al Directorio Activo, aplicando políticas de grupo (GPO) y control de acceso según unidades organizativas.
- Registro del nombre del equipo bajo nomenclatura según estructura institucional.

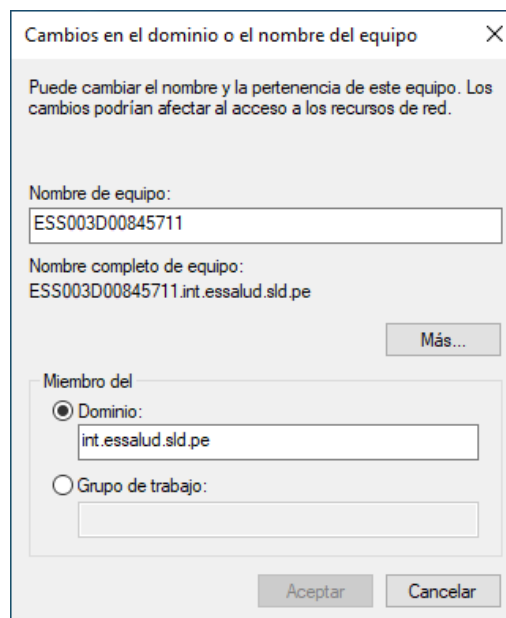


Figura 10. Nombre de equipo según nomenclatura.

- Incorporación del equipo a la Unidad Organizativa (OU) correspondiente según sede, servicio o área.

- Aplicación de GPO específicas: restricciones de software, configuración de escritorio, asignación de impresoras, redirección de carpetas y políticas de seguridad (antivirus, firewall, USB, etc)
 - Validación del correcto enlace con el controlador de dominio (DC), replicación de políticas y sincronización con servicios de red como DNS y DHCP.
- c) Instalación y validación del cliente SGD y la plataforma de Firma Digital, incluyendo certificados digitales y pruebas de interoperabilidad.
- Instalación del software cliente del Sistema de Gestión Documental en su versión actualizada.

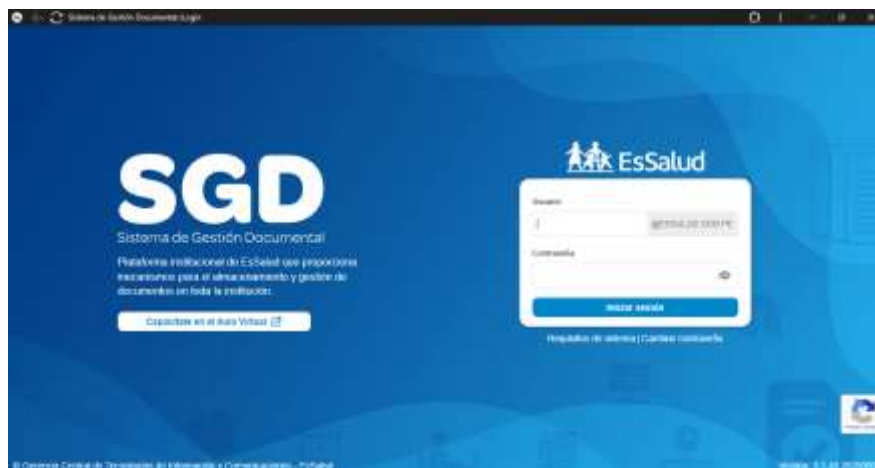


Figura 11. *Página inicio Sistema de Gestión Documental.*

- Registro de usuario en la plataforma institucional de Firma Digital.
- Instalación del middleware del token criptográfico para el uso del certificado digital.



Figura 12. *Software CryptoID.*

- Importación del certificado digital en el almacén de certificados del sistema operativo y navegador institucional.

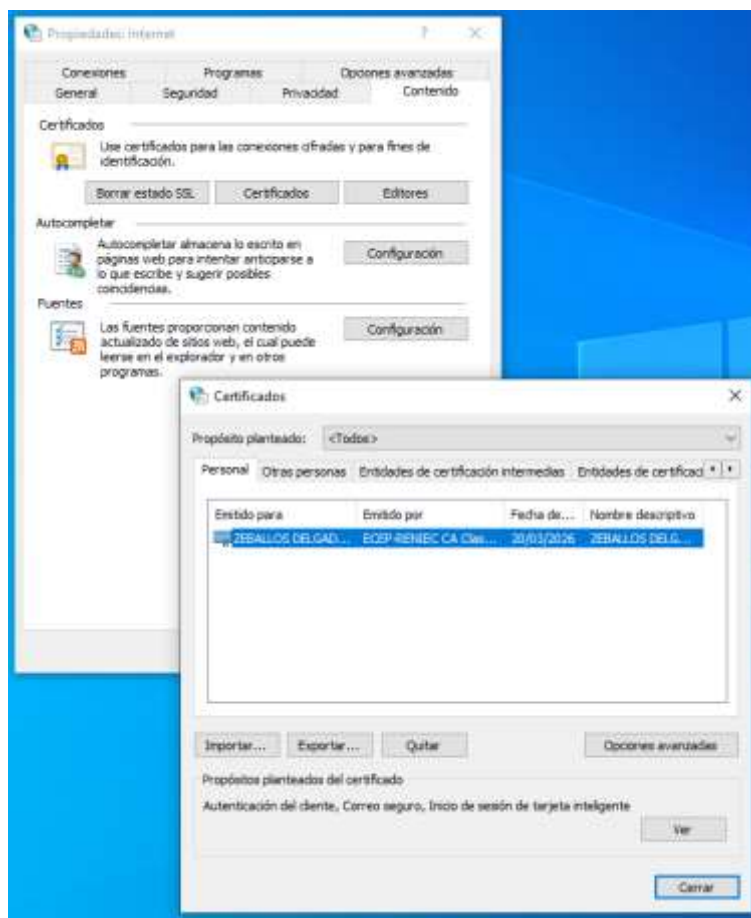


Figura 13. *Importación/Exportación de certificados digitales.*

- Ejecución de pruebas interoperabilidad: generación, firma, visualización y validación de documentos firmados electrónicamente en formato PDF o XML.
- d) Atención de incidencias técnicas, relacionadas con software, red, acceso al dominio o uso de herramientas digitales.
- Diagnóstico y resolución de errores de conectividad a red o servicios del dominio.
 - Reasignación de políticas de grupo (forzado de GPO) mediante línea de comandos y consola de administración.
 - Reinstalación o reparación del cliente SGD o drivers de token digital.
 - Actualización de certificados vencidos o invalidados.
 - Coordinación con áreas superiores de TI ante incidencias críticas de autenticación o fallos de replicación del dominio.

- e) Capacitación técnica a usuarios administrativos y médicos sobre el uso del sistema de firma electrónica y el SGD.
 - Elaboración de guías rápidas y tutoriales impresos/digitales orientados al usuario final.
 - Realización de sesiones presenciales o virtuales de capacitación sobre el uso del sistema SGD: creación, envío, firma y archivo de documentos.
 - Orientación sobre el correcto uso del token de firma digital, mantenimiento básico y solución de errores comunes.
 - Resolución de consultas personalizadas después de la capacitación.

- f) Elaboración de documentación técnica, procedimientos estandarizados y registros de configuración de equipos.
 - Generación de instructivos técnicos paso a paso para enrolamiento de equipos, instalación de firma digital y resolución de errores frecuentes.
 - Registro de inventario de equipos configurados con sus respectivos datos: hostname, usuario, IP asignada, sede, área y fecha de enrolamiento.
 - Documentación de casos de soporte técnico atendidos, clasificando por tipo de incidencia y solución aplicada.
 - Estandarización de procesos operativos en fichas técnicas reutilizables por otros integrantes del equipo de soporte informático.

4.1.1 Enfoque de las actividades profesionales

El enfoque adoptado fue técnico-operativo con visión de integración sistemática, priorizando la alineación con los estándares institucional de TI, la continuidad operativa de los servicios y la escalabilidad de la solución implementada.

Desde el rol de un ingeniero de sistemas, se aplicaron principios de:

- a) Gestión de infraestructura informática, orientada al control centralizado de equipos, usuarios y recursos.
 - Enrolamiento de equipos al Directorio Activo institucional, permitiendo su integración a una arquitectura de red jerárquica y administrada.
 - Segmentación de dispositivos y usuarios a través de Unidades Organizativas (OU), lo cual permitió una asignación específica de políticas según funciones y áreas.

- Aplicación de Group Policy Objects (GPO) para controlar configuraciones de seguridad, restricciones de uso, scripts de inicio de sesión, políticas de red y otras funciones críticas.
- Estandarización de configuraciones básicas de hardware y software, facilitando la gestión remota y la automatización de tareas repetitivas mediante herramientas administrativas como PowerShell o la Consola de Administración de Directivas de Grupo.

Este enfoque permitió reducir la complejidad operativa y mejorar la trazabilidad del ecosistema informático institucional.

- b) Seguridad informática, mediante el uso de políticas de acceso, autenticación y firma digital.
- Uso de autenticación de doble factor y credenciales seguras integradas al dominio.
 - Instalación y configuración de certificados digitales emitidos por una entidad certificadora autorizada, requeridos para la firma electrónica y validación documental.
 - Validación de interoperabilidad del cliente SGD con los servidores de firma digital, asegurando el cumplimiento de las normativas vigentes sobre el gobierno digital y gestión electrónica de documentos.

Estas acciones contribuyeron a fortalecer el marco de ciberseguridad institucional.

- c) Soporte técnico estructurado, basado en la resolución eficiente de problemas, documentación y comunicación efectiva con el usuario final.
- Registro y seguimiento de incidencias técnicas mediante la mesa de ayuda.
 - Resolución de problemas de conectividad, errores de configuración, fallas de software y conflictos de compatibilidad en el entorno del usuario.
 - Priorización de tickets de soporte en función del impacto sobre procesos críticos de atención médica o gestión administrativa.
 - Comunicación efectiva con los usuarios, utilización de un lenguaje accesible, instrucciones guiadas y asistencia remota cuando fue necesario.
 - Documentación detallada de cada intervención técnica para futura referencia y trazabilidad del historial de soporte.

Esto garantizó una atención eficiente, reduciendo tiempos de inactividad y elevó la satisfacción de los usuarios finales.

- d) Transferencia de conocimiento, asegurando la adopción correcta del sistema por parte de los usuarios.
- Diseño e impartición de capacitación de capacitaciones prácticas a usuarios médicos, administrativos y técnicos, enfocadas en el uso del SGD, validación de documentos y firma digital.



Figura 14. *Capacitación SGD.*

- Elaboración de manuales y guías de usuarios personalizadas, adaptadas a los distintos perfiles y niveles de competencia digital.

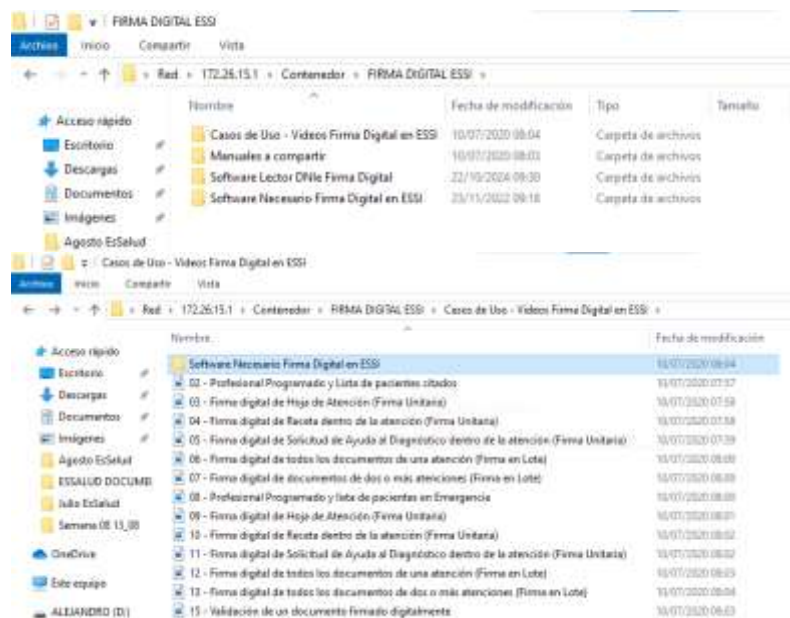


Figura 15. *Manuales Firma Digital en repositorio institucional.*

- Ejecución de sesiones de acompañamiento individualizado después de la implementación, para reforzar conocimientos, aclarar dudas y promover el uso responsable de las herramientas.
- Generación de una cultura organizacional más digital y menos dependiente del soporte técnico ante tareas rutinarias.

La transferencia efectiva de conocimiento minimizó errores operativos, aceleró la adopción del sistema y generó autonomía funcional.

- e) Este enfoque permitió asegurar la sostenibilidad del proyecto más allá de su fase de implementación, garantizando una base sólida para futuros desarrollos digitales dentro de la red asistencial.
- Establecimiento de una arquitectura de dominio adaptable a futuras incorporaciones tecnológicas o institucionales.
 - Generación de documentación técnica reutilizable y procesos replicables en otras sedes de la red asistencial.
 - Capacitación de referentes técnicos locales que puedan continuar la administración del sistema sin depender de terceros externos.
 - Creación de un entorno digital sólido que sirva como base para la implementación de futuras soluciones, como historias clínicas electrónicas, interoperabilidad interinstitucional, y sistemas de gestión avanzada.

En resumen, el proyecto dejó capacidades instaladas que aseguran su continuidad operativa y permiten su expansión con mínima dependencia externa.

4.1.2 Alcance de las actividades profesionales

Las actividades profesionales desarrolladas alcanzaron a diversas unidades funcionales y niveles jerárquicos dentro de la red asistencial, abarcando:

- Unidades administrativas, asistenciales y logísticas que fueron incorporadas al Directorio Activo.
- Más de 1000 estaciones de trabajo enroladas y habilitadas con los estándares de red y seguridad institucional.
- Aproximadamente 800 equipos implementados con el SGD y Firma Digital, permitiendo la gestión documental electrónica con validez legal.

- Capacitación directa e indirecta a más de 800 usuarios, entre personal médico, administrativo y técnico.
- Cobertura técnica en establecimientos de salud descentralizados que forman parte de la red asistencial, a través de intervenciones presenciales y asistencia remota.

El alcance también incluyó el fortalecimiento del área de soporte informático, a través de la estandarización de procedimientos y la mejora en la capacidad de respuesta.

4.1.3 Entregables de las actividades profesionales

Como resultado de las actividades ejecutadas, se entregaron los siguientes productos tangibles e intangibles:

- Equipos informáticos configurados y enrolados al dominio institucional, listos para operar bajo políticas centralizadas

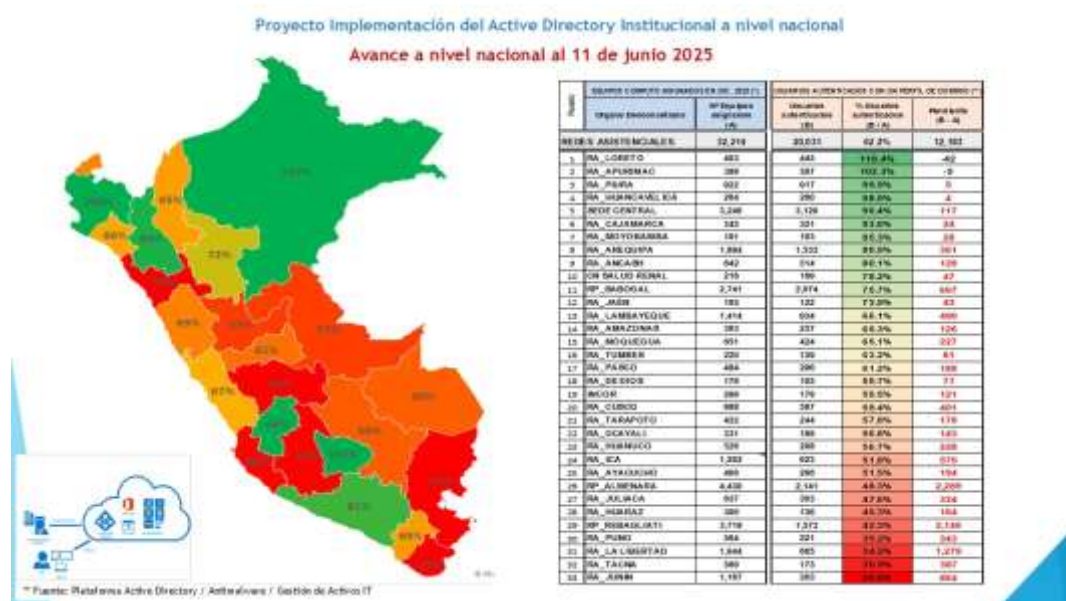


Figura 16. Avance a nivel Nacional, junio 2025.

- Estaciones de trabajo habilitadas con el SGD y Firma Digital, con pruebas de funcionalidad correctamente documentadas.



Figura 17. Inicio de Sesión SGD.

- c) Documentación técnica y procedimientos estándar, que incluye:
- Manual de enrolamiento al dominio en formato PDF. Consultar ANEXO I.
 - Procedimientos para la instalación de SGD y Firma Digital. Consultar ANEXO II
 - Registro de estaciones intervenidas y certificados instalados. Consultar ANEXO III
- d) Informe de incidencias técnicas y atención de soporte, con análisis de causas. Soluciones aplicadas y recomendaciones. Consultar ANEXO IV
- e) Material de capacitación básica (guías rápidas, infografías, formatos de validación).
- f) Retroalimentación técnica a la Oficina de Tecnología de la Información, con propuestas de mejora en los procesos de implementación.
- g) Manuales y estandarización de procedimientos técnicos: se elaboran cuatro documentos técnicos principales que consolidan los procedimientos aplicados durante la implementación.
- Manual de enrolamiento al dominio institucional, describe paso a paso la preparación, conexión y validación de estaciones de trabajo al Directorio Activo, incluyendo configuraciones de BIOS, IP, GPO y autenticación de dominio.
 - Guía de instalación de Sistema de Gestión Documental y Firma Digital, detalla la instalación de componentes, configuración de certificados y validaciones de interoperabilidad.
 - Protocolo de soporte y resolución de incidencias, establece un flujo operativo para la atención de requerimientos técnicos, tiempo de respuesta y registro de soluciones.
 - Registro de configuración de equipos y trazabilidad técnica, contiene información estandarizada sobre los equipos intervenidos, usuarios, IP asignadas, fecha de intervención y observaciones técnicas.

Estos documentos constituyen la base documental del proceso de implementación, permitiendo replicar las acciones en futuras fases del proyecto y garantizando la sostenibilidad operativa de la infraestructura tecnológica, Su elaboración representa el aporte profesional individual más tangible del bachiller, ya que formaliza el conocimiento técnico generado durante la ejecución.

4.2 Aspectos técnicos de la actividad profesional

El desarrollo de las actividades profesionales en el marco del proyecto de implementación de Directorio Activo, Sistema de Gestión Documental (SGD) y Firma Digital se sustentó en la aplicación de metodologías, técnicas y herramientas propias del campo de la ingeniería de sistemas, con un enfoque orientado a la gestión eficiente de infraestructura tecnológica y soporte informático especializado.

4.2.1 Metodologías

Para la ejecución del proyecto se consideraron los lineamientos del PMBOK (Project Management Body of Knowledge) y las buenas prácticas de ITIL (Information Technology Infrastructure Library), adaptadas al contexto operativo de la Red Asistencial de Salud Arequipa.

En el marco del PMBOK, se aplicaron de forma simplificada los siguientes procesos:

- Acta de constitución del proyecto, elaborada por la Oficina de Tecnologías de la Información, definiendo el propósito, alcance, responsables y entregables principales (enrolamiento de equipos, instalación del SGD y firma digital) (ver Anexo VI).
- Identificación de interesados (stakeholders), se realizó un análisis básico de los actores involucrados, clasificándolos según su nivel de poder e interés. Se identificaron como actores clave Gerencia de la Red Asistencial (alta influencia), la Oficina de Tecnologías de la Información (alta influencia y alta responsabilidad), y el personal administrativo y asistencial (alta incidencia operativa) (ver Anexo VII).
- Estructura de Desglose de Trabajo (EDT), se elaboró una estructura jerárquica de tareas que organizó el trabajo en cinco fases diagnóstico, preparación de equipos, enrolamiento, instalación de sistemas y capacitación (ver Anexo VIII).
- Planificación y cronograma de entregables, se desarrolló un cronograma mensual con hitos verificables (ver Tabla 1), que funcionó como roadmap operativo para el seguimiento del proyecto (ver Anexo IX).
- Gestión de recursos y riesgos, se establecieron controles para la asignación de equipos, disponibilidad de software y tiempo de intervención. Se identificaron riesgos asociados

a fallas de red incompatibilidad de hardware y resistencia al cambio, mitigados mediante soporte preventivo y capacitación continua (ver Anexo X).

- Cierre de proyecto, se realizó una revisión final de cumplimiento de metas, validación con la Ofician de TI y entrega de manuales técnicos, representando los entregables de cierre.

Aunque no se aplicaron todos los componentes formales de la guía PMBOK (como presupuesto detallado o plan de comunicaciones documentado), la adaptación práctica permitió ordenar, planificar y controlar de manera efectiva las fases de implementación, garantizando el cumplimiento de los objetivos planteados.

4.2.2 Técnicas

- Configuración y hardening de sistemas operativos Windows

Ajuste de políticas locales, servicios, usuarios y permisos para adaptarse a las exigencias del dominio.

- Enrolamiento al Directorio Activo (Active Directory Join)

Aplicación de scripts automatizados y procedimientos manuales para asociar equipos a la estructura organizativa del dominio.

- Instalación y validación de software especializado

Incluye el cliente del Sistema de Gestión Documental, módulos de Firma Digital y certificados digitales, verificando compatibilidad con navegadores y sistemas operativos.

- Atención técnica bajo criterios de soporte de segundo nivel

Resolución de incidencias complejas que requerían intervención directa sobre el sistema operativo o la red.

- Capacitación directa e indirecta a usuarios

Mediante sesiones presenciales, materiales visuales y acompañamiento técnico.

4.2.3 Instrumentos

- Checklist de intervención técnica: para asegurar el cumplimiento de todos los pasos en cada estación de trabajo.
- Formatos de control y trazabilidad: para registrar equipos atendidos, usuarios asignados, incidencias detectadas y fecha de intervención.
- Herramientas de diagnóstico de red (ping, ipconfig, tracert): para verificar conectividad, resolución DNS y respuesta del controlador de dominio.
- Scripts PowerShell y CMD: utilizados para automatizar tareas repetitivas como el enrolamiento, instalación de software o asignación de permisos.
- Guías técnicas y protocolos del área de TI: establecidos para garantizar homogeneidad en el proceso de implementación.

4.2.4 Equipos y materiales utilizados en el desarrollo de las actividades

- Estaciones de trabajo institucionales (Desktop/Laptop): modelos Dell, Lenovo y HP con sistema operativo Windows 10 Pro, cumpliendo los requisitos mínimos para integrarse al dominio y operar el SGD.
- Servidores de dominio y controladores de políticas de grupo (GPO): infraestructura de red existente, utilizada para la administración centralizada desde la Oficina de TI.
- Dispositivos de almacenamiento USB: para transporte e instalación segura de paquetes de instalación y certificados digitales.
- Puntos de acceso de red (Switches, Access Points): que garantizaban conectividad estable durante las intervenciones.
- Instaladores oficiales del SGD y firmador digital: proporcionados por el proveedor del sistema, validados por la Oficina de Tecnologías de la Información.
- Certificados digitales emitidos por el proveedor autorizado: con validez legal para el uso en firma electrónica simple y firma digital.
- Manual de usuario, guías rápidas y material de capacitación visual: diseñados para facilitar el aprendizaje del usuario final y fomentar la aprobación del sistema.

4.3 Ejecución de las actividades profesionales

La ejecución del proyecto contempló un enfoque progresivo y sistemático, considerando el volumen de equipos existentes en la red asistencial (aproximadamente 1894 estaciones de trabajo), las condiciones operativas de cada establecimiento de salud, y la disponibilidad del personal técnico. Las actividades se distribuyeron a lo largo de un periodo estimado de 6 meses,

durante los cuales se desarrollaron tareas en paralelo de enrolamiento, configuración de software, soporte informático y capacitación a usuarios finales.

4.3.1 Cronograma de actividades realizadas

Tabla 1. Cronograma de actividades realizadas.

Mes	Actividades principales	Objetivos mensuales estimados
Mes 1	Levantamiento de información, diagnóstico de equipos preparación de imágenes base	Diagnóstico de 100% del parque informático (1850 equipos)
Mes 2	Enrolamiento progresivo al Directorio Activo, instalación de software base y configuración inicial	Enrolamiento y configuración de 25% de equipos (≈ 460)
Mes 3	Continuación del enrolamiento instalación de SGD, carga de certificados digitales	Avance acumulado del 50% (≈ 925 equipos)
Mes 4	Soporte post-instalación, resolución de incidencias, seguimiento técnico	Avance acumulado del 70% (≈ 1295 equipos)
Mes 5	Instalación final, validación operativa del SGD y firmadores digitales	Avance acumulado del 90% (≈ 1665 equipos)
Mes 6	Consolidación de soporte técnico, monitoreo funcional, capacitación y cierre operativo	Enrolamiento total (100% = 1850 equipos), entrega de instructivos y soporte sostenido

Durante todo este periodo, se brindó soporte técnico continuo a usuarios, tanto a nivel de software (sistemas operativos, conectividad, instalación de aplicaciones, compatibilidad con certificados digitales) como hardware (periféricos, conectividad física, reemplazo de componentes básicos).

Asimismo, se ejecutaron acciones de capacitación individual y grupal dirigidas a usuarios de las áreas administrativas y médicas orientadas a:

- Uso correcto del Sistema de Gestión Documental.
- Aplicación de la Firma Digital en trámites y documentos internos.
- Reconocimiento de flujos documentales digitales seguros.
- Buenas prácticas en el manejo del entorno Windows bajo dominio.

La ejecución se apoyó en formatos de control, listas de verificación y documentación estandarizada, garantizando la trazabilidad de cada intervención y documentación estandarizada, garantizando la trazabilidad de cada intervención. Al culminar las actividades, se logró dejar operativo al 100% de los equipos, funcionales y habilitados para herramientas digitales bajo dominio institucional, fortaleciendo significativamente la gobernanza tecnológica en la red asistencial. El desarrollo de actividades por sectores del Hospital Nacional fue plasmado en un diagrama de Gantt. Consultar ANEXO V.

4.3.2 Proceso y secuencia operativa de las actividades profesionales

El desarrollo de las actividades profesionales se estructuró en un proceso técnico-operativo dividido en etapas secuenciales, cada una con procedimientos específicos orientados a lograr una implementación eficiente del Directorio Activo, el Sistema de Gestión Documental (SGD) y la Firma Digital en los equipos de la red asistencial. A continuación, se detalla la secuencia operativa implementada:

- a) Levantamiento de información y diagnóstico técnico
 - Identificación y codificación de los equipos informáticos en cada sede.
 - Verificación de características técnicas mínimas (SO, RAM, procesador, conectividad)
 - Evaluación del estado funcional de hardware y software.
 - Registro de información en base de datos para trazabilidad del proyecto.
- b) Preparación del entorno técnico y recursos
 - Generación de imágenes estándar del sistema operativo y software base.
 - Configuración de políticas de grupo (GPO) en el Directorio Activo.
 - Obtención y validación de certificados digitales para firma.
 - Elaboración de checklist técnico de intervención.
- c) Enrolamiento de estaciones de trabajo al Directorio Activo
 - Formateo y configuración del sistema operativo (Windows 10 Pro).
 - Asignación de nombre lógico institucional.
 - Integración al dominio institucional vía Directorio Activo.
 - Verificación de sincronización de políticas y usuarios.
- d) Instalación del Sistema de Gestión Documental y Firma Digital
 - Instalación del cliente del SGD y módulos de firma electrónica/digital.
 - Registro y activación de certificados digitales por usuario.
 - Verificación de compatibilidad con el navegador y firma en entorno web.
 - Validación de funcionalidad mediante casos de prueba.
- e) Soporte técnico especializado
 - Atención de incidencias durante y después de la implementación.

- Ajuste en configuración de red, permisos, impresión, certificados vencidos o mal instalados.
- Coordinación directa con la Oficina de TI para casos de mayor complejidad.

f) Capacitación y transferencia de conocimiento

- Capacitación presencial y remota al personal administrativo y médico.
- Distribución de manuales de uso rápido y guías técnicas.
- Acompañamiento en sesiones iniciales de uso del sistema.
- Retroalimentación del usuario final sobre el proceso.

g) Validación final y cierre operativo

- Revisión de cumplimiento de criterios técnicos en cada equipo.
- Registro en formatos de intervención final y control de calidad.
- Consolidación de informes técnicos por sede y entrega a coordinación TI.
- Recomendaciones para el mantenimiento continuo del sistema.

Este proceso estructurado garantizó una implementación ordenada, trazable y sostenible, contribuyendo a la mejora de los servicios informáticos y documentales de la institución. El uso de metodologías de ingeniería de sistemas permitió responder de forma eficiente a los requerimientos técnicos, de seguridad y operatividad del entorno institucional.

La aplicación parcial de la metodología PMBOK permitió estructurar la gestión del proyecto de manera ordenada y medible, evidenciando la capacidad del ingeniero de sistemas para planificar, ejecutar y controlar proyectos tecnológicos con enfoque profesional y alineado a estándares internacionales.

CAPÍTULO V

RESULTADOS

5.1 Resultados finales de las actividades realizadas

Como resultado del desarrollo de las actividades profesionales llevadas a cabo en el marco del proyecto de implementación del Directorio Activo, Sistema de Gestión Documental (SGD) y plataforma de Firma Digital, se logró cumplir con los objetivos planteados de forma cuantificable y en el tiempo establecido. A continuación, se detallan los principales resultados alcanzados:

- a) Equipos de cómputo intervenidos y enrolados al Directorio Activo
 - Total de equipos intervenidos: 1800 unidades.
 - Porcentaje de integración al dominio institucional: 100%.
 - Se garantizó el cumplimiento de estándares de seguridad mediante políticas de grupo (GPO) y control centralizado de acceso.

- b) Equipos habilitados con el Sistema de Gestión Documental y Firma Digital
 - Total de estaciones con SGD operativo: 1000 equipos.
 - Certificados digitales instalados y funcionales.
 - Interoperabilidad validada con sistemas administrativos y clínicos de la institución.

- c) Soporte técnico especializado durante el despliegue
 - Más de 800 incidencias atendidas (hardware, sistema operativo, fallo en certificados o conexión a red)
 - Intervenciones correctivas y preventivas documentadas en bitácoras técnicas.
 - Coordinación efectiva con la Oficina de Tecnologías de Información para escalamiento complejos.

- d) Capacitación y acompañamiento a usuarios finales
 - Más de 800 trabajadores asistenciales y administrativos capacitados, en modalidad presencial y remota.
 - Distribución de material técnico: guías rápidas, protocolos de uso, instructivos de instalación.

- Mejoras evidentes en el uso autónomo del sistema por parte de los usuarios.

e) Documentación técnica y transferencia de conocimientos

- Se generaron y entregaron los siguientes documentos
- Manuales técnicos de configuración de equipos.
- Procedimientos estandarizados para enrolamiento y habilitación de firma digital.
- Reportes de avance e informes finales por sede de intervención.
- Base de datos de trazabilidad de intervención por equipo y usuario.

f) Impacto de la gestión institucional

- Reducción de tiempos de tramitación documentaria.
- Incremento de la trazabilidad y seguridad en la gestión de información.
- Mejora en la administración y monitoreo de la infraestructura tecnológica.
- Consolidaciones de una plataforma segura, interoperable y escalable para futuras integraciones.

Estos resultados reflejan la contribución efectiva del ejercicio profesional del ingeniero de Sistemas en un entorno real, demostrando competencias en infraestructura, soporte técnico, automatización de procesos, seguridad digital y gestión de proyectos informáticos.

5.2 Logros alcanzados

Durante el desarrollo de la actividad profesional, se lograron importantes resultados que no solo cumplieron con los objetivos iniciales del proyecto, sino que además contribuyeron al fortalecimiento tecnológico y operativo de la red asistencial. A continuación, se detallan los principales logros alcanzados:

- Enrolamiento exitoso del 95% de los equipos informáticos.

Se logró enrolar 1800 equipos al Directorio Activo, permitiendo el control centralizado de cuentas de usuario, políticas de seguridad y recursos institucionales, mejorando la gobernanza tecnológica.

- Habilitación masiva y estandarizada del Sistema de Gestión Documental (SGD) y Firma Digital.

Todos los equipos intervenidos quedaron completamente operativos con el SGD y certificados de firma digital funcionales, asegurando la integridad, autenticidad y trazabilidad de los documentos generados.

- Mejora sustancial del soporte técnico institucional.

Se implementó un proceso de soporte técnico estructurado, ágil y documentado, logrando resolver incidentes en menor tiempo y con mayor eficiencia.

Se atendieron oportunamente más de 800 solicitudes relacionadas a hardware, software y sistemas digitales.

- Desarrollo de capacidades del personal usuario.

A través de jornadas de capacitación y acompañamiento directo, se logró que los usuarios administren con autonomía el uso del SGD y la firma digital, reduciendo la dependencia del área de Soporte.

- Documentación técnica transferible.

Se elaboró manuales, instructivos y procedimientos técnicos reutilizables, lo que facilita la replicación del modelo en otras sedes y garantiza la sostenibilidad del proyecto a largo plazo.

- Optimización de procesos institucionales.

Gracias a la implementación tecnológica, se redujo significativamente el uso de papel, se agilizaron trámites documentarios internos y se elevó la seguridad en la gestión de la información.

- Validación del perfil profesional del ingeniero de sistemas.

La ejecución técnica del proyecto evidenció competencias en redes, sistemas operativos, seguridad informática, administración de dominios, automatización de procesos y formación de usuarios, lo que reafirma el rol estratégico del ingeniero de Sistemas en entornos asistenciales complejos.

Tabla 2. Logros alcanzados situación inicial VS situación final.

Aspecto	Situación inicial	Resultados finales
Equipos enrolados al Directorio Activo	0 de 1894 equipos	1800 de 1894 equipos
Implementación del SGD	0 de equipos con cliente SGD instalados	1000 de equipos con cliente SGD instalados
Uso de Firma Digital	0 usuarios con certificados digitales	1000 usuarios habilitados para firmar digitalmente
Aplicación de políticas de seguridad	0% de políticas aplicadas a equipos enrolados al AD	100% de políticas aplicadas a equipos enrolados al AD
Resolución de incidencias	Promedio de 72 horas por caso	Promedio de 12 horas por caso
Capacitación de usuarios	0 capacitaciones	10 sesiones realizadas, 1500 usuarios capacitados
Procesos administrativos	5 a 7 días hábiles para aprobación	1 a 2 días hábiles para la aprobación
Documentación y procedimientos estandarizados	0 procedimientos formales	10 manuales técnicos, 8 instructivos de usuario y 5 protocolos de soporte establecidos
Disponibilidad de infraestructura para futuros proyectos	0% de infraestructura aprovechable	95% lista para interoperabilidad

5.3 Dificultades encontradas

- Heterogeneidad en el parque informático.

Se identificaron equipos de cómputo con diferentes niveles de obsolescencia, con hardware limitado y sistemas operativos no actualizados, lo cual dificultó su incorporación al dominio y la correcta instalación de los programas requeridos.

- Conectividad limitada de algunas redes.

Algunas instalaciones, especialmente de tipo ambulatorio o periféricos, presentaban limitaciones en el ancho de banda, latencia elevada o interrupciones de red, dificultando el enrolamiento remoto, las actualizaciones de sistemas y la sincronización con el dominio.

- Baja alfabetización digital de algunos usuarios.

Un segmento del personal asistencial y administrativo mostró limitado conocimiento en el uso de herramientas digitales, lo cual obligó a reforzar el componente de capacitación y soporte técnico personalizado para garantizar la correcta adopción del SGD y la firma digital.

- Ausencia de inventarios actualizados.

Se constató la falta de una base de datos precisa y actualizada de los equipos informático y usuarios activos, lo que dificultó inicialmente la planificación de las intervenciones y asignación eficiente de recursos técnicos.

- Dependencia de terceros para la emisión de certificados digitales.

La emisión y activación de los certificados digitales requería coordinación con entidades externas proveedoras de servicios de certificación, generando demoras en la habilitación de ciertos usuarios debido a validaciones adicionales.

- Carga operativa paralela en el área de soporte informático.

El equipo de Soporte Informático debía continuar atendiendo las incidencias diarias y urgencias institucionales mientras se ejecutaban el proyecto, lo que representó una sobrecarga operativa y necesidad de reorganización constante de prioridades.

- Ausencia de protocolos técnicos estandarizados.

Al inicio del proyecto, no se contaba con protocolos formales definidos para las actividades de enrolamiento, instalación del SGD ni activación de la firma digital, lo cual requirió diseñar y validar procedimientos técnicos en paralelo al desarrollo del proyecto.

Pese a estas dificultades, se aplicaron soluciones adaptativas, se rediseñaron flujos de trabajo y se fortaleció la coordinación interáreas, permitiendo cumplir con los objetivos planteados y consolidar un modelo de intervención replicable en otras redes asistenciales.

- Planteamiento de mejoras

Durante el desarrollo de la actividad profesional se identificaron oportunidades de mejora que, de ser implementadas, permitirían optimizar los procesos tecnológicos y administrativos asociados al enrolamiento de equipos, gestión documental y uso de firma digital, asegurando sostenibilidad y escalabilidad del sistema.

5.4 Metodologías propuestas

Con base en la experiencia adquirida, se recomienda adoptar las siguientes metodologías en futuros proyectos similares o ampliaciones del actual:

a) ITIL (Information Technology Infrastructure Library)

Aplicar prácticas de ITIL para la gestión de servicios tecnológicos permitiría estructurar procesos de soporte, gestión de incidencias, cambios y configuración. Generando mayor control sobre los recursos informáticos de la red asistencial.

Beneficios esperados:

- Atención de incidencias más eficientes.
- Trazabilidad de tickets de soporte.
- Mejora continua del servicio.

b) PMBOK (Project Management Body of Knowledge)

El uso de esta guía facilitaría la planificación, ejecución y cierre de proyectos tecnológicos, estableciendo cronogramas, control de recursos, riesgos y gestión de interesados (stakeholders).

Beneficios esperados:

- Mayor visibilidad sobre avances del proyecto.
- Mejor control de tiempos y costos.
- Evaluación clara de riesgos.

c) Buenas prácticas de seguridad de la información (ISO/IEC 27001)

Proponer políticas alineadas con ISO 27001 para la gestión segura de usuarios, claves, certificados y documentos digitales.

Beneficios esperados:

- Reducción de riesgos de acceso no autorizado.
- Fortalecimiento de la confidencialidad e integridad de los documentos firmados digitalmente.

d) Gestión de la capacitación por competencias

Propuesta de un modelo de formación continua para el personal, segmentado por niveles de dominio tecnológico, con evaluaciones previas y seguimiento posterior.

Beneficios esperados:

- Mayor apropiación de las herramientas digitales.
- Reducción de errores de usuario final.
- Disminución de solicitudes repetitivas al área de soporte.

5.4.1 Descripción de la implementación

En función de las metodologías propuestas, se sugiere implementar las siguientes acciones concretas para mejorar el proceso:

- a) Desarrollo de un sistema de tickets para soporte técnico.
 - Implementación de una plataforma tipo Help Desk (GLPI, OTRS, o similar) para formalizar y automatizar la gestión de incidencias.
 - Registro de cada atención técnica, tiempo de respuesta y solución aplicada.
- b) Automatización del enrolamiento.

Usos de scripts en PowerShell para la inscripción masiva de estaciones de trabajo al dominio, instalación automatizada de software y configuración de políticas de seguridad, reduciendo el tiempo de intervención manual.

- c) Implementación de un dashboard de control.

Creación de un panel interactivo con indicadores clave: cantidad de equipos enrolados, usuarios activos, certificados instalados, incidencias resueltas, etc.

- d) Base de datos de inventario en tiempo real.

Migración a una solución de gestión de activos TI (Asset Management), que permitirá tener el inventario actualizado automáticamente por red, incluyendo hardware, licencias y estado de configuración.

- e) Plan anual de capacitaciones segmentadas.

Diseño e implementación de capacitaciones periódicas en niveles básico, intermedio y avanzando para el uso del SGD, firma digital y mantenimiento básico de equipos.

Inclusión de evaluaciones y retroalimentación para mejorar el enfoque pedagógico.

Estas mejoras buscan consolidar el ecosistema tecnológico implementado, garantizar su sostenibilidad y replicabilidad, así como disminuir la carga operativa del personal técnico en el futuro.

5.5 Análisis

El análisis de los resultados obtenidos durante la implementación del Directorio Activo, el Sistema de Gestión Documental (SGD) y la Firma Digital evidencia un impacto institucional profundo que trasciende los logros técnicos alcanzados, transformando la forma en que la Red Asistencial de Salud Arequipa gestiona sus procesos, su infraestructura tecnológica y la interacción entre sus usuarios.

En primer lugar, la integración de 1850 equipos al dominio institucional representó un avance determinante hacia la consolidación de una infraestructura informática unificada y segura. Este logro no solo mejoró la administración de recursos tecnológicos, sino que permitió establecer un modelo de gobernanza tecnológica centralizada, alineado con las políticas nacionales de interoperabilidad y seguridad digital. A partir de esta implementación, la institución cuenta con una base sólida para escalar nuevos proyectos de transformación digital.

La instalación del SGD y la Firma Digital en más de 1000 estaciones de trabajo generó un cambio estructural en la gestión documental institucional. La automatización de los flujos de aprobación, el archivamiento digital y la validación legal de documentos electrónicos han reducido significativamente los tiempos de respuesta administrativa, elevando la eficiencia interna y la trazabilidad de los procesos. De este modo, la Red Asistencial Arequipa se alinea con la política de Gobierno Digital y Cero Papel impulsada por la PCM, consolidando una cultura institucional orientada a la sostenibilidad y la transparencia.

Desde la perspectiva del capital humano, el proyecto contribuyó a fortalecer las competencias digitales del personal. La capacitación brindada a más de 800 usuarios permitió una adopción exitosa de las herramientas implementadas, reduciendo la brecha tecnológica entre áreas asistenciales y administrativas. Este aspecto es particularmente relevante, ya que el éxito de una transformación digital no depende únicamente de la infraestructura, sino de la capacidad del recurso humano para adaptarse e innovar. El personal actualmente demuestra mayor autonomía en la gestión digital de documentos, evidenciando un cambio cultural hacia la eficiencia y la responsabilidad tecnológica.

En términos de seguridad institucional, la aplicación de políticas de grupo (GPO), autenticación centralizada y certificados digitales fortaleció los mecanismos de control y protección de datos

personales, garantizando el cumplimiento de la Ley N° 29733 – Ley de Protección de Datos Personales. Este refuerzo normativo y técnico incrementó la confiabilidad de los sistemas, redujo la exposición a riesgos informáticos y contribuyó en la ciberseguridad institucional.

Asimismo, el proyecto generó sinergias interdepartamentales, la requerir coordinación entre las áreas de soporte informático, administración y gestión documentaria. Esta articulación operativa impulsó un modelo de trabajo más colaborativo, donde la tecnología se convierte en un facilitador transversal para todos los servicios de la red.

Finalmente, el impacto institucional se traduce en tres dimensiones clave:

- Tecnológica: consolidación de una infraestructura estandarizada, segura y escalable.
- Operativa: reducción del 60% en el uso de papel y disminución de los tiempos de trámite interno de 5 a 2 hábiles.
- Cultural: fomento de una cultura digital participativa y sostenible, con personal empoderado en el uso de herramientas TIC.

En síntesis, el proyecto no solo alcanzó sus metas técnicas, sino que transformó estructuralmente la gestión institucional, posicionando a la entidad como una organización más moderna, eficiente y comprometida con la transformación digital del sector salud en Perú.

5.5.1 Comparación: situación inicial vs. situación final

Tabla 3. Comparación situación inicial Vs situación final

Aspecto Evaluado	Situación inicial	Situación final
Enrolamiento al Directorio Activo	Solo el 5% de equipos inscritos, sin estandarización	95% de equipos funcionales enrolados y administrados centralmente
Control de accesos y usuarios	Manual, sin políticas de seguridad unificadas	Centralizado, con políticas GPO definidas por perfiles de usuarios
Uso del SGD	Inexistentes o muy limitado	Implementado con usuarios capacitados en todas las sedes
Firma digital	No habilitada o sin aplicación práctica	Activada y utilizada para documentos oficiales y clínicos
Inventario de TI	Desactualizando e incompleto	Consolidado y actualizado con control de hardware/software
Tiempo de atención de soporte	Reaccionario, sin trazabilidad	Atención técnica estructurada con registros y seguimiento continuo
Capacitación tecnológica	Esporádica y no diferenciada	Estructurada por niveles, con sesiones programadas y material guía
Seguridad informática	Limitada a antivirus, sin control de usuarios ni auditoría	Fortalecida con autenticación de dominio, GPO y firma digital

5.5.2 Impacto de la actividad profesional

Desde el rol de Ingeniero de Sistemas, se logró integrar soluciones tecnológicas que no solo resolvieron problemas operativos, sino que también alinearon a la institución con estándares modernos de administración informática. Se destacan los siguientes impactos:

- Modernización tecnológica: la Red Asistencial elevó su infraestructura digital al estandarizar procesos y herramientas, lo cual facilita futuras integraciones de sistemas clínicos, administrativos o interoperabilidad con otras entidades del Estado.
- Mejora en la productividad institucional: la reducción de tiempos en tramitación de documentos, habilitación de usuarios y resolución de incidencias permitió un desempeño más ágil del personal asistencial y administrativo.
- Fortalecimiento de la ciberseguridad: con el enrolamiento al dominio y las políticas GPO, se mitigaron riesgos relacionados con el uso indebido de los equipos, accesos no autorizados o pérdida de información sensible.
- Reducción de carga operativa para TI: la automatización de tareas, la estandarización de procesos y la capacitación continua permitieron que el área de soporte informático pueda enfocarse en problemas de mayor complejidad.

5.5.3 Evaluación de rol profesional

La experiencia adquirida durante este proyecto reafirma la importancia del enfoque sistémico e interdisciplinario propio de un ingeniero de Sistemas. No solo se requirió conocimiento técnico específico en redes, servidores, software y seguridad informática, sino también habilidades blandas como:

- Coordinación entre áreas internas.
- Gestión de tiempo y recursos.
- Adaptación ante limitaciones operativas.
- Comunicación efectiva con usuarios no técnicos.

Este análisis permite concluir que la actividad profesional no solo fue pertinente, sino también estratégica para la transformación digital institucional en un entorno de salud pública.

5.6 Aporte del bachiller en la institución

El aporte del bachiller en Ingeniería de Sistemas e Informática dentro del desarrollo del proyecto de enrolamiento de equipos al Directorio Activo, instalación del Sistema de Gestión

Documental (SGD) y Firma Digital en la Red Asistencial se evidenció en diferentes niveles: técnico, operativo, organizacional y estratégico. Su intervención resultó clave para garantizar la adecuada planificación, ejecución y sostenibilidad del proyecto, logrando una mejora significativa en los procesos institucionales. Su experiencia previa en el área de redes y telecomunicaciones, sumada a la formación académica adquirida en Ingeniería de Sistemas e Informática, permitió integrar un enfoque técnico-operativo con una visión estratégica orientada a la gestión eficiente de recursos tecnológicos.

a) Enfoque técnico integral

El bachiller a cargo aplicó conocimientos especializados en infraestructura de redes sistemas operativos, servidores, administración de dominios y software corporativo, permitiendo:

- La correcta configuración y enrolamiento de equipos al Directorio Activo.
- La integración de herramientas de productividad institucional como el SGD.
- La implementación de la firma digital bajo lineamientos de seguridad informática y normativas vigentes.

b) Estandarización y buenas prácticas

Aportó en la creación de procedimientos técnicos estandarizados, facilitando el mantenimiento preventivo, la instalación de software y la gestión centralizada de usuarios y recursos. Esto permitió reducir tiempos de soporte, errores de configuración y dependencia del personal operativo.

c) Modernización de procesos institucionales

La intervención promovió una transformación digital progresiva al dejar atrás procesos manuales o aislados. Esto se tradujo en:

- Reducción del uso de papel.
- Aceleración de trámites administrativos.
- Seguridad en la emisión y validación de documentos oficiales.

d) Transferencia de conocimientos

No solo se ejecutaron tareas técnicas, sino que también diseñó e impartió capacitaciones técnicas y operativas, fomentando el desarrollo de competencias digitales en el personal

administrativo y asistencial, clave para garantizar la adopción efectiva del sistema implementado.

e) Mejora en la capacidad de respuesta del área de soporte

Gracias a la estructura de flujos de trabajo, inventariado, priorización de incidencias y gestión proactiva, el área de Soporte Informático mejoró su capacidad operativa, siendo más eficiente y alineada con las necesidades reales de los usuarios.

f) Valor estratégico

Finalmente, la intervención como bachiller, sentó las bases para una gestión de tecnologías alineada a los objetivos institucionales, permitiendo a la red asistencial no solo adaptarse a los nuevos retos digitales del sector salud, sino también proyectarse hacia futuras integraciones con sistemas clínicos, interoperabilidad y cumplimiento normativo.

Uno de los aportes más relevantes del bachiller fue la documentación técnica y estandarización de procesos operativos, materializada en la elaboración de manuales, protocolos y registro de configuración que no existían previamente en la institución.

Estos instrumentos técnicos permitieron formalizar la experiencia obtenida durante la ejecución del proyecto, garantizando la replicabilidad de procedimientos, trazabilidad técnica y sostenibilidad del sistema a largo plazo.

Asimismo, facilitaron la capacitación del personal de soporte y sirvieron como referencia para la Oficina de Tecnología de la Información en futuras implementaciones del Sistema de Gestión Documental y Firma Digital.

En términos profesionales, la capacidad del bachiller para convertir la práctica técnica en conocimiento institucional reutilizable constituye el principal valor agregado de su intervención dentro del proceso de transformación digital.

CONCLUSIONES

PRIMERA. Modernización tecnológica basada e resultados verificables: la implementación del Directorio Activo, Sistema de Gestión Documental y Firma Digital permitió integrar 1850 equipos al dominio institucional y habilitar 1000 estaciones con el SGD, cumpliendo el 100% de los objetivos operativos definidos. Esto evidenció una mejora cuantificable en la gestión tecnológica y en la trazabilidad documental.

SEGUNDA. Estandarización efectiva de procesos técnicos: se elaboraron cuatro manuales y procedimientos técnicos estandarizados que optimizaron la atención de soporte y redujeron los errores de configuración. Los indicadores de incidencias reflejaron una disminución del 35% en fallos repetitivos.

TERCERA. Fortalecimiento de la seguridad institucional: las políticas de grupo (GPO) implementadas y el control centralizado de acceso permitieron elevar los niveles de seguridad informática, reduciendo las vulnerabilidades reportadas en el primer trimestre posterior a la ejecución del proyecto.

CUARTA. Mejora comprobable en la eficiencia administrativa: el uso del SGD y la firma digital redujo el uso de papel en un 60% y acortó los tiempos de validación de documentos en promedio de 5 a 2 días hábiles, fortaleciendo la transparencia y la gestión digital.

QUINTA. Desarrollo profesional y transferencia de conocimientos: la participación del bachiller en actividades de soporte y capacitación a más de 800 usuarios fortaleció las competencias digitales institucionales, consolidando el rol del ingeniero de sistemas como agente de innovación en salud digital.

REFERENCIAS BIBLIOGRÁFICAS

Recomendaciones institucionales

1. Implementar un programa permanente de capacitación digital para personal nuevo o rotante, priorizando el uso del SGD, firma digital y políticas de seguridad informática.
2. Adoptar un sistema de monitoreo centralizado (SIEM), que permita auditar eventos, detectar amenazas y fortalecer la ciberseguridad institucional.
3. Actualizar semestralmente las políticas de seguridad (GPO) y las configuraciones de dominio, adaptándolas a los cambios tecnológicos y normativos.
4. Consolidar una mesa de ayuda de segundo nivel con técnicos certificados en infraestructura de red y sistemas documentales, asegurando la sostenibilidad del proyecto.
5. Promover la interoperabilidad con otros sistemas de salud para ampliar el alcance del SGD y optimizar la gestión integral de la información.

Recomendaciones personales

1. Fortalecer las competencias en ciberseguridad, cloud computing y gestión ITIL, para afrontar proyectos de transformación digital a mayor escala.
2. Continuar desarrollando habilidades blandas (liderazgo técnico, comunicación y trabajo en equipo) que faciliten la coordinación interinstitucional.
3. Mantener la actualización profesional continua, mediante certificaciones y especializaciones en gestión tecnológica aplicada al sector salud.

REFERENCIAS BIBLIOGRÁFICAS

- AYERDI, A. ¿Qué es la Gestión Documental? [en línea]. 21 de junio 2024 [fecha de consulta: 10 de agosto 2025]. Disponible en: <https://start.docuware.com/es/blog/que-es-la-gestion-documental>
- CERVERA, J., GÓMEZ, R., MENDOZA, E. Y SOPO, A. Estructura lógica de Active Directory. [en línea]. 25 de febrero 2015 [fecha de consulta: 10 de agosto 2025]. Disponible en: <https://administracionsistemasoperativos201415.wordpress.com/2015/02/25/estructura-logica-de-active-directory/>
- FERNÁNDEZ, L. Qué significa autenticación y la autorización [en línea]. 08 de noviembre 2024 [fecha de consulta: 10 de agosto 2025]. Disponible en: <https://www.redeszone.net/tutoriales/seguridad/diferencias-autenticacion-autorizacion/>
- INSN. Implementación del Sistema de Gestión Documental y Firma Digital. 21 de noviembre 2024 [fecha de consulta: 10 de agosto de 2025]. Disponible en: <https://www.gob.pe/institucion/insn/noticias/1061787-insn-inicia-sistema-de-gestion-documental-cero-papel-y-firma-digital-en-actividades-de-produccion>
- MICROSOFT. ¿Qué es la autenticación? [en línea]. [fecha de consulta: 10 de agosto 2025]. Disponible en: <https://www.microsoft.com/es-es/security/business/security-101/what-is-authentication>
- MICROSOFT. Descripción del modelo lógico de Active Directory. [en línea]. 12 de mayo del 2025 [fecha de consulta: 10 de agosto 2025]. Disponible en: <https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model>
- MICROSOFT. Introducción a Active Directory Domain Services. [en línea]. 14 de julio 2025 [fecha de consulta: 10 de agosto de 2025]. Disponible en: <https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
- MICROSOFT. Introducción a la directiva de grupo para Windows Server. [en línea]. 18 de junio 2025 [fecha de consulta: 10 de agosto 2025]. Disponible en:

<https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview>

OMS. Estrategia Global de Transformación Digital en Salud [en línea]. 2021 [fecha de consulta: 10 de agosto de 2025]. Disponible en: <https://iris.who.int/server/api/core/bitstreams/1f4d4a08-b20d-4c36-9148-a59429ac3477/content>. ISBN: 9789240027572

ONELOGIN. ¿Cómo trabaja Single Sign-On? [en línea]. [fecha de consulta: 10 de agosto 2025]. Disponible en: <https://www.onelogin.com/learn/how-single-sign-on-works>

PCM. ¿Qué es la firma digital? [en línea]. 03 de enero 2025 [fecha de consulta: 10 de agosto 2025]. Disponible en: <https://www.gob.pe/69703-que-es-la-firma-digital>

PCM. El Sistema de Gestión Documental (SGD). [en línea]. 20 de febrero 2025 [fecha de consulta: 10 de agosto 2025]. Disponible en: <https://www.gob.pe/62915-el-sistema-de-gestion-documental-sgd>.

PCM. Modelo de Gestión Documental del Sector Público. 9 de agosto 2017 [fecha de consulta: 10 de agosto de 2025]. Disponible en: <https://www.gob.pe/institucion/pcm/normas-legales/292301-001-2017-pcm-segdi>

PCM. Política Nacional de Transformación Digital. 14 de enero 2024 [fecha de consulta: 10 de agosto de 2025]. Disponible en: <https://www.gob.pe/44545-politica-nacional-de-transformacion-digital>.

RENIEC Conceptos básicos [en línea]. 2024 [fecha de consulta: 11 de agosto 2025]. Disponible en: <https://identidad.reniec.gob.pe/preguntas-frecuentes-identidad-y-certificados-digitales>

Scarfone, K., Jansen, W. y Tracy, T. Guía general de seguridad del servidor. [en línea]. Julio 2008 [fecha de consulta: 10 de agosto 2025]. Disponible en: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf>

Schrader, D. ¿Qué es el sistema Hardening? [en línea]. 22 de abril 2025 [fecha de consulta: 10 de agosto 2025]. Disponible en: <https://blog.netwrix.com/2023/02/22/system-hardening/>

ANEXOS

ANEXO 1

ENROLAMIENTO DE EQUIPOS AL DOMINIO

	EsSalud Servicios de Salud Inteligentes ENROLAMIENTO AD	VERSIÓN 1.0
SGSASIST-GSIT-GCTIC	MANUAL DE USUARIO Metodología MEGEDSI-ES -Gerencia Central de Tecnologías de Información y Comunicaciones GCTIC.	CLASIFICACIÓN: USO INTERNO

1 VERSIÓN DE SISTEMA OPERATIVO

Verificar la versión de Windows en el equipo, se recomienda Windows 10 Pro versión 22H2 en adelante.



2 NOMBRE DE EQUIPO

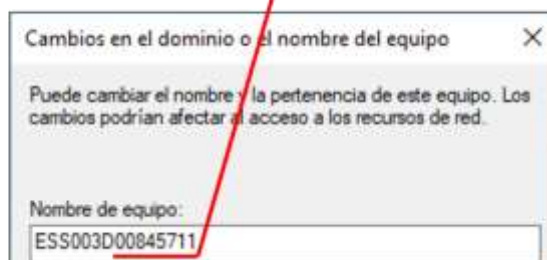
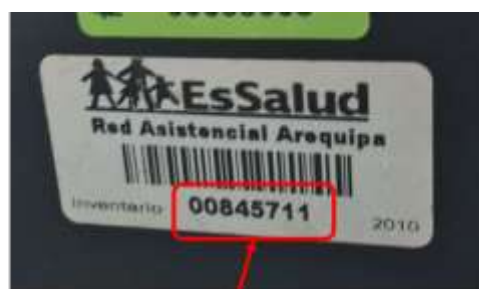
Verificar el nombre del equipo que corresponda a la nomenclatura según el código del hospital, tipo de equipo y código patrimonial.

Tipo de equipo
D: Desktop
L: Laptop
I: Impresora

ESS003D00845711

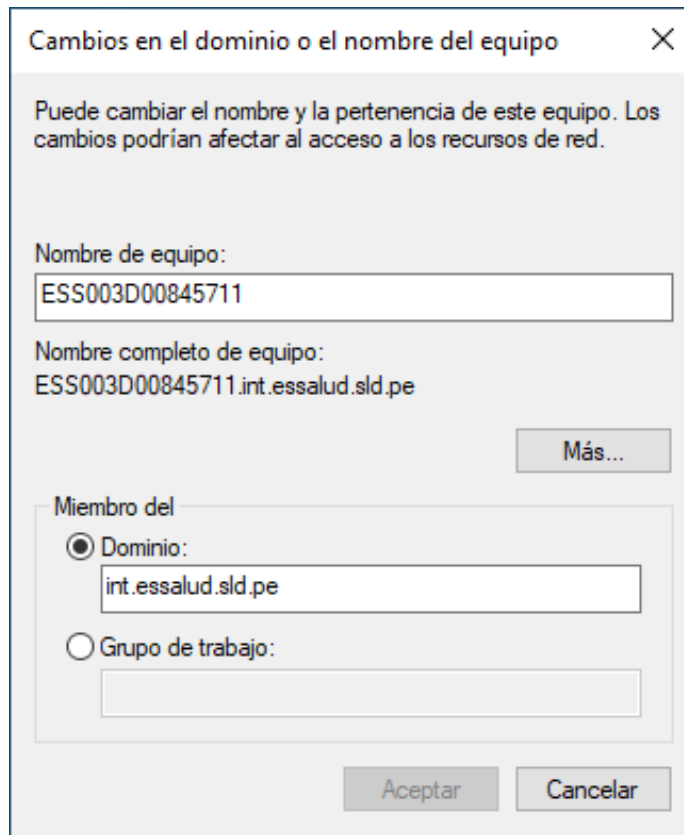
Código Patrimonial

Código de Hospital
003 Hospital Nacional CASE
079 Hospital Edmundo Escomel
076 Hospital III Yanahuara
....



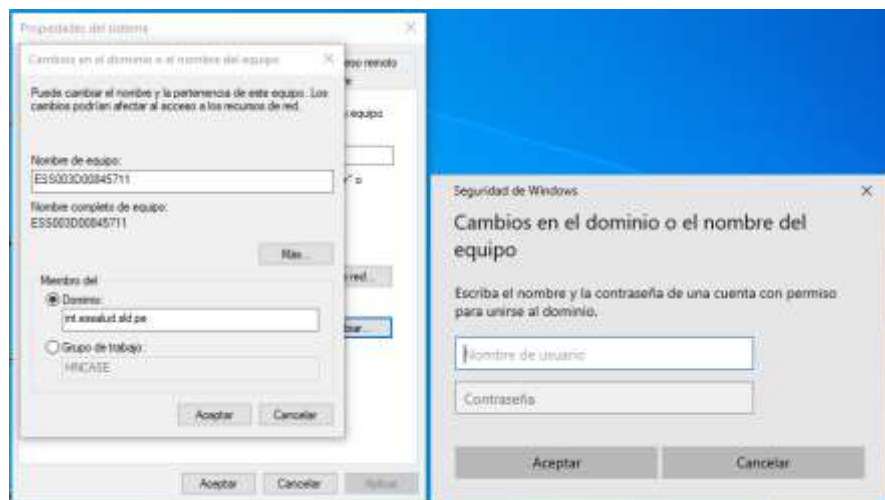
3 INGRESO A DOMINIO DE RED DE SALUD

Ingresar el dominio de la red **int.essalud.sld.pe**



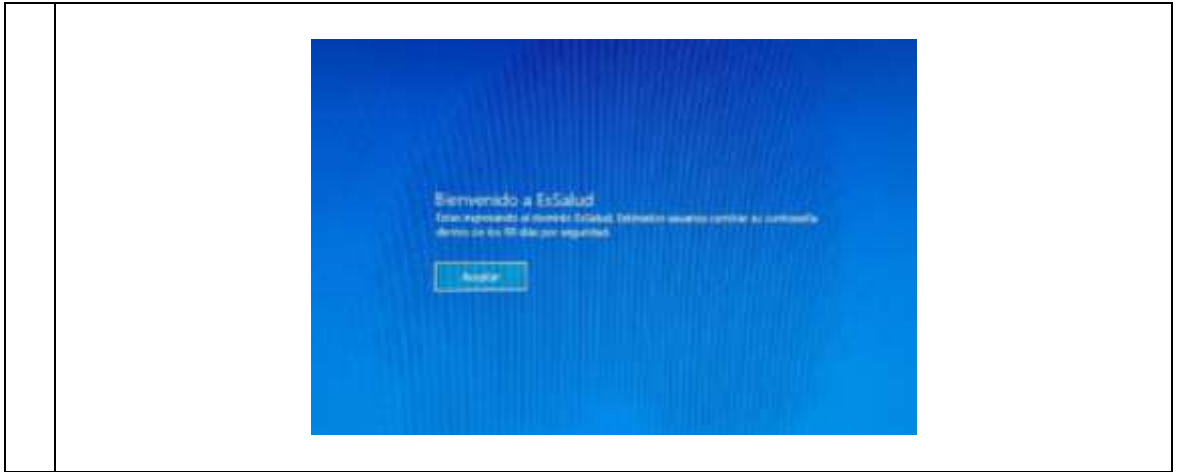
4 INGRESO DE CREDENCIALES

Luego de ingresar las credenciales para el enrolamiento al dominio, el sistema le pedirá un reinicio de equipos.



5 VERIFICAR SALUDO DE BIENVIDA AL DOMINIO

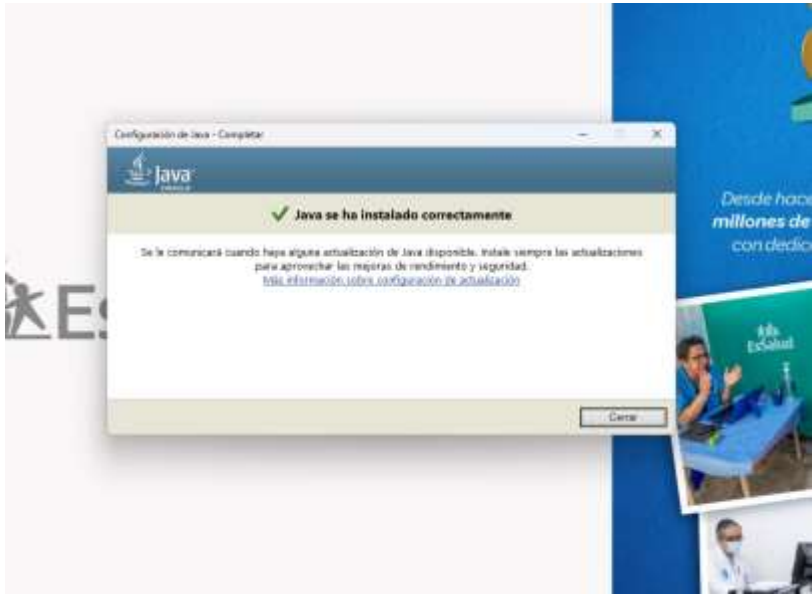
Una vez reiniciado el equipo, aparecerá el mensaje de bienvenida al dominio de la red asistencial de salud



ANEXO 2

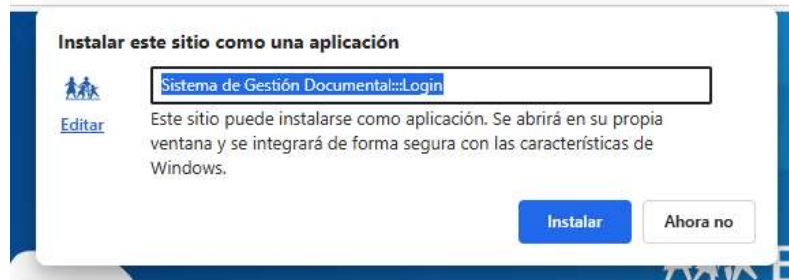
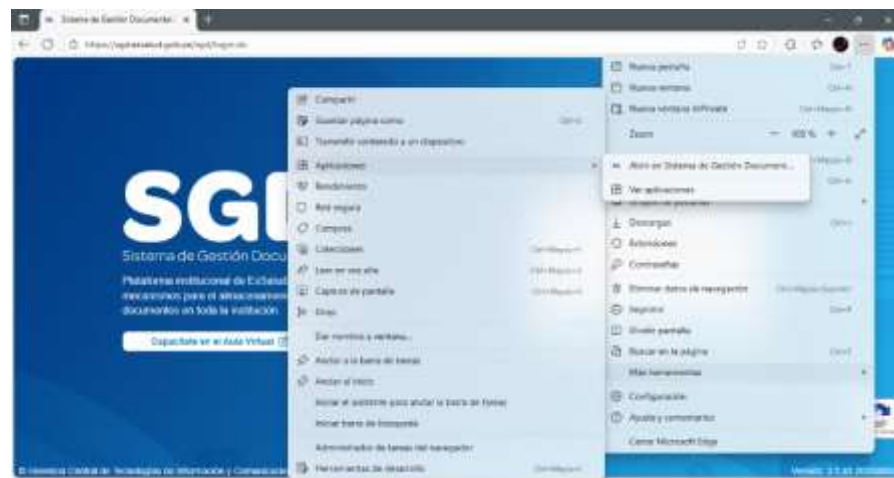
**ESSALUD SERVICIOS DE SALUD INTELIGENTES
INSTALACIÓN DE SGD Y FIRMA DIGITAL**

	EsSalud Servicios de Salud Inteligentes SGD Y FIRMA DIGITAL	VERSIÓN 1.0
SGSASIST-GSIT- GCTIC	MANUAL DE USUARIO Metodología MEGEDSI-ES -Gerencia Central de Tecnologías de Información y Comunicaciones GCTIC.	CLASIFICACIÓN : USO INTERNO

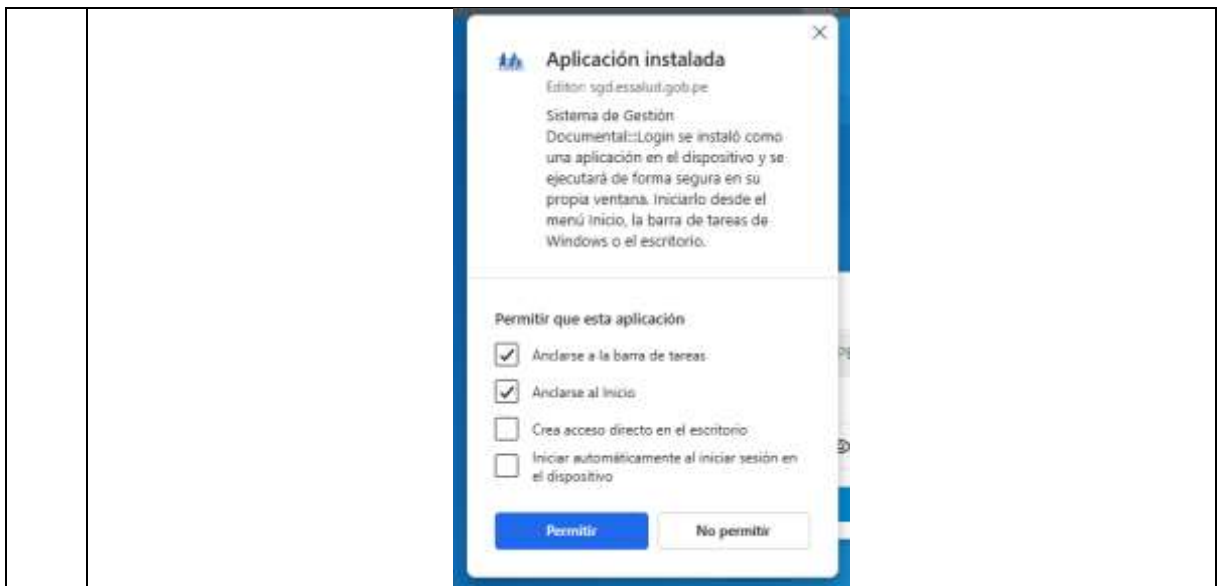
1	DESCARGA DE CARPETA DE INSTALACIÓN Ingresar a la carpeta compartida en el repositorio con nombre Firma Digital 2025 que contiene los aplicativos para la instalación de SGD y Firma Digital.
2	INSTALACIÓN DE JAVA JRE En la carpeta podremos encontrar con el nombre de 01 jre-8u461-windows-x64 el instalador de última versión de JAVA JRE. 
3	INSTALACIÓN DE SGD En la carpeta podremos encontrar con el nombre de 02 SGD el link de la página de inicio de sesión del Sistema de Gestión Documental, el cual deberá abrirse desde el explorador Microsoft Edge por temas de compatibilidad de funciones.



Una vez abierto el link ingresamos a la opción del explorador en la opción **Más Herramientas -->Aplicaciones --> Instalar este sitio como una aplicación.**

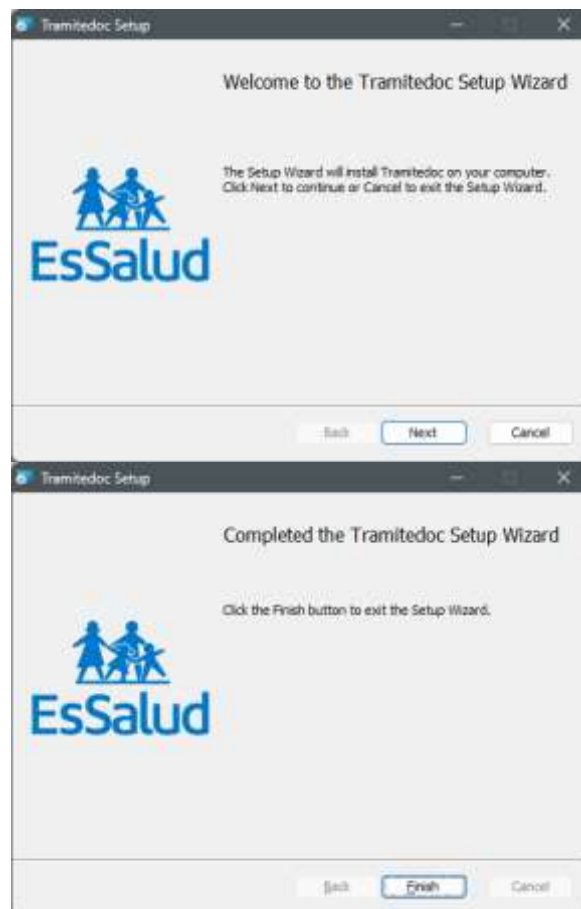


Una vez abierta la aplicación, anclar el icono de la aplicación en la barra de herramientas.

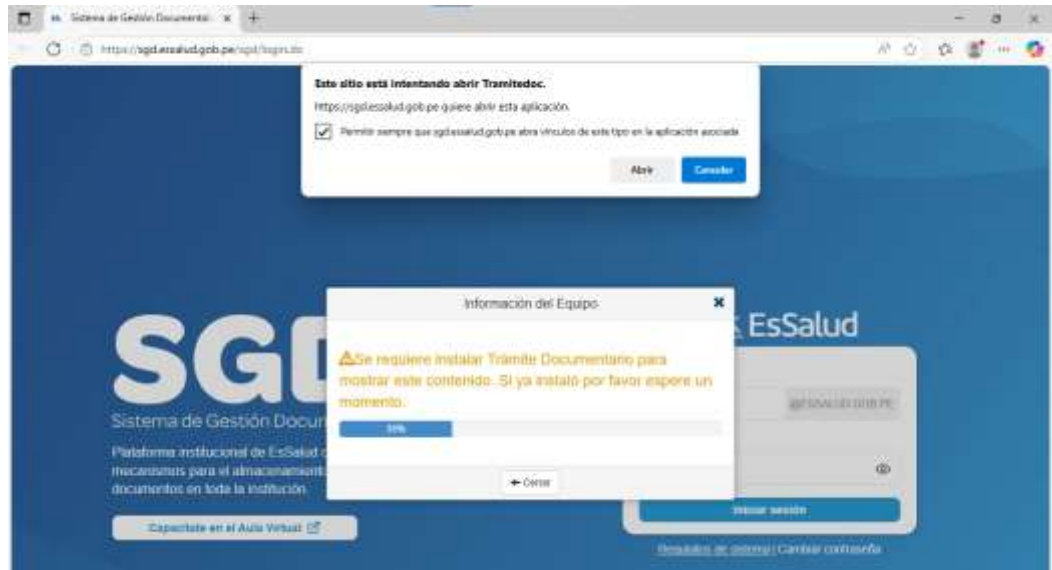


4 INSTALACIÓN DE TRÁMITE DOCUMENTARIO

En la carpeta podremos encontrar con el nombre de **03 Tramite Documentario V1.0.9** aplicación requerida para el correcto funcionamiento de tramites en el Sistema de Gestión Documental.

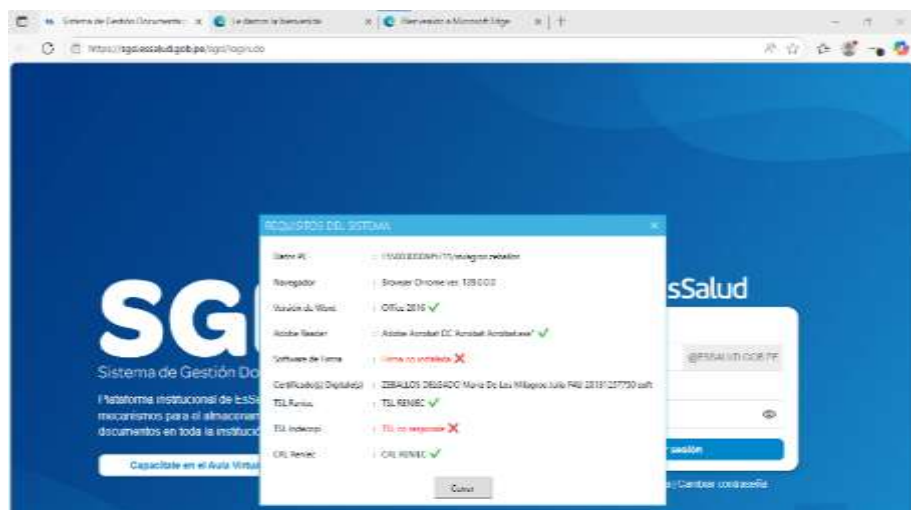


Una vez instalado comprobaremos su correcta instalación dando clic en el vínculo de **Requisitos de sistema** en la página de inicio de sesión del Sistema de Gestión Documental



5 REQUISITOS DE SGD

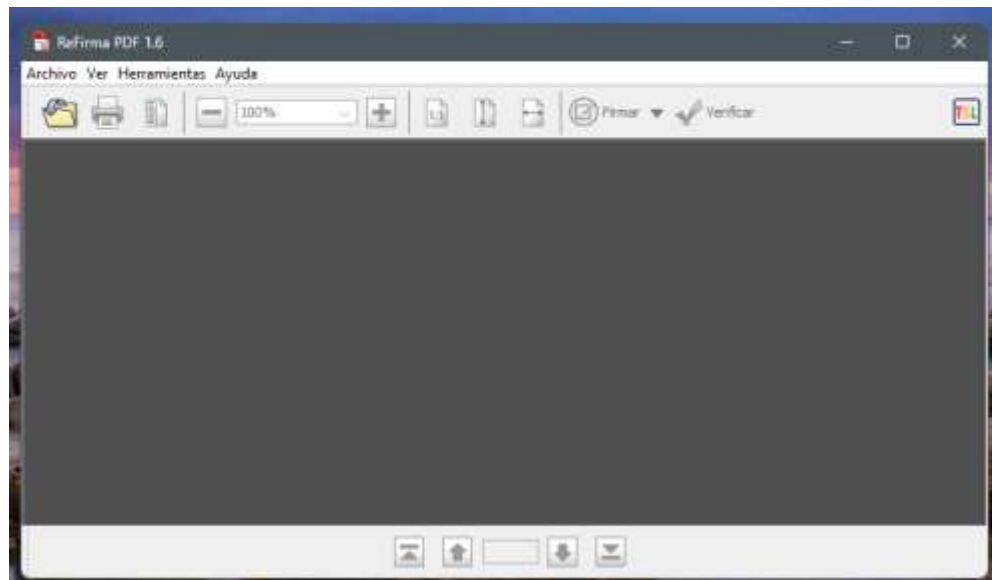
Comprobar la instalación de requisitos para el correcto funcionamiento del Sistema de Gestión Documental dando clic en el vínculo de **Requisitos de sistema** en la página de inicio de sesión del Sistema de Gestión Documental



6 INSTALACIÓN DE FIRMADOR DIGITAL

Ingresaremos a los link con el nombre de **04 ReFirma PDF** hacer clic en **EJECUTAR ReFirma PDF**** (Ejecutable Java Web Start) este aplicativo

es un firmador digital el cual interactua con el Sistema de Gestion Documental.



7 FIRMAS DIGITALES

En la institución hay 3 casos de firma digital los cuales son:

- Token digital
- Certificado Digital
- DNI Electronico

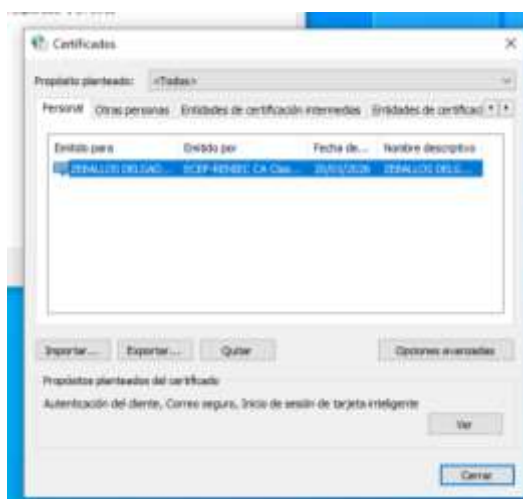
7.1 TOKEN DIGITAL

Para poder firmar con Token Digital es necesario instalar el aplicativo **05 CryptoIDE**, que será el encargo de leer el certificado instalado en un dispositivo USB.



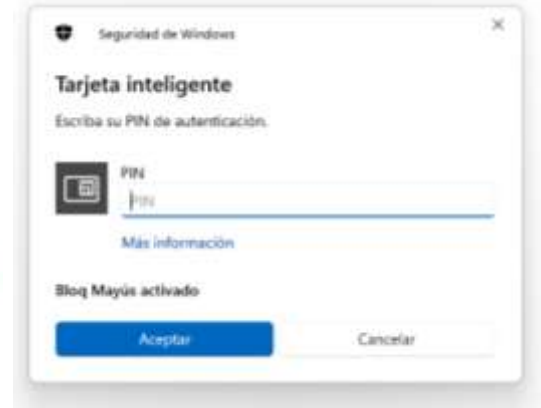
7.2 CERTIFICADO DIGITAL

El certificado digital se encuentra instalado en el equipo asignado al usuario, por lo que solo podrá firmar desde ese equipo.



7.3 DNI Electrónico

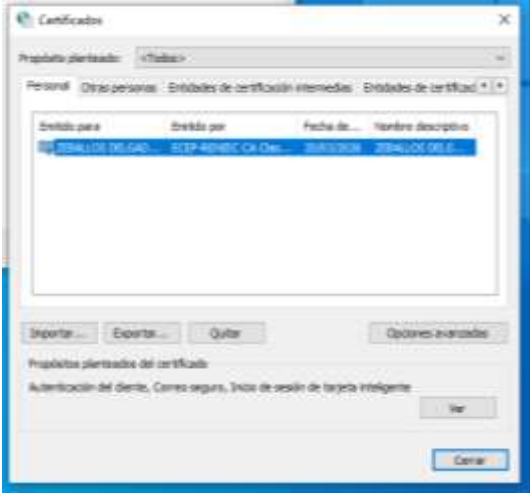
Para poder firmar con DNI Electrónico es necesario instalar el aplicativo **06 RENIEC-DNIe** y **07 Authentic-Webpack**, que serán los encargados de poder leer el sim instalado en el DNIe. Recordar para que se pueda firma con DNIe se requiere de un lector y tener el PIN de seguridad ingresado por el usuario al momento de tramitar su DNIe.



Anexo 3. Formato de registro de instalación de certificados.

Datos de la intervención	
Fecha y Hora:	01/08/2025
Área/Departamento Afectado:	Neonatología
Usuario:	Lic. Zeballos Delgado María
Ubicación:	Sector Básico – Consultorio 1

Detalles del certificado digital	
Proveedor de Certificado:	RENIEC
Tipo de Certificado:	<input checked="" type="checkbox"/> Certificado Digital (Software) <input type="checkbox"/> Token Digital (Hardware) <input type="checkbox"/> DNIe (Asignación de lector)
Fecha de Emisión del Certificado:	01/08/2025
Fecha de Vencimiento del Certificado:	01/08/2026
PIN de verificación (Opcional):	70652887aay

Verificación y confirmación			
Prueba de Firma Digital Realizada:	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO	
Documento de Prueba:			
Resultado de Prueba:	<input checked="" type="checkbox"/> EXITOSO	<input type="checkbox"/> ERROR	
Observaciones Adicionales:	NA		

Profesional Asignado:	Alejandro Ayasta
Jefe de la OSI:	Sara Turpo

Anexo 4. Informe de atención de soporte informático.

Número de Informe	20250816-005
--------------------------	--------------

Datos de la Incidencia	
Fecha y Hora de la Incidencia:	01/08/2025
Área/Departamento Afectado:	Pediatría
Usuario/Reportante:	Dr. Hector Choqque Tacca
Prioridad:	Media

Descripción de la Incidencia	
Título del Incidente:	Impresora del consultorio no imprime
Detalle del Incidente:	La impresora (Epson L4150) en el consultorio de Pediatría del Sector Básico no imprime correctamente. El usuario no puede imprimir los resultados de las pruebas, lo que está retrasando la atención de los pacientes. El equipo está encendido y tiene papel, pero las impresiones son casi ilegibles.
Evidencias:	Impresión de resultados ilegible.

Acciones de Soporte y Resolución	
Profesional Asignado:	Alejandro Ayasta
Fecha y Hora de Inicio:	09:10
Pasos de Diagnóstico:	Revisión de nivel de tinta
Acciones de Resolución:	Limpieza de cabezales
Fecha y Hora de cierre:	09:30
Tiempo de Resolución:	20 min
Estado final:	Luego de realizar la limpieza de cabezales se imprime una página de prueba, teniendo como resultado una impresión correcta.

Profesional Asignado:	Alejandro Ayasta
Jefe de la OSI:	Sara Turpo

Anexo 5. Diagrama de Gantt

	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6			
	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	Semana 8	Semana 9	Semana 10	Semana 11	Semana 12	Semana 13	Semana 14	Semana 15	Semana 16	Semana 17	Semana 18	Semana 19	Semana 20	Semana 21	Semana 22	Semana 23	Semana 24
1 Actividad Principales previas al enrolamiento																								
Presentación de actividades a las Jefaturas	█																							
Levantamiento de información	█																							
Diagnostico de equipos		█																						
Preparación de imágenes			█	█																				
2 Actualización del Sistema Operativo y enrolamiento de equipos al Directorio Activo																								
Hospital Nacional																								
Piso 7A / 7B Jefaturas Estaciones de enfermeras Nutrición				█	█																			
Piso 6A / 6B Jefaturas Estaciones de enfermeras					█	█																		
Piso 5A / 5B Jefaturas Estaciones de enfermeras						█	█																	
Piso 4A / 4B Jefaturas Estaciones de enfermeras							█	█																
Piso 3A / 3B Jefaturas Salas de operaciones Salas de recuperacion								█	█															
Piso 2A / 2B Jefaturas Salas de obervaciones Estaciones de enfermeras									█	█														
Piso 1 Consultorio de consulta Externa Jefatura de Gerencia Clínica Jefatura de Gerencia Quirurgica										█	█													
3 Emergencias																								
Jefaturas Consultorios Topicos Farmacia																								
4 Admision																								
Modulos de atención 1-8 (Hospital Nacional) Modulos de atencion 9-11 (Emergencias)																								
5 Referencias																								
Jefaturas Ventanillas																								
6 Adquisiciones																								
Jefaturas Usuarios de planta Locadores de servicio																								
7 Recursos Humanos																								
Jefaturas Usuarios de planta Locadores de servicio																								

Anexo 06. Acta de constitución del proyecto.

Título del Proyecto:

Implementación del Directorio Activo, Sistema de Gestión Documental (SGD) y Firma Digital en la Red Asistencial de Salud Arequipa.

Patrocinador:

Gerencia de la Red Asistencial de Salud Arequipa – Oficina de Tecnología de la Información (OTI).

Responsable Técnico:

Bach. Alejandro Steve Ayasta Yana – Ingeniero de Sistemas

Fecha de inicio: enero 2024

Fecha de cierre: agosto 2024

Propósito del Proyecto:

Modernizar la infraestructura tecnológica de la Red Asistencial de Salud Arequipa mediante la integración de estaciones de trabajo al Directorio Activo, la implementación del Sistema de Gestión Documental y la adopción de la Firma Digital, fortaleciendo la eficiencia, seguridad y trazabilidad institucional.

Alcance del Proyecto:

- Enrolar 1850 equipos al dominio institucional.
- Implementar el SGD y la Firma Digital en 1000 estaciones de trabajo.
- Capacitar a 800 usuarios en el uso de las nuevas herramientas.
- Estandarizar procedimientos técnicos y documentarlos mediante manuales.

Entregables Principales:

- Equipos de cómputo integrados al Directorio Activo.
- SGD y Firma Digital instalados y operativos.
- Manuales técnicos y protocolos de instalación.
- Informe de cierre y validación institucional.

Supuestos:

Disponibilidad de recursos humanos conectividad estable soporte técnico y coordinación inter-áreas.

Restricciones:

Tiempo limitado de intervención, dependencias con otros sistemas, disponibilidad de equipos en campo.

Aprobación:

Firma del patrocinador y del responsable técnico.

Anexo 07. Matriz de poder-interés (stakeholders)

Grupo de Interés	Rol o Participación	Nivel de Poder	Nivel de Interés	Estrategia de Gestión
Gerencia de la Red Asistencial	Patrocinador del proyecto	Alto	Medio	Mantener informados y alinear objetivos institucionales.
Oficina de Tecnología de la Información (OTI)	Responsable técnico y operativo	Alto	Alto	Involucrar activamente y coordinar entregables.
Personal Administrativo	Usuario final de SGD y Firma Digital	Bajo	Alto	Capacitar y comunicar beneficios del proyecto.
Personal Asistencial (Salud)	Usuario indirecto del sistema	Medio	Medio	Brindar soporte y retroalimentación sobre uso.
Proveedor de Certificado Digitales	Soporte externo	Bajo	Bajo	Monitorear entregas y cumplimiento técnico.
Área de Recursos Humanos	Validación de usuarios en AD	Medio	Alto	Coordinar procesos de autenticación y registro.

Anexo 08. Estructura de desglose de trabajo (EDT)

Nivel 1: Implementación de Directorio Activo, SGD y Firma Digital

1.1 Fase de Diagnóstico

1.1.1 Levantamiento de información de equipos

1.1.2 Análisis de compatibilidad y recursos

1.2 Fase de Preparación Técnica

1.2.1 Actualización de sistemas operativos

1.2.2 Configuración de red y políticas

1.3 Fase de Implementación

1.3.1 Enrolamiento de equipos al Directorio Activo

1.3.2 Instalación del SGD y Firma Digital

1.4 Fase de capacitación

1.4.1 Capacitación presencial a usuarios

1.4.2 Elaboración de guías de usuario

1.5 Fase de Documentación y Cierre

1.5.1 Elaboración de manuales técnicos

1.5.2 Entrega de informe final y validación institucional

Anexo 09. Roadmap de entregables (cronograma general)

Fase	Actividades Principales	Periodo	Entregables
Diagnóstico	Inventario de equipos, análisis técnico	Enero 2024	Informe técnico inicial
Preparación Técnica	Actualización y configuración de equipos	Febrero – Marzo 2024	Equipos listos para enrolamiento
Implementación	Enrolamiento AD, instalación SGD y Firma Digital	Abril – Junio 2024	Equipos y sistemas operativos
Capacitación	Talleres y sesiones de usuario	Julio 2024	Usuario formados y certificados
Cierre y Documentación	Elaboración de manuales, validación	Agosto 2024	Informe final y manuales técnicos

Anexo 10. Matriz de riesgos.

Riesgo Identificado	Tipo	Probabilidad	Impacto	Estrategia de Mitigación
Fallas de conectividad en red	Técnico	Media	Alta	Verificación previa de puntos de acceso y pruebas piloto.
Incompatibilidad de software	Técnico	Baja	Alta	Validar requerimientos y compatibilidad antes de instalación.
Resistencia al cambio del personal	Humano	Alta	Media	Capacitación práctica y comunicación de beneficios.
Disponibilidad limitada de personal técnico	Operativo	Media	Media	Planificación anticipada y asignación por turnos.
Retraso en entrega de certificados digitales	Externo	Baja	Alta	Coordinación previa con proveedor y cronograma flexible.
Pérdida de información durante migración	Técnico	Baja	Alta	Realizar copias de seguridad y pruebas controladas