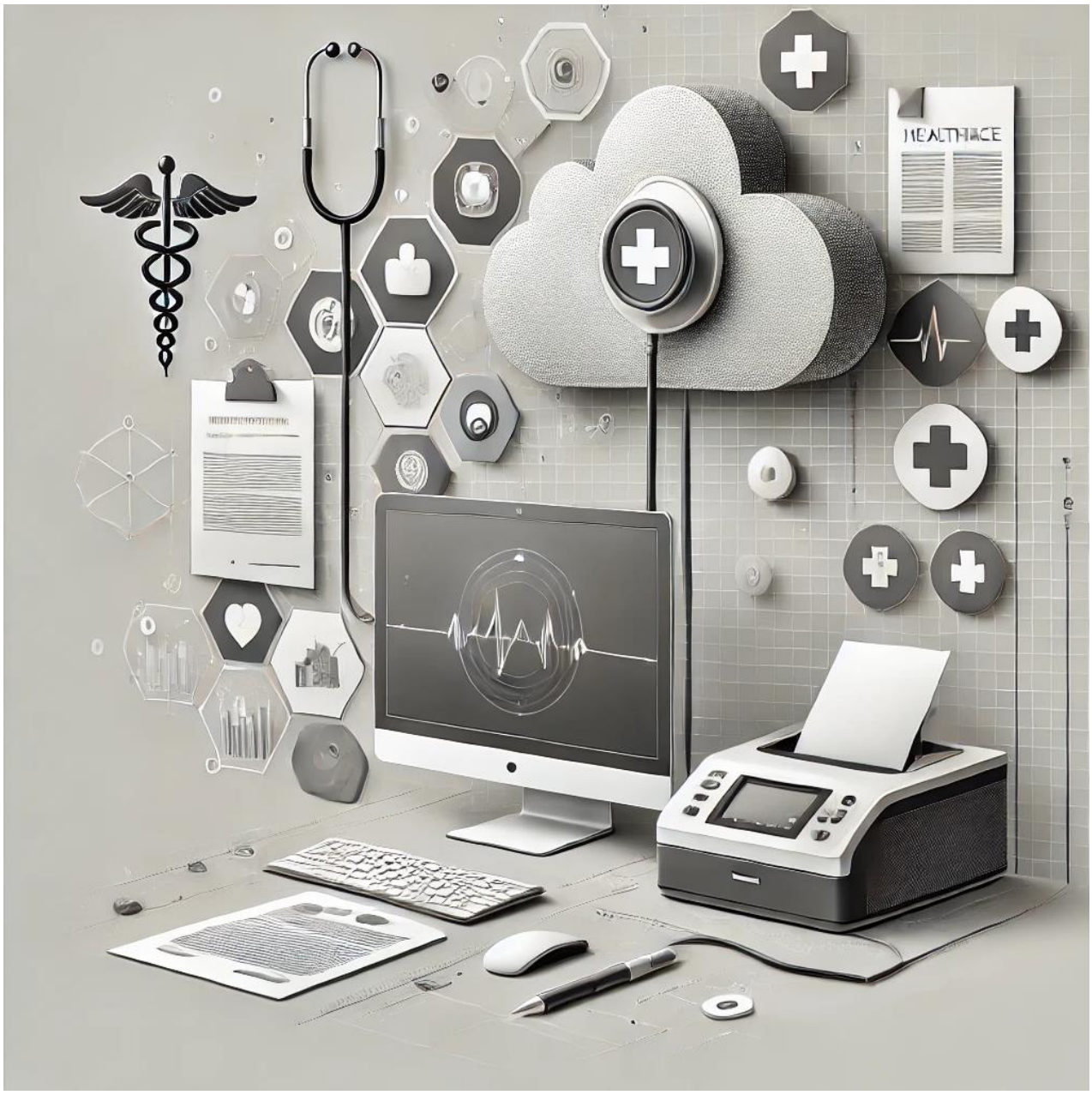


Análisis sobre el estado de los Sistemas de Impresión y Digitalización del Sistema Nacional de Salud

Autores:

Aday García del Toro

Juan Pérez Aragon

Laura Alonso Álvarez

Master en Dirección de Sistemas y TIC de la Salud y en Digitalización Sanitaria 2023-2024

S.E.I.S. Sociedad Española de Informática de la Salud

Instituto de Salud Carlos III

Gobierno de España. Ministerio de Ciencia, Innovación y Universidades

Fecha de entrega:

8 de Octubre 2024

Anexo II

Autorización del Tutor para la lectura y defensa del Trabajo Fin de Master.

Nombre Alumnos	Aday García del Toro Juan Pérez Aragon Laura Alonso Álvarez
Titulo Trabajo Fin de Máster	Análisis sobre el estado de los Sistemas de Impresión y Digitalización del Sistema Nacional de Salud

Dña. Elvira Alonso Suero

Como Tutor del Trabajo Fin de Máster arriba reseñado considera que ha sido realizado de acuerdo con las normas exigidas y reúne las condiciones de calidad necesarias para su presentación y defensa.

Firmado:

Elvira Alonso Suero
2024.10.07 14:05:08
+02'00'

GARCIA DEL TORO ADAY - 78506371B

Firmado digitalmente por GARCIA DEL TORO ADAY - 78506371B

JUAN| PEREZ| ARAGON

Firmado digitalmente por JUAN|PEREZ| ARAGON
Fecha: 2024.10.07 10:35:30 +02'00'

ALONSO ALVAREZ LAURA - DNI 71655356Y

Firmado digitalmente por ALONSO ALVAREZ LAURA - DNI 71655356Y
Fecha: 2024.10.07 07:46:29 +02'00'

Introducción

En la era de la información, la tecnología juega un papel fundamental en la eficiencia y efectividad de los sistemas de salud. Los Sistemas de Impresión y Digitalización, en particular, son componentes cruciales que afectan directamente la calidad de los servicios médicos y la gestión de la información sanitaria. Este trabajo de fin de máster se enfoca en un análisis exhaustivo del estado actual de estos sistemas dentro del Sistema Nacional de Salud (SNS) de España, con el objetivo de identificar fortalezas, debilidades y áreas de mejora.

El SNS, compuesto por una red de servicios sanitarios públicos distribuidos a lo largo del territorio español, se enfrenta al desafío constante de integrar y optimizar tecnologías que permitan una gestión eficiente de la información. La digitalización de los registros médicos y la implementación de sistemas de impresión avanzados son elementos clave para asegurar una atención sanitaria de calidad, reducir errores médicos y facilitar el acceso a la información tanto para los profesionales de la salud como para los pacientes.

A lo largo de este estudio, se analizarán diversos aspectos relacionados con los Sistemas de Impresión y Digitalización en el SNS, incluyendo la infraestructura tecnológica actual, las políticas de gestión de la información, y el grado de adopción de tecnologías emergentes. Además, se evaluarán las prácticas existentes y se compararán con modelos internacionales, buscando extraer lecciones y recomendaciones que puedan ser aplicadas para mejorar el sistema español.

En este trabajo, se propone un caso de uso que aborda una de las principales áreas de mejora identificadas: la gestión eficiente y segura de imágenes médicas y documentos clínicos. Este caso de uso se centra en la automatización y centralización de la carga y gestión de estos datos a través de un sistema que integra directamente los medios digitales, como CDs y otros soportes, en las plataformas hospitalarias (HIS y PACS). La propuesta busca mejorar la eficiencia operativa, asegurar el cumplimiento normativo y optimizar el uso de los recursos tecnológicos, garantizando una mayor seguridad en el manejo de la información sensible de los pacientes. Este enfoque no solo responde a las necesidades actuales del SNS, sino que también se alinea con las mejores prácticas internacionales en la gestión de datos sanitarios.

En resumen, este trabajo tiene como finalidad contribuir al entendimiento y mejora de los Sistemas de Impresión y Digitalización del Sistema Nacional de Salud, buscando impulsar la eficiencia, la seguridad y la calidad en la atención sanitaria a través de una gestión más eficaz de la información.

Tabla de Contenido

1 Resumen y Objetivos

En la actualidad, el SNS se enfrenta a una serie de desafíos relacionados con la gestión eficiente de la información sanitaria, uno de los recursos más valiosos para garantizar una atención médica de calidad. Entre los sistemas que juegan un papel crucial en este proceso se encuentran los sistemas de impresión y digitalización, que facilitan el manejo de grandes volúmenes de documentación e imágenes médicas. Estos sistemas no solo soportan los procesos clínicos y administrativos diarios, sino que también aseguran que la información esté disponible de manera oportuna y precisa para los profesionales de la salud. Sin embargo, a pesar de su importancia, estos sistemas presentan diversas áreas de mejora que deben ser abordadas para optimizar su rendimiento y alinearlos con las demandas actuales del sector sanitario.

El presente trabajo lleva a cabo un análisis del estado actual de los sistemas de impresión y digitalización en el SNS. Para ello, se realiza una evaluación detallada de la infraestructura tecnológica disponible en distintos centros sanitarios a lo largo de varias comunidades autónomas, así como un análisis de las políticas y procedimientos actuales que rigen su uso. Este análisis no solo contempla los aspectos técnicos, sino que también se enfoca en el grado de adopción de tecnologías emergentes y en la capacidad de estos sistemas para cumplir con las normativas vigentes, especialmente en lo que respecta a la protección de datos personales, como el Reglamento General de Protección de Datos (GDPR) y la Ley Orgánica de Protección de Datos (LOPDGDD).

A través de este análisis, se identifican las principales fortalezas y debilidades de los sistemas actuales, así como las oportunidades de mejora que pueden ser aprovechadas para implementar soluciones tecnológicas más eficientes. Un aspecto central de este estudio es la comparación de las prácticas en diferentes comunidades autónomas y centros sanitarios, con el fin de extraer lecciones y mejores prácticas que puedan ser aplicadas de manera generalizada en el SNS. Esta evaluación permite también hacer recomendaciones concretas sobre cómo mejorar la gestión de los sistemas de impresión y digitalización para que estos se integren de manera más efectiva con otros sistemas de información hospitalaria, como los sistemas de historia clínica electrónica y los sistemas de almacenamiento de imágenes médicas (HIS y PACS).

Como parte de las propuestas de mejora, este trabajo incluye un caso de uso específico que aborda uno de los desafíos más críticos en el manejo de la información sanitaria: la automatización y centralización de la gestión de imágenes médicas y documentos clínicos provenientes de soportes digitales tales como CDs u otros medios. La propuesta de este caso de uso tiene como objetivo implementar un sistema que permita la integración directa y segura de estos datos con las plataformas hospitalarias ya existentes, mejorando no solo la eficiencia operativa, sino también la seguridad y el cumplimiento normativo. La automatización de estos procesos no solo reducirá el tiempo dedicado a tareas manuales por parte del personal sanitario, sino que también disminuirá el riesgo de errores humanos y garantizará un manejo más seguro y controlado de la información sensible.

Los objetivos específicos de este trabajo son, por tanto, identificar las áreas clave en las que los sistemas de impresión y digitalización actuales pueden ser optimizados, proponer mejoras que aborden tanto aspectos operativos como de seguridad, y asegurar que estas mejoras estén alineadas con las normativas nacionales e internacionales en materia de protección de datos. Asimismo, se busca promover una mayor integración tecnológica entre los diferentes sistemas de información hospitalaria, facilitando el acceso rápido y seguro a los datos clínicos que son esenciales para una atención sanitaria de calidad.

En resumen, este trabajo tiene como finalidad contribuir a la modernización y mejora continua de los sistemas de impresión y digitalización dentro del SNS, impulsando una gestión más eficiente de la información sanitaria. Con ello, se busca no solo mejorar la eficiencia operativa, sino también garantizar que los sistemas de salud sean más seguros, ágiles y capaces de responder a las necesidades tanto de los profesionales como de los pacientes. La implementación de las propuestas presentadas, incluido el caso de uso, permitirá avanzar hacia una sanidad más digitalizada, eficiente y centrada en la protección de los datos personales.

2 Marco Legal

La legislación aplicable a este trabajo podría diferenciarse en varias partes por una a la propia de los dispositivos y lo relacionados con estos desde un punto de vista de los aparatos físicos y comunicaciones con los mismos. Y por otro lado, las que más nos interesarían, que sería la relacionada con la protección de datos y al tratarse de un entorno sanitario la legislación asociada a la historia clínica.

- Ley General de Sanidad (BOE, 1986)
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. (BOE, 2003)
- Ley 16/2003, de 28 mayo, de cohesión y calidad del Sistema Nacional de Salud. (BOE, Ley 16/2003 - Cohesión y Calidad del SNS, 2003)
- Ley 45/2007, de 13 de diciembre, de desarrollo sostenible del medio rural, en particular, su artículo 30 relativo a la sanidad. (BOE, Artículo 30 - Sanidad Rural - Ley 45/2007 - Desarrollo Sostenible del Medio Rural, 2007)
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. (BOE, Real Decreto 4/2010 - Esquema Nacional de Interoperabilidad, 2010)
- Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud. (BOE, Real Decreto 1093/2010 - Informes Clínicos, 2010)
- Real Decreto 1718/2010, del 17 de diciembre sobre receta médica y orden de dispensación. (BOE, Real Decreto 1718/2010 - Receta Médica, 2011)
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (RGPD). (Europea, 2016)
- Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público. (BOE, Real Decreto 1112/2018 - Accesibilidad de Sitios Web Públicos, 2018)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). (BOE, Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales, 2028)
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. (BOE, Real Decreto 203/2021 - Funcionamiento por Medios Electrónicos, 2021)
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (BOE, Real Decreto 311/2022 - Esquema Nacional de Seguridad, 2022)

De los dispositivos se pueden destacar ciertas normas o estándares:

- Consumo energético definidos en el estándar “Energy Star”, se trata de un programa internacional que promueve la eficiencia energética en productos electrónicos. (Star, s.f.)
- Los equipos no han de superar el nivel de ruido LWAd de 30 dB(A), calculados según EN ISO 7779:2001 (ISO, Acoustics — Measurement of airborne noise emitted by information technology and telecommunications equipment, 2018) y expresados según ISO 9296:1988 (ISO, Acoustics — Declared noise emission values of computer and business equipment, s.f.) o equivalentes y referido a la máquina sin accesorios.
- Certificado del Sistema de Gestión de Calidad UNE-EN ISO 9001 (ISO, Sistemas de gestión de la calidad — Requisitos, s.f.) y el certificado de Gestión Medioambiental UNE EN ISO 14001 (ISO, Sistemas de gestión ambiental — Requisitos con orientación para su uso, s.f.)
- La Ley 22/2011, de 28 de julio, de residuos y suelos contaminados (BOE, Ley 22/2011 de Residuos y Suelos Contaminados, 2011)

- EN 12281:2003 o equivalente en cuanto al soporte de uso de papel reciclado (UNE, 2023)

3 Planificación estratégica

Para poder detallar el estado del arte actual de los sistemas de impresión se ha realizado una búsqueda de diferentes pliegos a lo largo de las diferentes Comunidades Autónomas, las cuales detallamos a continuación, de estos nos hemos centrado en la información que nos afecta, no se hace hincapié por ejemplo en la parte asociada a medidas de impresoras, velocidad, ruido,… siendo todo ello importante a la hora de redactar un contrato, pero no para nuestro caso.

3.1 España

3.1.1 Principado de Asturias

El arrendamiento del dispositivo, con inclusión del transporte, instalación y configuración de todos los elementos del mismo, así como, el suministro, gestión y reposición de consumibles y fungibles, siendo este arrendamiento la prestación principal.

Características a destacar:

- Mantenimiento integral y a todo riesgo de los equipos anteriormente citados, así como el servicio de asistencia técnica para los mismos.
- Cabe destacar un disco duro dentro de los dispositivos y software OCR.
- La gestión de usuarios se hará mediante integración de las máquinas con el directorio LDAP del Servicio de Salud.
- Las máquinas deberán ser capaces de reconocer a los usuarios mediante código PIN, usuario y contraseña, ya sea a través de su introducción a través de teclado virtual en la propia máquina o mediante tarjeta identificativa de proximidad.
- Un sistema de retención en todos los dispositivos.
- Monitorización de todos los dispositivos.
- Prueba piloto de 15 días para comprobar que todo es correcto.
- Incluye instalación y formación a los usuarios.

Los dispositivos son impresoras multifunción, b/n o en color e impresoras conectadas directamente a un puesto de trabajo.

3.1.2 Comunitat Valenciana (Comunidad de Valencia)

Se ha realizado un acuerdo marco para el arrendamiento de dispositivos de impresión, copia y escaneo, así como su gestión, para la Administración de la Generalitat; sus entidades autónomas y entes del sector público empresarial y fundacional. (C Valencaina, 2023)

Entre las diferentes características del mismo cabe destacar:

- Se trata de un contrato de arrendamiento sin opción de compra.
- Dispositivos nuevos.
- Incluye la instalación de los mismos, así como su software.
- Configuración de los módulos de seguridad, autenticación y autorización en los equipos de impresión y MF, integradas con Directorio Activo, LDAP,..
- Implantación y configuración de la Plataforma de Gestión y monitorización en los dispositivos
- Asignación de contraseñas para la configuración remota de los equipos.
- Servicio de mantenimiento de correctivo y preventivo.
- Activar el modo de ahorro de los dispositivos.
- Configurado por defecto la impresión a doble cara y en blanco y negro.

- Los dispositivos multifunción con lector de banda magnética o tarjeta de proximidad.

Implantación de políticas de impresión.

La impresión retenida y recogida confidencial en los equipos multifunción.

La distribución de los archivos digitalizados vía correo electrónico y/o carpeta de red.

- Los equipos multifunción deberán incorporar las características tecnológicas necesarias para permitir la implementación de soluciones de copia electrónica auténtica según la normativa de Administración electrónica y las normas técnicas de interoperabilidad del Esquema Nacional de Seguridad y el Esquema Nacional de Interoperabilidad. Incluye dispositivos multifunción, de puesto, tarjetas de código de barras e impresoras de brazaletes para identificar a los pacientes.

3.1.3 Comunidad de Madrid

3.1.3.1 Hospital La Paz

En ciertas comunidades se han desarrollado pliegos por parte de hospitales de forma individual, como en este caso se ha ejecutado para el Hospital Universitario La Paz-Carlos III-Cantoblanco y de los Centros de Especialidades y Centros de Salud Mental adscritos a su Gerencia (Madrid, 2021).

Se incluye la instalación, puesta en marcha, mantenimiento, suministro de consumibles, asistencia técnica y software de gestión.

Son productos multifunción que pueden ser nuevos o reciclados/remanufacturados, en este caso con garantía como si fueran nuevos.

Incluyen multifunción en color y blanco/negro, además de equipos monedero al tener un uso público.

Revisiones:

- Revisión de consumibles y estado de los equipos diariamente en el Hospital La Paz.
- Revisión mensual en Centros de Especialidades, Centros de Salud Mental, Hospital de Cantoblanco y Hospital Carlos III.

Impresión directa desde el HCIS/HP HIS y NEXUS y la liberación y contabilidad de los trabajos de impresión desde este sistema.

Los equipos multifuncionales deberán permitir asociar los trabajos a los usuarios a través de un código y a través de la tarjeta identificativa desde el propio equipo y por el propio usuario.

Posibilidad de crear colas de impresión para retener los trabajos y poder liberarlos en un grupo de dispositivos multifunción previa identificación por parte del usuario en la multifunción elegida.

Deberá permitir la creación de una base de datos de usuarios a los que asociar los perfiles de privilegios de uso de los equipos. La empresa adjudicataria deberá realizar el volcado de la base de datos que existe actualmente y que contiene la información correspondiente a los perfiles, grupos…. Esta información será, por tanto, la base de funcionamiento del software desde el inicio de la contratación del servicio. Esto es diferente a la mayoría de los pliegos, ya que se basan en Directorio Activo/LDAP y no en una base de datos.

3.1.4 Andalucía

3.1.4.1 Cádiz – SSPA integrados en la Central Provincial de Compras

En este caso los centros del Sistema Sanitario Público de Andalucía (SSPA) también se trata de un suministro mediante arrendamiento sin opción de compra, su mantenimiento y soporte (Andalucía, s.f.). El contratista realizará pruebas del correcto funcionamiento de todos los equipos instalados, debiendo quedar estas documentadas.

Instrucciones de funcionamiento de los equipos: para el mejor aprovechamiento de los equipos, el adjudicatario pondrá a disposición de los usuarios un manual básico en castellano y un cartel explicativo en el mismo idioma, visible, junto a las máquinas donde se resuma su funcionalidad. Además, todas las máquinas llevarán una etiqueta que las identifique, como mínimo por su nº de serie, dirección IP , marca y modelo.

3.1.5 Catalunya (Cataluña)

3.1.5.1 Consorci Sanitari de L'Alt Penedès i Garraf

También consiste en un pliego de arrendamiento sin opción de compra, de impresión, escaneo y reprografía (Cataluña, s.f.).

La impresión se ejecuta desde dos servidores centralizados con software de gestión de colas.

Equipos nuevos y actuales.

Las pantallas táctiles funcionaran con guantes sanitarios (látex, nitrilo, vinilo,…)

Se podrán identificar a través de LDAP, tarjeta de empleado de tecnología sin cables (RFID), con PIN o con usuario administrador.

Se valora que los faxes tengan un registro de los FAXES enviados y recibidos.

La monitorización de los puestos USB se realizará por WIFI, y no instalando un agente en el PC, se centralizará en un servidor.

Además de un sistema de seguridad:

- Garantizar la impresión de información confidencial.
- Controlar la cantidad de impresiones.
- Imputar volúmenes de impresión a los diferentes usuarios y departamentos.

Pide una solución triple AAA (autenticación, autorización y contabilidad) abierta (multimarca y multifabricante).

Con sistema de retención de hojas impresas, asignación de cuotas basadas en LDAP.

Sistema de OCR para los documentos escaneados.

3.1.6 Castilla y León

Proyecto SILOS: Acuerdo marco con un único adjudicatario para el arrendamiento, sin opción a compra, de dispositivos de impresión para la Gerencia Regional de Salud de Castilla y León. (León, 2019)

Se trata de un acuerdo marco que cubre toda la comunidad, y se trata de un arrendamiento sin opción de compra de dispositivos de impresión y su mantenimiento.

Incluyen impresoras de puesto, multifunciones de A4 o A3 con color, pero no de brazaletes, matriciales, o la reprografía.

Para las impresoras multifunción se añade la opción de integrar con directorio activo, un código de usuario, u opción del lector integrado de chip (la Tarjeta Profesional Inteligente de los trabajadores) o detector de chip de proximidad myfare.

Las multifunciones A3, que son modelos que imprimen en color, además de lo anterior, deben de poder enviar por SMB o FTP, han de retener las impresiones.

Ambas multifunciones tendrán la opción “Follow me”, el documento queda en una cola virtual hasta que el usuario la imprime desde un impresora.

Con software de monitorización instalado en los ordenadores para las de puesto.

Y un software de control y seguridad integrado con el directorio activo. Pudiendo crear perfiles limitando copias, B/N o color).

Por otro lado requiere un software de gestión y auditoria en tiempo real de los consumos, de la monitorización de todos los dispositivos, estado, ubicación. Estado de los contadores.

3.1.7 Región de Murcia

Arrendamiento sin opción de compra de impresoras para el edificio policlínico del Hospital Clínico Universitario "Virgen de la Arrixaca". (Murcia, 2020)

Se trata de un suministro sin opción a compra, para Hospital Clínico Universitario “Virgen de la Arrixaca”, dependiente del Área I de Salud Murcia-Oeste.

Pero en el objeto indica que se trata de arrendamiento y mantenimiento de impresoras, sin opción a compra.

Solicita impresoras nuevas de menos de dos años en el mercado.

Y los productos ofertados deberán ser conformes con la normativa vigente de la Unión Europea y española en lo referente a sus aspectos de calidad, ergonómicos, medioambientales, de ahorro energético, compatibilidad electromagnética y seguridad.

Software de gestión, basado en grupos de directorio activo, pudiendo limitar número de copias y color.

Recalca que cumplan la protección de datos:

- Prohibición de acceder a los datos de carácter personal
- Deber de secreto, de carácter indefinido

3.1.8 Canarias

Servicio de mantenimiento del parque de impresoras monopuesto existente en los centros dependientes de la Gerencia de Atención Primaria del Área de Salud de Gran Canaria (Canarias, 2024)

Se trata de un servicio promovido por la Consejería de Sanidad del Gobierno de Canarias y son las propias Gerencias de las áreas de salud las que lo solicita en este caso el Área de Salud de Gran Canaria.

Es muy reciente, se publicó el 1 de octubre del 2024 en la plataforma de Contratación del Estado.

Comparado con el anterior pliego, del año 2020 se ha incrementado un 37% el valor base de la licitación. de 1.064.995,08€ a 1.460.094,33€. Pero la cantidad de dispositivos se mantiene prácticamente sin cambios.

Número de dispositivos

	2018	2023	Variación
Tipo A	1205	1219	101,16%
Tipo B	79	73	92,41%
TIP C	62	54	87,10%

Tabla 1. Valores de consumo de impresoras

Piden el mantenimiento de las actuales, y la renovación de aquellas que lleguen al fin de su vida útil. Las que se reemplacen han de ser modelos nuevos.

Serán supervisados por el Servicio de Sistemas y Nuevas Tecnologías a los cuales se les dotará de un cuadro de gestión y de mandos.

A destacar que todas las impresoras se conectan vía cable de red ethernet, lo cual facilita enormemente su gestión y mantenimiento.

Ofrecerá lo siguientes servicios:

- Gestión automática de contadores.
- Herramienta de gestión y control centralizada, incluyendo tarificador de costes.
- Informes periódicos.
- Reuniones periódicas para el seguimiento del servicio.
- Formación.

De requisitos mínimos se podría destacar:

- Entrega consumible quince días antes de su finalización.
- Renovación al finalizar la vida por modelos indicados por el fabricante, esto implica que se mantiene la marca de las impresoras.
- En la herramienta de gestión se podrá consultar la documentación de entrega de tintas.
- El adjudicatario debe ser “Servicio Técnico Oficial”.

Se tiene en cuenta un posible aumento del parque de 225 durante la vigencia del contrato (tres años), y de 75 anuales durante la prórroga.

Se propone Métrica V3 para la ejecución del proyecto.

Requiere un Plan de Contingencia y Gestión de Riesgos que lo elaborará el adjudicatario.

Detalles de la herramienta de gestión:

- La validación será solamente por usuario y se podrá cambiar, no indica que sea LDAP u otro sistema centralizado.
- Roles de usuarios diferentes.
- Integrada con LDAP, para definir los diferentes roles.

La monitorización ha de mostrar tanto los contadores de las impresoras como los contadores de la monitorización. A nivel de usuario se obtendrán los contadores a través de lo impreso en la impresora, y no de lo obtenido por el servidor.

Se podrá solicitar a las propuestas con solvencia técnica unos dispositivos y la herramienta de gestión para realizar un piloto para testearlas.

Hacen referencia a “Cláusulas de confidencialidad” citando la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, que han de cumplir frente al Servicio Canario de Salud. También aportará una memoria de las medidas de confidencialidad e integridad de los datos que empleará.

3.2 Portugal

Licitación pública publicada en el diario oficial de la Unión Europea para la adquisición de servicios de soluciones de impresión en régimen de subcontratación para diversas entidades del SNS, en el ámbito de la agregación 2024. (Online, 2023)

Se trata de un contrato de servicios de impresión y copia.

Indica que el prestatario ha de cumplir con la RGPD, pero está enfocado a nivel contractual no a la ejecución del contrato.

También indica que si por alguna circunstancia tiene datos personales estos serán destruidos o devueltos, esto se podría asociar a hojas impresas o documentos pendientes de imprimir en los discos de las impresoras.

Equipos nuevos y una única marca.

4 Contenido del Master y aplicación de la Metodología relacionada

En el contexto del análisis y mejora de los sistemas de impresión centralizados en entornos sanitarios y administrativos pertenecientes a los centros (centros de salud, centros periféricos, centros administrativos y centros hospitalarios) del Sistema Nacional de Salud (SNS), es crucial emplear herramientas y metodologías que permitan una evaluación exhaustiva y la implementación de soluciones efectivas. La metodología COBIT se presenta como la opción adecuada para este propósito, ya que ofrece un marco integral para la gobernanza y gestión de las TIC, alineando los objetivos de TI con los objetivos estratégicos de la organización.

Complementar este análisis con la matriz DAFO permite identificar de manera precisa las fortalezas, debilidades, oportunidades y amenazas que afectan al sistema, asegurando una visión completa y detallada de la situación actual y los posibles escenarios futuros.

Estas metodologías con su enfoque estructurado forman parte del área 4 temática *A2: Gestión Directiva de las TIC en Salud (Lazcano Arranz & Polo Moratilla, 2024)*, aportando el Anexo 3 *(Lazcano Arranz, ANEXO-3 (MATRIZ DAFO)*, 2024) una visión más profundizada de la aplicación de la matriz DAFO., proporciona una base sólida para aplicar teorías avanzadas en la práctica real y en la resolución de problemas complejos en el ámbito de la salud y la tecnología. Constituyen una parte del temario para el Master en Dirección de Sistemas y TIC para la Salud y en Digitalización Sanitaria de la SEIS,

4.1 Marco de Gobernanza TIC con metodología COBIT

La implementación y gestión de dispositivos periféricos en una entidad pública de salud es un tema crítico, especialmente en términos de seguridad, eficiencia y cumplimiento normativo. En este contexto, la metodología COBIT (*ISACA, 2019)* se presenta como un marco eficaz para gobernar y gestionar las Tecnologías de la Información (TI), asegurando que se alineen con los objetivos estratégicos de la organización y cumplan con las regulaciones vigentes, como el GDPR (*Europea, 2016)* y la LOPDGDD (BOE, Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales, 2028).

4.1.1 Objetivos de Gobernanza y Gestión

COBIT (Control Objectives for Information and Related Technologies) es un marco integral para el gobierno y la gestión de TI en organizaciones. Se enfoca en crear un sistema que asegure que la tecnología de la información esté alineada con los objetivos de la organización, contribuya al logro de los objetivos empresariales y mitigue los riesgos tecnológicos.

Aplicación a Dispositivos Periféricos en el Servicio Nacional de Salud (SNS):

- **Alineación con las necesidades empresariales:** El objetivo es asegurar que la infraestructura de TI, incluidas las impresoras, escáneres y otros dispositivos periféricos, soporte de manera efectiva los procesos críticos de la entidad de salud. En el contexto de los dispositivos periféricos deben estar disponibles, ser fiables y seguros para asegurar que el personal pueda realizar sus tareas sin interrupciones, como la impresión de documentos médicos importantes o la digitalización de registros de pacientes.
    - **COBIT APO01 (Gestión de la Estrategia):** Asegurar que la estrategia de TI esté alineada con los objetivos empresariales, integrando la gestión de dispositivos periféricos en la planificación estratégica de TI.
- **Gestión de riesgos:** Buscando cumplir el objetivo de identificar, evaluar y mitigar los riesgos asociados con el uso de dispositivos periféricos, incluyendo riesgos de seguridad, privacidad, y operativos. Más concretamente los riesgos asociados con dispositivos periféricos, como infecciones por malware a través de puertos USB o accesos no autorizados a dispositivos conectados en red, deben ser gestionados proactivamente.

    - **COBIT APO12 (Gestión del Riesgo):** Desarrollar un enfoque sistemático para la gestión de riesgos en torno a dispositivos periféricos, asegurando que se implementen controles adecuados para mitigar estos riesgos.
- **Cumplimiento normativo:** Asegurar que todas las operaciones relacionadas con dispositivos periféricos cumplan con las regulaciones, como GDPR y LOPDGDD. Garantizar que los datos personales procesados por estos dispositivos, como la impresión de historiales médicos o la digitalización de documentos de identificación, estén protegidos conforme a las leyes de privacidad de datos.
    - **COBIT EDM03 (Cumplimiento de Obligaciones Legales y Regulatorias):** Implementar procesos y controles que aseguren que la gestión de dispositivos periféricos esté alineada con las obligaciones legales y regulatorias.

4.1.2 Componentes del Sistema de Gobierno

COBIT estructura la gobernanza de TI en varios componentes fundamentales que ayudan a garantizar un enfoque holístico y efectivo para la gestión de TI.

Procesos: Se basa en el conjunto de actividades secuenciales que transforman entradas en salidas, apoyando el logro de los objetivos empresariales y de TI. Para aplicar a los dispositivos periféricos, se establecen procesos claros para la instalación, configuración, uso, mantenimiento, y desecho de dispositivos periféricos. Esto incluye procesos para la gestión de incidencias, actualizaciones de firmware, y auditorías de seguridad.

- **COBIT DSS01 (Gestión de las Operaciones de TI):** Implementar procesos operativos que aseguren el funcionamiento continuo y seguro de los dispositivos periféricos.

Estructuras organizativas: Nos centramos en la definición de los roles, responsabilidades y relaciones de autoridad dentro de la organización. Quedando claro quién es responsable de la gestión, seguridad, y mantenimiento de los dispositivos periféricos, así como de la conformidad con las normativas.

- **COBIT APO07 (Gestión de Recursos Humanos):** Asegurar que los roles y responsabilidades en torno a la gestión de dispositivos periféricos estén bien definidos y que el personal esté adecuadamente capacitado.

Cultura, ética y comportamiento: Los Factores culturales y de comportamiento que influyen en cómo las TI son utilizadas y gestionadas en la organización. Es correcto fomentar una cultura de seguridad y cumplimiento, donde el personal entienda la importancia de utilizar correctamente los dispositivos periféricos y seguir las políticas de la organización.

- **COBIT APO06 (Gestión de las Comunicaciones):** Desarrollar una cultura organizativa que valore la seguridad y el cumplimiento normativo, asegurando que se comuniquen claramente las expectativas sobre el uso de dispositivos periféricos.

Personas, habilidades y competencias: Capacidad de los empleados para cumplir con las responsabilidades asignadas, respaldados por las habilidades y competencias adecuadas. Aplicado a los dispositivos periféricos, se trata de capacitar al personal en el uso seguro de dispositivos, incluyendo la identificación de amenazas y la respuesta a incidentes.

- **COBIT APO07 (Gestión de Recursos Humanos):** Implementar programas de formación y desarrollo de competencias específicas para la gestión y uso seguro de dispositivos periféricos.

Servicios, infraestructura y aplicaciones: Los activos de TI que soportan la entrega de servicios de TI a la organización. Asegurar que la infraestructura que soporta los dispositivos periféricos esté bien gestionada, segura y actualizada, para soportar las necesidades de la entidad de salud.

- **COBIT BAI09 (Gestión de Activos):** Implementar una gestión de activos efectiva para asegurar que los dispositivos periféricos se mantengan en buen estado y actualizados conforme a las necesidades operativas y de seguridad.

Políticas y procedimientos: Conjunto de directrices y métodos establecidos para garantizar que los procesos y actividades de TI se ejecuten de manera consistente y efectiva. Desarrollar políticas que regulen el uso, acceso y mantenimiento de dispositivos periféricos, y procedimientos para garantizar que se sigan estas políticas.

- **COBIT APO01 (Gestión de la Estrategia):** Desarrollar y mantener políticas que alineen la gestión de dispositivos periféricos con los objetivos estratégicos y normativos de la entidad.

El marco de COBIT ofrece un enfoque estructurado y completo para la gobernanza y gestión de TI, proporcionando directrices que aseguran que los dispositivos periféricos, ya sean conectados directamente o en red, se gestionen de manera que apoyen los objetivos estratégicos, mitiguen los riesgos y aseguren el cumplimiento normativo. Este enfoque permite a la entidad pública de salud no solo optimizar el uso de sus recursos tecnológicos, sino también proteger la información sensible y cumplir con las regulaciones aplicables.

4.1.3 Análisis de Amenazas y Debilidades

El análisis de amenazas y debilidades en un entorno donde los dispositivos periféricos están conectados de diversas maneras es fundamental para entender los riesgos que enfrenta una organización. En una entidad pública de salud, donde la protección de datos sensibles es crucial, estos riesgos adquieren una importancia aún mayor. Entraremos en un contexto más profundo con el análisis mediante la herramienta de matriz DAFO.

4.1.3.1 Conexión Directa de Dispositivos Periféricos

Los dispositivos periféricos conectados directamente a los puestos de trabajo, ya sea mediante USB, cables paralelos u otras interfaces directas, presentan tanto ventajas operativas como riesgos significativos en términos de seguridad y gestión.

Debilidades

- **Inseguridad física y acceso no controlado:**
  - **Riesgo:** Los puertos USB y otras interfaces físicas son puntos de entrada que pueden ser explotados para inyectar malware, robar información o manipular datos.
  - **Debilidad:** La ausencia de controles físicos y lógicos robustos permite que cualquier persona con acceso físico al equipo conecte dispositivos externos no autorizados, como pendrives infectados con malware.
  - **Impacto:** Esto puede llevar a la introducción de software malicioso en la red de la entidad, comprometiendo datos sensibles como historiales médicos.
- **Falta de monitoreo y control centralizado:**
  - **Riesgo:** La dificultad de monitorear y gestionar dispositivos conectados directamente dificulta la implementación de políticas de seguridad centralizadas.
  - **Debilidad:** Cada dispositivo conectado directamente actúa de manera independiente, lo que significa que las medidas de seguridad y las actualizaciones de software deben aplicarse individualmente, aumentando la carga administrativa y el riesgo de errores.
  - **Impacto:** La falta de actualizaciones puede dejar vulnerabilidades explotables, permitiendo que los dispositivos sean objetivos fáciles para ciberataques.
- **Riesgo de pérdida o robo de información:**
  - **Riesgo:** La información procesada a través de dispositivos conectados directamente, como impresoras o escáneres, puede ser fácilmente accesible y susceptible de ser robada si no se aplican las medidas de seguridad adecuadas.
  - **Debilidad:** La falta de cifrado y otras protecciones de datos en estos dispositivos facilita el acceso no autorizado a información confidencial.
  - **Impacto:** Puede haber fugas de datos sensibles que violen las normativas GDPR y LOPDGDD, exponiendo a la entidad a sanciones legales y daños reputacionales.

Amenazas

- **Infección por malware a través de dispositivos USB:**
  - **Descripción:** Un atacante puede utilizar un dispositivo USB infectado para introducir malware en la red interna de la entidad. Este tipo de ataque es particularmente efectivo en entornos donde no se utilizan políticas estrictas de control de dispositivos.
  - **Ejemplo:** Un USB con malware puede activar un ransomware que cifre los datos del paciente, impidiendo su acceso hasta que se pague un rescate.
- **Ingeniería social y ataques de insiders:**
  - **Descripción:** Los empleados, por desconocimiento o malicia, podrían conectar dispositivos no autorizados, comprometiendo la seguridad de la red.
  - **Ejemplo:** Un empleado podría ser engañado para que conecte un USB aparentemente inofensivo pero que contenga malware, o un insider malintencionado podría robar datos utilizando dispositivos conectados directamente.
- **Ataques a través de dispositivos abandonados u olvidados:**
  - **Descripción:** Dispositivos como impresoras multifuncionales pueden contener información en sus memorias internas. Un atacante que obtenga acceso físico podría extraer información crítica.
  - **Ejemplo:** Una impresora que retiene copias digitales de documentos impresos podría ser robada o accedida para extraer datos confidenciales.

4.1.3.2 Dispositivos Conectados en Red

Cuando los dispositivos periféricos están conectados a la red y son accesibles por múltiples usuarios, se presentan tanto oportunidades para una mejor gestión como nuevas amenazas y vulnerabilidades.

Debilidades

- **Exposición a ataques de red:**
  - **Riesgo:** Los dispositivos conectados a la red, si no están debidamente asegurados, pueden ser atacados desde cualquier punto de la red, tanto interna como externamente.
  - **Debilidad:** La falta de segmentación de la red y de configuraciones de seguridad robustas en los dispositivos periféricos puede facilitar ataques como denegación de servicio (DDoS) o explotación de vulnerabilidades conocidas en firmware.
  - **Impacto:** Un ataque exitoso podría deshabilitar dispositivos críticos como impresoras o escáneres, interrumpiendo operaciones esenciales y comprometiendo la seguridad de la red.
- **Acceso no autorizado:**
  - **Riesgo:** Cuando los dispositivos periféricos están disponibles para todos los usuarios de la red, se incrementa el riesgo de accesos no autorizados.
  - **Debilidad:** La falta de controles de accesos específicos y autenticación robusta permite que cualquier usuario dentro de la red acceda a los dispositivos, pudiendo alterar, copiar o eliminar información sensible.
  - **Impacto:** Accesos no autorizados pueden llevar a la modificación o destrucción de datos importantes, así como a la filtración de información confidencial.
- **Dificultad en la gestión y aplicación de políticas de seguridad:**
  - **Riesgo:** La diversidad de dispositivos y la variedad de modelos y configuraciones hacen difícil la aplicación uniforme de políticas de seguridad.
  - **Debilidad:** Las inconsistencias en la aplicación de parches de seguridad, actualizaciones de firmware y configuraciones de seguridad pueden dejar algunas unidades vulnerables.
  - **Impacto:** La existencia de dispositivos no actualizados o mal configurados en la red aumenta la probabilidad de que un atacante explote una vulnerabilidad para ganar acceso no autorizado.

Amenazas

- **Ataques de denegación de servicio (DDoS):**
  - **Descripción:** Los dispositivos periféricos conectados a la red pueden ser objetivo de ataques de denegación de servicio que los inhabiliten o los sobrecarguen, impidiendo su uso.
  - **Ejemplo:** Un ataque DDoS dirigido a impresoras en red podría saturar su capacidad, impidiendo la impresión de documentos críticos en momentos importantes.
- **Explotación de vulnerabilidades en firmware:**
  - **Descripción:** Los dispositivos periféricos suelen utilizar firmware que, si no se actualiza regularmente, puede contener vulnerabilidades explotables.
  - **Ejemplo:** Un atacante podría utilizar una vulnerabilidad en el firmware de una impresora para ejecutar código malicioso en la red interna, comprometiendo la seguridad del sistema.
- **Intercepción de comunicaciones en la red:**
  - **Descripción:** Si la comunicación entre dispositivos periféricos y otros equipos de la red no está cifrada, un atacante podría interceptar estos datos.
  - **Ejemplo:** La interceptación de datos no cifrados durante la transferencia de documentos entre un ordenador y una impresora podría resultar en la exposición de información sensible de pacientes.

4.1.3.3 Medidas Mitigadoras

Para abordar las amenazas y debilidades mencionadas, es crucial implementar medidas de seguridad y gestión que incluyan:

- **Segmentación de red:** Separar los dispositivos periféricos en subredes específicas con reglas de acceso estrictas para limitar la exposición y prevenir la propagación de ataques.
- **Control de acceso:** Implementar autenticación multifactor y listas de control de acceso para asegurar que solo usuarios autorizados puedan utilizar ciertos dispositivos.
- **Actualización y parcheo regular:** Asegurar que todos los dispositivos, tanto conectados directamente como en red, reciban actualizaciones de seguridad y parches de firmware de manera oportuna.
- **Monitoreo y auditoría:** Establecer un sistema de monitoreo continuo y auditorías regulares para detectar y responder a actividades sospechosas.

El análisis de amenazas y debilidades revela los riesgos significativos que enfrentan las entidades de salud al gestionar dispositivos periféricos. Estas amenazas pueden comprometer tanto la seguridad de la red como la integridad y confidencialidad de la información manejada. Por ello, es esencial aplicar controles robustos que mitiguen estos riesgos, alineando las prácticas de gestión con marcos de gobernanza de TI como COBIT, para asegurar una operación segura, eficiente y conforme con la normativa aplicable.

4.1.4 Fortalezas en la Configuración de Dispositivos

La configuración de dispositivos periféricos (impresoras, escáneres, etc.), cuando se realiza de manera óptima, siguiendo las directrices de COBIT, ofrece una serie de fortalezas significativas que refuerzan la seguridad, eficiencia, y cumplimiento normativo en la entidad de salud.

4.1.4.1 Alineación con los Objetivos de Negocio

COBIT enfatiza la alineación entre la gestión de TI y los objetivos empresariales. En el contexto de una entidad pública de salud, esto significa que la configuración de los dispositivos periféricos debe apoyar la misión central de la entidad, que es proporcionar atención médica eficiente y segura, respetando la privacidad de los pacientes y cumpliendo con las regulaciones pertinentes.

Optimización de Recursos y Procesos:

- **Descripción:** La correcta configuración de los dispositivos periféricos, basada en los principios de COBIT, asegura que estos dispositivos funcionen de manera eficiente, minimizando tiempos de inactividad y mejorando el flujo de trabajo en la organización.
- **Impacto:** Los recursos tecnológicos son utilizados de manera óptima, reduciendo costos operativos y mejorando la eficiencia en el manejo de documentos médicos, con un impacto positivo directo en la calidad de la atención al paciente.

Mejor Control y Gestión de TI:

- **Descripción:** COBIT promueve el uso de procesos bien definidos y controles efectivos que faciliten la gestión de TI. Esto incluye la implementación de políticas para la configuración y uso de dispositivos periféricos.
- **Impacto:** La entidad puede gestionar estos dispositivos de forma centralizada, asegurando que se cumplan las políticas de seguridad, lo que reduce la posibilidad de errores humanos y mejora la capacidad de respuesta ante incidentes de seguridad.

4.1.4.2 Cumplimiento Normativo y Gestión de Riesgos

El cumplimiento de normativas descritas en *2.Marco Legal*, como por ejemplo el GDPR y la LOPDGDD, es crítico en cualquier entidad que maneje datos sensibles. COBIT proporciona un marco para asegurarse de que los controles y procesos estén alineados con las regulaciones aplicables, mitigando riesgos legales y de seguridad.

Cumplimiento Normativo Eficiente:

- **Descripción:** Implementar controles y auditorías basadas en COBIT asegura que los dispositivos periféricos cumplan con las normativas de protección de datos, lo que incluye el cifrado de datos sensibles y la restricción de acceso.
- **Impacto:** Se reduce el riesgo de sanciones legales y se mejora la confianza de los pacientes al saber que su información está protegida conforme a las leyes.

Gestión Eficaz del Riesgo:

- **Descripción:** COBIT permite a las organizaciones identificar y gestionar riesgos asociados con la tecnología, incluyendo aquellos relacionados con dispositivos periféricos, como amenazas de malware o accesos no autorizados.
- **Impacto:** Al implementar prácticas de gestión de riesgos, la entidad minimiza la probabilidad de incidentes de seguridad y sus posibles consecuencias, protegiendo la integridad de la red y los datos que maneja.

4.1.4.3 Control Centralizado y Monitoreo Continuo

El marco de COBIT promueve la implementación de un control centralizado para la gestión de TI, lo que facilita el monitoreo continuo y la administración eficiente de dispositivos periféricos.

Control Centralizado:

- **Descripción:** Centralizar el control de los dispositivos periféricos permite aplicar configuraciones uniformes y actualizaciones de seguridad de manera simultánea en toda la organización.
- **Impacto:** Esto reduce la complejidad operativa, asegurando que todos los dispositivos estén alineados con las políticas de seguridad y estén actualizados con los últimos parches y configuraciones, lo que reduce significativamente las vulnerabilidades.

Monitoreo y Auditoría Eficientes:

- **Descripción:** COBIT promueve el uso de herramientas de monitoreo y auditoría para rastrear el uso y el estado de los dispositivos periféricos en tiempo real.

- **Impacto:** El monitoreo continuo permite a la entidad detectar y responder rápidamente a cualquier anomalía o intento de intrusión, mejorando la seguridad global de la infraestructura de TI.

4.1.4.4 Flexibilidad y Adaptabilidad

La metodología COBIT es suficientemente flexible para adaptarse a diferentes tipos de configuraciones y entornos operativos, lo que permite a las organizaciones ajustar sus prácticas de TI según las necesidades cambiantes.

Adaptabilidad a Cambios Tecnológicos y Regulatorios:

- **Descripción:** COBIT facilita la implementación de cambios en la infraestructura de TI para cumplir con nuevas regulaciones o para adoptar nuevas tecnologías sin comprometer la seguridad ni la eficiencia operativa.
- **Impacto:** La entidad puede evolucionar su infraestructura de dispositivos periféricos sin incurrir en riesgos significativos o en incumplimientos regulatorios, manteniendo siempre un entorno seguro y conforme.

Escalabilidad de Soluciones:

- **Descripción:** La implementación de COBIT permite escalar la infraestructura de dispositivos periféricos de manera controlada, asegurando que las políticas y procedimientos se mantengan efectivos a medida que la organización crece.
- **Impacto:** La entidad puede expandir sus operaciones o incorporar nuevos dispositivos sin perder el control sobre la seguridad y la eficiencia de sus procesos

El uso de COBIT en la configuración y gestión de dispositivos periféricos para el Servicio Nacional de Salud (SNS) ofrece una serie de fortalezas que mejoran significativamente la seguridad, el cumplimiento normativo, la eficiencia operativa, y la capacidad de adaptación a cambios futuros. Al aplicar las mejores prácticas de COBIT, la entidad no solo optimiza la utilización de sus recursos tecnológicos, sino que también fortalece su capacidad para proteger datos sensibles y responder a las amenazas de seguridad, garantizando al mismo tiempo el cumplimiento de todas las normativas relevantes. Esto convierte a COBIT en una herramienta indispensable para la gestión efectiva y segura de la infraestructura de TI en el ámbito de la salud.

4.1.5 Aplicación de COBIT a la Gestión de Dispositivos Periféricos

La aplicación de COBIT a la gestión de dispositivos periféricos implica una alineación entre los objetivos de negocio y TI, asegurando que la infraestructura tecnológica no solo soporte, sino que también potencie la misión y los objetivos del Servicio Nacional de Salud (SNS). Esto se logra mediante la implementación de controles y procesos que garantizan la seguridad, eficiencia, cumplimiento normativo y adaptabilidad de la infraestructura de TI.

4.1.5.1 Identificación y Alineación de Objetivos

El primer paso en la aplicación de COBIT es identificar y alinear los objetivos estratégicos de la entidad con los objetivos de TI. En el caso del Servicio Nacional de Salud (SNS), al tratarse de una entidad pública salud, los objetivos clave podrían incluir:

- **Protección de Datos Sensibles:** Garantizar que los datos de los pacientes y otros datos confidenciales estén protegidos contra accesos no autorizados y filtraciones.
- **Cumplimiento Normativo:** Asegurar que la gestión de dispositivos periféricos cumpla con las regulaciones descritas en *2.Marco Legal*.
- **Continuidad del Servicio:** Asegurar que los dispositivos periféricos, como impresoras y escáneres, estén siempre disponibles y operativos, minimizando las interrupciones en el servicio.

Aplicación de COBIT

COBIT 5 y COBIT 2019 proporcionan un marco para la alineación de los objetivos de TI con los objetivos de negocio, utilizando cascadas de objetivos que permiten identificar cómo las TI pueden contribuir directamente al éxito de la organización.

Ejemplo: Se pueden establecer objetivos específicos para la seguridad de los datos, la disponibilidad del servicio y el cumplimiento normativo, que guíen la gestión de los dispositivos periféricos dentro de la entidad.

4.1.5.2 Establecimiento de Políticas y Controles

Una vez alineados los objetivos, COBIT sugiere la creación de políticas y controles que aseguren que los procesos y recursos de TI estén alineados con esos objetivos.

Aplicación de COBIT

- **Políticas de Seguridad:** COBIT recomienda la creación de políticas claras y específicas para la gestión de dispositivos periféricos. Estas políticas deberían incluir el control de acceso, el cifrado de datos, y el monitoreo continuo de los dispositivos.
- **Controles de Acceso:** Implementar controles de acceso estrictos para asegurar que solo el personal autorizado pueda acceder a los dispositivos periféricos y a la información que procesan. Esto incluye autenticación multifactor y listas de control de acceso (ACL).
- **Actualización y Parches de Seguridad:** COBIT enfatiza la importancia de mantener actualizados todos los dispositivos periféricos con los últimos parches y actualizaciones de firmware para mitigar vulnerabilidades.

Ejemplo: Establecer políticas que regulen el uso de dispositivos USB, imponiendo restricciones sobre qué tipos de dispositivos pueden conectarse a los sistemas y cómo se deben manejar los datos transferidos a través de ellos.

4.1.5.3 Implementación de Procesos de Gestión y Control

COBIT define una serie de dominios y procesos que son esenciales para la gestión de TI. La implementación de estos procesos asegura que los dispositivos periféricos sean gestionados de manera segura y eficiente.

Aplicación de COBIT

- **Procesos de Entrega, Servicio y Soporte (DSS):** Este dominio incluye la gestión de la continuidad, la seguridad de la información, y la gestión de los servicios de TI. En el contexto de dispositivos periféricos, esto significa asegurarse de que los dispositivos estén disponibles y protegidos contra fallas o ataques.
- **Proceso de Gestión de la Continuidad (DSS04):** Asegurar la disponibilidad continua de dispositivos críticos para la operación de la entidad de salud, implementando planes de recuperación y contingencia.
- **Proceso de Gestión de la Seguridad (DSS05):** Implementar medidas de seguridad que incluyan la protección de datos, control de acceso, y monitoreo de dispositivos periféricos, para prevenir el acceso no autorizado y el uso indebido.

Ejemplo: Establecer un proceso regular de auditoría y monitoreo que supervise la actividad de los dispositivos periféricos, detectando cualquier anomalía o intento de acceso no autorizado.

4.1.5.4 Monitoreo y Evaluación del Desempeño

COBIT recomienda la implementación de un sistema de monitoreo y evaluación continua del desempeño de TI para asegurar que los controles y procesos implementados están funcionando como se espera y cumpliendo con los objetivos de la organización.

Aplicación de COBIT

- **Monitoreo Continuo:** COBIT sugiere el uso de herramientas de monitoreo continuo para rastrear el rendimiento y la seguridad de los dispositivos periféricos. Esto permite la detección temprana de problemas y la respuesta rápida a incidentes.
- **Evaluación del Cumplimiento:** Evaluar regularmente el cumplimiento de las políticas y controles implementados, asegurándose de que se cumplan los requisitos de seguridad y normativos.
- **Medición del Desempeño:** Utilizar métricas y KPI para evaluar la eficacia de la gestión de dispositivos periféricos. Esto podría incluir la frecuencia de incidentes de seguridad, el tiempo de inactividad de los dispositivos, y el nivel de cumplimiento normativo.

Ejemplo: Implementar un tablero de control que muestre en tiempo real el estado de los dispositivos periféricos, alertando sobre cualquier fallo o intento de acceso no autorizado.

4.1.5.5 Mejora Continua y Adaptabilidad

COBIT enfatiza la mejora continua como parte del ciclo de vida de la gestión de TI. Esto es esencial en un entorno en constante evolución, como es el caso del Servicio Nacional de Salud (SNS), donde las amenazas y los requisitos normativos cambian con el tiempo.

Aplicación de COBIT

- **Evaluación y Revisión Periódica:** Establecer revisiones periódicas de los procesos y controles de gestión de dispositivos periféricos para identificar áreas de mejora y adaptarse a nuevos riesgos o requisitos normativos.
- **Mejora Continua:** Aplicar un enfoque de mejora continua para actualizar las políticas y procedimientos de gestión de dispositivos periféricos, adaptándolos a nuevas tecnologías, amenazas emergentes, y cambios en las regulaciones.

Ejemplo: Implementar un proceso de revisión anual que evalúe el desempeño de los dispositivos periféricos y los procesos de gestión, utilizando los hallazgos para actualizar políticas y mejorar la seguridad.

4.1.6 Conclusión

La aplicación de COBIT a la gestión de dispositivos periféricos en una entidad pública de salud proporciona un marco robusto y estructurado que garantiza la seguridad, eficiencia, y cumplimiento normativo. Al utilizar COBIT, la entidad puede alinear sus objetivos de TI con los objetivos de negocio, implementar controles efectivos, gestionar riesgos, y asegurar un monitoreo continuo. Además, la metodología de COBIT fomenta la mejora continua, permitiendo a la organización adaptarse a los cambios tecnológicos y normativos, manteniendo siempre un entorno seguro y conforme. Esto no solo protege la infraestructura de TI, sino que también refuerza la confianza de los pacientes y cumple con las obligaciones legales y regulatorias.

Después de analizar en detalle la aplicación de la metodología COBIT en la gestión de dispositivos periféricos dentro de una entidad pública de salud, se pueden extraer varias conclusiones clave sobre su efectividad y los beneficios que aporta a la gobernanza de las TIC en este contexto.

4.1.6.1 Alineación Estratégica y Objetivos de Negocio

COBIT permite una alineación clara entre los objetivos estratégicos de la entidad de salud y los objetivos de TI. Esto asegura que la infraestructura tecnológica, incluidas las configuraciones de dispositivos periféricos, está directamente enfocada en apoyar la misión de la entidad: proporcionar atención médica de calidad y proteger la privacidad de los pacientes. La alineación de objetivos permite que todas las acciones y recursos en TI contribuyan directamente al éxito de la organización, mejorando la eficiencia operativa y la satisfacción del paciente.

4.1.6.2 Fortalecimiento de la Seguridad y Cumplimiento Normativo

COBIT proporciona un marco sólido para establecer políticas de seguridad, controles de acceso, y procesos de gestión de riesgos que son esenciales para proteger la información sensible en un entorno de salud. En este escenario, donde se maneja información de pacientes que está sujeta a estrictas regulaciones descritas en el apartado ***2.Marco Legal***, como el GDPR y la LOPDGDD, COBIT garantiza que los dispositivos periféricos estén configurados y operados de manera que cumplan con estos requisitos legales. Esto no solo reduce el riesgo de sanciones, sino que también refuerza la confianza de los pacientes en la entidad.

4.1.6.3 Eficiencia Operativa y Optimización de Recursos

La aplicación de COBIT mejora la eficiencia operativa mediante la optimización del uso de los dispositivos periféricos y la reducción de tiempos de inactividad. Gracias a los procesos de monitoreo y control establecidos por COBIT, la entidad puede asegurar la disponibilidad continua de estos dispositivos, minimizando interrupciones en los servicios de salud y mejorando la productividad general. Además, la centralización y estandarización de la gestión de estos dispositivos permite un uso más eficiente de los recursos tecnológicos.

4.1.6.4 Mejora Continua y Adaptabilidad

COBIT enfatiza la importancia de la mejora continua y la adaptabilidad en la gestión de TI. En un entorno de salud en constante evolución, la capacidad de adaptarse a nuevos desafíos, como amenazas emergentes o cambios en la regulación, es fundamental. COBIT proporciona las herramientas necesarias para evaluar y mejorar constantemente los procesos y controles, asegurando que la entidad esté siempre preparada para enfrentar nuevos riesgos y oportunidades.

4.1.6.5 Gobernanza Efectiva y Responsabilidad

La metodología COBIT establece un marco claro para la gobernanza de TI, asignando responsabilidades y estableciendo procesos de auditoría y monitoreo que aseguran la transparencia y la rendición de cuentas. En el contexto de una entidad pública de salud, donde la responsabilidad ante los ciudadanos y los reguladores es crucial, COBIT ayuda a garantizar que las decisiones relacionadas con TI estén bien fundamentadas y que se cumplan los objetivos de gobernanza.

4.2 El Método DAFO como herramienta de análisis.

4.2.1 Definición

El análisis DAFO (también conocido como matriz DAFO o análisis FODA) es una metodología que nos permite explorar la situación de una empresa o proyecto. Se basa en evaluar elementos internos (como fortalezas y debilidades) y externos (como oportunidades y amenazas). Aunque pueda parecernos complejo, en realidad es bastante sencillo de llevar a cabo.

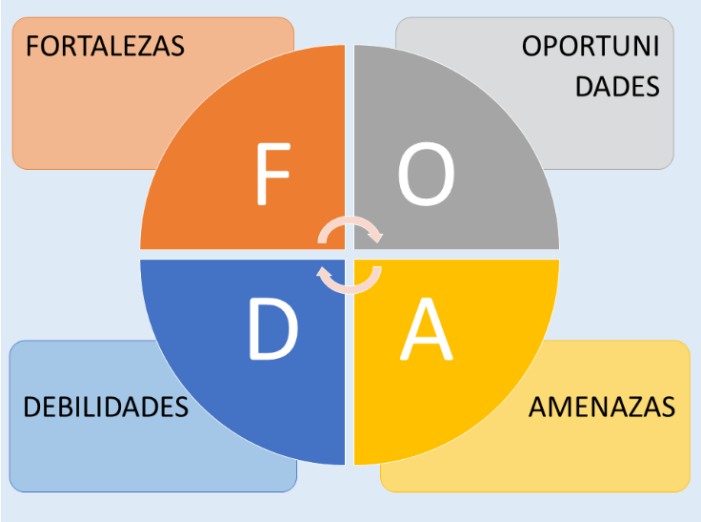


Ilustración 1. Matriz DAFO o FODA

El análisis DAFO tiene sus raíces en la década de 1960, cuando fue desarrollado en el Stanford Research Institute. Este responde al acrónimo de los cuatro elementos que se evalúan en el desarrollo del análisis: Debilidades, Amenazas, Fortalezas y Oportunidades, o SWOT en su acepción original (Strenghts, Weaknesses, Oportunities and Threats) (Lazcano Arranz, ANEXO-3 (MATRIZ DAFO), 2024). Su objetivo era evaluar los factores que afectan a una organización, tanto desde su interior como desde el entorno externo.

¿Para qué sirve? Este análisis te ayuda a:

- Analizar las debilidades internas que necesitan mejoras.
- Identificar las fortalezas internas que funcionan bien.
- Prever las amenazas externas que podrían afectar tu proyecto o negocio.
- Reconocer las oportunidades externas que puedes aprovechar.

En resumen, el análisis DAFO es como una brújula estratégica que te guía en el vasto territorio empresarial, permitiéndote tomar decisiones informadas y diseñar estrategias audaces. Es una herramienta viva, que debe mantenerse en constante actualización, con objeto de adaptar en cada momento la planificación estratégica de la empresa o sector.

4.2.2 Análisis interno

Una revisión hacia el interior de los sistemas de impresión y digitalización va a arrojar como resultados las debilidades y las amenazadas, junto con las oportunidades en el presente, en donde:

4.2.2.1 Debilidades y amenazas de seguridad

El uso de dispositivos periféricos conectados vía USB o compartidos vía red interna (LAN) para los usuarios, sin un control adecuado en los servicios de salud públicos representa importantes debilidades en términos de seguridad de la información. Además, estas prácticas podrían estar en incumplimiento de varios artículos clave descritos en *2.Marco Legal*, poniendo a la organización en riesgo de sanciones legales y pérdida de reputación.

4.2.2.1.1 Escenario de conexión directa (vía USB, cable en serial o paralelo)

- **Falta de control y supervisión:** Al conectar dispositivos USB directamente a los puestos de los usuarios, existe una falta de control centralizado. Esto dificulta la gestión, monitoreo y protección de la información que se maneja a través de estos dispositivos.
- **Ausencia de Cifrado:** Los datos transferidos entre los dispositivos periféricos y los equipos podrían no estar cifrados, lo que aumenta el riesgo de acceso no autorizado en caso de pérdida o robo de un dispositivo.
- **Dependencia del Equipo Compartido:** La conexión a dispositivos en modo compartido a través de otros puestos genera un punto único de fallos, ya que sí este puesto se apaga, se desconecta de la red o sufre algún tipo de fallo, todos los usuarios pierden el acceso al dispositivo compartido, lo que puede afectar la productividad y causar interrupciones en las operaciones. El uso compartido también puede ocasionar un rendimiento reducido, el dispositivo puede verse afectado si múltiples usuarios intentan acceder a él simultáneamente, especialmente si el PC que lo comparte no tiene la capacidad suficiente para manejar múltiples solicitudes de manera eficiente.
- **Exposición a Ataques Internos:** Un acceso no autorizado al compartir los dispositivos como recursos de un PC, cualquier usuario en la red con permisos puede acceder a estos recursos. Esto puede llevar a un uso indebido o acceso no autorizado a la información que se procesa o almacena en estos dispositivos.

4.2.2.1.2 Escenario de conexión LAN interna

- **Exposición a Ataques Internos:** El acceso no autorizado a la hora de compartir los dispositivos como recursos de un PC, cualquier usuario en la red con permisos puede acceder a estos recursos. Esto puede llevar a un uso indebido o acceso no autorizado a la información que se procesa o almacena en estos dispositivos. Se muestra una accesibilidad generalizada cuando un dispositivo es visible en toda la red, cualquier usuario con acceso a la red puede intentar conectarse al dispositivo, lo que amplía significativamente la superficie de ataque. Esto incluye no solo personal autorizado, sino también posibles atacantes internos o personas que accidentalmente accedan al dispositivo.
- **Exposición de Datos Sensibles:** La fuga de información deja que los documentos impresos o digitalizados pueden ser visibles para otros usuarios de la red, lo que aumenta el riesgo de exposición de datos sensibles, como información médica confidencial, datos personales, o información clasificada. Para el tráfico no cifrado cuando las comunicaciones entre los dispositivos y los equipos no están cifradas, queda expuesto a un atacante en la misma red podría interceptar datos sensibles durante la transmisión, comprometiendo la confidencialidad de la información.
- **Complejidad en la Gestión de Permisos**
    - **Gestión Inadecuada de Accesos:** Si no se configuran adecuadamente los permisos de acceso, usuarios no autorizados podrían tener acceso a estos dispositivos, lo que incrementa el riesgo de uso indebido. La gestión de permisos a nivel de PC compartido puede ser compleja y propensa a errores, lo que facilita el acceso no deseado.

  - **Uso Descontrolado:** Los dispositivos conectados a la red y visibles para todos pueden ser utilizados de manera indiscriminada, lo que puede llevar a una falta de trazabilidad sobre quién está utilizando los dispositivos y para qué fines. Esto dificulta la auditoría y el cumplimiento de políticas de seguridad.
  - **Colas de Impresión no Seguras:** Los trabajos de impresión o digitalización pueden quedar en las colas accesibles para cualquier usuario, lo que permite que documentos sensibles sean recuperados por personas no autorizadas.
- **Sobrecarga de Red y Dispositivos**
  - **Congestión de Recursos:** Con múltiples usuarios accediendo simultáneamente a un dispositivo, tanto la red como el dispositivo pueden sobrecargarse, lo que afecta la eficiencia operativa y podría llevar a fallos o ralentizaciones.
  - **Deterioro del Rendimiento:** Los dispositivos pueden no estar diseñados para manejar grandes volúmenes de solicitudes concurrentes, lo que podría reducir su vida útil o aumentar los costos de mantenimiento.
- **Configuración Incorrecta o Vulnerable:** Configurar correctamente un dispositivo para que sea visible y accesible de manera segura en toda la red es complejo. Errores en esta configuración pueden abrir brechas de seguridad, como accesos no autorizados o exposición de la interfaz de administración del dispositivo.

Cuando los dispositivos periféricos son compartidos en la red, ya sea como un recurso de PC o como dispositivos conectados directamente a la red interna del centro, se introducen varias amenazas y debilidades que pueden comprometer la seguridad de la información y la operatividad. Estas amenazas incluyen la exposición a accesos no autorizados, intercepción de datos, dependencias de un solo punto de fallo y la dificultad en la gestión adecuada de permisos. Para mitigar estos riesgos, es crucial implementar controles de acceso estrictos, cifrar las comunicaciones, mantener los dispositivos actualizados y segmentar la red para limitar la exposición y el impacto potencial de un ataque.

4.2.2.2 Fortalezas

Aunque el escenario planteado para este servicio donde los dispositivos periféricos de impresión y digitalización puede estar conectados de forma directa (vía USB, cable paralelo,…) o en red LAN a los puestos de los usuarios presenta diversas debilidades, también se pueden identificar algunas fortalezas centradas principalmente en la eficiencia operativa, la facilidad de gestión y el control centralizado:

- **Facilidad de Uso y Acceso Directo**
  - **Conectividad Directa:** La conexión directa de los dispositivos vía USB permite a los usuarios acceder fácilmente a impresoras y escáneres, lo que puede mejorar la productividad al reducir el tiempo y esfuerzo necesarios para realizar tareas de impresión y digitalización.
  - **Simplitud en la Instalación y Configuración:** Los dispositivos USB suelen ser "plug-and-play", es decir, son fáciles de instalar y configurar, lo que simplifica la administración técnica y reduce el tiempo de inactividad en caso de que se necesite reemplazar o actualizar un dispositivo.
  - **Acceso Remoto:** Los usuarios pueden acceder a los dispositivos desde cualquier punto de la red, lo que es especialmente útil en grandes organizaciones o en entornos donde el personal se mueve entre diferentes ubicaciones dentro del centro.
  - **Disponibilidad para Todos los Usuarios:** Todos los usuarios de la red tienen acceso a los recursos compartidos, lo que facilita la colaboración y el flujo de trabajo.
- **Independencia de la Red**
  - **Reducción de Cargas en la Red:** Al no depender de la red para funcionar, estos dispositivos no generan tráfico adicional en la infraestructura de red, lo que puede reducir la congestión y mejorar el rendimiento general de la red para otras aplicaciones críticas.
  - **Funcionamiento Offline:** En caso de que la red sufra una caída, los dispositivos USB aún pueden funcionar localmente, lo que permite la continuidad de algunas operaciones esenciales sin depender del estado de la red.

- **Control Localizado**
    - **Gestión Local de Dispositivos:** En entornos donde cada usuario tiene un puesto asignado y trabaja con información sensible específica, la conexión directa vía USB puede proporcionar un control más localizado de los dispositivos, reduciendo la posibilidad de que los dispositivos sean compartidos sin autorización entre diferentes usuarios o departamentos.
    - **Uso por Personal Capacitado:** Al tener los dispositivos periféricos directamente asociados a un puesto de trabajo, se puede asumir que sólo personal capacitado tiene acceso a estos, lo que podría reducir errores humanos o usos indebidos.
- **Gestión Centralizada**
    - **Gestión de Configuraciones:** Al tener los dispositivos conectados a la red, la administración puede centralizar la configuración, actualizaciones de firmware, y políticas de seguridad desde un único punto, lo que reduce la complejidad y el riesgo de configuraciones incorrectas.
    - **Monitoreo Centralizado:** Los administradores pueden monitorear el uso de los dispositivos, detectar problemas rápidamente y ajustar configuraciones o permisos sin necesidad de acceder físicamente a cada dispositivo.
    - **Aplicación de Políticas de Acceso:** Se pueden establecer políticas de acceso basadas en roles o departamentos, limitando el uso de los dispositivos a usuarios autorizados. Esto ayuda a mantener la seguridad de la información y a cumplir con regulaciones de protección de datos.
    - **Auditoría y Registro de Actividades:** Al centralizar el uso de los dispositivos, se puede registrar y auditar las actividades relacionadas con la impresión y digitalización, lo que es crucial para el cumplimiento normativo y para investigar incidentes de seguridad.
    - **Acceso Simultáneo:** Múltiples usuarios pueden acceder a los mismos dispositivos, lo que facilita el trabajo en equipo y permite una colaboración más fluida, especialmente en entornos donde se manejan grandes volúmenes de documentos.
    - **Flujo de Trabajo Optimizado:** La posibilidad de que varios usuarios envíen trabajos de impresión o digitalización al mismo dispositivo sin tener que transferir físicamente documentos promueve un flujo de trabajo más rápido y eficiente.
- **Coste Reducido**
    - **Menores Costes de Infraestructura:** No se requiere una infraestructura de red sofisticada o especializada para la conexión y el uso de estos dispositivos. Esto puede reducir los costos asociados con la implementación y mantenimiento de sistemas de impresión y digitalización centralizados o en red.
    - **Ahorro en Mantenimiento:** Los dispositivos conectados de forma directa son generalmente menos costosos de mantener que sus contrapartes de red, y las fallas en un dispositivo no afectan a otros, lo que puede reducir los costes de soporte técnico y mantenimiento.
    - **Menos Puntos de Fallo:** Al reducir la cantidad de dispositivos individuales y centralizar su gestión, los costos de mantenimiento y soporte técnico se reducen, ya que hay menos equipos que necesitan atención directa.
    - **Reducción en Costos de Energía:** Compartir dispositivos en lugar de tener múltiples dispositivos individuales puede llevar a un uso más eficiente de la energía, reduciendo el consumo general y, por tanto, los costos operativos.
    - **Menos Espacio Necesario:** Centralizar los dispositivos compartidos en áreas comunes o servidores de red permite liberar espacio en los puestos de trabajo individuales, optimizando el uso del espacio físico en la organización.
- **Mayor Disponibilidad de Dispositivos:** El acceso inmediato de los usuarios a los dispositivos periféricos sin necesidad de gestionar colas de impresión en servidores centralizados, lo que puede mejorar la eficiencia en tareas que requieren resultados rápidos, como la impresión de documentos médicos urgentes.

- **Segmentación de Riesgos:** Mostrando un aislamiento de fallos, en caso de que un dispositivo periférico falle o se comprometa, el impacto está limitado al puesto de trabajo específico, sin afectar a otros usuarios o sistemas conectados a la red.

Las fortalezas de este entorno radican principalmente en la simplicidad operativa, la facilidad de uso, la independencia de la red y el control localizado que permite la conectividad USB directa. Aunque hay riesgos asociados que deben ser gestionados, estas características pueden proporcionar beneficios en términos de eficiencia, coste y resiliencia operativa en contextos donde la simplicidad y el acceso directo son prioritarios. Sin embargo, para maximizar estas fortalezas sin comprometer la seguridad y el cumplimiento normativo, es crucial implementar políticas y controles adecuados que mitiguen las posibles debilidades mencionadas anteriormente.

4.2.3 Análisis externo

4.2.3.1 Debilidades y amenazas de seguridad

Estas debilidades podrían dar lugar a una variedad de ataques, incluyendo la introducción de malware, exfiltración de datos y otros accesos no autorizados.

4.2.3.1.1 Escenario de conexión directa (vía USB, cable en serial o paralelo,…)

- **Vulnerabilidad a Dispositivos No Autorizados:** Los usuarios podrían conectar dispositivos no autorizados (como memorias USB), lo que podría introducir malware o permitir la exfiltración de datos sensibles.
- **Exposición a Ataques Físicos:** El acceso físico a los puestos de trabajo podría permitir a un atacante conectar un dispositivo malicioso para robar datos o instalar software dañino.
    - **Ataques de Malware vía USB:** Un atacante podría utilizar un dispositivo USB infectado con malware para comprometer los sistemas de la entidad. Este malware podría extraer información, dañar archivos o permitir el acceso remoto a los sistemas.
    - **Exfiltración de Datos:** Un usuario malintencionado podría usar un USB para copiar datos sensibles (como historiales médicos o información personal de los pacientes) y sacarlos de la organización. Queda comprometida la integridad y confidencialidad que menciona el artículo 5 (Principios relativos al tratamiento) de GDPR, donde el tratamiento de datos debe garantizar la seguridad adecuada, lo que incluye protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.
    - **Ataques de Intercepción:** Sin medidas de seguridad adicionales (como cifrado), un atacante podría interceptar datos transferidos entre los dispositivos y los sistemas, accediendo así a información confidencial.
    - **Instalación de Keyloggers:** Un atacante podría instalar dispositivos como keyloggers físicos en los puertos USB para capturar información confidencial, como credenciales de acceso

4.2.3.1.2 Escenario de conexión LAN interna

- **Vulnerabilidades de Firmware:** Los dispositivos conectados a la red a menudo tienen firmware que puede ser explotado si no se actualiza regularmente, dejando abiertas posibles vulnerabilidades conocidas.
- **Ataques Man-in-the-Middle (MITM):** Un atacante podría posicionarse entre el dispositivo y los usuarios que lo utilizan, interceptando o manipulando la información en tránsito.
- **Riesgo de Ataques de Fuerza Bruta:** Los dispositivos de red a menudo cuentan con interfaces de administración que, si no están debidamente protegidas, pueden ser objetivo de ataques de fuerza bruta para obtener acceso administrativo.

- **Riesgo de Malware:** Si el equipo que comparte el dispositivo está comprometido, un atacante puede utilizar este acceso para distribuir malware o atacar otros sistemas en la red, utilizando el recurso compartido como un punto de entrada.

4.2.3.2 Oportunidades

Son todas aquellas situaciones externas a la organización que son o que pueden resultar favorables. Oportunidades o factores del mercado que las empresas reconocen y proponen como una mejora, para que sean aprovechas como beneficio o ayuda a las necesidades de todos los usuarios y trabajadores.

Como organización no debemos estar inactivos, no ser pasivos a todas estas oportunidades. Para aprovechar no puede quedarse a la espera, podemos incrementar nuestras fortalezas o disminuir nuestras debilidades para aprovecharlas, de otro modo no es una oportunidad.

- **Avances en Tecnologías de Seguridad de la Información**: Las innovaciones en tecnologías de seguridad, como el cifrado de datos, autenticación multifactor y gestión avanzada de identidades, ofrecen la oportunidad de mejorar la protección de los datos sensibles en el sistema de impresión. Estas tecnologías permiten una integración más segura con los Sistemas de Información Hospitalaria (HIS) y ayudan a cumplir con normativas descritas en *2.Marco Legal*.
- **Creciente Digitalización en el Sector Sanitario:** La tendencia hacia la digitalización de los procesos de salud abre una oportunidad para integrar sistemas de impresión que no solo gestionen documentos físicos, sino que también faciliten la transición a flujos de trabajo totalmente digitales. Esto permite mejorar la eficiencia operativa y reducir los costes asociados con la gestión de documentos impresos.
- **Incremento de Regulaciones que Favorecen la Seguridad de Datos:** El aumento de normativas orientadas a proteger los datos personales y de salud, reflejadas algunas en el apartado *2.Marco Legal* (como GDPR, LOPDGDD) genera una necesidad en el sector sanitario de adoptar soluciones tecnológicas avanzadas que garanticen el cumplimiento de estas leyes. Esto crea una oportunidad para ofrecer un sistema de impresión que asegure la trazabilidad, auditabilidad y confidencialidad de los datos.
  La presión regulatoria hacia la adopción de medidas de seguridad más estrictas, como la autenticación multifactorial (MFA) y el cifrado de datos, favorece la adopción de soluciones de impresión centralizadas que ya incorporen estos requisitos. Esto convierte al sistema en una opción atractiva para los centros o servicios de los centros adscritos al Servicio Nacional de Salud (SNS) que buscan soluciones que garanticen el cumplimiento normativo.
- **Crecimiento del Trabajo Remoto y Necesidad de Acceso Seguro:** Con la creciente adopción del trabajo remoto, existe una oportunidad para ofrecer servicios de impresión segura accesibles desde cualquier ubicación a través de VPNs o soluciones en la nube, cumpliendo con los estándares de seguridad y manteniendo la operatividad del sistema desde cualquier parte.
- **Avances en Soluciones de Gestión de Impresión:** Los avances en software de gestión de impresión, como NDD Print 360, permiten gestionar de manera centralizada y eficiente todos los dispositivos de impresión, aplicando políticas de seguridad, monitorizando el uso y reduciendo costes operativos. Estas herramientas refuerzan la propuesta de valor del sistema de impresión centralizado.
- **Facilidad de Implementación de Soluciones en la Nube:** La creciente confianza en soluciones basadas en la nube facilita la implementación de sistemas de impresión gestionados de manera remota, proporcionando flexibilidad y escalabilidad. Las soluciones en la nube permiten una gestión más ágil, con menos necesidad de infraestructura física y con una reducción de costes.

4.2.4 Tabla exposición Matriz DAFO

Tras llevar a cabo un análisis de todos los escenarios, se puede resumir mediante la matriz DAFO de manera clara las fortalezas, debilidades, oportunidades y amenazas identificadas en el análisis de la configuración de dispositivos periféricos en red.

Matriz DAFO	*Fortalezas (F)*	*Debilidades (D)*
Análisis Interno	1. Gestión centralizada de la impresión, facilitando el control y monitoreo de todos los dispositivos desde un solo punto.	1. Costos iniciales elevados de implementación e integración de los sistemas de impresión con la infraestructura existente.
	2. Seguridad robusta mediante autenticación multifactor (MFA), cifrado de datos y gestión de accesos basada en roles (RBAC).	2. Complejidad en la configuración inicial y la integración con sistemas ya existentes, lo que requiere personal especializado.
	3. Cumplimiento normativo con estándares de protección de datos, como el GDPR y la LOPDGDD, asegurando la confidencialidad y seguridad de la información.	3. Dependencia de la infraestructura de red para la operatividad y seguridad, lo que puede afectar el rendimiento en caso de fallos de red.
	4. Optimización del uso de recursos y reducción de costes operativos mediante políticas de impresión eficientes, como impresión segura, a doble cara y en blanco y negro por defecto.	4. Curva de aprendizaje para los usuarios finales y el personal de TI, lo que puede ralentizar la adopción y generar resistencia al cambio.
	5. Capacidades de auditoría y trazabilidad que facilitan el control y seguimiento de todas las actividades de impresión.	5. Necesidad de actualizaciones y mantenimiento continuo de hardware y software especializado para asegurar el funcionamiento óptimo del sistema.
Análisis Externo	*Oportunidades (O)*	*Amenazas(A)*
	1. Avances en tecnologías de seguridad y gestión de la información, como cifrado avanzado y gestión de identidades, que facilitan la protección de datos.	1. Cambios frecuentes en las regulaciones de protección de datos (GDPR, LOPDGDD) que pueden requerir ajustes continuos en las políticas de seguridad y gestión de datos.
	2. Creciente digitalización en el sector sanitario, impulsando la adopción de soluciones integradas de impresión y digitalización.	2. Amenazas de seguridad cibernética, como ransomware o ataques dirigidos a dispositivos conectados a la red sanitaria/administrativa.
	3. Incremento de normativas que favorecen la seguridad de los datos, impulsando la necesidad de sistemas que garanticen la trazabilidad y auditabilidad.	3. Dependencia de proveedores externos de hardware y software para actualizaciones, soporte y cumplimiento normativo continúo.
	4. Mejoras en la interoperabilidad de sistemas que facilitan la integración de dispositivos de impresión con otros sistemas tecnológicos del entorno sanitario/administrativo.	4. Resistencia al cambio por parte del personal sanitario debido a la adopción de nuevas tecnologías y flujos de trabajo digitalizados.
	5. Crecimiento del trabajo remoto y necesidad de acceso seguro, creando oportunidades para soluciones de impresión en la nube y mediante VPN.	5. Desgaste y obsolescencia tecnológica de los dispositivos periféricos y necesidad de reemplazo periódico.

Tabla 2. Tabla exposición Matriz DAFO

5 Objetivos, propuesta de mejora y solución.

En la búsqueda de los objetivos y la propuesta de un proyecto de mejora y obtener solución a todas las amenazas que se han identificados, podemos seguir un enfoque detallado basándonos en las etapas claves. Mediante la aplicación de la metodología COBIT (*ISACA, 2019*) en la gestión de dispositivos periféricos en una entidad pública como el Sistema Nacional de Salud (SNS) permite abordar de manera estructurada las debilidades y amenazas identificadas, mejorando la gobernanza de TI y asegurando que la infraestructura tecnológica esté alineada con los objetivos estratégicos de la organización. COBIT, al ser un marco de referencia ampliamente reconocido para la gobernanza y gestión de TI, proporciona un conjunto de mejores prácticas que facilitan la integración de TI con los procesos de negocio, garantizando tanto la eficiencia operativa como el cumplimiento normativo.

5.1 Objetivos

5.1.1 Planificación y Organización (PO)

El dominio de Planificación y Organización en COBIT establece la base para una gestión efectiva de TI. En el contexto de la gestión de dispositivos periféricos, es esencial que la entidad de salud desarrolle un plan estratégico de TI que contemple estos dispositivos como un componente crítico de la infraestructura. ***PO1 (Definir un Plan Estratégico de TI)*** exige que se alineen las estrategias de TI con los objetivos de negocio. Esto implica realizar un análisis exhaustivo de riesgos, donde se evalúen las amenazas específicas asociadas con la conectividad de dispositivos periféricos, como la posibilidad de ataques de malware o el acceso no autorizado a datos sensibles. Con base en este análisis, se deben definir políticas claras para el uso seguro de estos dispositivos, estableciendo protocolos para su conexión, autenticación y acceso.

Otro aspecto clave en esta fase es la ***gestión de la calidad (PO8)***, que requiere el establecimiento de estándares para asegurar que todos los dispositivos periféricos instalados cumplan con los requisitos técnicos y de seguridad. Esto incluye garantizar que cada dispositivo se someta a pruebas rigurosas antes de su implementación, y que exista un proceso para certificar que las configuraciones y actualizaciones de software cumplan con los estándares de seguridad y rendimiento. En el entorno sanitario, donde la calidad del servicio es crítica, esta etapa garantiza que los dispositivos periféricos no solo funcionen de manera eficiente, sino que también sean seguros y confiables.

5.1.2 Adquisición e Implementación (AI)

El dominio de Adquisición e Implementación en COBIT se enfoca en la identificación de soluciones tecnológicas adecuadas, su adquisición y su correcta implementación. ***AI2 (Adquirir y Mantener Infraestructura Tecnológica)*** es particularmente relevante para la gestión de dispositivos periféricos, ya que implica la selección e integración de tecnologías que permitan una gestión centralizada y segura de estos dispositivos. La implementación de un sistema de gestión de dispositivos periféricos debe incluir funcionalidades que permitan controlar y monitorear el acceso, gestionar configuraciones y realizar actualizaciones de manera eficiente y segura.

Además, el proceso ***AI7 (Instalar y Acreditar Soluciones y Cambios)*** enfatiza la necesidad de realizar pruebas piloto y certificaciones antes de desplegar dispositivos periféricos en un entorno de producción. Esto garantiza que cualquier cambio o nueva implementación sea minuciosamente evaluada para asegurar que no introduzca nuevas vulnerabilidades en la red. En un entorno de salud, donde la continuidad y seguridad de los servicios son esenciales, la implementación de estas pruebas es crucial para prevenir interrupciones o brechas de seguridad.

5.1.3 Entrega y Soporte (DS)

El dominio de Entrega y Soporte abarca la operación diaria de los servicios de TI y el soporte a los usuarios. ***DS5 (Asegurar los Servicios de Seguridad)*** es un proceso fundamental que se centra en la protección de la infraestructura de TI, incluyendo los dispositivos periféricos. En este contexto, la implementación de controles de seguridad robustos es esencial para garantizar que solo los usuarios autorizados puedan acceder a estos dispositivos. Esto incluye la adopción de medidas de autenticación segura, como el uso de tarjetas de proximidad o credenciales de usuario, y la implementación de herramientas de monitorización que permitan detectar y responder rápidamente a cualquier actividad anómala o intento de acceso no autorizado.

El proceso ***DS9 (Gestionar la Configuración)*** también es crucial, ya que garantiza que todos los dispositivos periféricos estén configurados de acuerdo con las políticas de seguridad de la organización. Mantener una base de datos centralizada con la configuración de todos los dispositivos permite un seguimiento eficaz de los cambios y actualizaciones, asegurando que cualquier modificación sea controlada y no comprometa la seguridad de la red. En un entorno sanitario, donde la precisión y la integridad de los datos son vitales, una gestión adecuada de la configuración asegura que los dispositivos periféricos funcionen de manera confiable y segura.

5.1.4 Monitoreo y Evaluación (ME):

Finalmente, el dominio de Monitoreo y Evaluación en COBIT se enfoca en asegurar que los procesos de TI sean efectivos y estén alineados con los objetivos de la organización. ***ME1 (Monitorizar y Evaluar el Desempeño)*** requiere el establecimiento de indicadores clave de rendimiento (KPI) para medir la eficiencia y seguridad de los dispositivos periféricos. Esto puede incluir métricas como el tiempo de actividad, la tasa de fallos, la detección de incidentes de seguridad y la satisfacción del usuario. La evaluación continua de estos indicadores permite a la entidad de salud ajustar sus políticas y procedimientos de TI para mejorar la eficiencia operativa y reducir riesgos.

El proceso ***ME4 (Proveer Gobernanza de TI)*** asegura que la gestión de dispositivos periféricos esté alineada con la gobernanza corporativa, integrando la gestión de riesgos y cumplimiento normativo dentro de la estructura de gobernanza de TI. Esto es especialmente relevante en un entorno sanitario, donde el cumplimiento con regulaciones como el GDPR es obligatorio. La implementación de controles y auditorías periódicas garantiza que las prácticas de gestión de dispositivos periféricos no solo sean eficientes, sino que también cumplan con las normativas aplicables, protegiendo la información sensible de los pacientes y la integridad de los servicios de salud.

5.2 Propuesta de solución y mejora

La implementación de un sistema centralizado de impresión y digitalización en una entidad del Servicio Nacional de Salud no solo aborda las debilidades y amenazas previamente identificadas, sino que también introduce múltiples fortalezas que optimizan la operatividad, seguridad y cumplimiento normativo en la gestión de dispositivos periféricos. Al utilizar la metodología COBIT y el análisis DAFO como guía, se puede estructurar esta propuesta de solución para maximizar los beneficios y minimizar los riesgos.

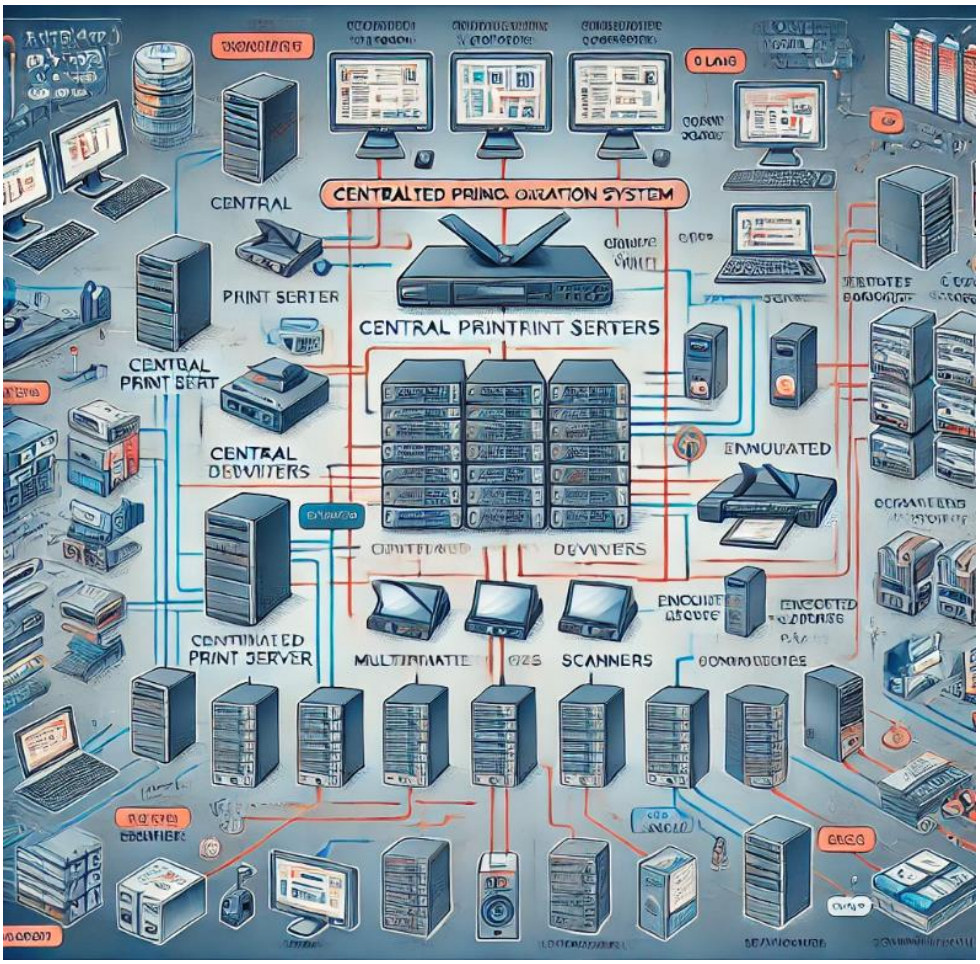


Ilustración 2. Un diagrama detallado de un sistema centralizado de impresión y digitalización.

5.2.1 Gestión Centralizada y Monitoreo Activo

Una de las principales fortalezas de configurar dispositivos periféricos como parte de un sistema centralizado es la capacidad de ***gestión y monitoreo centralizado***. Este enfoque permite a la organización controlar todos los dispositivos desde un único punto, facilitando la administración, el mantenimiento y la supervisión en tiempo real. Según los documentos, manuales o estándares de instalación para un sistema centralizado de impresión, la gestión unificada permite no solo la supervisión del estado de los dispositivos, sino también la configuración de parámetros de seguridad, lo que reduce significativamente el riesgo de accesos no autorizados y fallos operativos.

Con una infraestructura de impresión centralizada, se puede implementar un ***software de gestión de flotas*** que incluya características avanzadas como la asignación de trabajos de impresión, seguimiento del uso por usuario, y políticas de impresión segura (como la liberación de trabajos solo cuando el usuario está presente). Este sistema, alineado con el dominio ***DS5 (Asegurar los Servicios de Seguridad)*** de COBIT, permite la detección temprana de incidentes de seguridad, la respuesta rápida a fallos técnicos, y la implementación de medidas correctivas antes de que se produzcan interrupciones críticas en los servicios.

5.2.1.1 *Infraestructura Centralizada de Gestión y Monitoreo*

Una infraestructura centralizada de gestión y monitoreo típicamente se basa en la implementación de un ***Servidor de Gestión Centralizada*** (*SESPA, 2023*) (Centralized Management Server, CMS) que actúa como el núcleo de la administración de todos los dispositivos periféricos conectados a la red. Este servidor se encarga de recopilar datos de uso, aplicar políticas de seguridad, gestionar actualizaciones de software y firmware, y proporcionar informes detallados sobre el estado de los dispositivos.

Un ***sistema de gestión de flotas*** como ***Print Management Software (PMS)***. Este tipo de software puede ser alojado en un servidor central y permite la gestión de múltiples dispositivos desde una consola unificada. Tecnologías como HP Web Jetadmin, NDD Print o Kyocera Fleet Services son ejemplos de herramientas que permiten la supervisión remota de impresoras y escáneres, proporcionando funcionalidades como la visualización en tiempo real del estado de los dispositivos, la asignación de trabajos de impresión, y el control del acceso de usuarios.

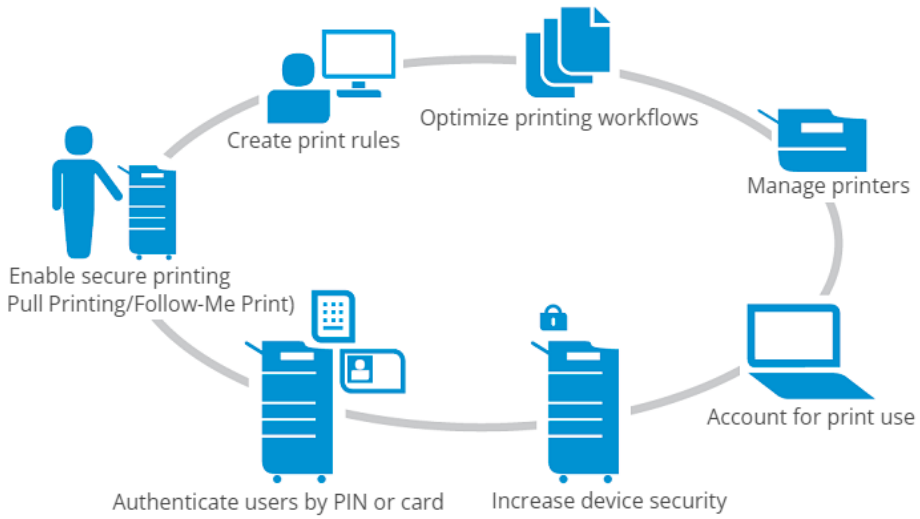


Ilustración 3. Sistema de gestión de flotas

HP Web Jetadmin, por ejemplo, es una solución de administración que permite controlar una flota de dispositivos de impresión desde un solo punto. Con esta herramienta, el administrador puede realizar tareas como la configuración remota de impresoras, la monitorización de consumibles, y la implementación de políticas de impresión seguras. Además, este sistema facilita la automatización de tareas de mantenimiento, como la actualización de firmware, asegurando que todos los dispositivos estén protegidos contra vulnerabilidades conocidas.

Microsoft Print Server o CUPS (Common Unix Printing System) son servidores de impresión dedicados que centralicen la gestión de trabajos de impresión. Estos servidores permiten un control más preciso de los trabajos de impresión, autentican a los usuarios antes de que se realicen las impresiones, y almacenan registros detallados para auditoría.

5.2.1.2 *Monitorización Activa y Gestión de Incidentes*

El ***monitoreo activo*** es un proceso continuo que permite a la organización detectar y responder a problemas antes de que afecten significativamente las operaciones. En el contexto de una entidad pública de salud, esto es especialmente importante, ya que una interrupción en los servicios de impresión o digitalización puede impactar directamente en la atención al paciente.

La implementación de un sistema que permita la ***monitorización en tiempo real*** de los dispositivos periféricos, podría realizarse utilizando tecnologías como ***SNMP (Simple Network Management Protocol)***, que permite la recolección de datos y el envío de alertas en caso de anomalías. Una solución como Nagios o Zabbix podría ser implementada para monitorizar la red y los dispositivos conectados, enviando alertas

al equipo de TI si se detectan problemas como caídas de conexión, errores en los dispositivos o niveles bajos de consumibles.

Por ejemplo, si una impresora comienza a mostrar signos de fallo, como atascos de papel frecuentes o errores de impresión, el sistema de monitorización activa podría enviar una notificación automática al equipo de soporte técnico antes de que el problema se convierta en una interrupción mayor. Este enfoque permite que los problemas se resuelvan de manera proactiva, minimizando el impacto en las operaciones diarias y asegurando que los servicios esenciales, como la impresión de recetas o la digitalización de documentos médicos, continúen sin interrupciones.

5.2.1.3 Seguridad en la Gestión Centralizada

Otro aspecto crucial de la gestión centralizada es la ***seguridad***. En un entorno sanitario, donde se manejan datos altamente sensibles, es esencial que todos los dispositivos periféricos estén protegidos contra accesos no autorizados y posibles ciberataques. La implementación de un servidor centralizado facilita la aplicación de ***políticas de seguridad uniformes*** en toda la red de dispositivos.

Por ejemplo, el uso de ***software de impresión segura***, como Papercut o SafeQ, permite la implementación de medidas como la impresión bajo demanda (pull printing), donde los trabajos de impresión no se ejecutan hasta que el usuario se autentica en el dispositivo. Esto previene que documentos sensibles queden expuestos en bandejas de impresión. Además, estas soluciones suelen ofrecer ***cifrado de datos en tránsito y en reposo***, utilizar protocolos de cifrado como ***IPsec*** o ***TLS*** para asegurar que todos los datos enviados a través de la red, incluyendo trabajos de impresión, estén cifrados. Esto protege la confidencialidad de la información sensible. Asegurando que la información confidencial se mantenga protegida durante todo el proceso de impresión o digitalización.

La integración con sistemas de ***autenticación centralizados*** como ***LDAP*** o ***Active Directory***. Esto permite que las credenciales de los usuarios sean verificadas de manera centralizada, y que las políticas de acceso se apliquen de manera consistente en todos los dispositivos periféricos. Al integrarse con el sistema de gestión de identidades de la organización, se asegura que solo el personal autorizado tenga acceso a funciones específicas, reduciendo el riesgo de filtraciones de datos.

Implementar la funcionalidad de ***Pull Printing*** nos ofrece que los trabajos de impresión no se liberan hasta que el usuario se autentica físicamente en el dispositivo de impresión. Esto garantiza que los documentos no se queden desatendidos en las bandejas de las impresoras, reduciendo el riesgo de exposición de datos sensibles.

5.2.1.4 Infraestructura de Red Segura y Segregada

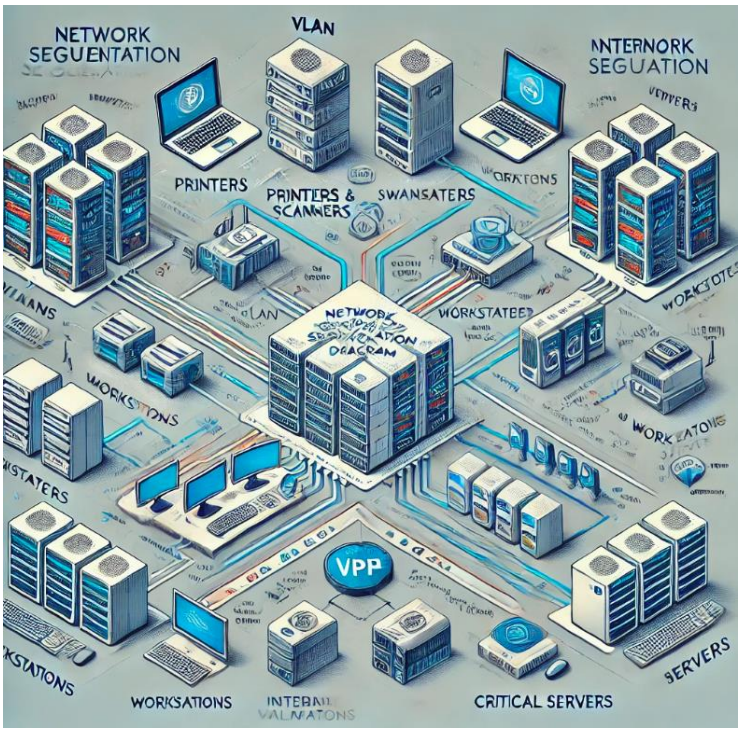


Ilustración 4. Diagrama detallado de una red segmentada, compuesta por VLANs, firewalls internos y accesos VPN.

Segmentación de la Red

La segmentación de la red mediante VLANs (Virtual Local Area Networks) es una práctica esencial en la arquitectura de redes seguras, especialmente en entornos que manejan dispositivos críticos como impresoras y escáneres. La implementación de VLANs ofrece varias ventajas y minimiza riesgos significativos:

- **Aislamiento del Tráfico**: Al segmentar la red, las impresoras y dispositivos de escaneo se colocan en una VLAN distinta de las estaciones de trabajo y servidores críticos. Esto asegura que el tráfico de datos de estos dispositivos periféricos no se mezcle con otros tipos de tráfico, lo que reduce la posibilidad de que un incidente de seguridad en un área afecte a otras partes de la red. Por ejemplo, si una impresora es comprometida a través de un malware, el aislamiento VLAN limitará la propagación del malware a los sistemas de usuario y servidores críticos.
- **Control Granular del Tráfico:** Mediante VLANs, los administradores de red pueden definir políticas precisas sobre qué tráfico se permite entre las distintas partes de la red. Por ejemplo, se puede restringir el acceso a impresoras y escáneres únicamente a ciertos usuarios o grupos, reduciendo así el riesgo de accesos no autorizados y manteniendo la integridad de la red.
- **Optimización del Rendimiento:** Además de la seguridad, la segmentación ayuda a optimizar el rendimiento de la red. Al limitar el tráfico broadcast y multicast a dentro de su propia VLAN, se reduce la carga sobre la red, mejorando la eficiencia del tráfico y el rendimiento global.
- **Facilidad de Gestión:** Las VLANs permiten una administración más sencilla y centralizada de la red. Si la organización crece, se pueden añadir nuevas VLANs sin necesidad de modificar la infraestructura física, lo que facilita la escalabilidad de la red. Por ejemplo, si se añaden más dispositivos de impresión en una nueva oficina, simplemente se pueden integrar en la VLAN existente para impresoras.

Firewalls Internos para Control del Tráfico entre VLANs

- **Políticas de Seguridad Específicas:** Los firewalls internos permiten establecer políticas de seguridad que controlen el tráfico entre las VLANs. Estas políticas pueden ser tan específicas como sea necesario, por ejemplo, permitiendo que solo ciertos tipos de datos pasen de la VLAN de las

estaciones de trabajo a la VLAN de las impresoras, o restringiendo el acceso entre VLANs solo durante ciertas horas del día.

- **Detección y Prevención de Amenazas:** Los firewalls internos pueden integrar funcionalidades de detección y prevención de intrusiones (IDS/IPS), que monitorean el tráfico en busca de comportamientos sospechosos. Esto es crucial en un entorno de impresión, donde un dispositivo comprometido podría intentar escanear o atacar otros dispositivos en la red.
- **Segmentación Física y Lógica:** Los firewalls permiten una segmentación tanto física (entre dispositivos conectados a distintos switches o routers) como lógica (entre dispositivos en la misma infraestructura física pero diferentes VLANs). Esto añade una capa adicional de seguridad al asegurarse de que las reglas de segmentación se apliquen correctamente a través de toda la red.

VPN para Acceso Remoto Seguro

La implementación de una VPN (Virtual Private Network) es crucial para garantizar un acceso seguro y controlado a la red interna desde ubicaciones remotas. Este es un componente vital en la gestión de infraestructuras de impresión, especialmente cuando los administradores necesitan acceder al sistema desde fuera del entorno de la oficina.

- **Cifrado de Datos:** Las conexiones VPN cifran todos los datos que se transmiten entre el dispositivo del usuario y la red interna. Esto es esencial para proteger la confidencialidad e integridad de los datos mientras se gestionan dispositivos de impresión desde ubicaciones remotas. El cifrado asegura que incluso si los datos son interceptados, no podrán ser leídos ni manipulados.
- **Autenticación Fuerte:** Las VPNs generalmente requieren autenticación fuerte, como MFA (Autenticación Multifactor), para garantizar que solo usuarios autorizados puedan acceder a la red. Esto es particularmente importante en la gestión de sistemas de impresión, donde el acceso no autorizado podría llevar a la exposición de información sensible o la alteración de configuraciones críticas.
- **Gestión y Monitoreo Centralizado:** La VPN permite que los administradores gestionen remotamente los dispositivos de impresión, monitoreen su estado, realicen actualizaciones, y respondan a incidentes sin necesidad de estar físicamente presentes en la oficina. Esto mejora la capacidad de respuesta y permite una administración más flexible.
- **Compatibilidad con Infraestructuras Existentes:** Las soluciones VPN modernas son compatibles con una amplia gama de dispositivos y sistemas operativos, lo que facilita su integración en infraestructuras de TI existentes sin necesidad de modificaciones extensivas. Esto permite a la organización aprovechar su infraestructura actual mientras mejora significativamente la seguridad.

5.2.1.5 Automatización y Reporting

La ***automatización*** es otra fortaleza clave en la gestión centralizada. Las soluciones modernas permiten automatizar tareas rutinarias como la ***generación de informes***, la ***programación de mantenimientos*** y la ***gestión de consumibles***. Por ejemplo, un sistema de gestión centralizada puede generar automáticamente informes detallados sobre el uso de los dispositivos, identificando tendencias y áreas donde se podrían implementar mejoras en eficiencia.

Con la integración de un sistema de gestión de impresión con una plataforma ***SIEM*** como Splunk o IBM QRadar sirve para centralizar la recolección y análisis de logs de seguridad. Esto permite detectar patrones de comportamiento inusuales que puedan indicar un ataque o abuso del sistema.

Los informes también pueden incluir métricas clave como el tiempo de inactividad de los dispositivos, el número de trabajos de impresión procesados, y la tasa de errores, lo que facilita la toma de decisiones informadas y la planificación de recursos. Esta capacidad de reporting avanzado es fundamental para la ***auditoría y cumplimiento normativo***, permitiendo a la entidad de salud demostrar su adherencia a regulaciones como el GDPR.

5.2.2 Autenticación y Control de Accesos

La autenticación y el control de accesos son elementos fundamentales en la gestión de dispositivos periféricos, especialmente en un entorno sanitario donde la seguridad de los datos es crítica. La implementación de un sistema robusto de autenticación y control de accesos no solo garantiza que solo personal autorizado pueda acceder a funciones sensibles, sino que también protege la integridad y la confidencialidad de los datos manejados por estos dispositivos.

Otra fortaleza clave en la configuración de un sistema centralizado de impresión es la posibilidad de ***integrar sistemas de autenticación robusta***. Tal como se describe en los documentos del pliego técnico, la solución centralizada permite el uso de ***tarjetas de proximidad, PINs y credenciales de usuario*** para acceder a las funciones de impresión, escaneo y copia. Este tipo de autenticación asegura que solo el personal autorizado pueda utilizar los dispositivos, protegiendo así la confidencialidad de la información sensible, especialmente en un entorno donde se manejan datos médicos.

Además, la integración con un sistema de ***gestión de identidades*** (IDM) o ***Active Directory*** (AD) permite que las políticas de acceso se sincronicen con las credenciales de usuario ya existentes en la organización. Esto no solo simplifica la administración de usuarios, sino que también asegura que cualquier cambio en los permisos o roles del usuario se refleje automáticamente en los dispositivos periféricos, alineándose con el proceso ***DS9 (Gestionar la Configuración)*** de COBIT. La capacidad de restringir el acceso a funciones específicas en los dispositivos periféricos según el rol del usuario refuerza la seguridad y previene el uso indebido de los recursos.

5.2.2.1 Infraestructuras de Autenticación y Control de Accesos

En el contexto de una entidad en el servicio público de salud, la infraestructura de autenticación y control de accesos debe integrarse con el sistema de gestión de identidades de la organización, como ***Active Directory (AD)*** o ***LDAP (Lightweight Directory Access Protocol)***. Esto permite una administración centralizada de las credenciales de usuario, donde cada empleado tiene un único perfil de usuario con permisos claramente definidos.

Por ejemplo, una solución como Microsoft Active Directory puede ser utilizada para gestionar las credenciales de los usuarios y sus permisos en toda la red, incluyendo el acceso a dispositivos periféricos como impresoras y escáneres. Esta integración asegura que cualquier cambio en los permisos del usuario se refleje automáticamente en todos los dispositivos periféricos, facilitando la aplicación de políticas de seguridad consistentes y reduciendo el riesgo de errores humanos.

LDAP, por otro lado, permite un acceso rápido y eficiente a la información de autenticación de usuarios desde múltiples aplicaciones y dispositivos. Al utilizar LDAP, las impresoras y escáneres pueden validar directamente las credenciales de los usuarios contra la base de datos centralizada, asegurando que solo el personal autorizado pueda realizar operaciones como imprimir o escanear documentos.

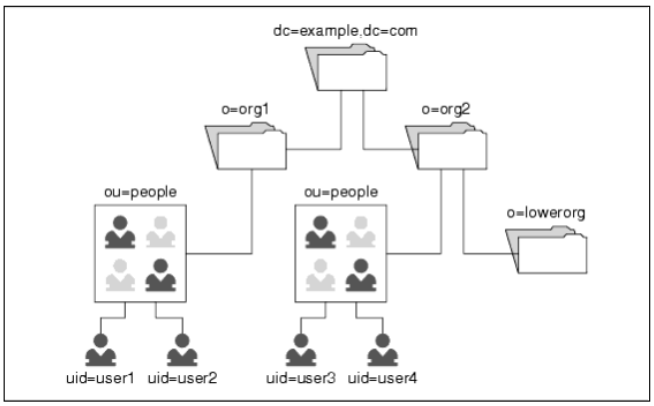


Ilustración 5. Estructura LDAP de ejemplo.

5.2.2.2 Control de Accesos Basado en Roles (RBAC)

El ***Control de Accesos Basado en Roles (RBAC)*** es un enfoque eficaz para gestionar quién puede acceder a qué funciones en los dispositivos periféricos. Bajo este modelo, los permisos se asignan según el rol del usuario dentro de la organización. Por ejemplo, un médico puede tener permisos para imprimir, escanear y copiar, mientras que el personal administrativo solo puede imprimir documentos no confidenciales.

PaperCut y SafeQ son ejemplos de software de gestión de impresión que soportan RBAC, permitiendo a los administradores definir políticas de acceso detalladas basadas en los roles de los usuarios. Este tipo de control granular es crucial en un entorno de salud, donde la diferenciación clara de permisos asegura que los datos sensibles se mantengan protegidos y solo sean accesibles por personal autorizado.

Por ejemplo, en un centro sanitario o administrativo perteneciente a SNS, las funciones de escaneo de documentos médicos podrían estar restringidas solo a médicos y enfermeras, mientras que las funciones de impresión básica podrían estar disponibles para todo el personal. El sistema PaperCut MF permite configurar estas restricciones de manera sencilla, garantizando que solo los usuarios correctos accedan a las funciones adecuadas.

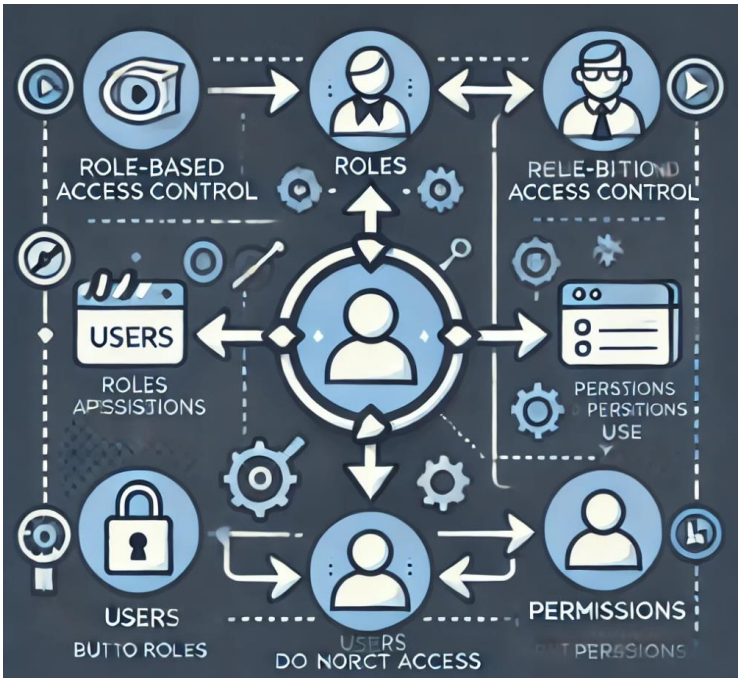


Ilustración 6. Esquema basado en Control RBAC

5.2.2.3 Tecnologías de Autenticación

Para implementar un control de acceso efectivo, es común utilizar una combinación de tecnologías de autenticación. A continuación, se describen algunas de las tecnologías relevantes:

Autenticación basada en tarjeta de proximidad o RFID:

Esta tecnología es ampliamente utilizada en entornos sanitarios debido a su conveniencia y seguridad. Los usuarios pueden autenticarse simplemente acercando su tarjeta de identificación (equipada con un chip RFID) a un lector instalado en el dispositivo periférico. Por ejemplo, las impresoras multifuncionales de Xerox o Ricoh pueden integrar lectores de tarjetas RFID, lo que permite a los usuarios autenticarse rápidamente y acceder a las funciones del dispositivo según sus permisos.

La solución Xerox Secure Print permite que los documentos enviados a la impresora solo se liberen cuando el usuario autorizado se autentica en el dispositivo con su tarjeta RFID. Este enfoque asegura que los documentos no queden expuestos en bandejas de impresión, protegiendo así la confidencialidad de la información.

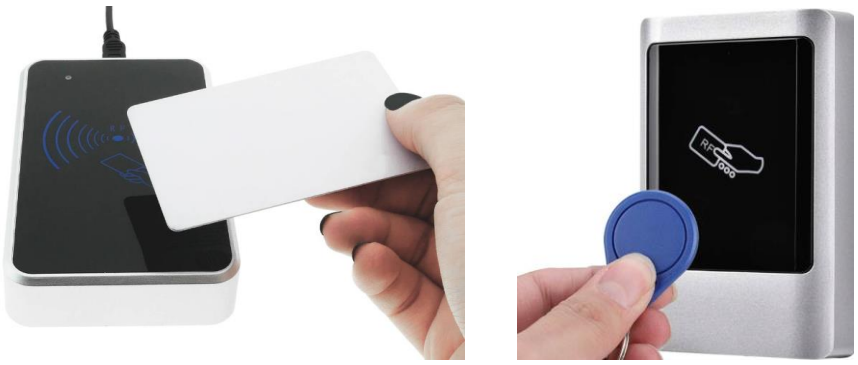


Ilustración 6. Ejemplos de llaves RFID

Autenticación mediante PIN o contraseñas

Otra forma de asegurar el acceso a dispositivos periféricos es mediante la autenticación con un PIN o contraseña. Los usuarios deben ingresar un código personal en el dispositivo para desbloquear las funciones de impresión o escaneo. Esta tecnología es fácil de implementar y ofrece una capa adicional de seguridad en caso de pérdida o robo de tarjetas de proximidad.

Autenticación biométrica

Aunque menos común en entornos de impresión, la autenticación biométrica (como huellas dactilares o reconocimiento facial) está ganando terreno en la protección de dispositivos periféricos. Esta tecnología ofrece un alto nivel de seguridad al requerir características físicas únicas del usuario para el acceso.

Algunos dispositivos de impresión de alta seguridad, como los proporcionados por Samsung o Konica Minolta, ofrecen opciones de autenticación biométrica, permitiendo un control de acceso extremadamente seguro y reduciendo el riesgo de uso no autorizado.

5.2.2.4 Monitorización y Auditoría de Accesos

Una infraestructura de autenticación y control de accesos robustos debe incluir capacidades de ***monitorización y auditoría***. Estas capacidades permiten rastrear quién accede a los dispositivos y qué operaciones realiza, proporcionando un registro completo que puede ser utilizado para auditorías de seguridad y cumplimiento normativo.

El uso de herramientas como LogRhythm o Splunk permite una integración con la infraestructura de autenticación, capturando eventos de acceso y proporcionando alertas en tiempo real en caso de intentos de acceso no autorizados. Esto asegura que cualquier anomalía en el comportamiento de acceso pueda ser detectada y gestionada de manera inmediata.

5.2.3 Optimización del Uso de Recursos y Reducción de Costes

La centralización también aporta una significativa optimización del uso de recursos. Con el control detallado de los dispositivos y el seguimiento del uso, es posible identificar patrones de uso ineficiente y ajustar las operaciones para reducir los desperdicios. Esto se traduce en una reducción del consumo de papel y tóner, además de minimizar el uso innecesario de los dispositivos, lo que prolonga la vida útil de los mismos.

Por ejemplo, la implementación de políticas de impresión como la impresión a doble cara por defecto, la prohibición de impresiones en color a menos que sea necesario, o la consolidación de trabajos de impresión, puede resultar en ahorros considerables. Esta capacidad de gestionar recursos eficientemente está alineada con los objetivos de COBIT en los dominios de ***Adquisición e Implementación (AI)***, donde se busca maximizar el valor de las inversiones tecnológicas y minimizar los costos operativos. Además, la centralización permite un control más efectivo del inventario y de los costes asociados a la impresión, lo que facilita una mejor planificación presupuestaria y la reducción de gastos.

A continuación, se exploran estrategias clave para lograr estos objetivos.

5.2.3.1 Implementación de Sistemas de Gestión Centralizada

Una de las formas más efectivas de optimizar el uso de recursos es la centralización de la gestión de dispositivos periféricos. Esto implica la consolidación de impresoras y escáneres bajo un sistema centralizado de gestión, lo que permite un control más eficiente de los recursos y una reducción en el número de dispositivos necesarios.

Infraestructura y Tecnologías

Print Management Software (PMS), como PaperCut, Equitrac o NDD Print, son ejemplos de soluciones que permiten una gestión centralizada de la flota de impresión. Estos sistemas ofrecen funcionalidades para rastrear y controlar el uso de cada dispositivo, identificar patrones de uso ineficientes y ajustar las políticas de impresión para reducir el desperdicio de papel y tinta.

PaperCut MF, por ejemplo, permite establecer políticas como la impresión en doble cara o la conversión automática de trabajos de impresión en blanco y negro, lo que reduce significativamente el consumo de papel y tóner. Además, al integrar todos los dispositivos en una plataforma única, se puede reducir la redundancia de equipos y consolidar las funciones de impresión en menos dispositivos más eficientes.

En la necesidad de trabajar con sistemas que puedan gestionar de forma centralizada las impresoras, obtenemos una parte esencial para reducir los costes asociados a la gestión descentralizada, como el mantenimiento fragmentado y la compra innecesaria de consumibles.

5.2.3.2 Reducción del Consumo Energético

El consumo energético de los dispositivos periféricos representa un coste importante en el funcionamiento diario de una entidad de salud. Optimizar este aspecto puede llevar a una reducción considerable de los costes operativos.

Infraestructura y Tecnologías

Sistemas de Gestión de Energía integrados en los dispositivos periféricos permiten controlar y reducir el consumo energético. Tecnologías como Eco Mode o Sleep Mode que se encuentran en impresoras de HP o Canon reducen automáticamente el consumo de energía cuando los dispositivos no están en uso.

Xerox Managed Print Services es un ejemplo de tecnología que incluye la gestión de energía dentro de su suite de herramientas. Los dispositivos administrados bajo MPS pueden configurarse para entrar en modo de bajo consumo durante horas no pico, lo que reduce la factura energética.

5.2.3.3 Optimización del Uso de Consumibles

El uso eficiente de consumibles, como papel y tinta, es una de las áreas más directas donde se pueden reducir costes en la gestión de dispositivos periféricos. La implementación de tecnologías y políticas que minimicen el desperdicio es crucial para lograr este objetivo.

Infraestructura y Tecnologías

Los programas de administración de impresión como SafeQ y PaperCut incluyen funcionalidades que permiten la monitorización del uso de consumibles en tiempo real. Estas plataformas pueden alertar a los administradores sobre el uso excesivo de papel o tóner, permitiendo ajustes inmediatos en las políticas de impresión.

El uso de estas políticas puede incluir restricciones como la impresión en color, la obligatoriedad de la impresión a doble cara o la impresión bajo demanda (***pull printing***), donde los trabajos de impresión se liberan solo cuando el usuario se autentica en el dispositivo, lo que reduce el número de trabajos de impresión no recogidos y, por tanto, el desperdicio de papel.

Al disponer de un sistema centralizado y monitorizado añade posibilidades de que rastrean el uso de papel y tinta, y optimizan su reposición de forma automática.

5.2.3.4 Mantenimiento Predictivo y Reducción de Tiempo de Inactividad

El mantenimiento predictivo es una estrategia clave para reducir costes asociados a la reparación y el reemplazo de dispositivos. Implementar sistemas que monitoricen de forma continua el estado de los dispositivos permite anticiparse a fallos y planificar el mantenimiento de manera eficiente.

Infraestructura y Tecnologías

Con un sistema de monitorización activa, las herramientas como HP Web Jetadmin o Xerox CentreWare permiten monitorizar el estado de los dispositivos en tiempo real. Estos sistemas pueden predecir cuándo un dispositivo está a punto de fallar basándose en patrones de uso y desgaste, lo que permite programar intervenciones antes de que se produzcan averías costosas.

El mantenimiento automatizado, como Kyocera Fleet Services, proporcionan herramientas donde los dispositivos pueden auto diagnosticarse y enviar alertas para la intervención técnica. Esto no solo reduce el tiempo de inactividad, sino que también optimiza la vida útil de los equipos, reduciendo la necesidad de reemplazos prematuros.

5.2.3.5 Impresión Bajo Demanda y Reducción de Residuos

La impresión bajo demanda (***Pull Printing***) es una tecnología que ayuda a reducir significativamente los residuos de papel y tinta, al asegurarse de que los trabajos de impresión solo se completan cuando el usuario está presente para recogerlos.

Infraestructura y Tecnologías

Estos sistemas, como Equitrac o Papercut MF, integran esta funcionalidad en las impresoras, permitiendo a los usuarios enviar trabajos a una cola de impresión centralizada y luego autenticarse en cualquier impresora disponible para liberar su trabajo. Esta funcionalidad no solo reduce el desperdicio, sino que también mejora la seguridad al garantizar que los documentos impresos no queden desatendidos en las bandejas de salida.

5.2.3.6 Automatización de Procesos de Reposición

La automatización en la reposición de consumibles puede mejorar la eficiencia y reducir los costes asociados a la gestión manual de stock.

Infraestructura y Tecnologías

Soluciones como las ofrecidas por Xerox Managed Print Services (MPS) permiten la automatización de la reposición de suministros, asegurando que el stock de consumibles como cartuchos de tinta y papel se mantenga en niveles óptimos sin intervención manual, lo que evita interrupciones en el servicio y reduce el riesgo de sobre stock.

Como beneficio adicional decir que esta automatización también ofrece informes detallados sobre el uso de consumibles, permitiendo a la organización ajustar sus pedidos y reducir gastos innecesarios.

5.2.4 Cumplimiento Normativo y Protección de Datos

El cumplimiento normativo y la protección de datos en la gestión de dispositivos periféricos en un entorno sanitario requieren la implementación de infraestructuras y tecnologías avanzadas que aseguren la confidencialidad, integridad y disponibilidad de la información. La integración de soluciones como la gestión centralizada de impresoras, el cifrado de datos, la autenticación multifactorial, la monitorización continua y la gestión de derechos de información permite a las organizaciones sanitarias no solo cumplir con las estrictas normativas del GDPR y la LOPDGDD, sino también proteger de manera efectiva la información sensible de los pacientes. Estas prácticas no solo previenen brechas de seguridad, sino que también fortalecen la confianza del público en la capacidad de la organización para manejar datos sensibles de manera segura y responsable.

En un entorno de salud, el ***cumplimiento con regulaciones como el GDPR la LOPDGDD*** es crítico. La solución centralizada facilita la implementación de políticas de retención y eliminación de documentos, asegurando que los datos personales sean manejados de acuerdo con los requisitos legales. El sistema puede configurarse para borrar automáticamente los trabajos de impresión una vez que han sido liberados o después de un tiempo determinado, minimizando el riesgo de exposición de datos sensibles.

La trazabilidad de las acciones realizadas en los dispositivos periféricos también se ve mejorada, permitiendo auditorías detalladas que registran quién imprimió qué documento y cuándo. Esto no solo fortalece la seguridad, sino que también facilita el cumplimiento de auditorías externas, alineándose con el proceso ***ME4 (Proveer Gobernanza de TI)*** de COBIT. Al garantizar que todas las acciones en los dispositivos periféricos son monitoreadas y registradas, la organización puede demostrar fácilmente su cumplimiento con las normativas vigentes y protegerse contra posibles sanciones.

5.2.4.1 Gestión Centralizada y Control de Accesos

Una de las principales estrategias para asegurar el cumplimiento normativo es la gestión centralizada de dispositivos periféricos y el control riguroso de accesos. Esto implica la integración de sistemas que puedan rastrear, auditar y limitar el acceso a los datos sensibles manejados por impresoras, escáneres y otros dispositivos.

Infraestructura y Tecnologías

Print Management Solutions (PMS) como PaperCut MF y Equitrac permiten una gestión centralizada que incluye la capacidad de auditar cada trabajo de impresión, escaneo o copia realizado. Estas soluciones registran información detallada sobre quién realizó cada acción, cuándo se hizo, y qué documentos fueron procesados, lo cual es fundamental para cumplir con las exigencias del GDPR y la LOPDGDD en cuanto a la trazabilidad y control de datos personales.

Ante la necesidad de gestionar de forma centralizada todos los dispositivos de impresión, asegurando que cada operación sea auditada y que solo el personal autorizado tenga acceso a la información. Estas soluciones pueden integrarse con sistemas de control de acceso como ***Active Directory (AD)***, para garantizar que solo usuarios autenticados puedan realizar ciertas acciones, alineándose con las normativas de protección de datos.

5.2.4.2 Cifrado de Datos y Almacenamiento Seguro

El cifrado de datos es una medida esencial para proteger la información sensible almacenada o transmitida a través de dispositivos periféricos. Esto garantiza que incluso si los datos son interceptados, no pueden ser leídos por personas no autorizadas.

Infraestructura y Tecnologías

Las tecnologías de encriptación en dispositivos periféricos modernos, como las impresoras multifuncionales de HP y Xerox, incluyen capacidades de cifrado para proteger los datos almacenados en sus discos duros o transmitidos a través de la red. Además, soluciones de software como BitLocker pueden ser implementadas para cifrar los discos duros de los servidores que almacenan trabajos de impresión o documentos escaneados.

Por ejemplo, la implementación de dispositivos con ***Disco Duro Encriptado*** y funcionalidades de ***Secure Erase*** para la eliminación segura de datos ayuda a garantizar que los datos confidenciales no puedan ser recuperados de los dispositivos una vez que han sido eliminados. Esto es crucial para cumplir con las normativas sobre el tratamiento y eliminación segura de datos personales.

5.2.4.3 Autenticación Multifactorial (MFA)

La autenticación multifactorial (MFA) agrega una capa adicional de seguridad, asegurando que el acceso a dispositivos periféricos y a la información que manejan solo se otorga después de verificar múltiples factores de identidad.

Infraestructura y Tecnologías

La implementación de MFA en dispositivos periféricos puede realizarse mediante la integración con sistemas de autenticación como Microsoft Azure AD o Okta, que soportan MFA. Esto implica que, además de la autenticación básica, los usuarios deben proporcionar un segundo factor, como un código enviado a su teléfono móvil o una huella digital, para acceder a los dispositivos.

Al configurar impresoras y escáneres para que requieran MFA antes de procesar trabajos sensibles, se asegura que solo los usuarios verificados puedan acceder a la información confidencial, reduciendo así el riesgo de acceso no autorizado.

5.2.4.4 Monitorización y Auditoría Continua

Para cumplir con las normativas de protección de datos, es crucial implementar soluciones que permitan una monitorización y auditoría continua de las actividades relacionadas con los dispositivos periféricos.

Infraestructura y Tecnologías

Security Information and Event Management (SIEM) tiene soluciones como Splunk o LogRhythm permiten la monitorización en tiempo real de las actividades de los dispositivos, registrando y alertando sobre cualquier acceso no autorizado o comportamiento anómalo. Estos sistemas no solo capturan eventos de acceso, sino que también permiten analizar patrones de uso y generar informes detallados que pueden ser utilizados en auditorías de cumplimiento normativo.

Integrar dispositivos periféricos con un sistema SIEM como Splunk permite detectar intentos de acceso no autorizados o actividades sospechosas en tiempo real. Además, la generación de logs detallados y su correlación con otros eventos de la red es clave para mantener un cumplimiento continuo con las normativas descritas en el apartado 2.Marco Legal.

5.2.4.5 Gestión de Derechos de Información (IRM)

La Gestión de Derechos de Información (IRM) es una tecnología que permite establecer políticas sobre cómo se pueden utilizar y compartir los documentos una vez impresos, escaneados o copiados. Esto es especialmente relevante en entornos donde la confidencialidad de los datos es prioritaria.

Infraestructura y Tecnologías

Plataformas como Microsoft Azure Information Protection permiten aplicar etiquetas y políticas de seguridad a los documentos en el momento en que se crean, y estas políticas permanecen activas incluso cuando los documentos son impresos o escaneados. Esto asegura que los datos sensibles no sean compartidos o utilizados de manera inapropiada.

Por ejemplo, implementar una solución de IRM que se integre con el sistema de impresión y escaneo del centro permite aplicar políticas de seguridad específicas a los documentos manejados, asegurando que solo las personas autorizadas puedan acceder, copiar o distribuir información sensible, como se requiere en las normativas GDPR y LOPDGDD.

5.2.5 Flexibilidad y Escalabilidad

La flexibilidad y escalabilidad son aspectos clave para garantizar que la infraestructura de dispositivos periféricos pueda adaptarse y crecer con las necesidades de nuestra entidad de salud. La implementación de tecnologías como impresoras multifunción modulares, soluciones basadas en la nube, y plataformas de

gestión centralizada escalables asegura que la organización pueda ampliar su capacidad operativa sin sacrificar eficiencia o seguridad. Estas capacidades no solo preparan a la organización para manejar el crecimiento futuro, sino que también permiten una adaptación rápida y eficiente a los cambios en las necesidades operativas o regulatorias. La infraestructura flexible y escalable es, por lo tanto, una inversión estratégica que asegura la sostenibilidad y la capacidad de respuesta de la organización a lo largo del tiempo.

Esta escalabilidad está alineada con la necesidad de adaptarse a los cambios en el entorno tecnológico y regulatorio, tal como se describe en los procesos de ***Adquisición e Implementación (AI)*** y ***Monitoreo y Evaluación (ME)*** de COBIT. Al adoptar un sistema que puede crecer con la organización, se asegura una inversión sostenible y se facilita la implementación de nuevas tecnologías que mejoren la operatividad y seguridad.

5.2.5.1 Infraestructura Modular y Escalable

Una infraestructura modular permite que las organizaciones de salud amplíen o reduzcan su entorno de TI sin necesidad de una reconfiguración completa. Esto es especialmente importante en entornos donde la demanda de servicios puede variar significativamente.

Infraestructura y Tecnologías

Las impresoras multifunción (MFPs) modulares, como los Xerox VersaLink o HP LaserJet Enterprise son ejemplos de impresoras multifunción que pueden integrarse en una infraestructura modular. Estas impresoras permiten agregar módulos adicionales, como bandejas de papel adicionales, capacidades de acabado, o funcionalidades de escaneo mejoradas a medida que aumentan las necesidades de la organización.

Por ejemplo, en un entorno sanitario/administrativo de SNS, se puede comenzar con una configuración básica y, a medida que crece la demanda de impresión o escaneo, se pueden añadir módulos sin necesidad de reemplazar el hardware existente.

5.2.5.2 Soluciones en la Nube

Las soluciones basadas en la nube ofrecen una flexibilidad incomparable y la capacidad de escalar rápidamente en función de las necesidades de la organización. Estas soluciones permiten a las entidades de salud ampliar su capacidad de gestión de dispositivos periféricos sin necesidad de invertir en infraestructura física adicional.

Infraestructura y Tecnologías

Los servicios de Cloud Print como Papercut Mobility Print o Microsoft Universal Print son plataformas que permiten gestionar impresoras y trabajos de impresión a través de la nube. Estas soluciones son altamente escalables, lo que permite a las organizaciones añadir más usuarios o dispositivos sin necesidad de modificar la infraestructura local.

La adopción de una solución de impresión en la nube permitiría a la organización manejar la impresión de documentos desde cualquier lugar, facilitando el trabajo remoto o la expansión a nuevos sitios sin complicaciones logísticas significativas.

5.2.5.3 Integración con Sistemas Existentes

La flexibilidad también se manifiesta en la capacidad de las nuevas tecnologías para integrarse sin problemas con los sistemas y aplicaciones existentes en la organización. Esto es fundamental para minimizar la interrupción del servicio y aprovechar al máximo las inversiones previas en tecnología.

Infraestructura y Tecnologías

Muchas soluciones de gestión de impresión, como Papercut MF o Equitrac, ofrecen ***APIs*** abiertas y conectores para integrarse con sistemas de gestión documental, historiales médicos electrónicos (EHR), y otras aplicaciones críticas utilizadas en los entornos de salud.

La capacidad de integrar nuevos dispositivos y sistemas con las soluciones de gestión documental ya existentes (por ejemplo, sistemas de EHR como Cerner o Epic) es esencial. Esto asegura que los datos de los pacientes se puedan imprimir, escanear y gestionar de manera segura sin necesidad de reestructurar el flujo de trabajo.

5.2.5.4 Escalabilidad Horizontal y Vertical

La escalabilidad puede ser abordada tanto de manera horizontal (añadiendo más dispositivos al mismo nivel de funcionalidad) como vertical (mejorando las capacidades de los dispositivos existentes).

Infraestructura y Tecnologías

Los servidores de impresión en red escalables, como HP JetAdvantage y Xerox Workplace Suite, permiten la escalabilidad horizontal, permitiendo añadir más impresoras y usuarios a la red de impresión sin comprometer el rendimiento o la seguridad. Estos servidores de impresión en red son diseñados para manejar un número creciente de dispositivos y usuarios.

Algunos dispositivos periféricos pueden ser actualizados con kits que mejoran sus capacidades (por ejemplo, aumentar la velocidad de impresión, añadir nuevas funciones de seguridad, o mejorar la calidad de impresión). Esta escalabilidad vertical es crucial para extender la vida útil de los equipos y adaptarse a nuevas demandas sin necesidad de reemplazos costosos.

Un entorno sanitario/administrativo de SNS que empieza con una cantidad limitada de impresoras multifunción puede, con el tiempo, añadir más dispositivos (escalabilidad horizontal) o actualizar los existentes para manejar mayores volúmenes de trabajo o introducir nuevas funcionalidades (escalabilidad vertical), todo sin interrupciones significativas en el servicio.

5.2.5.5 Gestión Centralizada con Capacidad de Expansión

La gestión centralizada que puede expandirse para incluir más dispositivos y usuarios es fundamental en entornos donde la carga de trabajo y la infraestructura están en constante crecimiento.

Infraestructura y Tecnologías

Las plataformas de gestión centralizada, como Papercut MF y Equitrac, están diseñadas para gestionar miles de dispositivos y usuarios desde una única interfaz. Estas plataformas permiten la expansión de la red de impresión sin la necesidad de reconfigurar la infraestructura existente, y pueden escalar desde pequeñas implementaciones hasta entornos empresariales de gran tamaño.

Por ejemplo, en una entidad de salud que planea expandir su infraestructura de impresión y escaneo, el uso de una plataforma como Papercut MF facilita la adición de nuevas impresoras, sin importar su ubicación física, todo gestionado desde una consola central. Esto es clave para mantener la eficiencia operativa a medida que la organización crece.

5.2.6 Integración con Sistemas de Información Hospitalaria (HIS)

Un sistema de impresión centralizado en un entorno sanitario/administrativo de SNS que funcione en conjunto con un HIS (INTECO, 2018) no solo debe cumplir con altos estándares de seguridad y protección de datos, sino que también debe ser eficiente y fácil de gestionar. La implementación de tecnologías avanzadas, junto con el cumplimiento de normativas como las descritas en *2.Marco Legal*, asegura que el sistema esté preparado para manejar la información sensible de los pacientes de manera segura y conforme a la ley. Además, la infraestructura adecuada, como la segmentación de red y la autenticación robusta, es crucial para mantener la integridad del sistema en todo momento.

A continuación, se detallan algunos de los aspectos que debe cumplir este sistema:

5.2.6.1 Normativas y Cumplimiento

Para integrar de manera efectiva los documentos digitalizados en un Sistema de Información Hospitalaria (HIS), es esencial cumplir con una serie de normativas y estándares que aseguran la protección de la información de salud, la interoperabilidad entre sistemas y la seguridad de los datos. A continuación, se detallan las principales normativas y estándares a tener en cuenta:

Reglamento General de Protección de Datos (GDPR)

- **Protección de Datos Personales:** El sistema debe asegurar la protección de todos los datos personales impresos, asegurándose de que se cumplan los principios de minimización de datos, integridad y confidencialidad.
- **Derecho al Acceso y Borrado:** Debe ser posible rastrear y, si es necesario, eliminar registros de impresión que contengan datos personales, para cumplir con las solicitudes de acceso o borrado de datos por parte de los pacientes.

Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)

- **Gestión de Consentimientos:** El sistema debe ser capaz de gestionar y respetar los consentimientos otorgados por los pacientes respecto a la impresión de sus datos personales.
- **Registro de Actividades de Tratamiento:** Toda actividad de impresión que involucre datos personales debe registrarse adecuadamente para cumplir con los requisitos de la LOPDGDD.
- **Tratamiento de Datos Sensibles:** Esta ley complementa al GDPR en España y regula específicamente el tratamiento de datos sensibles, como los datos de salud. Es crucial asegurar que los documentos digitalizados que contienen datos de salud se manejen conforme a estas normativas.

Normas de Seguridad ISO/IEC 27001 e ISO/IEC 27799

- **ISO/IEC 27001:** Esta norma internacional establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Asegura que los datos de salud digitalizados estén protegidos contra amenazas de seguridad. (ISO, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, 2022)
- **ISO/IEC 27799:** Se centra en la gestión de la seguridad de la información en el sector de la salud y establece guías para proteger la información de salud personal. (ISO, Health informatics — Information security management in health using, 2016)

Ley de Autonomía del Paciente

- **Confidencialidad y Acceso:** Los sistemas que manejan documentos digitalizados deben garantizar que la información del paciente sea accesible únicamente por personal autorizado, manteniendo la confidencialidad y la privacidad del paciente.

Normativas Sanitarias Específicas

- **Normas de Seguridad de la Información en Entornos Sanitarios:** Cumplir con las guías establecidas para la protección de la información en sistemas de salud, como las especificaciones del Instituto Nacional de Ciberseguridad (INCIBE).

Estándares de Interoperabilidad HL7 y DICOM

- **HL7 (Health Level 7):** Es un conjunto de estándares para el intercambio electrónico de información clínica. Asegura que los documentos digitalizados se puedan integrar y compartir fácilmente entre diferentes sistemas HIS. (Standards Developing Organization, s.f.)
- **DICOM (Digital Imaging and Communications in Medicine):** Este estándar se utiliza principalmente para imágenes médicas, pero también puede aplicarse a documentos digitalizados que se deben

almacenar o transmitir de forma segura en un entorno sanitario/administrativo de SNS. (Standard, s.f.)

5.2.6.2 Necesidades Funcionales

Integración con el HIS

- **Interoperabilidad:** El sistema de impresión debe integrarse sin problemas con el HIS, permitiendo la impresión directa de documentos clínicos, resultados de pruebas, recetas y otros informes desde cualquier terminal conectada al HIS.
- **Gestión de Accesos Basada en Roles (RBAC):** Los permisos de impresión deben alinearse con las funciones del personal en el HIS. Por ejemplo, solo personal autorizado debería poder imprimir documentos sensibles como historiales médicos o resultados de pruebas.
- **Auditoría y Trazabilidad:** Debe ser posible rastrear quién imprimió qué documentos, cuándo y desde qué terminal. Esta trazabilidad es esencial para mantener un registro preciso y cumplir con las normativas de protección de datos.

Seguridad de la Información

- **Cifrado de Datos:** Tanto los datos en tránsito (desde el HIS al sistema de impresión) como los datos en reposo (almacenados temporalmente en servidores de impresión) deben estar cifrados para evitar accesos no autorizados.
- **Autenticación y Autorización:** Es crucial implementar mecanismos de autenticación robustos, como tarjetas inteligentes, autenticación biométrica o códigos PIN, para asegurar que solo el personal autorizado pueda liberar los trabajos de impresión.
- **Protección contra Fugas de Información:** Deben existir políticas que eviten que documentos sensibles se queden sin recoger en impresoras compartidas, utilizando técnicas como la liberación segura de impresión o impresión confidencial.

5.2.6.3 Necesidades para Cifrar Documentos Digitalizados en Formato DICOM

Para cifrar documentos digitalizados en formato DICOM y garantizar su seguridad durante el almacenamiento y transmisión, se deben seguir ciertas pautas y utilizar tecnologías específicas:

Cifrado DICOM

- **DICOM Secure Transport Connection Profile:** Este perfil especifica el uso de cifrado TLS (Transport Layer Security) para proteger los datos durante la transmisión. Es fundamental para asegurar que los documentos digitalizados no sean interceptados o alterados durante su transferencia entre sistemas.
- **Uso de Certificados Digitales:** El cifrado en DICOM suele requerir el uso de certificados digitales para autenticar las conexiones y asegurar que los datos se transmitan entre partes confiables.
- **Cifrado de Datos en Reposo:** Además del cifrado en tránsito, es esencial cifrar los datos en reposo. Esto significa que los archivos DICOM almacenados en servidores, discos duros o cualquier otro medio de almacenamiento deben estar cifrados usando algoritmos como AES (Advanced Encryption Standard) para evitar accesos no autorizados.

Gestión de Claves Criptográficas

- **Infraestructura de Clave Pública (PKI):** Para manejar de manera efectiva el cifrado y descifrado de documentos DICOM, es necesario implementar una infraestructura de clave pública. PKI permite la emisión, distribución y validación de certificados digitales, asegurando que solo las partes autorizadas puedan acceder a los datos cifrados.
- **Rotación de Claves:** Las claves criptográficas deben ser rotadas regularmente para reducir el riesgo de que sean comprometidas. Además, es fundamental implementar políticas de gestión de claves, asegurando que estas sean almacenadas y protegidas adecuadamente.

Autenticación y Control de Acceso

- **Integración con Active Directory:** Para asegurar que solo personal autorizado pueda acceder y manipular documentos digitalizados en formato DICOM, se recomienda integrar el sistema de cifrado con Active Directory u otro sistema de autenticación centralizado. Esto permite aplicar políticas de acceso basadas en roles y garantizar que solo los usuarios con los permisos adecuados puedan descifrar y acceder a los documentos.
- **Autenticación Multifactor (MFA):** Implementar MFA es crucial para proteger el acceso a los sistemas que manejan documentos cifrados en DICOM. Esto añade una capa adicional de seguridad, reduciendo el riesgo de accesos no autorizados.

Interoperabilidad y Cumplimiento Normativo

- **Cumplimiento con HL7 y DICOM:** Es esencial que los sistemas que gestionan documentos cifrados en DICOM cumplan con los estándares de interoperabilidad HL7 y DICOM. Esto asegura que los documentos puedan ser integrados y compartidos eficientemente entre diferentes sistemas HIS, sin comprometer su seguridad.
- **Auditorías y Registros de Acceso:** Los sistemas deben registrar todas las actividades relacionadas con el acceso y manipulación de documentos DICOM cifrados. Esto no solo es crucial para el cumplimiento normativo, sino también para la identificación y mitigación de posibles incidentes de seguridad.

5.2.6.4 Necesidades Técnicas

Para integrar un sistema centralizado de impresión que sea compatible con un Sistema de Información Hospitalaria (HIS) y que los documentos impresos se generen en formato DICOM, se requiere una infraestructura especializada, un sistema de ficheros adecuado, y software específico que permita esta funcionalidad. A continuación, se detallan los componentes necesarios:

Infraestructuras

Partimos de un escenario ya en funcionamiento por lo que el servicio de DICOM y PACS (Picture Archiving and Communication System), donde se almacenan, gestionan, y distribuyen imágenes médicas y documentos en este formato. Además, un sistema PACS puede integrarse para gestionar grandes volúmenes de datos de imágenes médicas, incluyendo documentos impresos en formato DICOM.

A esta arquitectura podemos añadir el servicio de impresoras médicas DICOM, dispositivos especializados que puedan recibir y procesar directamente archivos en formato DICOM. Estas impresoras están diseñadas para el entorno sanitario/administrativo de SNS y pueden integrarse con sistemas HIS y PACS.

Sistema de Ficheros

- **Sistema de Ficheros DICOM-Optimizado:** El sistema de ficheros debe estar optimizado para manejar grandes cantidades de datos en formato DICOM. Se recomienda utilizar sistemas como ***NFS (Network File System)*** o ***CIFS (Common Internet File System)*** con soporte para archivos de gran tamaño y características como de duplicación y compresión, que son útiles para gestionar eficientemente el almacenamiento de imágenes médicas.
- **Compatibilidad con PACS:** El sistema de ficheros debe ser compatible con PACS para facilitar el almacenamiento, recuperación, y distribución de documentos DICOM, integrándose sin problemas con el flujo de trabajo de imágenes médicas de los centros sanirarios de SNS.

Software

- **Software de Integración DICOM:**
    - **Middleware DICOM:** Es necesario un middleware que permita convertir los documentos generados por el sistema centralizado de impresión al formato DICOM. Software como DICOM Print Server o DICOM Printer puede transformar cualquier documento en un archivo DICOM, listo para ser archivado o impreso.

- **Integración con HIS y PACS:** El software debe ser capaz de integrarse con el HIS del centro sanitario de SNS para garantizar que los documentos generados y convertidos a DICOM se asocien correctamente con los registros de los pacientes. Esto incluye la vinculación de los documentos con los IDs de los pacientes y su almacenamiento adecuado en el PACS.
- **Software de Gestión de Impresión:** Implementar un sistema de gestión de impresión que sea compatible con DICOM. Este software debe manejar la cola de impresión, aplicar políticas de impresión seguras y garantizar que los documentos se conviertan y almacenen en el formato correcto. Ejemplos de este tipo de software incluyen NDD Print 360 y Cortado Cloud Print.

Seguridad y Cifrado

- **Cifrado de Documentos DICOM:** Es fundamental incluir software que cifre los documentos en formato DICOM tanto en reposo como en tránsito. Soluciones de cifrado como Vormetric Data Security Platform pueden integrarse para ofrecer un cifrado robusto con gestión centralizada de claves.

5.2.6.5 Beneficios Operacionales y de Seguridad

- **Reducción de Errores Humanos:** Al automatizar la gestión de permisos y accesos mediante la integración con el HIS, se minimiza el riesgo de errores humanos que puedan llevar a la divulgación de información sensible.
- **Eficiencia y Productividad:** La capacidad de gestionar y liberar trabajos de impresión de manera centralizada reduce el tiempo que el personal médico dedica a tareas administrativas, permitiéndoles concentrarse en la atención al paciente.
- **Mejora en la Seguridad de la Información:** Al implementar medidas de seguridad robustas y asegurar el cumplimiento normativo, se reduce el riesgo de violaciones de datos y se protege la privacidad de los pacientes.

La integración de documentos digitalizados con un HIS requiere un enfoque robusto en términos de cumplimiento normativo, seguridad y cifrado. Cumplir con normativas como el GDPR y la LOPDGDD, utilizar estándares de interoperabilidad como HL7 y DICOM, y aplicar medidas de seguridad como el cifrado de datos en tránsito y en reposo son pasos fundamentales para proteger la información de salud en un entorno sanitario/administrativo de SNS. Implementar una infraestructura adecuada para la gestión de claves criptográficas, autenticación y control de accesos garantiza que solo personal autorizado pueda acceder a documentos críticos, reduciendo el riesgo de violaciones de seguridad y mejorando la protección de los datos de los pacientes.

6 Caso de Uso Aplicado al Servicio Nacional de Salud

En el contexto actual de la sanidad digital, la correcta gestión de la información médica es un factor determinante para garantizar una atención sanitaria de calidad. No solo las imágenes médicas, sino también la documentación clínica, deben gestionarse de manera eficiente para asegurar un tratamiento integral del paciente. Los sistemas de archivo y comunicación de imágenes (PACS) juegan un papel crucial en la gestión de las imágenes médicas dentro del Sistema Nacional de Salud (SNS), facilitando el almacenamiento, acceso y análisis de estudios como radiografías, tomografías y resonancias magnéticas. Sin embargo, para ofrecer una visión completa del historial clínico del paciente, es igualmente importante integrar los informes clínicos y documentos asociados en el Sistema de Información Hospitalaria (HIS). Esta integración garantiza que, además de las imágenes, los profesionales de la salud tengan acceso instantáneo a toda la información relevante del paciente, como informes médicos y consentimientos informados, mejorando así la toma de decisiones y la continuidad del tratamiento.

A medida que los hospitales reciben un volumen creciente de imágenes médicas y documentación clínica provenientes de clínicas y centros externos en formatos digitales como CDs, memorias USB, entre otros, la necesidad de un proceso automatizado, seguro y centralizado se vuelve cada vez más crítica. Este caso de uso propone la implementación de un sistema centralizado que no solo permita la verificación, carga y gestión segura de las imágenes en el PACS, sino que también integre de manera automatizada la documentación clínica en el HIS del hospital. Esta solución asegura la integridad de todos los datos, tanto imágenes como informes médicos, y facilita su disponibilidad inmediata para los profesionales de la salud. Al mismo tiempo, se garantiza el cumplimiento de normativas vigentes, como el Reglamento General de Protección de Datos (GDPR) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), reforzando la seguridad y la confidencialidad de la información sensible del paciente.

El Complejo Hospitalario Universitario Insular Materno Infantil de Gran Canaria (CHUIMI), como uno de los centros de referencia del archipiélago canario, enfrenta el desafío de integrar tanto las imágenes médicas como la documentación clínica proveniente de CDs (u otros formatos digitales) entregados por centros externos y trasladados en mano por el paciente o médicos al propio hospital. Este proceso, que hasta ahora ha sido gestionado de manera manual y descentralizada, no solo presenta riesgos en términos de eficiencia y seguridad de los datos, sino que también constituye una barrera para la optimización del flujo de trabajo y la integración de la información clínica. La falta de automatización en la inclusión de imágenes en el PACS y la digitalización de los informes clínicos impide un acceso rápido y seguro a toda la información del paciente, afectando la calidad de la atención y dificultando el cumplimiento de las normativas de protección de datos.

Por tanto, este caso se centra en implementar un sistema centralizado para la inclusión automatizada de imágenes médicas y de la documentación clínica provenientes de centros externos y recibidas en formatos físicos, integrándolas en el PACS y HIS del propio hospital. Este proceso se alinea con las mejores prácticas en gobernanza de TI y gestión de riesgos. El análisis se enmarca dentro de la aplicación de la metodología COBIT para la gobernanza y gestión de tecnologías de la información, y utiliza herramientas como el análisis DAFO para identificar las fortalezas, debilidades, oportunidades y amenazas del proceso actual. Con ello, se busca desarrollar una propuesta de mejora que no solo optimice el flujo de trabajo, sino que también fortalezca la seguridad y el cumplimiento normativo, contribuyendo así a la eficiencia global del Sistema Nacional de Salud.

6.1 Contexto del Caso

6.1.1 Descripción del Entorno

El CHUIMI se compone de dos grandes áreas: el Hospital Universitario Insular de Gran Canaria y el Hospital Materno Infantil de Canarias, ambas instalaciones forman parte del Servicio Canario de Salud y atienden a una amplia población tanto en Gran Canaria como en las islas cercanas.

- **Especialidades y Servicios:** Este hospital es un centro de atención terciaria, lo que significa que ofrece una amplia gama de servicios especializados, incluyendo cardiología, neurología, oncología, y cirugía de alta complejidad. Además, es un centro de referencia para la formación de profesionales sanitarios, colaborando estrechamente con la Universidad de Las Palmas de Gran Canaria.
- **Especialización en Salud Infantil y Materna:** Esta instalación se dedica principalmente a la atención de la salud de mujeres y niños. Es un centro de referencia en ginecología, obstetricia, neonatología, y pediatría. Ofrece servicios especializados como cirugía pediátrica y unidades de cuidados intensivos neonatales.
- **Tecnología e Innovación:** Es pionero en la incorporación de tecnologías avanzadas en la atención médica, con un enfoque en la innovación. Uno de sus recursos clave es el uso del PACS para la gestión de imágenes médicas, permitiendo a los profesionales de la salud acceder de manera rápida y eficiente a las imágenes diagnósticas desde cualquier área del hospital. Este sistema no solo agiliza el flujo de trabajo, sino que también garantiza un acceso inmediato a las imágenes en situaciones críticas. En esta línea, es crucial avanzar hacia una integración completa, incorporando no solo las imágenes en el PACS, sino también la documentación clínica en HIS. Esto asegurará que, junto con las imágenes, los informes médicos y demás documentación relevante sean fácilmente accesibles y gestionados de forma centralizada, optimizando la atención al paciente y mejorando la toma de decisiones clínica
- **Colaboración y Referencia:** Debido a su relevancia en el área de la salud materno-infantil, este hospital colabora frecuentemente con otros centros sanitarios, gestionando un flujo constante de pacientes remitidos desde otras islas o centros médicos. Esto genera la necesidad no solo de gestionar las imágenes médicas a través del PACS, sino también de integrar adecuadamente la documentación clínica que acompaña a estos pacientes en el HIS. La gestión correcta de estos informes clínicos y las imágenes garantizan que toda la información relevante esté disponible inmediatamente para los especialistas, mejorando la calidad de la atención y facilitando el seguimiento clínico de los pacientes hospitalizados.

Interacción con Centros Externos

El CHUIMI recibe regularmente una cantidad considerable de imágenes médicas y su documentación clínica asociada de pacientes provenientes de otros hospitales, clínicas privadas y centros de salud, no solo de Gran Canaria, sino también de las islas vecinas y centros privados. Esta información se recibe en soportes digitales (tales como CDs), incluyendo estudios radiológicos esenciales y, en muchos casos, informes clínicos que son fundamentales para la continuidad del tratamiento. La correcta gestión de esta información es vital para garantizar que los profesionales de la salud puedan acceder no solo a las imágenes en el PACS, sino también a los informes y otros documentos clínicos a través del HIS, permitiendo un tratamiento integral del paciente. Además, los pacientes también pueden acceder a su historial médico e imágenes a través de la Carpeta de Salud (miHistoria), una plataforma electrónica que facilita el acceso a su información médica y sanitaria de forma segura y confidencial, (Canarias G. d., 2023).

A continuación, se presenta un gráfico que muestra la evolución del volumen de órdenes de inclusión de imágenes en el sistema PACS, desde enero de 2023 hasta agosto de 2024 en el CHUIMI. Durante este período, se observa una tendencia al alza, con picos significativos que reflejan una carga de trabajo considerable en ciertos meses. Este incremento destaca la creciente importancia de contar con un sistema automatizado y eficiente que permita gestionar tanto las imágenes como la documentación asociada de manera rápida y segura, mejorando la capacidad del hospital para manejar un flujo de datos cada vez mayor.

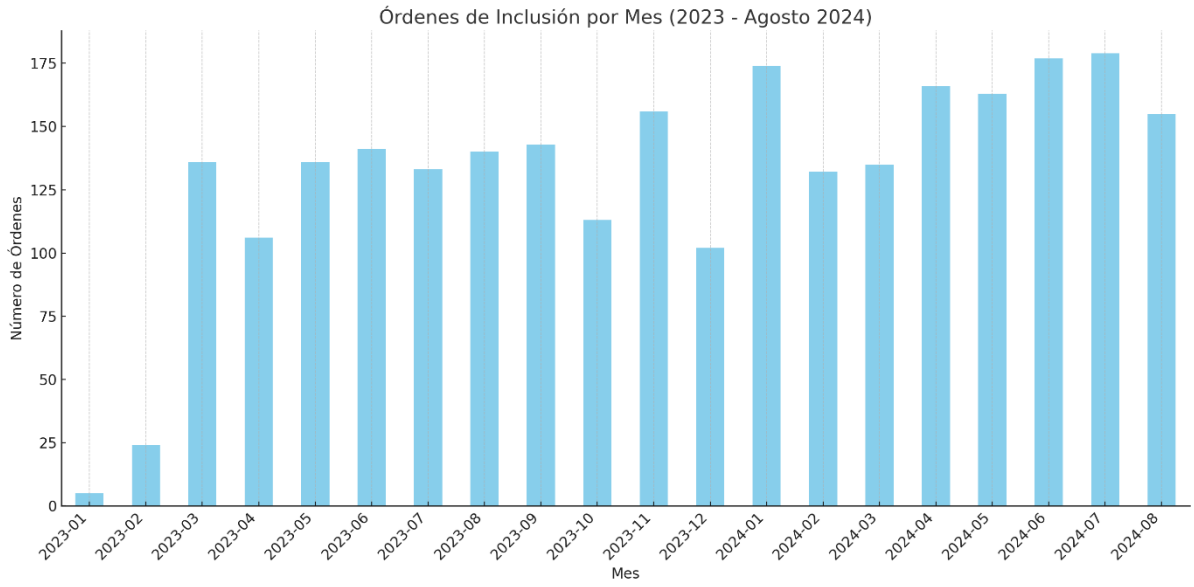


Ilustración 7. Evolución del volumen de órdenes de inclusión de imágenes de centros externos

El año 2023 comienza con un volumen de órdenes moderado, con alrededor de 100 a 140 órdenes por mes durante los primeros cinco meses. Este rango ya representa una carga de trabajo significativa, pero aún manejable por el equipo de trabajo. Sin embargo, a partir de junio de 2023, se nota un incremento drástico en el número de órdenes, superando las 140 órdenes mensuales y alcanzando un pico de aproximadamente 180 órdenes en julio de 2023. Al entrar en 2024, el volumen de órdenes continúa en ascenso. Cada mes desde enero hasta agosto de 2024 presenta un incremento constante, con cifras que superan las 150 órdenes por mes, alcanzando un máximo de alrededor de 179 órdenes en julio de 2024. Esta tendencia indica una creciente demanda y posiblemente una expansión en las actividades o necesidades que requieren la inclusión de imágenes en el sistema PACS.

Este incremento sostenido sugiere que el equipo responsable de gestionar estas órdenes ha enfrentado un volumen de trabajo considerablemente alto, especialmente en los últimos meses del periodo analizado. La carga máxima registrada en julio de 2024 es aproximadamente un 80% mayor que la observada a principios de 2023. En resumen, el gráfico refleja no solo el volumen de órdenes procesadas, sino también el creciente desafío que supone mantener el ritmo frente a una demanda en constante aumento. Esta tendencia indica que, si no se toman medidas para gestionar la carga de trabajo, el equipo podría enfrentarse a problemas de capacidad en un futuro cercano.

La integración adecuada de las imágenes y documentos clínicos en los sistemas del hospital es de vital importancia para garantizar una atención médica de calidad. El PACS es el sistema central donde se almacenan y gestionan todas las imágenes médicas, permitiendo a los profesionales de la salud acceder de manera rápida y eficaz a la información necesaria para emitir diagnósticos precisos y ofrecer tratamientos oportunos. Aunque el HIS se encarga de gestionar la información administrativa y clínica, los informes médicos y la documentación clínica asociados a las imágenes aún no pueden integrarse en el HIS.

Actualmente, el proceso de inclusión de las imágenes médicas provenientes de soportes digitales en el PACS es completamente manual, lo que requiere la intervención de técnicos para verificar y cargar las imágenes en el sistema. Este procedimiento, además de ser laborioso, puede generar retrasos y errores que impactan la eficiencia operativa. Por otro lado, los informes clínicos que también llegan en dichos soportes no pueden integrarse en el HIS, ni de forma manual ni automatizada, lo que obliga a gestionar estos documentos por separado. Esta falta de integración no solo afecta la rapidez en el acceso a la información médica, sino que también incrementa el riesgo de comprometer la seguridad y privacidad de los datos, un aspecto fundamental para cumplir con normativas como el GDPR y la LOPDGDD.

El volumen de datos que maneja el hospital es considerable, con un flujo constante de imágenes médicas que deben ser procesadas y almacenadas de manera segura.

Dentro de este contexto, a nivel Comunidad Autónoma, el Servicio Canario de Salud se encuentra en la fase de puesta en marcha de un proyecto que establece los requisitos y condiciones de un visor universal de imagen diagnóstica . Este proyecto tiene como objetivo mejorar la gestión, acceso y almacenamiento de las imágenes médicas tanto radiológicas como no radiológicas en todo el sistema sanitario canario. El visor será del tipo Zero-Footprint, lo que permite acceder a las imágenes desde cualquier dispositivo sin necesidad de instalar software adicional. Además, se contempla la integración con los sistemas de gestión de imagen actuales (PACS) y la interoperabilidad con otros sistemas del SCS, incluyendo un sistema RIS para dar soporte a las distintas pruebas diagnósticas (Servicio Canario de la Salud, 2023). Sin embargo, el proyecto no aborda los estudios realizados de forma privada por el paciente que requieran de su inclusión en el HIS/PACS del SCS.

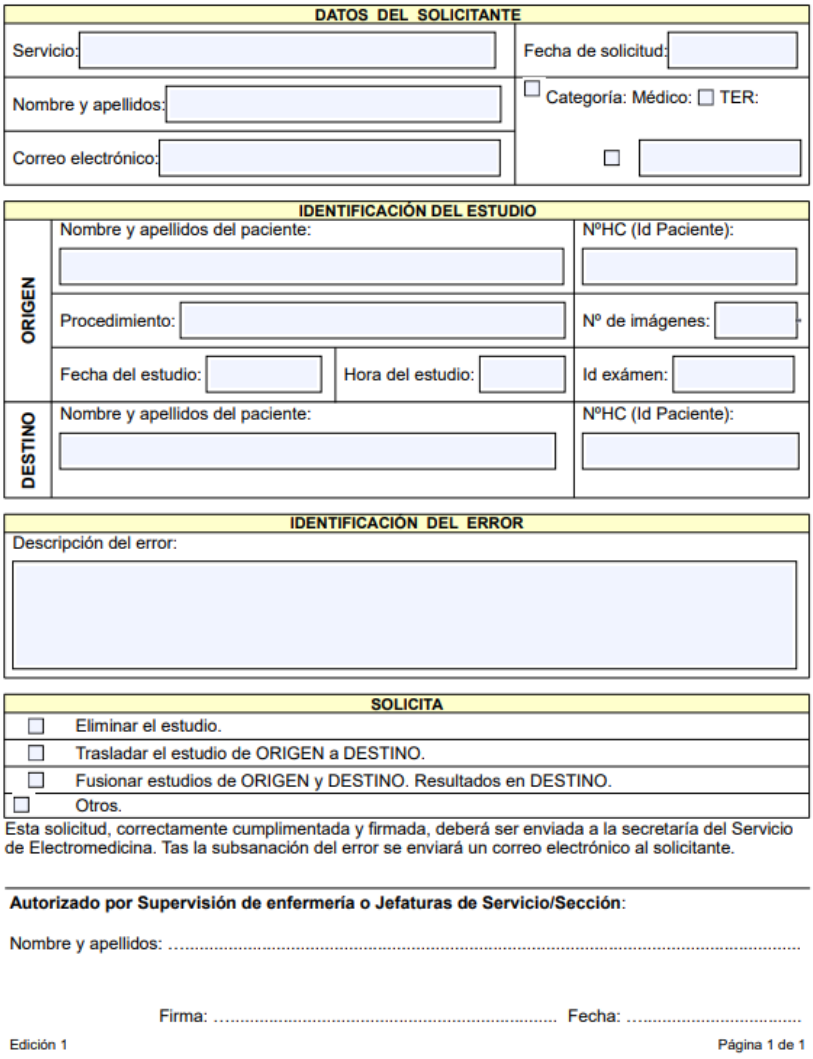
En este contexto, es evidente la necesidad de un sistema más robusto y eficiente que permita la inclusión rápida y segura de estas imágenes en el PACS. Aunque actualmente los informes clínicos no pueden integrarse directamente en el HIS actualmente, avanzar hacia soluciones que permitan mejorar el manejo de ambos tipos de información es clave para garantizar que la infraestructura tecnológica del hospital esté a la altura de su papel como centro de referencia en la atención sanitaria del archipiélago.

6.2 Problemas Actuales

El proceso actual de inclusión de soportes digitales (tales como CDs) con imágenes médicas y documentación clínica provenientes de centros externos en el PACS y el HIS del CHUIMI presenta varias limitaciones y desafíos que afectan tanto la eficiencia operativa como la seguridad de los datos y el cumplimiento normativo.

En la actualidad, son entregados físicamente al hospital por los propios pacientes o por el médico de referencia. Este proceso manual no solo es propenso a errores humanos, sino que también representa un riesgo logístico importante, ya que la pérdida o daño de los CDs podría resultar en la pérdida de información médica crucial, tanto de las imágenes como de los informes clínicos asociados.

Una vez que el CD llega al hospital, el médico responsable debe generar manualmente un documento de solicitud de corrección de errores (siguiente figura). Este documento contiene los datos identificativos del paciente y del estudio a incluir en el PACS. Además, si el CD contiene un informe clínico, el médico debe leerlo y, si es necesario, mecanizar manualmente la información relevante en el HIS del hospital, lo que añade una carga adicional al proceso. La generación manual de este documento es un proceso que consume tiempo y está sujeto a posibles errores, como la entrada incorrecta de datos, lo que podría complicar la correcta asociación tanto de las imágenes con el PACS. Estos errores no solo retrasan el proceso, sino que también incrementan el riesgo de afectar la calidad del tratamiento al no disponer de toda la información necesaria en tiempo y forma.



DATOS DEL SOLICITANTE

Servicio: | Fecha de solicitud:

Nombre y apellidos: | ☐ Categoría: Médico: ☐ TER:

Correo electrónico: | ☐

IDENTIFICACIÓN DEL ESTUDIO

ORIGEN

Nombre y apellidos del paciente: | NºHC (Id Paciente):

Procedimiento: | Nº de imágenes:

Fecha del estudio: | Hora del estudio: | Id exámen:

DESTINO

Nombre y apellidos del paciente: | NºHC (Id Paciente):

IDENTIFICACIÓN DEL ERROR

Descripción del error:

SOLICITA

☐ Eliminar el estudio.

☐ Trasladar el estudio de ORIGEN a DESTINO.

☐ Fusionar estudios de ORIGEN y DESTINO. Resultados en DESTINO.

☐ Otros.

Esta solicitud, correctamente cumplimentada y firmada, deberá ser enviada a la secretaría del Servicio de Electromedicina. Tas la subsanación del error se enviará un correo electrónico al solicitante.

Autorizado por Supervisión de enfermería o Jefaturas de Servicio/Sección:

Nombre y apellidos: .....

Firma: ..... Fecha: .....

Edición 1 Página 1 de 1

Ilustración 8. Documento de solicitud de corrección de errores

Tras generar la solicitud, el documento es impreso y enviado en conjunto con el CD al servicio de electromedicina. Este paso adicional no solo retrasa el proceso, sino que también aumenta la probabilidad de que se produzcan errores en la transferencia de datos, así como la posibilidad de pérdida o mal manejo de los documentos impresos y CDs.

El servicio de electromedicina es responsable de incluir los estudios en el PACS utilizando estaciones de trabajo especializadas en radiodiagnóstico. Este proceso manual implica la inserción del CD, la verificación de los datos, y la carga de las imágenes en el sistema PACS. La dependencia de estaciones específicas y la necesidad de intervención manual aumentan el riesgo de errores en la inclusión de los estudios, además de limitar la capacidad del hospital para procesar múltiples solicitudes de manera eficiente.

Finalmente, una vez que el estudio ha sido incluido en el PACS, el servicio de electromedicina notifica al usuario (ya sea el médico que solicitó el proceso o el paciente) de que la imagen está disponible. Este proceso de notificación manual puede generar demoras adicionales y no siempre garantiza que el usuario reciba la información de manera oportuna, lo que puede afectar la continuidad de la atención médica. La siguiente figura presenta un diagrama de flujo del proceso actual descrito.

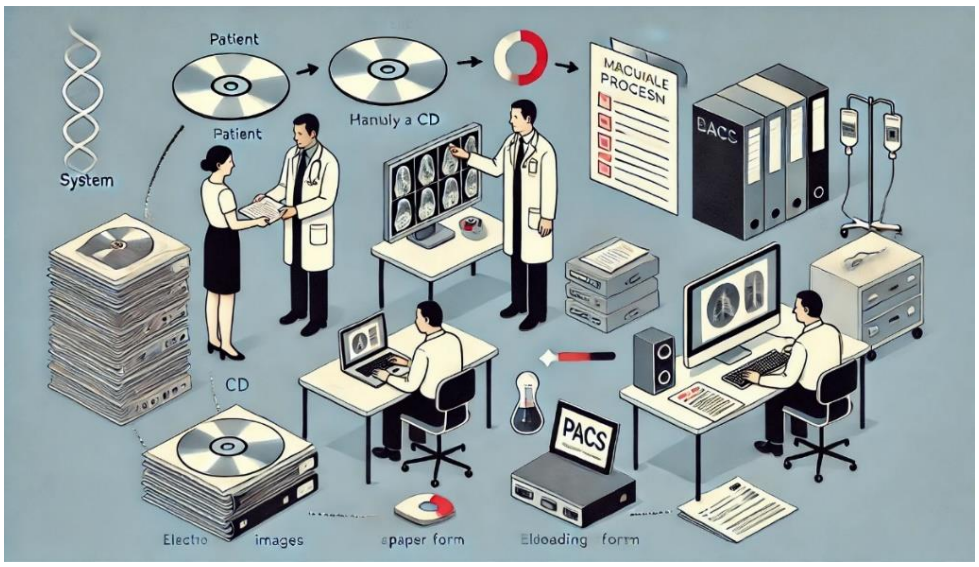


Ilustración 9. Diagrama de flujo del proceso actual de integración de estudios externos en soportes físicos

6.2.1 Principales Desafíos

- **Ineficiencia Operativa**: La dependencia de procesos manuales y físicos (entrega de CDs, generación de documentos, impresión y traslado de materiales) introduce varios puntos de ineficiencia. Cada uno de estos pasos consume tiempo y recursos, lo que puede retrasar la disponibilidad de las imágenes en el PACS y, por lo tanto, la capacidad del personal médico para tomar decisiones clínicas informadas. Además, la ineficiencia se agrava por el hecho de que los informes clínicos incluidos en el CD deben ser leídos y, si es necesario, mecanizados manualmente por el médico en el HIS, lo que añade más tiempo al proceso y aumenta la posibilidad de errores.
- **Riesgos de Seguridad y Cumplimiento**: El manejo manual de datos sensibles (tanto en formato físico como digital) presenta riesgos significativos para la seguridad y privacidad de la información del paciente. La falta de automatización y control centralizado dificulta la implementación de medidas de seguridad robustas y el cumplimiento de normativas como el GDPR y la LOPDGDD. La intervención manual en la gestión de los informes clínicos también incrementa la exposición a riesgos de privacidad y posibles fugas de información.
- **Alta Dependencia de Recursos Humanos**: El proceso actual depende en gran medida del personal de electromedicina para la inclusión de imágenes en el PACS. Esto no solo genera una carga adicional para el equipo, sino que también crea un cuello de botella en el flujo de trabajo, especialmente en momentos de alta demanda. Asimismo, la necesidad de que el médico lea y mecanice el informe clínico manualmente en el HIS añade más trabajo, lo que puede retrasar la atención y generar aún más presión sobre el personal.
- **Inconsistencia en la Calidad de Datos**: La generación manual de documentos y la intervención manual en la inclusión de imágenes pueden dar lugar a errores en la entrada de datos, lo que a su vez puede afectar la correcta asociación de las imágenes con la historia clínica del paciente. Además, el hecho de que los informes clínicos deban ser mecanizados manualmente por el médico en el HIS aumenta el riesgo de errores en la transcripción de datos, comprometiendo la precisión de los diagnósticos y la efectividad del tratamiento.

6.3 Objetivos del Proyecto

OBJ-1. Centralización del Proceso de Inclusión de CDs

- **Descripción**: Desarrollar e implementar un sistema centralizado que automatice la inclusión de CDs en el PACS para imágenes y en el HIS para la documentación clínica. Esto eliminará la necesidad de manejar físicamente los CDs y de mecanizar manualmente los informes, permitiendo que ambos tipos de datos se integren automáticamente en sus respectivos sistemas.

- **Beneficio**: Reducir los tiempos de procesamiento, mejorar la eficiencia operativa y minimizar la posibilidad de pérdida o daño de datos durante el manejo manual.

OBJ-2. Automatización del Flujo de Trabajo

- **Descripción**: Automatizar las tareas involucradas en la inclusión de CDs, desde la verificación de datos hasta la carga de imágenes en el PACS y la integración automática de los informes clínicos en el HIS. Esto incluye la eliminación de tareas manuales como la generación de documentos, lectura de informes y mecanización de datos.
- **Beneficio**: La automatización reducirá la carga de trabajo del personal técnico y médico, minimizará los errores humanos, y permitirá que el personal se enfoque en tareas de mayor valor. Además, asegurará una disponibilidad más rápida tanto de las imágenes como de la documentación clínica para su uso clínico.

OBJ-3. Mejorar de la Seguridad de los Datos

- **Descripción**: Implementar medidas de seguridad avanzadas para proteger tanto las imágenes médicas como la documentación clínica durante el proceso de inclusión automática. Esto incluye el cifrado de datos, la autenticación de usuarios y la auditoría constante del acceso a la información, garantizando que se cumplan las normativas de seguridad como el GDPR y la LOPDGDD.
- **Beneficio**: Se asegurará un manejo seguro y confidencial de los datos médicos y clínicos, reduciendo significativamente el riesgo de brechas de seguridad y garantizando la privacidad del paciente en cada fase del proceso automatizado.

OBJ-4. Optimización del Tiempo de Respuesta

- **Descripción**: Optimizar el tiempo que transcurre desde la recepción del CD hasta que las imágenes estén disponibles en el PACS y los informes clínicos sean accesibles en el HIS. Esto se logrará a través de la automatización del proceso de inclusión y la eliminación de los pasos manuales.
- **Beneficio**: Aumentará la velocidad con la que los profesionales de la salud pueden acceder a la información crítica, mejorando significativamente la capacidad del hospital para ofrecer diagnósticos y tratamientos oportunos y eficientes.

OBJ-5. Integración con Otros Sistemas del Hospital

- **Descripción**: Asegurar que el nuevo sistema automatizado de inclusión de CDs se integre completamente con los sistemas de gestión de información de salud (HIS) y otros sistemas digitales del hospital, permitiendo que tanto las imágenes como los informes clínicos se gestionen de manera centralizada y automática.
- **Beneficio**: Mejorará la interoperabilidad y garantizará un flujo de información continuo y sin interrupciones, facilitando el acceso a datos tanto de imágenes como de documentos clínicos, mejorando así la eficiencia operativa y la calidad de la atención médica.

6.4 Alcance del Proyecto

El proyecto de implementación de un sistema centralizado y automatizado para la inclusión de CDs en el PACS del CHUIMI abarca diversas áreas clave del hospital, implicando tanto a departamentos especializados como a procesos críticos dentro de la institución. Este proyecto no solo se enfoca en la automatización de la inclusión de imágenes médicas, sino que también busca integrar de manera eficiente la documentación clínica asociada en el HIS, optimizando el flujo de trabajo en todo el hospital. La implementación afectará áreas como electromedicina, radiología y administración, garantizando una mejora en la gestión de la información médica y reduciendo los tiempos de respuesta, minimizando riesgos y asegurando el cumplimiento de normativas de seguridad de datos.

6.4.1 Áreas Involucradas

El Servicio de Radiología será uno de los principales beneficiados por este proyecto, ya que es el usuario principal del PACS. La centralización y automatización de la inclusión de CDs permitirá a los radiólogos acceder tanto a las imágenes médicas como a la documentación clínica asociada de manera más rápida y confiable, mejorando su capacidad para emitir diagnósticos oportunos (OBJ-4).

El Servicio de Electromedicina también tendrá un papel crucial en esta transición. Actualmente, este servicio se encarga de la inclusión manual de los CDs en el PACS, así como de la gestión de informes clínicos que deben mecanizarse en el HIS. Con la automatización, ambas tareas se volverán más eficientes y menos propensas a errores (OBJ-2). Además, el personal de este servicio recibirá formación específica para manejar el nuevo sistema y gestionar posibles incidencias técnicas relacionadas con la inclusión automatizada de imágenes y documentos (OBJ-3).

Por otro lado, el Servicio de Informática será responsable de la implementación técnica del sistema, asegurando que se integre sin problemas tanto con el PACS como con el HIS y otros sistemas ya existentes en el hospital (OBJ-5). Este departamento también se encargará de mantener la infraestructura de TI y las medidas de seguridad, lo cual es esencial para el éxito del proyecto (OBJ-3).

Finalmente, la Dirección Médica, en conjunto con la Dirección de Gestión y Servicios, supervisarán el proyecto desde una perspectiva estratégica, garantizando que los recursos se asignen adecuadamente y que el proyecto avance según lo planificado. Además, se asegurarán de que el sistema respete las normativas y se alinee con los objetivos institucionales, mejorando tanto la operativa como el cumplimiento normativo (OBJ-3 y OBJ-5).

6.4.2 Procesos Incluidos

El proyecto tiene como objetivo automatizar varios procesos que actualmente son manuales y consumen tiempo. Se implementará un sistema que valide automáticamente los CDs cuando sean recibidos, asegurando que tanto las imágenes como los informes clínicos sean correctos antes de su inclusión en el PACS y HIS, respectivamente (OBJ-2 y OBJ-3). Esta automatización eliminará la mayor parte de la intervención manual, reduciendo significativamente los errores y mejorando la seguridad de los datos.

Además, la generación y gestión de la documentación clínica, que hoy en día es una tarea que recae sobre los médicos, será completamente automatizada. Esto acelerará el proceso y garantizará que los datos clínicos se manejen con mayor precisión y consistencia, tanto en el PACS para las imágenes como en el HIS para los informes clínicos (OBJ-2).

Uno de los aspectos clave será la inclusión automatizada de las imágenes en el PACS y de los informes clínicos en el HIS. Este nuevo sistema permitirá que tanto las imágenes como la documentación se carguen de manera rápida y segura, mejorando la disponibilidad de información crítica para los profesionales médicos y agilizando los diagnósticos (OBJ-1 y OBJ-4).

Finalmente, se implementará un sistema de notificaciones automatizadas que informará a los usuarios, ya sean médicos o pacientes, cuando las imágenes y los informes clínicos estén disponibles en el PACS y HIS. Esto mejorará la comunicación interna y reducirá los tiempos de espera para el acceso a la información médica (OBJ-4).

6.4.3 Sistemas y Tecnologías

El PACS, como núcleo central de este proyecto, se verá significativamente beneficiado por las mejoras implementadas. Con la inclusión automatizada tanto de imágenes como de informes clínicos desde los CDs, el PACS podrá gestionar las imágenes de manera más eficiente, asegurando que estén disponibles para su revisión en menos tiempo y con una mayor seguridad (OBJ-4 y OBJ-3). Además, esto reducirá la intervención manual, minimizando los errores y mejorando la rapidez del proceso.

El HIS también jugará un papel crucial, ya que se establecerá una interoperabilidad perfecta entre este sistema y el PACS. La automatización permitirá que tanto las imágenes como la documentación clínica se integren automáticamente en ambos sistemas, garantizando que toda la información relevante del paciente esté disponible de manera unificada y mejorando la gestión general de la atención médica (OBJ-5).

Para que este sistema funcione correctamente, la infraestructura de TI del hospital deberá estar preparada para soportar el nuevo flujo de trabajo. Esto incluye la actualización de servidores, estaciones de trabajo, y la implementación de medidas de seguridad robustas como el cifrado de datos y firewalls. La infraestructura deberá ser capaz de manejar la carga adicional y los procesos automatizados sin comprometer el rendimiento ni la seguridad (OBJ-3 y OBJ-5).

6.4.4 Límites del Proyecto

Es importante señalar que este proyecto no cubrirá todos los aspectos relacionados con el manejo de imágenes médicas. Por ejemplo, no se incluirá el mantenimiento del hardware de las estaciones de radiodiagnóstico ni la gestión de imágenes fuera del PACS. El proyecto se centrará exclusivamente en la automatización de la inclusión de CDs, abarcando tanto las imágenes como los informes clínicos, pero no abordará otros flujos de trabajo manuales que no estén directamente relacionados con este proceso (OBJ-1 y OBJ-2).

El éxito del proyecto dependerá de la disponibilidad de recursos humanos, en especial en lo que respecta a la formación necesaria para que el personal maneje el nuevo sistema de manera eficiente. Asimismo, estará limitado por el presupuesto asignado, lo que podría influir en el alcance de ciertas funcionalidades avanzadas. Se priorizarán estas funcionalidades según los recursos disponibles, asegurando que se logre una implementación efectiva con las herramientas esenciales (OBJ-2 y OBJ-3).

Por último, el tiempo será un factor crítico. El proyecto deberá completarse en un plazo específico, con etapas definidas para asegurar que los objetivos se alcancen en el plazo previsto. Esta planificación permitirá que tanto la integración de imágenes en el PACS como la incorporación de informes clínicos en el HIS se realicen de manera eficiente y dentro de los tiempos acordados (OBJ-4 y OBJ-5).

6.4.5 Desafíos y Consideraciones

La implementación de este sistema centralizado y automatizado no está exenta de desafíos. Reconocer estos desafíos de manera anticipada es crucial para asegurar que el proyecto se ejecute de manera eficiente y cumpla con sus objetivos. A continuación, se describen los principales desafíos y las consideraciones que se deben tener en cuenta:

- **Resistencia al Cambio**
  Uno de los mayores desafíos en cualquier proyecto de transformación tecnológica es la resistencia al cambio por parte del personal. Los empleados que están acostumbrados a procesos manuales y descentralizados pueden mostrar reticencia a adoptar nuevos sistemas automatizados. Para mitigar este riesgo, será fundamental llevar a cabo una gestión del cambio eficaz, que incluya programas de capacitación específicos, sesiones de sensibilización sobre los beneficios del nuevo sistema, y apoyo continuo durante la transición. Además, involucrar al personal desde las etapas iniciales del proyecto puede ayudar a reducir la resistencia y fomentar una mayor aceptación.
- **Complejidad de la Integración Tecnológica**
  Integrar el nuevo sistema de inclusión de CDs con los sistemas existentes, como el PACS y el HIS, puede ser técnicamente complejo. La falta de interoperabilidad entre los sistemas podría generar problemas como la duplicación de datos, errores en la transferencia de información, o incluso la pérdida de datos críticos. Para superar este desafío, es esencial planificar y realizar pruebas exhaustivas de integración antes de la implementación completa. Además, se debe contar con el soporte técnico adecuado para resolver cualquier problema de compatibilidad que pueda surgir durante el proceso.

- **Seguridad y Cumplimiento Normativo**
  Otro desafío clave es garantizar que el nuevo sistema cumpla con las estrictas normativas de seguridad y privacidad de los datos, como el GDPR y la LOPDGDD. Cualquier vulnerabilidad en el sistema podría exponer datos sensibles de los pacientes, lo que no solo tendría consecuencias legales sino también reputacionales para el hospital. Para abordar este riesgo, es crucial implementar medidas de seguridad robustas, como el cifrado de datos, la autenticación multifactor, y auditorías regulares del sistema. Asimismo, se debe mantener una vigilancia continua sobre las actualizaciones de las normativas para asegurar que el sistema siga cumpliendo con los requisitos legales.
- **Gestión del Tiempo y los Recursos**
  El proyecto debe completarse dentro de un marco de tiempo específico y con recursos limitados. Una mala planificación o la subestimación de los recursos necesarios podrían llevar a retrasos, sobrecostos, o una implementación incompleta del sistema. Para evitar esto, es vital realizar una planificación detallada, que incluya la identificación de todas las tareas necesarias, la asignación adecuada de recursos, y la definición de hitos claros. La monitorización continua del progreso del proyecto y la flexibilidad para ajustar los planes según sea necesario también son esenciales para mantener el proyecto en curso.
- **Fiabilidad y Mantenimiento del Sistema**
  Una vez implementado, el sistema debe ser altamente fiable para garantizar su funcionamiento continuo. Cualquier fallo en el sistema podría interrumpir el flujo de trabajo en el hospital, afectando la calidad de la atención al paciente. Además, el mantenimiento del sistema será crucial para asegurar su longevidad y eficiencia operativa. Esto requiere establecer un plan de mantenimiento preventivo, contar con personal capacitado para resolver problemas técnicos, y asegurar que el sistema sea escalable para adaptarse a futuras necesidades del hospital.

Además de los desafíos mencionados, es importante considerar la comunicación continua con todas las partes interesadas a lo largo del proyecto. Mantener una transparencia sobre el progreso del proyecto, los desafíos que se enfrentan, y las soluciones implementadas contribuirá a generar confianza y apoyo en todas las etapas de la implementación. También es crucial documentar todas las etapas del proyecto para facilitar futuras mejoras y asegurar que el hospital esté preparado para adaptarse a cambios tecnológicos o regulatorios en el futuro.

6.5 Aplicación de Metodologías

6.5.1 Marco COBIT (Control Objectives for Information and Related Technologies)

El marco COBIT será la principal metodología utilizada para guiar la gobernanza y gestión de TI en este proyecto. COBIT ofrece un enfoque integral para alinear los objetivos de TI con los objetivos estratégicos del hospital, asegurando que los recursos de TI se gestionen de manera eficaz y eficiente. Este marco, ampliamente reconocido en la gobernanza y gestión de TI, nos ofrece una estructura sólida para alinear los objetivos tecnológicos con las metas estratégicas del hospital. A lo largo del proyecto, COBIT nos guiará para garantizar que todas las decisiones y acciones se tomen de manera eficiente y con un enfoque claro hacia la mejora continua.

- **Definir la Arquitectura de la Información (PO2)**
  El primer paso crucial es asegurarnos de que la arquitectura de la información del hospital esté bien diseñada y alineada con la nueva solución que vamos a implementar. Esto significa que debemos planificar cómo se integrará el nuevo sistema automatizado con el PACS existente, el HIS y otros sistemas críticos. La meta aquí es que toda la información fluya de manera coherente y sin interrupciones, eliminando redundancias y potenciando la eficiencia operativa. Al definir correctamente esta arquitectura, estamos sentando las bases para que el sistema funcione de manera óptima y se adapte fácilmente a futuras necesidades.
- **Habilitar la Operación y Uso (AI4)**

Una vez que la arquitectura esté bien definida, el siguiente desafío es garantizar que el sistema sea accesible y fácil de usar para todo el personal involucrado. Esto implica no solo la integración técnica, sino también asegurarnos de que los usuarios reciban la formación necesaria para utilizar el nuevo sistema de manera eficaz desde el primer día. Además, debemos proporcionar soporte técnico adecuado para resolver cualquier duda o problema que pueda surgir. Al facilitar la adopción del sistema, reducimos los errores operativos y mejoramos la eficiencia en las tareas diarias.

- **Asegurar los Servicios de Seguridad (DS5)**
  En un entorno hospitalario, la seguridad de la información es primordial. Con la implementación del nuevo sistema, es esencial que se establezcan controles de seguridad robustos que protejan los datos sensibles de los pacientes. Esto incluye implementar medidas como el cifrado de datos, la autenticación de usuarios y la realización de auditorías regulares. Al asegurar que la información esté protegida en cada etapa del proceso, no solo cumplimos con las normativas legales, sino que también ganamos la confianza de los pacientes y del personal.
- **Definir y Gestionar los Niveles de Servicio (DS1)**
  Un aspecto clave del proyecto será establecer niveles de servicio que aseguren que el nuevo sistema cumpla con las expectativas de rendimiento y disponibilidad del hospital. Esto significa que el sistema debe ser capaz de procesar las imágenes rápidamente y estar disponible cuando se necesite, sin interrupciones. Al definir estos niveles de servicio, garantizamos que el sistema no solo sea eficiente, sino que también satisfaga las necesidades operativas diarias del hospital, mejorando la experiencia de todos los usuarios.
- **Gestionar los Cambios (AI6)**
  Finalmente, es fundamental que el proceso de cambio se gestione de manera cuidadosa y controlada. La implementación de un nuevo sistema siempre implica desafíos, pero al gestionar los cambios de manera estructurada, minimizamos los riesgos de interrupciones y aseguramos una transición suave. Esto incluye planificar cada etapa de la implementación, comunicar claramente con todas las partes interesadas, y estar preparados para ajustar el plan si surgen imprevistos. Al manejar los cambios con eficacia, podemos integrar el nuevo sistema sin problemas en la rutina diaria del hospital, maximizando sus beneficios desde el primer momento.

6.5.2 Relación de los Objetivos con COBIT

Los objetivos establecidos en este proyecto apuntan a transformar el proceso actual de inclusión de CDs en el del hospital, mejorando no solo la eficiencia operativa y la seguridad de los datos, sino también garantizando un mayor cumplimiento normativo y mejorando la calidad de la atención al paciente.

Además, estos objetivos han de ser alineados con los principios y áreas clave del marco COBIT, asegurando que la implementación optimice la operación del hospital y cumpla con las mejores prácticas en gobernanza y gestión de TI. Esto garantizará que los procesos sean eficientes, seguros, y cumplan las regulaciones y objetivos estratégicos de la organización.

A continuación, se presenta la relación existente entre los objetivos planteados en el proyecto y el marco COBIT.

OBJ-1. Centralización del Proceso de Inclusión de CDs

- **COBIT Relevante:** PO2 - Definir la Arquitectura de la Información
- **Relación**: La centralización y automatización de la inclusión tanto de imágenes como de documentación clínica asegura que la arquitectura de la información esté alineada con los objetivos estratégicos del hospital, mejorando la accesibilidad y la gestión eficiente de la información en el PACS y el HIS. Este enfoque centralizado y automatizado optimiza el flujo de datos, eliminando procesos manuales que comprometen la integridad y disponibilidad de la información.

OBJ-2. Automatización del Flujo de Trabajo

- **COBIT Relevante**: AI4 - Habilitar la Operación y Uso

- **Relación**: La automatización del flujo de trabajo, desde la verificación de datos hasta la inclusión de imágenes en el PACS y la integración automática de informes clínicos en el HIS, está directamente relacionada con el principio de COBIT de habilitar la operación y uso. Este objetivo mejora la eficiencia operativa y minimiza los errores humanos, garantizando que los sistemas de TI dentro del hospital faciliten el uso efectivo y continuo por parte del personal médico y técnico.

OBJ-3. Mejora de la Seguridad de los Datos

- **COBIT Relevante**: DS5 - Asegurar los Servicios de Seguridad
- **Relación**: La implementación de medidas de seguridad robustas en el proceso de automatización, como el cifrado de datos y la autenticación de usuarios, garantiza la protección de los datos médicos y clínicos, tanto de imágenes como de informes. Esto se alinea con los principios de COBIT para asegurar los servicios de seguridad, protegiendo la información contra accesos no autorizados y amenazas, y asegurando el cumplimiento normativo con GDPR y LOPDGDD.

OBJ-4. Optimización del Tiempo de Respuesta

- **COBIT Relevante**: DS1 - Definir y Gestionar los Niveles de Servicio
- **Relación**: La reducción del tiempo de respuesta en la inclusión automática de imágenes en el PACS y la documentación clínica en el HIS está directamente relacionada con la gestión eficiente de los niveles de servicio, un principio clave en COBIT. Este objetivo asegura que los sistemas de TI soporten las necesidades operativas del hospital, permitiendo diagnósticos y tratamientos más rápidos y oportunos.

OBJ-5. Integración con Otros Sistemas del Hospital

- **COBIT Relevante**: AI6 - Gestionar los Cambios
- **Relación**: La integración de un sistema automatizado de inclusión de CDs, que abarque tanto imágenes como informes clínicos, con el resto de los sistemas del hospital está relacionada con la gestión del cambio. Este objetivo asegura que las nuevas implementaciones se integren sin problemas con los sistemas existentes, minimizando interrupciones en el flujo de trabajo y facilitando una interoperabilidad eficaz entre el PACS, HIS y otros sistemas hospitalarios.

La siguiente tabla resume los objetivos propuestos en este caso de uso y su relación con el marco COBIT.

Objetivo	*Descripción*	*COBIT Relevante*	*Relación*
OBJ-1	Centralización del Proceso de Inclusión de CDs	PO2 - Definir la Arquitectura de la Información	Asegurar que la arquitectura de la información esté alineada con los objetivos estratégicos del hospital.
OBJ-2	Automatización del Flujo de Trabajo	AI4 - Habilitar la Operación y Uso	Mejorar la eficiencia operativa y minimizar los errores humanos.
OBJ-3	Mejora de la Seguridad de los Datos	DS5 - Asegurar los Servicios de Seguridad	Gestionar la seguridad de la información para proteger los datos contra accesos no autorizados.
OBJ-4	Optimización del Tiempo de Respuesta	DS1 - Definir y Gestionar los Niveles de Servicio	Gestionar eficientemente los niveles de servicio para soportar las necesidades operativas.
OBJ-5	Integración con Otros Sistemas del Hospital	AI6 - Gestionar los Cambios	Asegurar una integración sin problemas de las nuevas implementaciones con los sistemas existentes.

Tabla 3. Objetivos propuestos y su relación con el marco COBIT

6.5.3 Análisis DAFO (Debilidades, Amenazas, Fortalezas, Oportunidades)

El análisis DAFO se utilizará para identificar y evaluar los factores internos y externos que podrían afectar el éxito del proyecto. Esto ayudará a tomar decisiones informadas durante la planificación e implementación.

Fortalezas:

- **Alta Cualificación del Personal:** Los ingenieros encargados de la inclusión de CDs ya están bien capacitados y familiarizados con los sistemas actuales, lo que facilitará la transición al nuevo sistema automatizado.
- **Infraestructura Tecnológica Sólida:** El HIS, PACS y la infraestructura de TI del hospital son robustos y están bien integrados, proporcionando una base sólida para la implementación de nuevas tecnologías.

Debilidades:

- **Procesos Manuales Actuales:** La dependencia de procesos manuales introduce ineficiencias y aumenta el riesgo de errores humanos, especialmente en la cumplimentación de formularios.
- **Falta de Automatización:** La falta de sistemas automatizados para la inclusión de CDs es un cuello de botella en el flujo de trabajo.

Oportunidades:

- **Automatización de Procesos:** La implementación de un sistema automatizado ofrece la oportunidad de mejorar significativamente la eficiencia operativa y reducir los tiempos de respuesta.
- **Mejoras en la Seguridad:** La automatización también permitirá implementar mejores controles de seguridad, protegiendo mejor los datos sensibles.

Amenazas:

- **Resistencia al Cambio:** Existe la posibilidad de que algunos miembros del personal se resistan a la adopción de un nuevo sistema, lo que podría retrasar la implementación.
- **Riesgos de Integración:** La integración con los sistemas existentes, si no se realiza correctamente, podría generar problemas técnicos que afecten la operación diaria del hospital.

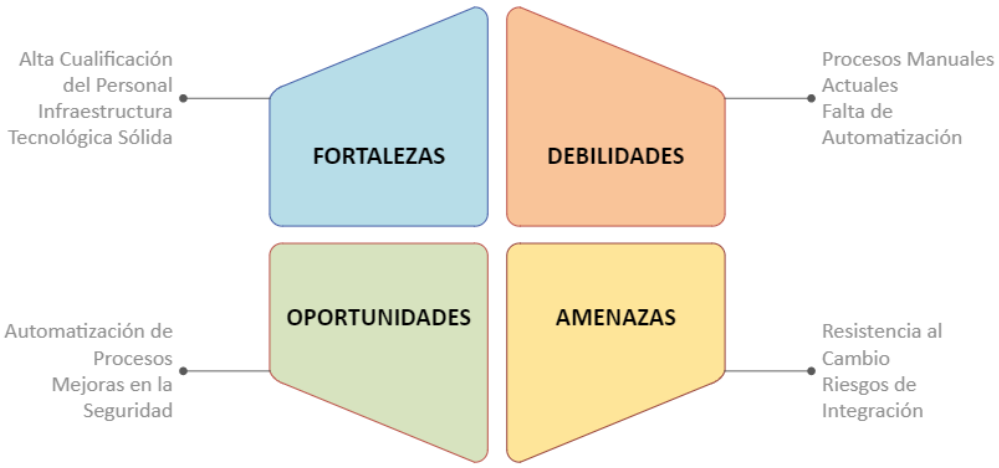


Ilustración 10. Caso de uso, análisis DAFO

6.6 Propuesta de Solución

6.6.1 Diseño y Arquitectura del Sistema

El sistema estará diseñado en torno a un servidor central gestionado por Ensemble, que gestionará la comunicación entre los diferentes componentes. Ensemble se encargará de recibir los datos tanto de DICOM Gateway (para las imágenes) como de DocuWare (para los informes clínicos), procesarlos y transferirlos automáticamente al PACS y al HIS, respectivamente. Esto garantiza que las imágenes y los informes clínicos se gestionen de forma automatizada y estén disponibles en los sistemas correspondientes sin intervención manual.

Ensemble también se encargará de la correcta asociación de los formularios electrónicos con los estudios cargados en el PACS, eliminando la necesidad de que los médicos mecanicen manualmente la información de los informes clínicos en el HIS. Esta automatización asegura una mayor eficiencia y reduce los riesgos de errores.

Tecnologías Seleccionadas:

- **Software de Automatización de Imágenes**: Se utilizará DICOM Gateway para gestionar la recepción y transferencia de imágenes desde los CDs hacia el PACS. Este software es compatible con el estándar DICOM, lo que garantiza la correcta interoperabilidad con el sistema PACS existente.
- **Sistema de Gestión de Documentos Electrónicos (EDM)**: Se implementará DocuWare para la generación y almacenamiento de documentos electrónicos, eliminando la necesidad de formularios impresos. Esto permitirá que los informes clínicos se completen y validen electrónicamente, facilitando la integración automática de los mismos en el HIS.
- **Middleware de Integración**: Ensemble actuará como middleware, integrando todos los sistemas implicados: DICOM Gateway (para imágenes), DocuWare (para documentos), el PACS y el HIS. Facilitará la transferencia de datos y asegurará que la integración entre los sistemas se realice de manera fluida y segura.

Servidor Central y Middleware: Ensemble

Ensemble actuará como el núcleo de la arquitectura, funcionando como middleware que orquesta la comunicación entre los distintos sistemas involucrados: DICOM Gateway, DocuWare, PACS, y HIS. Ensemble, al ser una plataforma robusta y ya implementada en el hospital, facilita su integración con la nueva solución, optimizando tanto la inclusión de imágenes médicas como de informes clínicos. Sus funciones clave serán las siguientes:

- **Integración Completa:** Ensemble gestionará la integración de los flujos de datos desde DICOM Gateway (que recibe y procesa las imágenes de los CDs) hacia el PACS. Además, se encargará de integrar DocuWare, asegurando que tanto las imágenes como los informes clínicos se asocien correctamente y de forma automatizada con los estudios correspondientes en el PACS y el HIS. Esto eliminará la necesidad de mecanización manual de los informes clínicos.
- **Gestión de Procesos:** Ensemble manejará el flujo de trabajo completo, desde la recepción de datos hasta la notificación al usuario. Esto incluye la validación automática de las imágenes y documentos provenientes de los CDs, el enrutamiento de información hacia el PACS y el HIS, así como la gestión de excepciones. La automatización de estos procesos permitirá una operación más eficiente y segura.
- **Monitoreo y Alerta:** Ensemble estará configurado para monitorear todos los procesos en tiempo real, detectando cualquier anomalía o fallo en la transferencia de datos, tanto de imágenes como de informes clínicos. En caso de error, Ensemble generará alertas automáticas y activará procesos de recuperación para asegurar la continuidad del flujo de información y minimizar cualquier impacto en la atención médica.

Recepción y Procesamiento de CDs: DICOM Gateway

DICOM Gateway es el software seleccionado para gestionar la recepción y el procesamiento de los CDs que contienen tanto estudios de imágenes médicas como la documentación clínica asociada. Este componente es fundamental para extraer los datos del CD y prepararlos para su inclusión automática en el PACS (para imágenes) y en el HIS (para informes clínicos). Dentro de las funciones clave de DICOM Gateway destacan las siguientes:

- **Detección Automática:** Cuando un CD es insertado en una estación de trabajo, DICOM Gateway detecta automáticamente la inserción y comienza el proceso de extracción de las imágenes DICOM, así como de los documentos clínicos asociados, si los hubiera.
- **Validación de Imágenes y Documentos:** Antes de transferir los datos a Ensemble, DICOM Gateway realiza una validación inicial de los archivos DICOM y de los documentos clínicos para asegurar que cumplen con los estándares y que no están corruptos. Esto reduce el riesgo de errores durante la inclusión en el PACS y el HIS, garantizando la integridad de la información.
- **Transferencia a Ensemble:** Una vez validados, tanto las imágenes como los informes clínicos son transferidos a Ensemble, que se encargará de su posterior procesamiento, asegurando su almacenamiento en el PACS para las imágenes y en el HIS para los informes clínicos.

Gestión de Documentos Electrónicos: DocuWare

DocuWare se integrará en la arquitectura para gestionar todos los aspectos relacionados con la documentación clínica electrónica, eliminando la necesidad de formularios impresos y garantizando la precisión de los datos tanto en el PACS como en el HIS.

- **Generación Automática de Formularios y Documentos Clínicos:** Cuando un CD es procesado por DICOM Gateway, Ensemble genera automáticamente un formulario de solicitud en DocuWare. Este formulario electrónico incluye los datos necesarios que el usuario debe completar, como la identificación del paciente y el tipo de estudio. Además, DocuWare gestiona la captura de cualquier informe clínico incluido en el CD, asegurando que se integre adecuadamente en el HIS.
- **Validación de Datos:** DocuWare asegura que todos los campos requeridos en los formularios y documentos clínicos estén correctamente llenados antes de permitir la transferencia de datos al PACS y al HIS. Esto minimiza los errores comunes de entrada de datos y garantiza que la información sea precisa.
- **Asociación con Estudios en el PACS y HIS:** Una vez completado, el formulario y los documentos clínicos se vinculan automáticamente con los estudios correspondientes en el PACS (para las imágenes) y en el HIS (para los informes clínicos). Esto garantiza que toda la información del paciente esté centralizada, accesible y organizada, facilitando el acceso a los profesionales de la salud.

Almacenamiento y Gestión de Imágenes: PACS

El PACS sigue siendo el sistema principal de almacenamiento y gestión de imágenes médicas en el hospital. La arquitectura propuesta asegura que el PACS reciba tanto imágenes como informes clínicos que han sido validados, optimizando su funcionamiento y garantizando la integridad de los datos.

- **Almacenamiento Centralizado:** Una vez que Ensemble ha procesado y validado los datos, las imágenes se almacenan en el PACS, mientras que los informes clínicos se integran automáticamente en el HIS. El PACS se encarga de organizar las imágenes por paciente y tipo de estudio, asegurando que estén disponibles para los profesionales médicos de manera rápida y segura. La correcta asociación de los informes clínicos con los estudios permite una gestión más eficiente y completa de la información del paciente.
- **Acceso Rápido y Seguro:** El PACS facilita el acceso a las imágenes por parte de los radiólogos y otros profesionales de la salud, con capacidades de búsqueda avanzada que permiten localizar rápidamente cualquier estudio previo. A la vez, la información clínica relevante almacenada en el HIS se puede consultar paralelamente, mejorando la calidad del diagnóstico y tratamiento al tener una visión completa del historial del paciente.

Interfaz con el HIS

La interoperabilidad entre el nuevo sistema de inclusión de CDs y el HIS es crucial para asegurar que tanto las imágenes como los datos clínicos se mantengan coherentes y centralizados, ofreciendo una visión integral de la información del paciente.

- **Integración con Ensemble:** Ensemble se encargará de sincronizar los datos entre el PACS y el HIS, garantizando que tanto las imágenes médicas como los informes clínicos se integren de manera automática y sin errores. Esto incluye la actualización de registros de pacientes y la incorporación de nuevos estudios y documentos clínicos, asegurando que toda la información esté disponible en ambos sistemas de manera simultánea.
- **Gestión Integral de Pacientes:** Gracias a esta integración automatizada, el HIS podrá acceder a los estudios almacenados en el PACS y relacionarlos con otros datos clínicos del paciente, como informes médicos y registros de visitas. Esta interoperabilidad permitirá una gestión más completa y eficiente de la atención médica, facilitando un acceso rápido y centralizado a toda la información relevante del paciente.

Seguridad y monitorización

La seguridad y la monitorización continua son aspectos fundamentales de la arquitectura propuesta, asegurando que el sistema no solo sea eficiente sino también seguro y confiable.

Medidas de Seguridad:

- **Cifrado de Datos:** Todos los datos transferidos entre DICOM Gateway, Ensemble, DocuWare, PACS y HIS estarán cifrados utilizando AES-256 para protegerlos contra accesos no autorizados.
- **Autenticación Multifactor (MFA):** Se implementará MFA para el acceso a todos los componentes críticos del sistema, utilizando Duo Security para garantizar que solo el personal autorizado pueda realizar cambios o acceder a los datos sensibles.

Monitorización con Splunk:

- **Monitorización en Tiempo Real:** Splunk será utilizado para monitorizar el rendimiento del sistema en tiempo real, con Ensemble proporcionando datos detallados sobre el estado de cada componente. Esto permitirá identificar y resolver problemas antes de que afecten al rendimiento del sistema.
- **Auditorías de Seguridad:** Se realizarán auditorías regulares utilizando Splunk para asegurar que todas las actividades del sistema cumplen con las normativas vigentes y que no se producen accesos no autorizados.

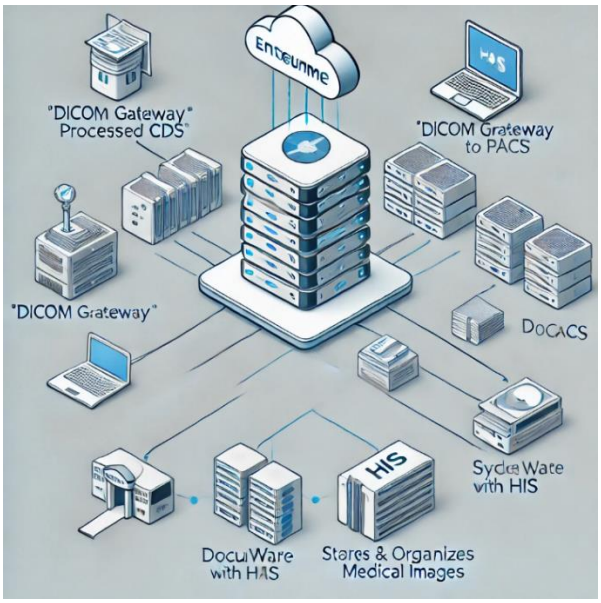


Ilustración 11. Arquitectura propuesta

6.6.2 Desarrollo e Implementación del Sistema

Automatización del Proceso de Inclusión de CDs

Se instalará DICOM Gateway en las estaciones de trabajo del Servicio de Electromedicina. Este software detectará automáticamente la inserción de CDs, extraerá tanto las imágenes médicas como los documentos clínicos asociados, y enviará estos datos a Ensemble. Ensemble se encargará de la transferencia automatizada de las imágenes al PACS y de los informes clínicos al HIS, asegurando que ambos tipos de datos se gestionen de manera eficiente y sin intervención manual, optimizando el proceso y minimizando los errores.

Gestión de Documentos Clínicos

DocuWare se integrará con Ensemble para permitir la generación electrónica de formularios de solicitud y la captura automática de informes clínicos asociados con los CDs. Cuando se reciba un CD, se generará automáticamente un formulario electrónico que contendrá toda la información relevante del paciente y el estudio. Ensemble se encargará de asegurar que tanto estos formularios como los informes clínicos se vinculen correctamente con los estudios en el PACS (para las imágenes) y en el HIS (para la documentación clínica), reduciendo significativamente los errores de entrada de datos y eliminando la necesidad de mecanización manual.

Pruebas y Validación

Se llevarán a cabo pruebas exhaustivas para validar la integración de DICOM Gateway, DocuWare, y Ensemble con el PACS y el HIS. Estas pruebas incluirán escenarios de carga completa, validación de la automatización tanto de imágenes como de documentos clínicos, y simulación de situaciones adversas, como la pérdida de datos o errores en la transferencia. El objetivo será asegurar que el sistema pueda manejar de manera eficiente el volumen de CDs y documentos sin comprometer el rendimiento o la seguridad de los datos.

6.6.3 Gestión del Cambio y Formación del Personal

Formación Específica

El personal técnico recibirá una formación integral enfocada en el uso de DICOM Gateway, DocuWare, y su interacción con Ensemble. Esta formación cubrirá tanto la gestión automatizada de las imágenes y los informes clínicos, como el proceso de integración de datos en el PACS y el HIS. Además, se incluirán módulos sobre la gestión de excepciones y la resolución de problemas comunes relacionados con la validación automática de imágenes y documentos, asegurando que el personal esté capacitado para enfrentar cualquier desafío que pueda surgir durante la operación del sistema.

Soporte Técnico

Se establecerá un soporte técnico intensivo durante los primeros tres meses posteriores a la implementación del sistema automatizado. Este soporte estará disponible durante el horario de atención (de 8h a 15h) para ayudar al personal con la adaptación al nuevo sistema, brindando asistencia en la resolución de incidencias técnicas relacionadas con la automatización de la inclusión de imágenes y documentos clínicos. El objetivo es asegurar una transición fluida y eficiente al nuevo flujo de trabajo automatizado.

6.6.4 Seguridad y Cumplimiento Normativo

Medidas de Seguridad

Ensemble gestionará la seguridad de los datos tanto de las imágenes médicas como de los informes clínicos mediante el cifrado AES-256 durante su transferencia y almacenamiento, asegurando que los datos sensibles estén protegidos en todo momento. Además, se implementará una autenticación multifactor (MFA), garantizando que solo el personal autorizado tenga acceso a los sistemas que gestionan el PACS y el

HIS. Estas medidas de seguridad protegerán la integridad y privacidad de los datos, tanto en la inclusión automatizada de imágenes como en la documentación clínica.

Auditorías y Monitorización

Se utilizará Splunk para monitorizar en tiempo real la actividad de todo el sistema, incluyendo la transferencia de imágenes y documentos clínicos entre DICOM Gateway, DocuWare, Ensemble, el PACS y el HIS. Ensemble registrará y transmitirá cualquier anomalía detectada a Splunk para su análisis, lo que permitirá realizar auditorías de seguridad regulares y asegurar el cumplimiento continuo con las normativas GDPR y LOPDGDD. Esta monitorización proactiva garantizará que cualquier problema de seguridad sea detectado y abordado de manera oportuna, manteniendo la integridad del sistema.

6.6.5 Monitorización y Evaluación Continua

Indicadores de Rendimiento Clave (KPIs)

Se establecerán KPIs específicos para medir tanto el tiempo de procesamiento de los CDs como la automatización de la inclusión de imágenes y documentos clínicos en el PACS y el HIS. Estos indicadores incluirán la tasa de error en la carga de imágenes, la validación de los informes clínicos, y el tiempo de respuesta general del sistema. Ensemble, en combinación con Splunk, permitirá una monitorización en tiempo real de estos KPIs, asegurando que el sistema funcione según los niveles de servicio esperados y que cualquier anomalía sea detectada y resuelta rápidamente. Esto garantizará que la automatización del proceso de inclusión sea efectiva y sin interrupciones.

Actualizaciones y Mantenimiento

Se realizarán revisiones periódicas del sistema, aprovechando las capacidades de Ensemble para aplicar actualizaciones de software y mejoras tanto al PACS como al HIS sin interrumpir el servicio. Estas revisiones periódicas asegurarán que el sistema mantenga los más altos niveles de seguridad, eficiencia, y funcionalidad, adaptándose a las últimas tecnologías y normativas. Además, la integración de nuevas funcionalidades o mejoras en el manejo de imágenes y documentos clínicos podrá implementarse de manera fluida sin afectar el rendimiento general del sistema.

7 Conclusiones

7.1 Conclusiones sobre Marco de Gobernanza TIC con metodología COBIT

La aplicación de la metodología COBIT como marco de gobernanza para la gestión de las Tecnologías de la Información y la Comunicación (TIC) en el contexto de los sistemas de impresión y digitalización del Sistema Nacional de Salud (SNS). La elección de COBIT se justifica por su enfoque integral, que proporciona un equilibrio entre el control de los recursos tecnológicos y el alineamiento de estos con los objetivos estratégicos del SNS.

- **Alineación Estratégica y Valor para el Negocio:** La aplicación de COBIT permite al SNS alinear las inversiones en TI con sus objetivos estratégicos, asegurando que los recursos tecnológicos, incluidos los sistemas de impresión y digitalización, apoyen la misión central de mejorar la calidad de la atención al paciente. Esta alineación estratégica garantiza que todas las decisiones de TI generen un valor tangible, optimizando los costes y mejorando los resultados operativos.
- **Gestión Eficaz de Riesgos:** COBIT proporciona un marco robusto para la identificación, evaluación y gestión de los riesgos asociados con la infraestructura tecnológica, particularmente en la gestión de datos sensibles en los sistemas de impresión. La metodología permite implementar controles adecuados que minimicen el riesgo de incidentes de seguridad, garantizando la continuidad del servicio y protegiendo la información confidencial de los pacientes.
- **Mejora Continua y Adaptabilidad:** El marco COBIT se basa en un ciclo de mejora continua que es especialmente relevante en el entorno sanitario, donde los cambios regulatorios, tecnológicos y operativos son constantes. La metodología facilita la adaptación a nuevas normativas de protección de datos (como GDPR y LOPDGDD) y a las mejores prácticas emergentes, asegurando que el sistema de impresión y digitalización esté siempre actualizado y preparado para responder a nuevos desafíos.
- **Transparencia y Auditoría:** COBIT fomenta la transparencia en la gestión de TI al proporcionar mecanismos claros para la auditoría y el reporte de actividades. Esto es esencial en el contexto del SNS, donde la rendición de cuentas y el cumplimiento normativo son críticos. El uso de COBIT permite mantener un registro detallado de todas las actividades relacionadas con los sistemas de impresión, lo que facilita las auditorías internas y externas.
- **Eficiencia Operativa y Reducción de Costes:** La implementación de COBIT como marco de gobernanza TIC ha demostrado ser eficaz en la optimización de procesos operativos y la reducción de costes. Al estandarizar y centralizar la gestión de los sistemas de impresión, se reducen redundancias, se minimizan tiempos de inactividad, y se optimiza el uso de los recursos tecnológicos y humanos, lo cual contribuye a una mayor eficiencia general del sistema de salud.

La adopción de la metodología COBIT como marco de gobernanza TIC en el SNS proporciona una estructura sólida y flexible para gestionar los sistemas de impresión y digitalización de manera eficiente, segura y conforme a las normativas vigentes. Este enfoque integral no solo mejora la alineación estratégica y el control de riesgos, sino que también facilita la adaptabilidad a un entorno cambiante y asegura la transparencia en la gestión de TI. En conjunto, la implementación de COBIT fortalece la infraestructura tecnológica del SNS, optimizando sus procesos y contribuyendo a una atención sanitaria más segura y de calidad.

7.2 Conclusiones sobre Método DAFO como herramienta de análisis.

El método DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades) como herramienta de análisis estratégico para evaluar la situación actual del sistema centralizado de impresión y digitalización en el Sistema Nacional de Salud (SNS). Este método ha permitido identificar los factores internos y externos que influyen en la gestión de los sistemas de impresión, proporcionando una visión clara y estructurada de las áreas que requieren atención y de los aspectos que pueden ser aprovechados para mejorar la eficiencia y seguridad del sistema.

- **Identificación de Fortalezas Clave:** El análisis DAFO ha destacado varias fortalezas importantes del sistema de impresión centralizado, como la gestión centralizada de los dispositivos, que facilita el control y el monitoreo, la robustez en la seguridad mediante la autenticación multifactorial (MFA) y el cifrado de datos, y el cumplimiento normativo con regulaciones como GDPR y LOPDGDD. Estas fortalezas proporcionan una base sólida para construir un sistema eficiente y seguro, que pueda adaptarse a los desafíos de un entorno sanitario cambiante.
- **Detección de Debilidades Internas:** El uso del método DAFO ha permitido identificar debilidades críticas que deben ser abordadas para optimizar el sistema. Entre estas debilidades se encuentran los costos iniciales elevados de implementación, la complejidad en la configuración inicial y la integración con sistemas existentes, y la dependencia de la infraestructura de red para la operatividad y seguridad del sistema. Además, se destaca la necesidad de formación del personal para reducir la curva de aprendizaje y la resistencia al cambio, así como la complejidad de mantener hardware y software especializados.
- **Aprovechamiento de Oportunidades Externas:** El análisis ha revelado oportunidades significativas que pueden ser aprovechadas para mejorar el sistema de impresión. Entre estas oportunidades se encuentran los avances tecnológicos en seguridad de la información, la creciente digitalización del sector sanitario, el aumento de normativas que favorecen la seguridad de los datos, y las mejoras en la interoperabilidad de los sistemas. Estas oportunidades ofrecen un marco ideal para fortalecer el sistema de impresión centralizado, mejorar su integración con otros sistemas de salud, y maximizar su eficiencia operativa.
- **Mitigación de Amenazas:** El método DAFO también ha permitido identificar diversas amenazas externas que podrían afectar negativamente al sistema de impresión, como los cambios frecuentes en las regulaciones de protección de datos, las amenazas cibernéticas (ransomware, ataques dirigidos), y la dependencia de proveedores externos para actualizaciones y soporte. Además, se ha identificado la resistencia al cambio por parte del personal sanitario y la obsolescencia tecnológica de los dispositivos periféricos. Estas amenazas requieren la implementación de estrategias proactivas de mitigación, como la actualización continua de políticas de seguridad, la inversión en formación del personal, y la planificación de la renovación tecnológica.
- **Visión Integral para la Toma de Decisiones:** El método DAFO ha proporcionado una visión integral de los factores internos y externos que afectan al sistema de impresión, facilitando la toma de decisiones estratégicas informadas. Esta herramienta de análisis ha permitido priorizar acciones que maximicen las fortalezas, aprovechen las oportunidades, minimicen las debilidades, y mitiguen las amenazas, contribuyendo a una gestión más eficaz y eficiente del sistema.

El método DAFO ha sido fundamental para realizar un análisis exhaustivo del sistema centralizado de impresión en el SNS, proporcionando un marco claro para identificar las fortalezas y oportunidades que deben ser explotadas, así como las debilidades y amenazas que requieren una atención urgente. Esta herramienta ha permitido desarrollar una estrategia integral que mejora la seguridad, eficiencia y conformidad del sistema, apoyando la misión del SNS de proporcionar una atención sanitaria de calidad. El análisis DAFO, por tanto, se establece como una metodología clave para la evaluación continua y la mejora de los sistemas de impresión y digitalización en entornos sanitarios.

7.3 Conclusión sobre Objetivos, propuesta de mejora y solución

Se han definido claramente los objetivos a alcanzar con la implementación de un sistema centralizado de impresión y digitalización en el Sistema Nacional de Salud (SNS) y se ha presentado una propuesta detallada para cumplir con estos objetivos. Este enfoque ha sido fundamental para alinear las necesidades estratégicas y operativas del SNS con las soluciones tecnológicas necesarias para optimizar la gestión de la información sanitaria.

7.3.1 Conclusiones Principales sobre los Objetivos

- **Mejora de la Eficiencia Operativa:** Uno de los objetivos clave identificados es la mejora de la eficiencia operativa mediante la centralización de la gestión de los sistemas de impresión y digitalización. Este enfoque busca reducir la duplicidad de esfuerzos, optimizar el uso de los recursos, y minimizar los tiempos de inactividad de los dispositivos. Al centralizar la gestión, se facilita la administración de políticas de impresión, la monitorización en tiempo real, y la aplicación de medidas de seguridad uniformes.
- **Incremento de la Seguridad y Cumplimiento Normativo:** Otro objetivo crucial es garantizar un alto nivel de seguridad en la gestión de documentos sensibles y asegurar el cumplimiento con las normativas vigentes, como el GDPR y la LOPDGDD. Para ello, se busca implementar controles de acceso robustos, mecanismos de autenticación multifactor, y políticas de cifrado de datos tanto en tránsito como en reposo. Esto minimiza los riesgos de acceso no autorizado y protege la confidencialidad de la información de salud.
- **Reducción de Costes y Optimización de Recursos:** La reducción de costes operativos es otro de los objetivos principales. Se pretende lograrlo mediante la implementación de políticas de impresión eficientes (como impresión a doble cara o en blanco y negro por defecto), el monitoreo del uso de consumibles, y la automatización de procesos de mantenimiento y reposición. Esto no solo reduce el consumo de papel y tóner, sino que también prolonga la vida útil de los dispositivos periféricos.
- **Facilitación de la Interoperabilidad y la Integración:** El sistema debe facilitar la interoperabilidad y la integración con otros sistemas tecnológicos existentes en el SNS, asegurando un flujo de trabajo más fluido y una mejor coordinación entre diferentes áreas y departamentos. Este objetivo implica que la solución de impresión debe ser flexible y capaz de adaptarse a nuevas tecnologías y necesidades emergentes.

7.3.2 Conclusiones Principales sobre Propuesta de mejora y solución

- **Propuesta de Infraestructura Centralizada:** La propuesta se centra en la creación de una infraestructura centralizada para la gestión de dispositivos de impresión y digitalización, apoyada en servidores dedicados y herramientas de gestión centralizada. Esto incluye la implementación de sistemas de control de impresión, servidores de impresión seguros, y soluciones en la nube que permitan el acceso remoto seguro mediante VPN, optimizando la eficiencia operativa y la capacidad de respuesta ante incidentes.
- **Integración de Tecnologías Avanzadas:** La propuesta destaca la necesidad de integrar tecnologías avanzadas de seguridad, como autenticación multifactor (MFA), cifrado de datos, y gestión de acceso basada en roles (RBAC). Estas tecnologías fortalecen la seguridad de los sistemas de impresión, minimizan el riesgo de violaciones de datos, y aseguran que solo el personal autorizado pueda acceder a información sensible.
- **Optimización del Uso de Recursos:** Se propone la implementación de políticas de impresión eficientes y la utilización de software de gestión de impresión que permita la monitorización en tiempo real del uso de consumibles y la generación de informes detallados sobre el rendimiento de los dispositivos. Esta propuesta busca maximizar el aprovechamiento de los recursos existentes y reducir significativamente los costes asociados a la impresión y digitalización.
- **Flexibilidad y Escalabilidad del Sistema:** La propuesta también contempla la necesidad de que el sistema de impresión sea flexible y escalable, permitiendo su adaptación a futuras necesidades del

SNS y a cambios en las normativas o en la demanda de servicios. Se sugiere la implementación de soluciones modulares que permitan añadir o actualizar funcionalidades sin necesidad de grandes inversiones adicionales.

- **Formación y Gestión del Cambio:** Como parte de la propuesta, se enfatiza la importancia de la formación del personal para asegurar una adopción efectiva del sistema de impresión centralizado. Además, se recomiendan estrategias de gestión del cambio para minimizar la resistencia del personal y garantizar que todos los usuarios se sientan cómodos utilizando las nuevas tecnologías.

Ilustración 12. Esquema de propuesta de Sistema Centralizado tras conclusiones

El estudio de los objetivos y la propuesta revela un enfoque estratégico integral para la implementación de un sistema centralizado de impresión y digitalización en el SNS. Se destacan las metas de mejorar la eficiencia operativa, aumentar la seguridad, reducir costes, y facilitar la integración con otros sistemas, todos alineados con la misión de proporcionar una atención sanitaria de alta calidad. La propuesta presentada ofrece soluciones tecnológicas avanzadas y prácticas de gestión óptimas que aseguran la sostenibilidad y adaptabilidad del sistema ante futuros desafíos. En conjunto, este enfoque garantiza que el sistema no solo cumpla con los requisitos actuales del SNS, sino que también esté preparado para evolucionar en un entorno dinámico y regulado.

7.4 Conclusiones del caso de uso

El desarrollo e implementación de un sistema centralizado y automatizado para la inclusión de CDs en el PACS y HIS en el Complejo Hospitalario Universitario Insular Materno Infantil de Gran Canaria ha permitido cumplir con los objetivos clave definidos para este caso de uso, logrando una optimización significativa tanto en la gestión de imágenes médicas como en la documentación clínica. En este caso de uso, se abordan todos los aspectos críticos del proyecto, desde la identificación de las ineficiencias actuales hasta la propuesta de solución y la planificación detallada de la implementación, asegurando el cumplimiento de cada objetivo.

La revisión del estado actual reveló diversas ineficiencias, como la dependencia de procedimientos manuales, que ralentizan el flujo de trabajo y comprometen la seguridad de los datos. Estos problemas son abordados de manera directa con la centralización y automatización del proceso (OBJ-1) lo que permite la inclusión automática de datos en los sistemas del hospital, reduciendo la intervención manual y optimizando la eficiencia operativa.

En respuesta a estos desafíos, se diseñó una solución que integra tecnologías avanzadas como DICOM Gateway, DocuWare y Ensemble para gestionar automáticamente tanto las imágenes como los informes clínicos (OBJ-2). Esta automatización reduce los tiempos de procesamiento y minimiza los errores, mejorando la calidad del servicio.

La seguridad de los datos es otra prioridad establecida en este proyecto. La implementación de medidas de protección avanzadas, como el cifrado AES-256 y la autenticación multifactor, junto con la monitorización en tiempo real mediante Splunk, asegura que los datos sensibles sean manejados de forma segura (OBJ-3). Estas medidas garantizan el cumplimiento de las normativas de seguridad como el GDPR y la LOPDGDD.

El sistema automatizado reduce significativamente el tiempo necesario para que las imágenes y los informes clínicos estén disponibles para los profesionales de la salud (OBJ-4). Los médicos dispondrán de acceso inmediato tanto a las imágenes en el PACS como a los informes en el HIS, lo que mejora la capacidad del hospital para ofrecer diagnósticos más rápidos y tratamientos oportunos.

Finalmente, la integración fluida entre el PACS y el HIS mediante Ensemble (OBJ-5), permite un flujo de información sin interrupciones entre ambos sistemas. Esto mejora la interoperabilidad y facilita una gestión integral y más eficiente de la información clínica.

En conjunto, este caso de uso demuestra cómo un enfoque bien planificado y ejecutado puede transformar un proceso clave en el entorno hospitalario, mejorando tanto la eficiencia operativa como la calidad del servicio. Al cumplir con los cinco objetivos estratégicos propuestos, el CHUIMI no solo puede optimizar sus operaciones, sino que también fortalecer su capacidad para brindar atención de alta calidad y segura a sus pacientes. Este proyecto se alinea con la visión estratégica del hospital de aprovechar la tecnología para mejorar continuamente la atención al paciente y la gestión de la salud.

8 Índice de figuras y tablas.

9 Referencias

- AEPD. (s.f.). Guía para el Cumplimiento del RGPD. Obtenido de , Agencia Española de Protección de Datos: https://www.aepd.es/guias-y-herramientas/herramientas/facilita-rgpd
- Al Hadad, R. S. (2023). A Comprehensive Review of COBIT and ISO 27001: Approaches to Auditing Credit Bureau Automation System (CBAS) at PT XYZ. In 2023 9th International Conference on Signal Processing and Intelligent Systems (ICSPIS) (pp. 1-8). IEEE.
- Analytics, H. I. (s.f.). Health IT Analytics. Obtenido de Data Security in Healthcare: Emerging Trends: https://www.healthitanalytics.com
- Andalucía, C. P. (s.f.). Obtenido de https://www.juntadeandalucia.es/haciendayadministracionpublica/apl/pdc_sirec/perfiles-licitaciones/detalle-licitacion.jsf?idExpediente=538479
- BOE. (29 de 05 de 2003). Ley 16/2003 - Cohesión y Calidad del SNS. Obtenido de https://www.boe.es/eli/es/l/2003/05/28/16/con
- BOE. (16 de 05 de 2003). Ley 41/2002 - Autonomía del Paciente. Obtenido de https://www.boe.es/eli/es/l/2002/11/14/41/con
- BOE. (14 de 12 de 2007). Artículo 30 - Sanidad Rural - Ley 45/2007 - Desarrollo Sostenible del Medio Rural. Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2007-21493&p=20091021&tn=1#a30
- BOE. (16 de 09 de 2010). Real Decreto 1093/2010 - Informes Clínicos. Obtenido de https://www.boe.es/eli/es/rd/2010/09/03/1093/con
- BOE. (29 de 01 de 2010). Real Decreto 4/2010 - Esquema Nacional de Interoperabilidad. Obtenido de https://www.boe.es/eli/es/rd/2010/01/08/4/con
- BOE. (29 de 07 de 2011). Ley 22/2011 de Residuos y Suelos Contaminados. Obtenido de https://www.boe.es/eli/es/l/2011/07/28/22/con
- BOE. (20 de 01 de 2011). Real Decreto 1718/2010 - Receta Médica. Obtenido de https://www.boe.es/eli/es/rd/2010/12/17/1718/con
- BOE. (19 de 07 de 2018). Real Decreto 1112/2018 - Accesibilidad de Sitios Web Públicos. Obtenido de https://www.boe.es/eli/es/rd/2018/09/07/1112
- BOE. (31 de 03 de 2021). Real Decreto 203/2021 - Funcionamiento por Medios Electrónicos. Obtenido de https://www.boe.es/eli/es/rd/2021/03/30/203/con
- BOE. (04 de 05 de 2022). Real Decreto 311/2022 - Esquema Nacional de Seguridad. Obtenido de https://www.boe.es/eli/es/rd/2022/05/03/311/con
- BOE. (06 de 12 de 2028). Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales. Obtenido de https://www.boe.es/eli/es/lo/2018/12/05/3/con
- BOE, L. G. (24 de 03 de 1986). Ley 14/1986. Obtenido de https://www.boe.es/eli/es/l/1986/04/25/14/con
- C Valencaina, C. d. (19 de 05 de 2023). Obtenido de https://contrataciondelestado.es/wps/poc?uri=deeplink%3Adetalle_licitacion&idEvl=pId8Zwj7S0CGCFcHcNGIlQ%3D%3D
- Canarias, C. d. (01 de 10 de 2024). Obtenido de https://contrataciondelestado.es/wps/poc?uri=deeplink:detalle_licitacion&idEvl=23w4Oe2WjbR%2FP7lJ7Fu0SA%3D%3D

- Canarias, G. d. (22 de 12 de 2023). miHistoria. Obtenido de Historia Clínica Electrónica: https://www3.gobiernodecanarias.org/sanidad/scs/contenidoGenerico.jsp?idDocument=03274b04-f14a-11e7-9d56-c37102939259&idCarpeta=eaea55f8-97ee-11ed-a068-475b2f79c0a5
- Cataluña, P. d. (s.f.). Obtenido de https://contractaciopublica.cat/es/detall-publicacio/dd9fd771-c1cf-902f-3715-8a816e299994/90750212
- Corp, I. I. (2024). DICOM Gateway. IEI Integration Corp. Obtenido de https://www.ieiworld.com/medical-solution/de/DICOM-Gateway.php
- DocuWare. (2024). La solución para la gestión documental digital de tu empresa. Obtenido de https://start.docuware.com/es/
- Eichelberg, M. K. (2020). Cybersecurity in PACS and Medical Imaging: an Overview. Journal of Digital Imaging, 33, 1527–1542. Obtenido de https://doi.org/10.1007/s10278-020-00393-3
- Enaizan, O. Z. (2020). Electronic medical record systems: decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. Health Technol., 10, 795–822. Obtenido de https://doi.org/10.1007/s12553-018-0278-7
- EUR-Lex. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. (GDPR). Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679&qid=1727779024133
- Europea, P. E. (2016). Reglamento General de Protección de Datos (GDPR). Obtenido de Reglamento (UE) 2016/679: https://eur-lex.europa.eu
- INTECO, I. N. (2018). Guía para la Integración de Sistemas de Información Hospitalaria (HIS).
- InterSystems, M. d. (2024). Obtenido de https://www.intersystems.com/es-productos/ensemble/
- ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. Obtenido de https://www.isaca.org/resources/cobit
- ISO. (2016). Health informatics — Information security management in health using. Obtenido de https://www.iso.org/standard/62777.html
- ISO. (2018). Acoustics — Measurement of airborne noise emitted by information technology and telecommunications equipment. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso:7779:ed-4:v1:en
- ISO. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Obtenido de https://www.iso.org/es/contents/data/standard/08/28/82875.html
- ISO. (s.f.). Acoustics — Declared noise emission values of computer and business equipment. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso:9296:ed-1:v1:en
- ISO. (s.f.). Sistemas de gestión ambiental — Requisitos con orientación para su uso. Obtenido de https://www.iso.org/obp/ui#iso:std:iso:14001:ed-3:v1:es
- ISO. (s.f.). Sistemas de gestión de la calidad — Requisitos. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:es
- Journal of Healthcare Management, V. 6. (2020). Strategic Alignment of IT with Healthcare Needs: Framework for Improving Operational Efficiency. Journal of Healthcare Management.
- Juan Carlos Cobacho Montilla, M. R. (2023). Debilidades y Amenazas en las TIC de ámbito sanitario 3.

- Lapão, L. (2019). The Future of Healthcare: The Impact of Digitalization on Healthcare Services Performance. In: Pereira Neto, A., Flynn, M. (eds) The Internet and Health in Brazil. Springer, Cham. Obtenido de https://doi.org/10.1007/978-3-319-99289-1_22
- Law, E. U. (s.f.). GDPR Portal. Obtenido de https://gdpr-info.eu
- Lazcano Arranz, A. J. (2024). ANEXO-3 (MATRIZ DAFO).
- Lazcano Arranz, A. J., & Polo Moratilla, E. (2024). Tema 2.4 Metodologías TIC.
- León, P. d. (10 de 09 de 2019). Obtenido de https://contrataciondelestado.es/wps/poc?uri=deeplink%3Adetalle_licitacion&idEvl=iLvFlNoH6FEuf4aBO%2BvQlQ%3D%3D
- Madrid, P. d. (26 de Abril de 2021). Obtenido de https://contratos-publicos.comunidad.madrid/contrato-publico/pa-312020-servicio-integral-equipos-impresion-multifuncion-servicio-reprografia
- Ministerio de Sanidad, E. (s.f.). Recomendaciones para la Digitalización de Documentos Sanitarios. Obtenido de https://www.sanidad.gob.es/areas/saludDigital/doc/Estrategia_de_Salud_Digital_del_SNS.pdf
- Murcia, C. P. (27 de 02 de 2020). Obtenido de https://www.carm.es/web/pagina?IDCONTENIDO=1618&IDTIPO=200&RASTRO=c709$m&vigente=1&id=8a26229c708489ed017086a0d9a5123d
- Online, I. B. (28 de 03 de 2023). Obtenido de https://www.base.gov.pt/Base4/en/detail/?type=contratos&id=10607680
- Oracle. (s.f.). LDAP. Obtenido de https://docs.oracle.com/cd/E19957-01/817-4240-10/provisioning.html
- Patricia Fernán Pérez, J. C. (2023). ANÁLISIS DEL NIVEL DE IMPLANTACIÓN DE LA CARPETA DE SALUD EN EL SISTEMA. TFM de la SEIS.
- Salud, S. C. (2023). Pliego de prescripciones técnicas para el contrato del suministro, integración y soporte de un visor universal de imagen diagnóstica y de un VNA centralizado en el Servicio Canario de la Salud.
- SESPA, S. d. (2023). Pliego Prescripciones Técnicas para la Instalación de un Sistema Centralizado de Impresión. Oviedo, Asturias, España.
- Splunk. (2024). Splunk: The Data Platform for the Hybrid World. Obtenido de https://www.splunk.com/
- Standard, T. D. (s.f.). Digital Imagen and Comunications in Medicine. Obtenido de https://www.dicomstandard.org/current
- Standards Developing Organization, S. (s.f.). HL7. Obtenido de https://es.wikipedia.org/wiki/HL7
- Star, E. (s.f.). Obtenido de https://www.energystar.gov/
- Tiase, V. L. (2020). Patient-generated health data and electronic health record integration: a scoping review. JAMIA Open, 3(4), 619–627. Obtenido de https://doi.org/10.1093/jamiaopen/ooaa052
- Torab-Miandoab, A. S.-S. (2023). Interoperability of heterogeneous health information systems: a systematic literature review. BMC Medical Informatics and Decision Making, 23, 18. Obtenido de https://doi.org/10.1186/s12911-023-02115-5
- UNE. (06 de 09 de 2023). EN 12281:2003 o equivalente en cuanto al uso de papel reciclado. Obtenido de https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0028809