AR-NC-001

INSTRUCTIVO ARQUITECTURA DE REFERENCIA PARA DESARROLLO DE SISTEMAS DEL SECTOR SALUD

Ministerio de Salud

Versión Oficial v01 – mayo 2025

Resolución Aprobatoria: _____

	Responsable	Fecha	Firma
Elaborado	**Rodrigo Baeza G.** Unidad de Arquitectura, Desarrollo y Calidad	Mayo 2025	
Revisado	**José Villa C.** Encargado de Seguridad de la Información y Ciberseguridad	Mayo 2025	
Revisado	**Catalina Arenas A.** Encargado de Unidad de Arquitectura, Desarrollo y Calidad	Mayo 2025	
Aprobado	**Jorge Herrera R.** Jefe Departamento de Tecnologías de Información y Comunicaciones	Mayo 2025	

MINISTERIO DE SALUD
ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

MINISTERIO DE SALUD
DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
GABINETE DE MINISTRA

1 PROPÓSITO

El presente documento de arquitectura de referencia TIC ofrece una guía integral para la planificación, diseño y despliegue **de infraestructuras tecnológicas sólidas y adaptativas**, para el desarrollo e implementación de sistemas informáticos.

Propone una estructura modular interconectada, que garantiza una distribución equilibrada de cargas y redundancia, necesarios para asegurar la disponibilidad de servicios críticos. Además, se enfoca en la adopción de estándares abiertos, fomentando la interoperabilidad entre sistemas internos y externos al Sector Salud.

2 ALCANCE O ÁMBITO DE APLICACIÓN

Este documento se aplica a todos los sistemas de información que se quieran desarrollar, actualizar o mantener en Ministerio de Salud (Minsal) y las instituciones del Sector Salud, independientemente de si el trabajo es realizado por equipos internos de la institución o por proveedores y profesionales externos contratados para dichos fines.

Es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales, a quienes se les otorgue una casilla de correo electrónico.

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- **Marco Normativo**
  - ISO 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos.
  - ISO I27002:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad
- **Normas legales y reglamentarias relacionada:**
  - **Normas Generales**
    - Ley N° 19.799, de firmas y documentos electrónicos.
    - Ley N° 19.927, de Delitos de Pornografía Infantil.
    - Ley N° 19.628, de Protección de vida privada y datos personales.
    - Ley N° 20.285 regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado.
    - Ley 19.880 que establece las bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado.
    - Ley N° 21.180, de Transformación Digital del Estado.
    - Ley N°21.459/2022: Establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al

DEPARTAMENTO TIC VISADO

Convenio de Budapest. Esta ley establece los delitos informáticos reconocidos en Chile.

- Ley N° 21.719/2024: Que modifica la ley N°19.628, de protección de datos personales. Esta ley entra en vigor el 1 de diciembre de 2026.
- Ley N° 21.459, que Establece normas sobre Delitos Informáticos, deroga la Ley N°19.223 y modifica otros cuerpos legales con el Objeto de Adecuarlos al Convenio de Budapest.
- Decreto N° 4, 2021, Ministerio Secretaría General de la Presidencia, Reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la ley Nº 21.180 sobre transformación digital del estado.
- Resolución Exenta N°372/2025 que aprueba texto de las recomendaciones del Consejo para la Transparencia sobre Transparencia Algorítmica y Oficio N°7286/2025 Guía del Consejo para la Transparencia para la adopción de las Recomendaciones sobre Transparencia Algorítmica.
- Circular N° 711/2023 establece lineamientos sobre el uso de herramientas de inteligencia artificial (IA) en el sector público de Chile, proporcionando directrices para una implementación ética, segura y transparente de estas tecnologías en servicios gubernamentales. Con el objetivo de asegurar que las aplicaciones de IA en el sector público se alineen con los valores de protección de derechos, transparencia y seguridad de la información, además de fomentar la eficiencia y mejorar la calidad de los servicios público.

- **Normas de Ciberseguridad**

  - Decreto N° 83, 2004, Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
  - Ley N° 21.663 sobre Marco de Ciberseguridad, esta ley proporciona un marco para asegurar la ciberseguridad de infraestructuras críticas, que indirectamente impacta en la protección de datos.
  - Decreto N° 295, de 2024, del Ministerio del Interior y Seguridad Pública: Aprueba reglamento de reporte de incidentes de ciberseguridad de la ley N° 21.633.
  - Decreto N°483, de 2024, del Ministerio del Interior y Seguridad Pública: Aprueba Reglamento que determina la estructura interna de la Agencia Nacional de Ciberseguridad.
  - Decreto N°164, de 2023, del Ministerio del Interior y Seguridad Pública: Aprueba Política Nacional de Ciberseguridad 2023-2028.

DEPARTAMENTO TIC VISADO

- Decreto Supremo N° 7, 2023, Ministerio secretaría General de la Presidencia, que establece una Norma Técnica de Seguridad de la Información y Ciberseguridad, en concordancia con la Ley Nº 21.180
- Decreto N°273, 2022, Ministerio del Interior y Seguridad Pública, Establece obligación de reportar incidentes de ciberseguridad.
- Decreto N°273, 2022, Ministerio del Interior y Seguridad Pública, Establece obligación de reportar incidentes de ciberseguridad.
- Circular N° 711/2023 establece lineamientos sobre el uso de herramientas de inteligencia artificial (IA) en el sector público de Chile, proporcionando directrices para una implementación ética, segura y transparente de estas tecnologías en servicios gubernamentales. Con el objetivo de asegurar que las aplicaciones de IA en el sector público se alineen con los valores de protección de derechos, transparencia y seguridad de la información, además de fomentar la eficiencia y mejorar la calidad de los servicios público.

- **Normativa Sanitaria**

  - DFL Nº 1, de 24 de abril de 2006, Ministerio de Salud, que fija el texto refundido, coordinado y sistematizado del Decreto Ley Nº 2.763, de 1979 y de las leyes Nº 18.933 y 18.469;
  - DFL Nº 725, Ministerio de Salud, Código Sanitario;
  - Ley N°19.966, de 2004, que establece un régimen de garantías de salud;
  - Ley N° 19.650, que perfecciona normas del área de la salud;
  - Ley N° 20.120 de 22 de septiembre de 2006, sobre la investigación científica en el ser humano, su genoma, y prohíbe la clonación humana y demás normativa del área de la salud.
  - Ley N°20.584, referida a Deberes y Derechos que tienen las Personas en relación con acciones vinculadas a su Atención de Salud;
  - Ley N° 20.724, de 2014, que modifica el Código Sanitario en materia de regulación de medicamentos;
  - Ley N° 20.850, de 2016, que crea un sistema de protección financiera para diagnósticos y tratamientos de alto costo y rinde homenaje póstumo a don Luis Ricarte Soto Gallegos;
  - Ley N° 21.258, de 2020, que crea la ley nacional del cáncer, que rinde homenaje póstumo al doctor Claudio Mora.
  - Ley 21.541, de 17 de marzo de 2023, que modifica la normativa que indica para autorizar a los prestadores de salud a efectuar atenciones mediante telemedicina.
  - Decreto Nº 41, de 24 de julio de 2012, del Ministerio de Salud, Reglamento de Ficha Clínica;

DEPARTAMENTO TIC VISADO

- Decreto Nº 31 de 15 de junio de 2012, del Ministerio de Salud, Reglamento sobre entrega de información y expresión de consentimiento informado en las atenciones de salud;
- Decreto N° 38, de 2005, del Ministerio de Salud, Reglamento Orgánico de los establecimientos de salud de menor complejidad y de los establecimientos de autogestión en red.
- Decreto N° 38, de 26 de diciembre de 2012, del Ministerio de Salud, que aprueba Reglamento sobre derechos y deberes de las personas en relación con las actividades vinculadas con su atención de salud.
- Decreto N° 38, de 2013, del Ministerio de Salud, que modifica decreto N° 466 de 1984, Reglamento de Farmacias, Droguerías, almacenes farmacéuticos, botiquines y depósitos autorizados.
- Decreto N° 6, de 16 de abril de 2021, del Ministerio de Salud, Reglamento sobre acciones de vinculadas a la atención de salud realizadas a distancia.
- Decreto N° 820, 2011, Ministerio de Salud.

- **Documentos Relacionados**

  - Arquitectura de Referencia [1].
  - Política General de Seguridad de la Información y Ciberseguridad del Minsal
  - Política desarrollo de sistemas
  - Política protección de datos personal
  - Política para entornos de nube pública
  - Política de seguridad para el control de acceso lógico
  - Política de uso de criptografía
  - Política de seguridad para la clasificación y manejo de información
  - Política seguridad para las relaciones con los proveedores
  - Stack tecnológico de seguridad

4 ROLES Y RESPONSABILIDADES

- **Jefe Departamento TIC**
  - Responsable de establecer y aplicar los controles y políticas necesarios que garanticen la seguridad, escalabilidad y estabilidad de la arquitectura de los sistemas de información bajo su control.
  - Responsable de controlar la homologación arquitectónica de los ambientes, pudiendo ser desarrollo, pruebas, preproducción y producción.

- **Arquitecto de sistemas.**
  - Encargado de diseñar la arquitectura de sistemas en base a los lineamientos del documento de arquitectura, cumplimiento de políticas y estándares de seguridad y las buenas prácticas indicadas en el Well-Architected Framework para entornos Cloud.
  - Coordinar y supervisar revisiones de la implementación de arquitectura.
  - Proponer y actualizar mejoras en el diseño de arquitectura.
    Realizar evaluaciones de la implementación.
- **Operaciones TIC (Soporte).**
  - Documentar y escalar incidentes que estén relacionados a la configuración arquitectónica.

- **Operaciones TIC (desarrollo de sistemas) / Áreas de Negocio que cuenten con equipos de desarrollo de sistemas.**
  - Diseñar, implementar y gestionar soluciones en base a los lineamientos de arquitectura tecnológica y estándares de desarrollo.
  - Cumplir con todos los lineamientos y requisitos establecidos en esta política en cada fase del desarrollo y actualización de sistemas.
  - Documentar de manera exhaustiva la arquitectura definida para sistemas, incluyendo sus modificaciones y actualizaciones, asegurando trazabilidad y coherencia con los estándares de seguridad.

- **Operaciones TIC (Infraestructura).**
  - Validar que la arquitectura definida para sistemas esté alineada a los estándares definidos.
  - Implementar y mantener medidas de protección adecuadas para garantizar la integridad, disponibilidad y seguridad de la arquitectura de los entornos de desarrollo, pruebas y producción.
  - Asegurar que los entornos de infraestructura estén configurados acorde a la arquitectura definida y monitoreados para soportar el desarrollo seguro y continuo de los sistemas de información del Minsal.

- **Encargado de Seguridad de la Información y Ciberseguridad**
  - Responsable de definir, supervisar y actualizar las políticas de seguridad de la información y ciberseguridad que deben ser consideradas en el diseño e implementación de la arquitectura de referencia para el desarrollo de sistemas.
  - Validar que la arquitectura cumpla con los requisitos normativos, estándares nacionales e internacionales y políticas institucionales de seguridad.
  - Asesorar en la incorporación de controles de seguridad desde el diseño y participar en las revisiones arquitectónicas críticas.

DEPARTAMENTO TIC VISADO

- Coordinar con las áreas técnicas la aplicación de medidas de mitigación ante riesgos identificados en la arquitectura.

5 MATERIAS QUE ABORDA.

- **Arquitectura de referencia.**
  - Abstracción empresarial.
  - Abstracción técnica.
- **Marcos de trabajo y lineamientos para diseño de arquitectura de soluciones.**
  - Principios arquitectónicos.
  - Patrones de diseño.
  - Metodología de desarrollo.
  - Lineamientos de seguridad.
  - Lineamientos de cumplimiento.
  - Lineamientos de rendimiento.
  - Lineamientos de Integración.
  - Consideraciones de Infraestructura.
  - Gestión de Ciclo de vida.
  - Evaluación de tecnologías.

5.1 Definiciones asociadas a la Seguridad en Arquitectura de Sistemas

- Gestión de identidad y acceso: mecanismos para autenticar y autorizar a usuarios y sistemas, asegurando que solo las personas y aplicaciones autorizadas tengan acceso a los recursos apropiados.
- Control de Acceso: políticas y tecnologías de verificación de identidad para controlar el acceso a datos y sistemas, con diferentes niveles de privilegios según los roles y responsabilidades de los usuarios, que buscan proteger la integridad y confidencialidad de la información.
- Cifrado de Datos: proceso que transforma la información, volviéndola ilegible para quienes no cuentan con las claves de cifrado específicas que les permitan acceder a ella. Se aplica cifrado para proteger la información confidencial mientras se almacena y se transfiere.
- Gestión de Amenazas y Vulnerabilidades: Estrategia para proteger la seguridad de los sistemas y la red de telecomunicaciones. Se implementan sistemas de detección y prevención de intrusiones para identificar actividades maliciosas o anómalas en tiempo real, y se toman medidas proactivas para mitigar riesgos potenciales.
- Cumplimiento Normativo: conjunto de normas que rigen a la institución. Se asegura que la arquitectura cumpla con regulaciones y estándares de seguridad y privacidad relevantes, como leyes de protección de datos y requisitos gubernamentales.
- Auditoría y Monitoreo: actividades que se realizan de forma continua para identificar y tratar los riesgos. Se establecen registros detallados de actividades para permitir

la revisión y el análisis de eventos en caso de incidentes de seguridad, garantizando la trazabilidad y la rendición de cuentas.

- Gestión de Incidentes: proceso que se encarga de responder a eventos no planificados que afectan el servicio de forma negativa. Se definen procedimientos para responder y recuperarse de incidentes de seguridad, minimizando el impacto y restaurando la normalidad lo más rápido posible.
- Privacidad de los Datos: derecho de los usuarios a controlar como se utilizan sus datos personales. Se establecen políticas y prácticas para proteger la privacidad de los datos personales, asegurando que se recopilen, almacenen y procesen de acuerdo con regulaciones de privacidad.
- Educación y Concienciación: promover la formación continua y la sensibilización sobre cuestiones de seguridad entre el personal, reduciendo los riesgos asociados con errores humanos.
- Evaluación de Vulnerabilidades: Proceso para identificar, clasificar y priorizar posibles vulnerabilidades en la arquitectura de sistema, permitiendo tomar medidas preventivas antes de la implementación.

6 DIRECTRICES

6.1 Lineamientos generales

- Todo desarrollo deberá ajustarse con las políticas de seguridad vigentes del Minsal o las políticas definidas por Instituciones del Sector Salud. Entre estas se incluyen la Política General de Seguridad de la Información y Ciberseguridad, la Política de Desarrollo de Sistemas, la Política de Uso de Criptografía, y las normas de continuidad operativa, gestión de datos y proveedores.
- Toda arquitectura de sistemas ya sea desarrollada internamente o a través de terceros, debe cumplir con los lineamientos establecidos en este Instructivo, garantizando el principio de "Seguridad desde el Diseño", la interoperabilidad con el ecosistema tecnológico de salud, y el estricto cumplimiento de las normativas vigentes, tales como la Ley N° 19.628 sobre protección de datos personales, la Ley N° 21.663 sobre ciberseguridad, y las políticas específicas del MINSAL.

  En este contexto, las medidas de control de acceso y seguridad aplicadas en el diseño arquitectónico deben alinearse con los requisitos establecidos en el Sistema de Gestión de Seguridad de la Información del MINSAL, la Guía Técnica de Lineamientos de Desarrollo de Software del Gobierno Digital (SEGPRES), y cualquier otra regulación o estándar aplicable, asegurando así una base sólida de protección legal, técnica y operativa para los sistemas de información del sector salud.
- Toda arquitectura de sistemas debe cumplir con los lineamientos establecidos en este Instructivo, independientemente de si son implementados internamente o por terceros.

DEPARTAMENTO TIC VISADO

- Toda arquitectura de sistemas implementada por terceros debe respetar íntegramente las etapas de diseño y evaluación arquitectónica definidas, incluyendo controles de calidad, pruebas de seguridad, pruebas funcionales y técnicas, además de evidencias documentadas de cumplimiento con los controles exigidos.

7 ARQUITECTURA REFERENCIA

El presente instructivo se vincula y complementa directamente con el **Documento de Técnico de Arquitectura Referencia**, el cual proporciona una visión integral y estructurada del ecosistema tecnológico institucional.

Mientras el instructivo establece las fases, roles y lineamientos técnicos y normativos para el desarrollo seguro y escalable de sistemas, el documento referencial entrega una arquitectura de referencia dividida en dos niveles de abstracción: empresarial y técnica.

Este abarca zonas críticas como la seguridad y privacidad de la información, interoperabilidad, gestión de datos, infraestructura y usuarios, así como principios arquitectónicos, patrones de diseño, metodologías de desarrollo y lineamientos clave en seguridad, cumplimiento normativo y rendimiento.

En conjunto, ambos documentos permiten alinear el diseño e implementación de sistemas con las políticas institucionales, marcos normativos vigentes (como la Ley 19.628 y Ley N° 21.663), y las buenas prácticas de arquitectura, asegurando consistencia, trazabilidad y sostenibilidad tecnológica en el sector salud.

7.1 Fases de la Arquitectura de Sistemas

7.1.1 Cumplimiento de la legislación

Las medidas de control de acceso y seguridad aplicadas en el diseño de arquitectura de sistemas deben cumplir con todas las normativas y requisitos legales vigentes, en concordancia con lo establecido en la "Normativa del Sistema de Gestión de Seguridad de la Información del MINSAL", la Guía Técnica "Lineamientos de Desarrollo de Software" y sus actualizaciones emitidas por el Gobierno Digital de SEGPRES, así como las leyes aplicables en protección de datos y ciberseguridad vigentes.

7.1.2 Planificación

Durante la planificación, se deben estimar los plazos necesarios para el desarrollo de las fases de análisis, diseño, implementación y pruebas. Se debe definir un plan de mantenimiento para la operación.

7.1.3 Análisis y requisitos de la arquitectura de sistema.

Durante la fase de análisis, se deben incluir los siguientes elementos:

- Seguridad y privacidad de la información: su objetivo es salvaguardar la confidencialidad, integridad y disponibilidad de los datos del Ministerio. Se enfoca en establecer un entorno seguro y confiable, garantizando que la información sensible esté protegida de amenazas y riesgos. Entre los aspectos fundamentales

se encuentran: gestión de identidad y acceso, control de acceso, cifrado de datos, gestión de amenazas y vulnerabilidades, cumplimiento normativo, auditoria y monitoreo, gestión de incidentes y privacidad de datos.

- Usuarios: se debe comprender y abordar diversas necesidades y expectativas de los diferentes actores que interactúan con los sistemas de información. Se destaca la identificación de grupos de interés, análisis de requerimientos, segmentación de usuarios, diseño centrado en el usuario, feedback continuo, pruebas de usuario capacitación y soporte, medición de experiencia del usuario, comunicación con stakeholders.
- Canales de comunicación: se define el o los canales de comunicación que se utilizarán entre los usuarios objetivos y el sistema. Se define la personalización, accesibilidad, interacción en tiempo real, notificaciones y alertas, análisis del uso de los datos, seguridad en la comunicación, integración con sistemas internos, monitoreo y mejora continua.
- Procesos: se debe definir si la solución estará enfocada en flujos de trabajo y operaciones, que sean eficientes y automatizados, alineados con los objetivos estratégicos de la entidad. Entre sus aspectos clave se encuentran: identificación de procesos clave, modelamiento de procesos, optimización y automatización, flujo de trabajo digital, integración de sistemas, gestión de casos, monitoreo y reportes, mejora continua, cumplimiento regulatorio, capacitación y adopción.
- Integración e interoperabilidad: su objetivo es facilitar la conexión y el intercambio de información entre sistemas internos y externos. La infraestructura deberá permitir una colaboración efectiva y una transferencia de datos fluida. Dentro de los aspectos claves se encuentra: plataforma de integración, interfaces y protocolos estándar, orquestación de procesos, transformación de datos, adaptadores y conectores, gestión de mensajes, seguridad en la integración, monitoreo y tráfico de datos, integración de terceros, pruebas de integración.
- Datos e información: se enfoca en la gestión, almacenamiento y utilización efectiva de los datos. Entre sus aspectos clave se encuentra la gestión de datos maestros, almacenamiento de datos, modelamiento de datos, integración de datos, calidad de datos, acceso y privacidad, gobierno de datos, análisis de datos, visualización de datos, respaldo y recuperación.
- Servicios de infraestructura: su objetivo es proporcionar los recursos tecnológicos necesarios para el funcionamiento óptimo de los sistemas y aplicaciones. Entre los aspectos claves se encuentran: virtualización y Cloud, servidores y almacenamiento, redes y comunicaciones. Balanceo de carga, seguridad de la infraestructura, respaldo y recuperación, monitoreo y gestión, escalabilidad automatizada, gestión de configuración, eficiencia energética.

- En base a las definiciones previas, se debe determinar el enfoque de la aplicación o sistema, determinando así si tendrá un enfoque monolítico o de microservicios. Luego se debe definir las tecnologías que se utilizarán para su implementación, las cuales deben utilizar las indicadas en el documento de arquitectura de referencia.

7.2 Diseño y construcción de arquitectura.

Consideraciones en el Diseño y construcción de Arquitectura:

- El conjunto estructurado de enfoques, principios y directrices proporcionan un conjunto de mejores prácticas y pautas que guían el proceso de diseño y construcción de soluciones tecnológicas.
- Durante la fase de diseño, se deben considerar los siguientes elementos:
  - Principios arquitectónicos: fundamentos y pautas que orientan el diseño de la arquitectura de soluciones tecnológicas. Ente los aspectos a considerar se encuentran: modularidad, reutilización, separación de responsabilidades, escalabilidad, desacoplamiento, abstracción, coherencia y consistencia, flexibilidad, eficiencia y seguridad.
  - Patrones de diseño: soluciones probadas y documentadas para problemas recurrentes en el diseño de software y sistemas. Estos patrones representan soluciones a nivel de diseño que ofrecen un lenguaje común y una guía que ha demostrado ser efectiva para abordar desafíos comunes en el desarrollo de aplicaciones.
  - Metodologías de desarrollo: enfoques sistemáticos y estructurados utilizados para planificar, diseñar, construir, probar y entregar software y sistemas.
  - Lineamientos de seguridad: conjunto de principios, reglas y pautas diseñados para garantizar la protección de los activos y datos del Ministerio, así como para mitigar los riesgos de seguridad cibernética y mantener la integridad, confidencialidad y disponibilidad de la información. Destacan entre los lineamientos por abordar la protección de datos, control de acceso, gestión de riesgos, Seguridad de la infraestructura, criptografía, gestión de incidentes de seguridad, sensibilización y formación y cumplimiento normativo.
  - Lineamientos de cumplimiento: conjunto de directrices y reglas establecidas por el Ministerio para asegurar que sus operaciones, procesos y actividades cumplan con regulaciones, leyes, estándares de la industria y políticas internas relevantes. Se deberá poner atención a las regulaciones y normativas, políticas internas, protección de datos, seguridad de la información, informes y auditorías, adaptación y actualización.
  - Lineamientos de rendimiento: conjunto de pautas y directrices establecidas para garantizar el rendimiento óptimo de los sistemas, aplicaciones y procesos del Ministerio. Aspectos para considerar son establecer objetivos, el diseño eficiente, optimización de código, gestión de carga, monitorización y análisis, ajuste y

optimización continua, almacenamiento y memoria, redes y comunicación, tiempos de respuesta, pruebas de rendimiento, optimización de base de datos.

- Lineamientos de integración: conjunto de directrices y mejores prácticas diseñadas para facilitar la conexión y la interoperabilidad efectiva entre sistemas, aplicaciones y componentes del Ministerio. Se deberá tener consideración en la estandarización, claridad en las interfaces, APIs y Servicios Web, Formatos de Datos, Middleware, Integración en tiempo real, automatización, gestión de identidad, sincronización y migración de datos, pruebas de integración, monitorización y mantenimiento.
- Consideraciones de infraestructura: factores clave en el diseño, implementación y mantención de la base tecnológica del Ministerio. Estas consideraciones son esenciales para asegurar que los sistemas, aplicaciones y recursos tecnológicos funcionen de manera eficiente, segura y confiable. Se deberá considerar la escalabilidad, el rendimiento, seguridad, cumplimiento, almacenamiento y redes.
- Evaluación de tecnologías: proceso crítico que implica analizar y comparar diferentes soluciones tecnológicas para determinar cuál es la más adecuada para satisfacer las necesidades y los objetivos del Ministerio. Esta evaluación puede aplicarse a hardware, software, herramientas, plataformas y otros componentes tecnológicos.

7.3 Implementación

En esta fase se deben desarrollar y configurar los componentes del sistema conforme al diseño arquitectónico aprobado en la fase de diseño. Los equipos técnicos desarrollan, configuran e integran los distintos componentes del sistema, asegurando el cumplimiento de los estándares definidos en las fases anteriores. La implementación debe considerar el despliegue de controles de seguridad desde el inicio, tales como el cifrado de datos en tránsito y en reposo, la autenticación robusta, la segmentación de servicios, y la gestión de identidades y accesos.

Durante esta etapa, se debe documentar exhaustivamente los componentes implementados, registrar cualquier desviación respecto del diseño original, y mantener trazabilidad entre los requisitos funcionales, no funcionales y los elementos construidos. Además, de aplicar prácticas de desarrollo seguro, revisiones de código, y asegurarse de que los entornos (desarrollo, pruebas, preproducción y producción) estén debidamente separados, gestionados y protegidos según los lineamientos del instructivo y la política de desarrollo de sistemas.

7.4 Pruebas y Verificación

Una vez que el sistema ha sido implementado, se deben ejecutar pruebas exhaustivas para verificar su correcto funcionamiento. Estas pruebas deben contemplar:

- Pruebas funcionales: Validan que el sistema cumpla con los requerimientos esperados por el usuario final.

DEPARTAMENTO TIC VISADO

- Pruebas de rendimiento: Evalúan el comportamiento del sistema bajo condiciones normales y de alta demanda.
- Pruebas de seguridad: Incluyen análisis de vulnerabilidades, pruebas de penetración, revisión de configuraciones seguras y validación de controles de acceso.
- Pruebas de interoperabilidad: Son especialmente relevantes en el sector salud, para garantizar la correcta integración con otros sistemas como registros clínicos, RNI, laboratorios, etc.

Es fundamental que esta fase se ejecute tanto en ambientes de pruebas como en preproducción, y que cuente con evidencia documentada que respalde que el sistema está en condiciones de ser liberado. Toda no conformidad o debilidad encontrada debe ser abordada antes del paso a producción.

7.5 Despliegue

El despliegue consiste en poner el sistema en operación en un entorno de producción controlado. Esta fase debe planificarse cuidadosamente, incluyendo procedimientos de rollback, validación post-despliegue y coordinación con los equipos responsables de continuidad operativa y soporte. En sistemas críticos como los del sector salud, es indispensable que el despliegue se realice con medidas de alta disponibilidad, monitoreo activo y respaldo inmediato.

El proceso de despliegue debe garantizar que todos los componentes se hayan configurado correctamente, que los controles de seguridad estén activos, y que los datos sensibles estén debidamente protegidos. También debe activarse un plan de pruebas funcionales acotadas y un monitoreo reforzado durante el periodo inicial de operación.

7.6 Mantenimiento y Evolución

La arquitectura de sistemas no debe entenderse como un resultado estático, sino como un proceso en constante evolución. Esta fase contempla el monitoreo continuo del desempeño del sistema, la aplicación de mejoras, actualizaciones de componentes tecnológicos, parches de seguridad, y ajustes a medida que cambian los requerimientos del negocio, la normativa o el entorno tecnológico.

En este contexto, las instituciones del sector salud deben aplicar procesos de gestión de cambios controlados, mantener la documentación actualizada, y realizar revisiones arquitectónicas periódicas para asegurar que el sistema siga alineado con la seguridad desde el diseño, interoperabilidad, eficiencia y cumplimiento normativo.

Además, deben incluirse planes de continuidad operacional, recuperación ante desastres, y pruebas regulares de recuperación (DRP) para garantizar la disponibilidad y resiliencia de los sistemas que soportan procesos críticos del sector salud.

7.7 Tabla resumen de las Fases de la Arquitectura de Sistemas

Fase	Descripción	Objetivo
1. Planificación	Se identifican los objetivos del sistema, restricciones, necesidades del negocio y requerimientos regulatorios (ej. Ley 21.663, Ley 19.628, ISO 27.001).	Alinear la arquitectura con los objetivos estratégicos y marcos normativos vigentes.
2. Análisis de Requisitos	Se recopilan y documentan los requisitos funcionales, no funcionales (seguridad, rendimiento, interoperabilidad) y técnicos de la solución.	Establecer una base sólida y completa para el diseño de la arquitectura.
3. Diseño de Arquitectura	Se define la arquitectura lógica y física, considerando componentes, servicios, integraciones, capas de seguridad y lineamientos cloud/híbridos.	Establecer una estructura robusta, escalable y segura del sistema.
4. Evaluación y Validación	Se revisa el diseño arquitectónico en función de buenas prácticas (ej. Well-Architected Framework, NIST 800-160), políticas y estándares institucionales.	Asegurar que la arquitectura cumpla con criterios de calidad, seguridad y viabilidad.
5. Implementación	Se desarrollan y configuran los componentes del sistema conforme al diseño aprobado. Incluye la implementación de controles de seguridad.	Ejecutar el diseño arquitectónico asegurando la trazabilidad y cumplimiento.
6. Pruebas y Verificación	Se validan las funcionalidades, desempeño, integraciones y controles de seguridad. Incluye pruebas de arquitectura, rendimiento y vulnerabilidades.	Confirmar que la solución funciona según lo definido y cumple estándares.
7. Despliegue	Se publica la solución en entornos de producción (o fases previas como pre-producción), aplicando planes de continuidad y recuperación.	Asegurar una entrega controlada y segura del sistema.
8. Mantenimiento y Evolución	Se monitorea, ajusta y mejora la arquitectura según nuevas necesidades, hallazgos o cambios en normativas.	Garantizar la sostenibilidad, seguridad y adaptabilidad del sistema a largo plazo.

8 MECANISMO DE DIFUSIÓN.

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios.

A lo menos se deberá hacer difusión mediante los siguientes canales:

- Publicación en el sitio web Minsal http://www.minsal.cl/seguridad_de_la_informacion/
- Publicación en la intranet de Minsal http://isalud.minsal.cl/
- Correo informativo.

9 PERÍODO DE REVISIÓN.

El presente documento deberá ser revisado cada dos años o cuando ocurran cambios significativos para garantizar que:

DEPARTAMENTO TIC VISADO

- Sigue siendo adecuado para su propósito y preciso.
- Refleja los cambios en las tecnologías.
- Está alineado con legislación vigente, los estándares internacionales y mejores prácticas.

10 EXCEPCIONES AL CUMPLIMIENTO DE LA ARQUITECTURA DE REFERENCIA

En situaciones excepcionales, el jefe TIC, tendrá la facultad de evaluar y establecer condiciones específicas para la excepción al cumplimiento de las directrices establecidas en esta política, siempre que tales excepciones no infrinjan la legislación vigente ni comprometan la seguridad de la información ni el desempeño de la arquitectura.

Cada excepción deberá ser debidamente documentada, y se deberá iniciar un proceso de revisión del documento de arquitectura de referencia en el que se determinará si es necesario incorporar directrices adicionales o realizar modificaciones específicas.

11 HISTORIAL Y CONTROL DE VERSIONES

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio
01	Mayo 2025	Todas	Creación del Documento

DEPARTAMENTO TIC VISADO

12 REFERENCIAS

12.1 DOCUMENTO TECNICO ARQUITECTURA DE REFERENCIA – *Documento con lineamientos generales de arquitectura de sistemas informáticos del Ministerio de Salud.*

12.2 Referencias Internacionales para Arquitectura de Sistemas

Referencia / Estándar	Descripción	Aplicación
ISO/IEC 42010	Define principios y estructuras para describir arquitecturas de sistemas.	Base para documentar arquitecturas de forma estandarizada.
TOGAF (The Open Group Architecture Framework)	Marco para desarrollar arquitecturas empresariales alineadas al negocio.	Arquitectura de referencia institucional, interoperabilidad y alineamiento estratégico.
Archimate (Open Group)	Lenguaje de modelado para representar arquitecturas.	Visualización de relaciones entre componentes tecnológicos, aplicaciones y procesos.
COBIT Framework	Gobernanza y gestión de TI alineada con los objetivos de la organización.	Control y trazabilidad de decisiones arquitectónicas y cumplimiento normativo.
NIST SP 800-160 Vol. 1 y 2	Ingeniería de sistemas seguros; integra ciberseguridad desde el diseño.	Diseño seguro de infraestructuras críticas
AWS / Azure / GCP Well-Architected Framework	Buenas prácticas para arquitecturas en la nube.	Evaluación y mejora continua de arquitecturas cloud
ISO/IEC 25010	Modelo de calidad de productos de software.	Evaluación de atributos como seguridad, mantenibilidad, eficiencia.
ISO/IEC/IEEE 42030	Evaluación formal de arquitecturas.	Análisis estructurado de riesgos, cumplimiento y desempeño.
HL7 / FHIR	Estándares de interoperabilidad clínica y de salud.	Integración entre sistemas clínicos

DEPARTAMENTO TIC VISADO

Documento Técnico
Arquitectura de Referencia para Sector Salud
VERSIÓN 1.0

Ministerio de Salud

2025

Versión: 1.0
Vigencia:
Resolución:

DEPARTAMENTO TIC VISADO

Contenido

1.- OBJETIVOS

1.1.- Objetivo General

El objetivo principal de este documento de arquitectura de referencia TIC para el Ministerio de Salud y el Sector Salud es ofrecer una guía integral que facilite la planificación, el diseño y el despliegue de una infraestructura tecnológica moderna, eficiente y segura. Además, busca establecer pilares sólidos para la construcción de software a medida.

Esta arquitectura tiene como finalidad optimizar la gestión interna, fortalecer la colaboración interinstitucional y mejorar la comprensión de los equipos de desarrollo, mediante la implementación de estándares de seguridad, interoperabilidad y escalabilidad. Todo ello en línea con las mejores prácticas del entorno tecnológico actual.

1.2.- Objetivos Específicos

- Definir una arquitectura modular y escalable que permita la adaptación ágil a las cambiantes necesidades tecnológicas del Ministerio.
- Establecer lineamientos precisos para la implementación de estándares abiertos y protocolos de interoperabilidad, facilitando la integración de sistemas internos y la colaboración con otras instituciones gubernamentales.
- Diseñar mecanismos de seguridad robustos que salvaguarden la integridad y confidencialidad de los datos, incluyendo segmentación de red, encriptación de comunicaciones y sistemas avanzados de detección y respuesta ante amenazas cibernéticas.
- Definir interfaces de usuario intuitivas y modernas que mejoren la experiencia de los ciudadanos al interactuar con los servicios y recursos proporcionados por el Ministerio.
- Proporcionar pautas detalladas para la implementación de soluciones tecnológicas que respalden la toma de decisiones basada en datos, a través de la gestión eficiente de información y análisis de datos relevantes.
- Establecer criterios de sostenibilidad y mantenimiento a largo plazo, garantizando la continuidad operativa de los sistemas y servicios TIC del Ministerio.
- Fomentar la cultura de innovación tecnológica y la capacitación continua del personal, con el objetivo de maximizar el aprovechamiento de las soluciones implementadas y estar al tanto de las tendencias tecnológicas emergentes.
- Evaluar periódicamente la implementación de la arquitectura de referencia y realizar ajustes necesarios para garantizar su alineación con los objetivos estratégicos del Ministerio y los avances tecnológicos en el sector.
- Facilitar la generación de informes y métricas que permitan medir el impacto y la eficacia de la implementación de la arquitectura de referencia en términos de eficiencia, seguridad y satisfacción ciudadana.

2.- DESTINATARIOS DEL DOCUMENTO

Este documento de arquitectura de referencia TIC está dirigido a diversas audiencias clave dentro del **Ministerio de Salud, Servicios de Salud, Establecimientos de Salud, Seremis y Organismos Autónomos**. También está pensado para quienes participan en la implementación, gestión y supervisión de soluciones tecnológicas, con el fin de que todos tengan una guía común y puedan trabajar de manera coordinada.

Los destinatarios específicos incluyen:

- **Profesionales TIC**: Incluyendo arquitectos, ingenieros, desarrolladores y administradores de sistemas, estos expertos tecnológicos encontrarán orientación detallada sobre cómo diseñar, implementar y gestionar soluciones en línea con las mejores prácticas y estándares que deben existir en el Ministerio.
- **Equipos de Seguridad de la Información y Ciberseguridad:** Los profesionales encargados de la seguridad información y Ciberseguridad del Sector, se beneficiarán de las directrices y enfoques detallados para garantizar la protección de datos y sistemas contra amenazas cibernéticas.
- **Personal de Gestión de Proyectos:** Los líderes y administradores de proyectos encontrarán información útil para planificar y ejecutar proyectos de TIC de manera efectiva, asegurando la alineación con los objetivos estratégicos del Ministerio.
- **Instituciones del Sector Salud:** Servicios de Salud, Establecimientos, Seremis, Organismos Autónomos y Otras instituciones gubernamentales y entidades con las que el Ministerio colabora pueden comprender cómo la arquitectura de referencia promueve la interoperabilidad y la cooperación efectiva.

En resumen, este documento está diseñado para ser una herramienta útil y guía de referencia para una amplia variedad de audiencias que participan en la transformación tecnológica y en la prestación de servicios gubernamentales efectivos y eficientes.

3.- ARQUITECTURA DE REFERENCIA

La arquitectura de referencia TIC que proponemos está diseñada de manera modular y escalable, cubriendo desde la infraestructura tecnológica subyacente hasta las interfaces de usuario. Además, pone énfasis en la seguridad, la interoperabilidad y la eficiencia en la prestación de servicios. A continuación, se presentan los componentes clave de esta arquitectura:

- **Infraestructura Tecnológica:** La base de la arquitectura se compone de servidores, redes y sistemas de almacenamiento distribuidos. Se prioriza la virtualización y la nube para lograr la escalabilidad y la disponibilidad requeridas.
- **Plataforma de Servicios:** Esta capa proporciona servicios compartidos como autenticación, autorización, gestión de identidades y servicios de mensajería. Estos servicios se implementan con enfoque en estándares abiertos para facilitar la interoperabilidad.

DEPARTAMENTO TIC VISADO

- **Integración de Datos:** Se establecen mecanismos de integración de datos que permiten la consolidación y el intercambio de información entre sistemas internos y externos. Se utilizan protocolos como API REST y SOAP para lograr una comunicación efectiva.
- **Seguridad y Privacidad:** La arquitectura incorpora un modelo de seguridad por diseño, centrado en la protección integral de los activos de información a lo largo de todo el ciclo de vida. Incluye cifrado robusto de datos en tránsito y reposo, autenticación multi-factor, control de accesos por roles, monitoreo continuo con SIEM y soluciones EDR/XDR, así como gestión activa de vulnerabilidades y cumplimiento normativo en privacidad conforme a la Ley N° 19.628 y la Ley N° 21.663 sobre Marco de Ciberseguridad. Se refuerza la resiliencia mediante planes de continuidad operativa, respaldos cifrados y respuesta ante incidentes, asegurando una base segura y confiable para los servicios TI.
- **Analítica de Datos:** Se integran herramientas de análisis de datos para permitir la toma de decisiones informadas basadas en información relevante. Se emplean técnicas de análisis de big data y visualización para extraer información valiosa.
- **Gestión de Procesos:** Se incorpora una capa de gestión de procesos que permite automatizar flujos de trabajo internos y la interacción con ciudadanos, mejorando la eficiencia operativa y la calidad de los servicios.
- **Interoperabilidad y Colaboración:** Se establecen interfaces y protocolos estandarizados que permiten la colaboración con otras instituciones gubernamentales, facilitando el intercambio seguro de datos y recursos.
- **Escalabilidad y Resiliencia:** La arquitectura se diseña para ser escalable horizontalmente, lo que garantiza la capacidad de manejar aumentos en la carga de trabajo. Además, se implementan estrategias de respaldo y recuperación para mantener la continuidad de los servicios.
- **Mantenimiento y Actualización:** Se definen procesos y procedimientos para el mantenimiento continuo de la arquitectura, asegurando que las soluciones tecnológicas se mantengan actualizadas y seguras a lo largo del tiempo.

En conjunto, esta arquitectura de referencia TIC proporciona un marco sólido y flexible para la evolución tecnológica del Ministerio, permitiéndole aprovechar plenamente las ventajas de las tecnologías modernas mientras cumple con los más altos estándares de seguridad, interoperabilidad y eficiencia en la prestación de servicios públicos.

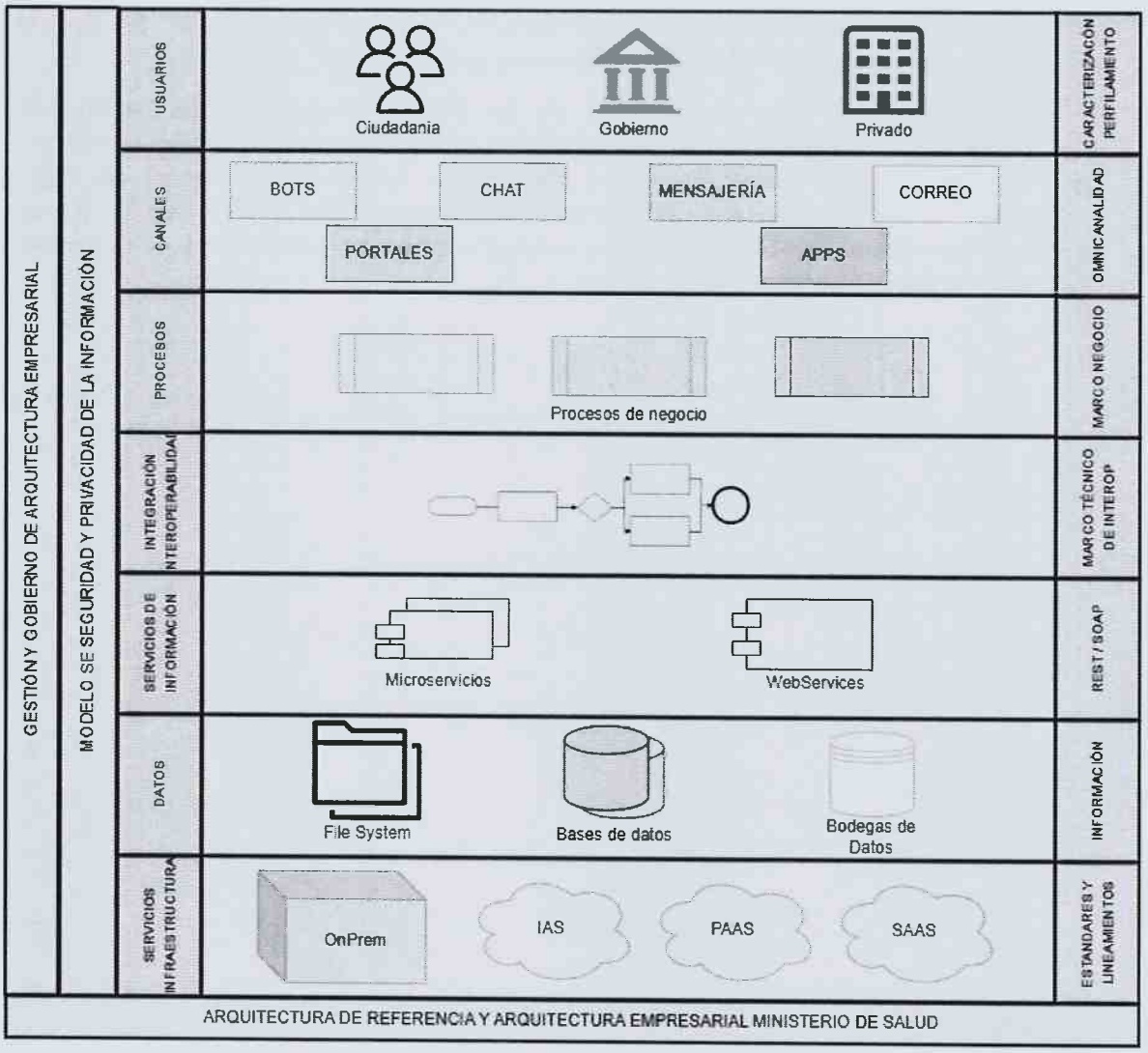
El propósito fundamental de esta arquitectura de referencia es proporcionar una plantilla sólida para el análisis y diseño de sistemas de información dentro del Ministerio, con el objetivo central de impulsar la transformación digital y la arquitectura empresarial de la entidad. En esencia, esta arquitectura de referencia se define como un conjunto estructurado de zonas, cada una compuesta por componentes base, principios, metodologías, estándares, directrices y tecnologías específicas. Todo ello tiene la finalidad de brindar a los usuarios que consulten este documento las herramientas necesarias para llevar a cabo el análisis y diseño de arquitecturas de soluciones basadas en estas zonas predefinidas.

A continuación, se presenta de manera detallada la arquitectura de referencia, la cual aglutina los componentes genéricos esenciales que serán utilizados en el proceso de análisis y diseño de sistemas de información dentro del Ministerio. Esta estructura proporciona una base sólida para la creación de soluciones tecnológicas que estén alineadas con los objetivos de transformación digital y que impulsen la eficiencia y efectividad de los servicios proporcionados por la entidad.

Para propósitos de entendimiento de las partes interesadas, se ha dividido la arquitectura de referencia en dos secciones complementarias, primero se describe la arquitectura de referencia como tal, desde un punto de vista abstracto y posteriormente desde un punto de vista mucho más técnico, enfocado principalmente para los equipos que tendrán directa participación en las definiciones de herramientas al momento de construir soluciones.

3.1.- Arquitectura Referencia (Abstracción Empresarial)

El siguiente diagrama muestra la arquitectura de referencia del Ministerio de Salud



La arquitectura de referencia está compuesta por las siguientes zonas:

3.1.1.- Zona de gestión y gobierno de arquitectura empresarial.

La Zona de Gestión y Gobierno de Arquitectura Empresarial juega un rol fundamental en el diseño y mantenimiento de la estructura organizativa y estratégica del Ministerio. Esta zona abarca los componentes esenciales para establecer un marco sólido que garantice una toma de decisiones coherente y eficiente en relación con la arquitectura empresarial. Entre los aspectos clave se incluyen:

- **Gobernanza de Arquitectura:** Se establecen principios, políticas y procesos para supervisar y gestionar la evolución de la arquitectura. Esto asegura que todas las

decisiones de diseño sean coherentes con los objetivos estratégicos y se alineen con las directrices de la organización.

- **Planificación Estratégica:** Se definen las metas a largo plazo de la organización y cómo la arquitectura tecnológica puede apoyar y potenciar estos objetivos. Esto implica la identificación de oportunidades y desafíos tecnológicos clave.
- **Gestión de Cambios:** Se establecen procedimientos para administrar cambios y actualizaciones en la arquitectura de manera controlada y con mínimo impacto en la operación actual. Esto ayuda a evitar interrupciones innecesarias y garantiza la continuidad del servicio.
- **Control de Calidad:** Se implementan mecanismos para evaluar la calidad y eficacia de la arquitectura implementada. Esto puede involucrar revisiones periódicas, evaluaciones de riesgos y aseguramiento de la conformidad con estándares y regulaciones.
- **Colaboración y Comunicación:** Se establecen canales de comunicación efectivos entre los equipos de arquitectura, los líderes y los stakeholders clave. Esto fomenta la colaboración y el intercambio de conocimiento en toda la organización.
- **Gestión de Recursos:** Se determinan los recursos necesarios para implementar y mantener la arquitectura. Esto puede incluir personal especializado, herramientas de software, presupuesto y otros recursos necesarios.

En conjunto, la Zona de Gestión y Gobierno de Arquitectura Empresarial proporciona la estructura y dirección necesarias para asegurar que la arquitectura tecnológica del Ministerio sea coherente con los objetivos organizacionales y esté en constante evolución para abordar las demandas cambiantes del entorno tecnológico y las necesidades de la entidad.

3.1.2.- Zona del modelo de seguridad y privacidad de la información.

La Zona del Modelo de Seguridad y Privacidad de la Información es un componente crítico de la arquitectura de referencia, diseñada para salvaguardar la confidencialidad, integridad y disponibilidad de los datos del Ministerio. Esta zona se enfoca en establecer un entorno seguro y confiable, garantizando que la información sensible esté protegida de amenazas y riesgos. Entre los aspectos fundamentales se encuentran:

- **Seguridad en Capas:** Se despliegan controles técnicos y administrativos desde la capa de red hasta la aplicación, incluyendo firewalls de próxima generación, WAF, segmentación de redes, y monitoreo continuo mediante SIEM y sistemas de detección y respuesta (EDR/XDR).
- **Gestión de Identidad y Acceso:** Se implementan mecanismos para autenticar y autorizar a usuarios y sistemas, asegurando que solo las personas y aplicaciones autorizadas tengan acceso a los recursos apropiados. Se implementa autenticación multifactor (MFA), control de accesos basado en roles (RBAC), principios de mínimo privilegio y políticas de acceso dinámico.

- **Control de Acceso Granular:** Definición e implementación de políticas y tecnologías para controlar el acceso a datos y sistemas, asignando niveles de privilegio específicos según los roles y responsabilidades de los usuarios dentro del Sector.
- **Cifrado de Datos**: Se aplica cifrado para proteger la información confidencial mientras se almacena y se transfiere, garantizando que incluso si los datos caen en manos equivocadas, no sean accesibles sin la correspondiente clave. Utilizando el cifrado robusto de los datos en reposo y en tránsito mediante algoritmos criptográficos fuertes (AES-256, TLS 1.2 o superior), junto con una adecuada gestión de claves y certificados.
- **Gestión de Amenazas y Vulnerabilidades:** Se deben implementar sistemas de detección y prevención de intrusiones para identificar actividades maliciosas o anómalas en tiempo real, y se toman medidas proactivas para mitigar riesgos potenciales.
- **Gestión Integral de Actualizaciones:** Los servicios y plataformas se diseñarán para facilitar la recepción e implementación oportuna de actualizaciones y parches de seguridad. Esto asegura la protección continua contra vulnerabilidades conocidas y emergentes, manteniendo la integridad de la infraestructura.
- **Continuidad Operacional y Recuperación ante Incidentes de Ciberseguridad:** Integración de estrategias de continuidad del negocio y planes de recuperación ante desastres cibernéticos. Esto incluye la implementación de respaldos cifrados, la definición de planes de respuesta a incidentes y la realización de simulacros periódicos.
- **Cumplimiento Normativo:** Aseguramiento de que la arquitectura cumpla con las leyes, regulaciones y estándares de seguridad y privacidad relevantes para el sector salud y las normativas gubernamentales vigentes.
- **Auditoría y Monitoreo:** Se establecen registros detallados de actividades para permitir la revisión y el análisis de eventos en caso de incidentes de seguridad, garantizando la trazabilidad y la rendición de cuentas.
- **Gestión de Incidentes:** Definición de procedimientos claros y eficientes para la respuesta, contención, erradicación y recuperación ante incidentes de seguridad, minimizando el impacto y restaurando la operatividad normal en el menor tiempo posible.
- **Privacidad de los Datos**: Establecimiento de políticas y prácticas para proteger la privacidad de los datos personales, asegurando que se recopilen, almacenen y procesen de acuerdo con regulaciones de privacidad de conformidad con las leyes de privacidad aplicables. Todos los accesos a sitios web institucionales, así como los procesos de comunicación entre el cliente y el servidor, deben ser protegidos mediante HTTPS/TLS. Esto incluye todas las formas de comunicación como HTTPS para el tráfico web y SSH para la administración de servidores. Los certificados digitales deben ser gestionados y actualizados conforme a las mejores prácticas de la industria, asegurando su validez y la robustez de la criptografía utilizada. Se deben implementar tokens de sesión únicos, seguros y de corta duración, con mecanismos

de rotación y cifrado para prevenir el secuestro de sesión. Los mensajes de error deben ser genéricos, evitando la exposición de información sensible o detalles internos del sistema. Además, las contraseñas deben almacenarse con funciones de hash seguras como bcrypt, Argon2 o scrypt, utilizando salting y stretching para protegerlas frente a ataques de fuerza bruta y diccionario.

- **Seguridad por Diseño en APIs:** Las interfaces de programación de aplicaciones (APIs) internas y externas se deben desarrollar bajo principios de seguridad por diseño, implementando autenticación robusta (OAuth 2.0), autorización granular, cifrado TLS 1.3 y protecciones contra las vulnerabilidades comunes identificadas en el OWASP API Top 10. Se deben incluir la validación de entradas, limitación de tasas de consumo, la trazabilidad completa de los accesos y una documentación actualizada. Para la exposición de los servicios API REST debe utilizar mecanismos de autenticación para su consumo privado, ya sea tokens (JWT u otros), certificados o llaves criptográficas, u otros como medios de autenticación entre puntos.
- **Educación y Concienciación:** Se promueve la formación continua y la sensibilización sobre cuestiones de seguridad entre el personal, reduciendo los riesgos asociados con errores humanos.

La implementación efectiva de la Zona del Modelo de Seguridad y Privacidad de la Información es fundamental para garantizar la resiliencia de la arquitectura tecnológica del Ministerio de Salud y del Sector Salud, frente a las crecientes amenazas cibernéticas, protegiendo la información sensible y fortaleciendo la confianza de los ciudadanos en los servicios de salud.

3.1.3.- Zona de Usuarios.

La Zona de Usuarios es un componente esencial en la arquitectura de referencia, diseñada para comprender y abordar las diversas necesidades y expectativas de los diferentes actores que interactúan con los sistemas de información del Ministerio. Esta zona se centra en identificar y priorizar los requerimientos de los usuarios finales y otros stakeholders clave.

Entre los aspectos fundamentales se encuentran:

- **Identificación de Grupos de Interés:** Se identifican y clasifican a los diferentes grupos de usuarios y stakeholders que tienen un interés en los sistemas de información del Ministerio, como ciudadanos, funcionarios, entidades gubernamentales colaboradoras, entre otros.
- **Análisis de Requerimientos:** Se recopilan y analizan los requerimientos y expectativas de cada grupo de interés, asegurando una comprensión completa de sus necesidades en términos de funcionalidad, usabilidad y experiencia general.
- **Segmentación de Usuarios:** Se segmentan los usuarios en categorías basadas en sus roles, responsabilidades y necesidades específicas, lo que permite una personalización efectiva de la experiencia de usuario.

DEPARTAMENTO TIC VISADO

- **Diseño Centrado en el Usuario:** Se utiliza la información recopilada para diseñar interfaces y funcionalidades que sean intuitivas y relevantes para cada grupo de usuarios, mejorando su satisfacción y eficiencia.
- **Feedback Continuo:** Se establecen canales para recopilar comentarios y sugerencias de los usuarios, lo que facilita la mejora constante de los sistemas de información según las necesidades cambiantes.
- **Pruebas de Usuario:** Se realizan pruebas de usuario para validar el diseño y la funcionalidad de los sistemas antes de su implementación, garantizando que cumplan con las expectativas de los usuarios.
- **Capacitación y Soporte**: Se implementan programas de capacitación y se proporciona soporte continuo para ayudar a los usuarios a utilizar eficazmente los sistemas y resolver posibles problemas.
- **Medición de la Experiencia del Usuario:** Se recopilan métricas para evaluar la satisfacción y la experiencia general de los usuarios, lo que permite ajustes y mejoras basados en datos.
- **Comunicación con Stakeholders:** Se establecen canales de comunicación efectivos con los stakeholders, manteniéndolos informados sobre las actualizaciones y mejoras en los sistemas de información.

La Zona de Usuarios asegura que los sistemas de información del Ministerio estén diseñados teniendo en cuenta las necesidades y expectativas de quienes los utilizan, lo que conduce a una mayor adopción, satisfacción del usuario y cumplimiento de los objetivos organizacionales.

3.1.4.- Zona de canales

La Zona de Canales está diseñada para definir cómo el Ministerio se comunica y ofrece sus servicios a los diferentes grupos de interés y usuarios. Esta zona se enfoca en proporcionar una variedad de canales de comunicación y acceso que sean accesibles, intuitivos y eficientes. Entre los aspectos clave se encuentran:

- **Canal de Comunicación:** Se establecen los canales a través de los cuales el Ministerio interactúa con los ciudadanos, otros organismos gubernamentales, y su personal interno. Esto puede incluir sitios web, aplicaciones móviles, correos electrónicos, líneas de atención telefónica, y redes sociales.
- **Multicanalidad:** Se asegura que los diferentes canales estén integrados de manera coherente, permitiendo a los usuarios acceder a los mismos servicios y recursos independientemente del canal que utilicen.
- **Personalización:** Se proporciona la capacidad de adaptar la experiencia del usuario según sus preferencias y necesidades, ofreciendo contenido y servicios relevantes a través de diversos canales.
- **Accesibilidad:** Se garantiza que los canales sean accesibles para personas con discapacidades y cumplan con estándares de accesibilidad web para garantizar la inclusión de todos los ciudadanos.

- **Interacción en Tiempo Real:** Se implementan características que permiten la interacción en tiempo real con los usuarios, como chats en línea y respuestas automáticas para brindar asistencia instantánea.
- **Notificaciones y Alertas:** Se establecen mecanismos para enviar notificaciones y alertas a los usuarios sobre actualizaciones, cambios o eventos relevantes a través de diferentes canales.
- **Análisis de Datos de Uso**: Se recopila y analiza información sobre cómo los usuarios interactúan con los diferentes canales para identificar áreas de mejora y optimización.
- **Seguridad en la Comunicación:** Se implementan medidas de seguridad para proteger la información transmitida a través de los canales, incluyendo encriptación de datos y autenticación.
- **Integración con Sistemas Internos:** Se asegura que los canales estén conectados con los sistemas internos del Ministerio para una gestión eficiente de la información y una experiencia de usuario coherente.
- **Monitoreo y Mejora Continua:** Se establecen procesos para monitorear el rendimiento de los canales y recopilar retroalimentación de los usuarios, lo que permite realizar ajustes y mejoras en respuesta a sus necesidades.
- La Zona de Canales garantiza que el Ministerio brinde servicios y se comunique de manera efectiva y accesible a través de una variedad de medios, mejorando la experiencia de los usuarios y fortaleciendo su compromiso con la entidad.

3.1.5.- Zona de procesos

La Zona de Procesos de Negocio está enfocada en definir y optimizar los flujos de trabajo y operaciones esenciales dentro del Ministerio. Esta zona se concentra en diseñar procesos eficientes, automatizados y alineados con los objetivos estratégicos de la entidad. Entre los aspectos clave se encuentran:

- **Identificación de Procesos Clave:** Se identifican los procesos centrales y críticos para el funcionamiento del Ministerio, desde la gestión interna hasta la interacción con los ciudadanos y otras entidades.
- **Modelado de Procesos:** Se crea una representación visual de los flujos de trabajo, destacando las actividades, los actores involucrados y las interacciones entre ellos, lo que facilita la comprensión y mejora de los procesos.
- **Optimización y Automatización**: Se analizan los procesos existentes para identificar oportunidades de optimización y automatización, con el objetivo de mejorar la eficiencia y reducir errores.
- **Flujos de Trabajo Digitales:** Se diseña la transición de los procesos tradicionales a flujos de trabajo digitales, aprovechando herramientas y tecnologías para facilitar la colaboración y la toma de decisiones.
- **Integración de Sistemas:** Se establecen conexiones entre los sistemas internos y externos necesarios para llevar a cabo los procesos de manera fluida, permitiendo la transferencia de datos y la sincronización de información.

- **Gestión de Casos:** Se implementa una estructura para gestionar casos complejos que involucran múltiples etapas y partes interesadas, asegurando una resolución eficiente y coherente.
- **Monitorización y Reportes:** Se establece un seguimiento constante de los procesos para recopilar datos y generar informes que permitan evaluar el rendimiento y la eficacia de las operaciones.
- **Mejora Continua:** Se establecen mecanismos para recopilar retroalimentación de los usuarios y realizar ajustes en los procesos en función de los resultados y las necesidades cambiantes.
- **Cumplimiento Regulatorio:** Se asegura que los procesos estén en conformidad con regulaciones y normativas relevantes, garantizando que se respeten los estándares legales y éticos.
- **Capacitación y Adopción:** Se proporciona capacitación a los usuarios para garantizar la correcta ejecución de los procesos, así como para promover la adopción exitosa de nuevas formas de trabajar.

La Zona de Procesos busca garantizar que las operaciones internas sean eficientes, coherentes y alineadas con los objetivos estratégicos, permitiendo al Ministerio brindar servicios de calidad y cumplir con sus responsabilidades de manera efectiva.

3.1.6.- Zona de integración o interoperabilidad

La Zona de Integración o Interoperabilidad está diseñado para facilitar la conexión y el intercambio de información entre sistemas internos y externos del Ministerio. Esta zona se enfoca en establecer una infraestructura que permita una colaboración efectiva y una transferencia de datos fluida. Entre los aspectos clave se encuentran:

- **Cumplimiento de Estándares HL7:** Los sistemas de información en Salud deben ser compatibles con el estándar HL7 (Health Level Seven) en sus versiones vigentes, incluyendo HL7 v2.x y FHIR (Fast Healthcare Interoperability Resources), este último en sus versiones R4 y posteriores, para asegurar un intercambio de datos entre sistemas de información de salud que respete la consistencia y precisión clínica. Esto permitirá la interoperabilidad eficaz de información entre sistemas de historia clínica electrónica (HCE), sistemas de apoyo clínico (RIS, LIS, etc.) y otras aplicaciones de salud.
- **Estándares de Integración y Protocolos:** Los sistemas deben utilizar estándares de integración ampliamente aceptados (como REST, GraphQL, JSON, XML) y protocolos de comunicación seguros (como HTTPS, SFTP y TCP/IP) que permitan la transmisión de datos de manera confiable y segura entre sistemas de información de salud.
- **Gestión de Datos Interoperables:** Los datos deben manejarse en formatos estructurados y normalizados según las directrices organizacionales y normativas vigentes, permitiendo su fácil intercambio y procesamiento entre aplicaciones sin pérdida de consistencia o integridad de la información.

- **Plataforma de Integración:** Se establece una plataforma que actúa como intermediario entre los sistemas, facilitando la comunicación y el flujo de datos de manera estandarizada.
- **Interfaces y Protocolos Estándar:** Se definen interfaces y protocolos de comunicación estandarizados que permiten a los sistemas intercambiar datos de manera coherente y uniforme.
- **Orquestación de Procesos:** Se implementa la capacidad de orquestar procesos complejos que involucran varios sistemas, garantizando una ejecución fluida y secuencial.
- **Transformación de Datos:** Se permite la transformación de datos para asegurar que la información se ajuste a los formatos requeridos por los sistemas de destino.
- **Adaptadores y Conectores:** Se desarrollan adaptadores y conectores específicos para conectarse con sistemas externos, asegurando una integración efectiva.
- **Gestión de Mensajes:** Se establece un sistema de gestión de mensajes para asegurar la entrega y el enrutamiento adecuado de la información entre sistemas.
- **Seguridad en la Integración:** Se implementan medidas de seguridad para proteger la información durante la transferencia entre sistemas, incluyendo encriptación y autenticación.
- **Monitorización y Tráfico de Datos:** Se establece un mecanismo para monitorear el tráfico de datos y verificar el estado de la integración en tiempo real.
- **Integración de Terceros:** Se permite la integración con sistemas y servicios de terceros, como proveedores externos o agencias gubernamentales, para una colaboración más amplia.
- **Pruebas de Integración:** Se realizan pruebas exhaustivas de la integración para asegurar que los sistemas interactúen de manera efectiva y sin problemas.
- **APIs Documentadas y Consistentes:** Es obligatorio desarrollar APIs (interfaces de programación de aplicaciones) documentadas y consistentes, que faciliten el acceso y la integración de funcionalidades y datos entre diferentes sistemas de información de salud, tanto internos como de terceros, asegurando una comunicación clara y eficaz.

La Zona de Integración o Interoperabilidad asegura que los sistemas del Sector Salud trabajen en conjunto de manera efectiva, lo que permite una gestión fluida de la información y una colaboración eficiente con otras entidades.

3.1.7.- Zona de servicios de información

La Zona de Servicios de Información está orientada a definir y estructurar los sistemas tecnológicos y aplicaciones que respaldan los procesos y operaciones del Ministerio. Esta zona se enfoca en garantizar que las soluciones tecnológicas sean eficientes, escalables y alineadas con las necesidades organizacionales. Entre los aspectos clave se encuentran:

- **Inventario de Aplicaciones:** Se realiza un inventario completo de las aplicaciones utilizadas por la organización, identificando su propósito, funcionalidades y relación con los procesos de negocio.
- **Diseño de Aplicaciones:** Se definen las especificaciones técnicas y funcionales de las aplicaciones, asegurando que se adapten de manera óptima a los requerimientos de los usuarios y a los objetivos organizacionales.
- **Desarrollo de Software:** Se implementan metodologías de desarrollo ágil y buenas prácticas para construir, mantener y mejorar las aplicaciones de manera efectiva y eficiente.
- **Integración de Sistemas:** Se establecen conexiones entre las diferentes aplicaciones y sistemas para permitir el flujo de datos y la interoperabilidad, evitando duplicación de esfuerzos.
- **Implementación y Despliegue:** Se define la estrategia y el proceso para implementar y desplegar nuevas aplicaciones y actualizaciones en un entorno controlado y minimizando el impacto en la operación.
- **Mantenimiento y Soporte**: Se establecen procedimientos para el mantenimiento y soporte continuo de las aplicaciones, incluyendo la corrección de errores, actualizaciones de seguridad y mejoras funcionales.
- **Arquitectura de Aplicaciones:** Se define la estructura y el diseño general de las aplicaciones, asegurando que sigan principios de modularidad, escalabilidad y reutilización de componentes.
- **Seguridad de Aplicaciones:** Se deben implementar medidas de seguridad a nivel de aplicaciones, como autenticación, autorización y pruebas de seguridad, para proteger la integridad y confidencialidad de los datos. Se deben adoptar estándares reconocidos de desarrollo seguro, como los establecidos por el OWASP (Open Web Application Security Project) o el NIST (National Institute of Standards and Technology), y aplicar marcos de trabajo como el Secure Software Development Lifecycle (SSDLC). Implementar medidas para prevenir ataques de inyección de código, como SQL Injection, XSS (Cross-Site Scripting) y CSRF (Cross-Site Request Forgery). Las consultas a bases de datos deben utilizar procedimientos almacenados y consultas preparadas para prevenir ataques de inyección SQL. En los desarrollos, debe emplear librerías y frameworks de terceros reconocidos por su fiabilidad y que integren mecanismos de seguridad robustos.
- **Gestión de Versiones:** Se establece un proceso para gestionar las versiones de las aplicaciones, lo que facilita el control de cambios y la implementación ordenada de nuevas funcionalidades.
- **Interfaz de Programación de Aplicaciones (API):** Se define una estrategia de API que permite a las aplicaciones interactuar de manera coherente y eficiente, fomentando la interoperabilidad y la integración.

La Zona de servicios de Información garantiza que el Ministerio cuente con soluciones tecnológicas sólidas y alineadas con sus objetivos, permitiendo una gestión eficiente de la información y la provisión de servicios de alta calidad a los ciudadanos y otros stakeholders.

3.1.8.- Zona de datos e información

La Zona de Datos e Información está centrado en la gestión, almacenamiento y utilización efectiva de los datos en el entorno del Ministerio. Esta zona se enfoca en asegurar que los datos sean precisos, accesibles y estén disponibles para respaldar las operaciones y la toma de decisiones. Entre los aspectos clave se encuentran:

- **Gestión de Datos Maestros**: Se establecen fuentes confiables y únicas de datos maestros, como registros de ciudadanos, empleados o activos, para garantizar la integridad y coherencia de la información.
- **Almacenamiento de Datos:** Se determinan las tecnologías y estrategias para el almacenamiento eficiente y seguro de los datos, incluyendo bases de datos, sistemas de archivos y almacenamiento en la nube.
- **Modelado de Datos:** Se definen modelos de datos que representan la estructura y relaciones entre los diferentes tipos de información utilizados en el Ministerio.
- **Integración de Datos:** Se establecen mecanismos para la integración de datos entre sistemas y aplicaciones, garantizando la consistencia y disponibilidad de la información.
- **Calidad de Datos:** Se implementan prácticas para asegurar la calidad de los datos, incluyendo la limpieza, normalización y validación de la información.
- **Acceso y Privacidad:** Se definen políticas de acceso a los datos, asegurando que solo los usuarios autorizados puedan acceder a la información relevante y se respete la privacidad de los datos personales.
- **Gobierno de Datos:** Se establecen procesos y responsabilidades para la gestión y el control de los datos, incluyendo la definición de roles y responsabilidades de administración de datos.
- **Análisis de Datos:** Se habilita la capacidad de analizar datos para extraer conocimientos y patrones que respalden la toma de decisiones informadas.
- **Visualización de Datos:** Se implementan herramientas de visualización de datos para representar la información de manera comprensible y fácil de interpretar.
- **Respaldo y Recuperación:** Se establecen estrategias de respaldo y recuperación de datos para asegurar la continuidad operativa en caso de fallos o pérdidas de información.

La Zona de Datos e Información asegura que el Ministerio aproveche al máximo su información, permitiendo una gestión efectiva, la toma de decisiones basadas en datos y una colaboración más informada en todos los niveles de la organización.

3.1.9.- Zona de servicios de infraestructura

La Zona de Servicios de Infraestructura está enfocada en proporcionar los recursos tecnológicos necesarios para el funcionamiento óptimo de los sistemas y aplicaciones del Ministerio. Esta zona se concentra en garantizar la disponibilidad, escalabilidad y rendimiento de la infraestructura tecnológica. Entre los aspectos clave se encuentran:

- **Virtualización y Cloud:** Se implementan tecnologías de virtualización y se aprovechan servicios en la nube para crear una infraestructura flexible y escalable.
- **Servidores y Almacenamiento:** Se establecen servidores y sistemas de almacenamiento que satisfagan las necesidades de procesamiento y capacidad de datos requeridas por las aplicaciones.
- **Redes y Comunicaciones:** Se asegura una red robusta y segura que permita la comunicación eficiente entre sistemas y usuarios, tanto internos como externos.
- **Balanceo de Carga:** Se implementan mecanismos de balanceo de carga para distribuir equitativamente la carga de trabajo entre los servidores, mejorando la disponibilidad y el rendimiento.
- **Seguridad de la Infraestructura:** Se establecen medidas de seguridad para proteger la infraestructura tecnológica, incluyendo cortafuegos, detección de intrusiones y soluciones de seguridad en red.
- **Respaldo y Recuperación:** Se implementa una estrategia de respaldo y recuperación de la infraestructura para garantizar la continuidad de los servicios en caso de fallas o desastres.
- **Monitoreo y Gestión:** Se establecen herramientas y procesos para monitorear el rendimiento de la infraestructura y abordar proactivamente problemas potenciales.
- **Escalabilidad Automatizada:** Se implementan sistemas para escalar automáticamente los recursos según las demandas cambiantes, garantizando el rendimiento incluso en momentos de alta carga.
- **Gestión de Configuración:** Se establecen prácticas de gestión de configuración para asegurar que la infraestructura esté correctamente configurada y documentada.
- **Eficiencia Energética:** Se consideran prácticas de eficiencia energética en el diseño y la operación de la infraestructura, minimizando el consumo de recursos.

La Zona de Servicios de Infraestructura es crucial para asegurar que los sistemas y aplicaciones del Ministerio funcionen de manera confiable y eficiente, permitiendo una experiencia de usuario sin problemas y un respaldo sólido para las operaciones organizacionales.

3.2.- Arquitectura Referencia (Abstracción Técnica)

El siguiente diagrama muestra la referencia técnica para la arquitectura Propuesta para el Ministerio,

En el diagrama se presenta una arquitectura orientada a microservicios, que cuenta con una capa de front end, la cual propone un desarrollo en Cluster, se recomienda que este dockerizada, pero también se contempla la posibilidad de que esté en máquinas virtuales solamenteA continuación, el apigee que es el gateway que sirve para llevar la gobernanza de las apis, y la interoperabilidad de todos los sistemas con los servicios y también del front con el back. Dentro de la capa de back end dependiendo del sistema que sea se pueden usar herramientas como OpenHim (que es un bus de integración HL7), en esta capa también se

encuentran las apis, las colas, las etl's. Y por último la capa de datos, en la que se recomienda el uso de Mongo DB para BD no relaciones y PostgreSQL para BD relacionales.

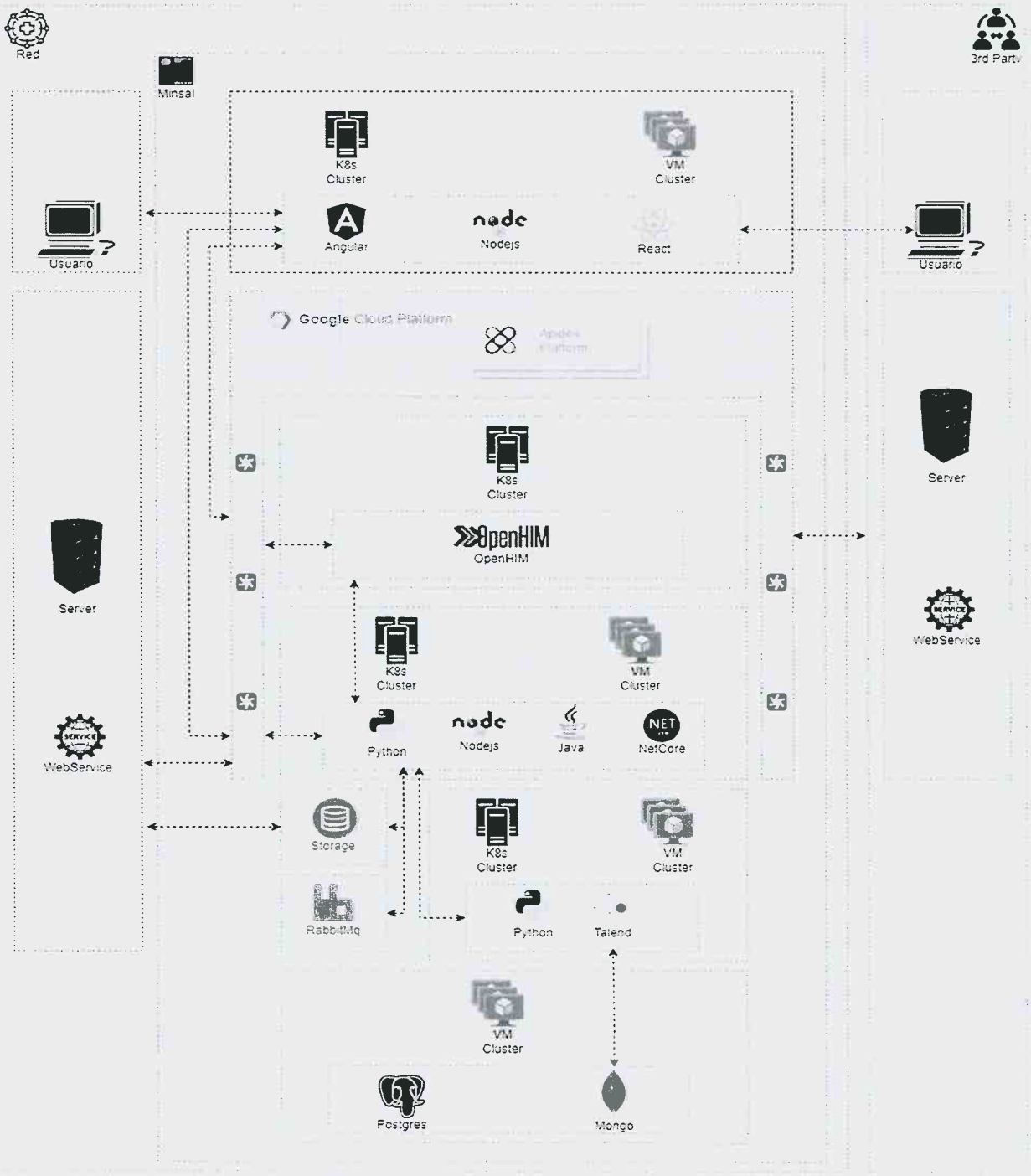


Figure 2 Arquitectura de Referencia. vista técnica

3.2.1.- Enfoque

MONOLÍTICO

En el ambiente monolítico, toda la aplicación o sistema se desarrolla como un solo y gran componente, donde todas las funcionalidades y características están interconectadas y desplegadas en conjunto. Algunas características de un ambiente monolítico son:

a.- **Simplicidad Inicial:** Los desarrollos monolíticos suelen ser más simples en términos de arquitectura y estructura, lo que facilita la implementación inicial.
b.- **Despliegue Unificado:** Dado que todo está en un solo componente, el despliegue y la actualización se realizan como una unidad, lo que puede simplificar la administración.
c.- **Comunicación Interna Fácil:** Debido a la estrecha integración, las comunicaciones internas entre componentes son más directas.
d.- **Escalabilidad Limitada:** Si una parte del sistema experimenta un aumento en la demanda, es difícil escalar solo esa parte sin afectar el sistema en su conjunto.
e.- **Acoplamiento Fuerte**: Los cambios en una parte del sistema pueden afectar otras partes debido al acoplamiento estrecho entre componentes.
f.- **Dificultad en Mantenimiento:** A medida que el sistema crece, puede volverse complicado de mantener y evolucionar debido a su naturaleza monolítica.

Se recomienda este enfoque en escenarios donde la simplicidad y la rapidez en el desarrollo y despliegue son prioritarios sobre la flexibilidad y escalabilidad a largo plazo. Algunos de estos escenarios incluyen:

a.- **Aplicaciones Pequeñas y Simples:** Cuando se trata de aplicaciones pequeñas con funcionalidades limitadas y requisitos técnicos simples, un enfoque monolítico puede ser más eficiente y rápido de implementar.
b.- **Equipos con Recursos Limitados:** Si el equipo de desarrollo tiene recursos y habilidades limitadas para trabajar con arquitecturas más complejas, un enfoque monolítico puede ser más manejable.
c.- **Prototipos y MVPs:** En la etapa de creación de prototipos o versiones mínimas viables (MVP) de una aplicación, un enfoque monolítico puede permitir un desarrollo más rápido y una validación temprana de la idea.
d. **Aplicaciones con Pocos Cambios Futuros:** Si se espera que los requisitos de la aplicación sean estables y no cambien drásticamente en el futuro, un enfoque monolítico podría ser suficiente.
e.- **Tiempo de Lanzamiento Rápido:** Si la prioridad es llevar la aplicación al mercado lo más rápido posible, el enfoque monolítico puede ser más conveniente debido a su simplicidad y menor complejidad de gestión.
f.- **Aplicaciones Internas:** En el caso de aplicaciones internas, donde los requisitos son conocidos y la escalabilidad no es una preocupación primordial, un enfoque monolítico puede ser adecuado.

g.- **Proyectos de Aprendizaje:** En proyectos de aprendizaje o capacitación, donde el objetivo principal es adquirir conocimientos y habilidades, trabajar con una aplicación monolítica puede ser más manejable.

MICROSERVICIOS

En el ambiente de microservicios se podrá dividir en componentes pequeños e independientes llamados microservicios. Cada microservicio es responsable de una funcionalidad específica y puede ser desarrollado, implementado y escalado de manera independiente. Algunas características de este enfoque son:

a.- **Desacoplamiento:** Los microservicios son independientes entre sí, lo que permite cambios y actualizaciones sin afectar otros componentes.
b.- **Escalabilidad Granular:** Puede escalar solo los microservicios que requieren más recursos en lugar de escalar todo el sistema.
c.- **Flexibilidad Tecnológica:** Diferentes microservicios pueden estar desarrollados con diferentes tecnologías según su mejor adecuación.
d.- **Facilita la Innovación:** Dado que los microservicios son independientes, es más fácil experimentar con nuevas tecnologías o enfoques en componentes específicos.
e.- **Complejidad de Gestión:** Coordinar múltiples microservicios puede ser complicado en términos de despliegue, monitoreo y gestión.
f.- **Comunicación Distribuida:** La comunicación entre microservicios a menudo se realiza a través de la red, lo que puede aumentar la latencia.
g.- **Mayor Inversión Inicial:** El desarrollo inicial puede requerir más esfuerzo debido a la necesidad de diseñar, implementar y gestionar varios microservicios.

Se recomienda el enfoque de microservicios en escenarios donde la flexibilidad, escalabilidad y modularidad son esenciales para el éxito de la aplicación. Algunos de los casos en los que se recomienda el enfoque de microservicios incluyen:

3.2.1.- Tecnología

Nos referimos con tecnología a las herramientas, lenguajes de programación, frameworks, librerías y plataformas tecnológicas específicas utilizadas para implementar y respaldar los componentes y funcionalidades de un sistema o aplicación. Estas tecnologías son fundamentales para dar vida a la visión arquitectónica y asegurar que los sistemas sean eficientes, seguros y cumplan con los requisitos funcionales y no funcionales.

Abarcan los siguientes aspectos y capas de la arquitectura:

a.- **Lenguajes de Programación:** Para asegurar la estabilidad y seguridad del proyecto, la selección del lenguaje de programación debe considerar versiones que cuenten con soporte a largo plazo (LTS) y actualizaciones de seguridad activas. La compatibilidad con los requisitos del proyecto y las preferencias del equipo de desarrollo también son factores importantes en esta decisión.

DEPARTAMENTO TIC VISADO

A continuación, se presenta una lista de recomendaciones de lenguajes, cuyas versiones recomendadas se encuentran en el documento de stack tecnológico:

- Java
- Python
- Php

b.- Marcos de Trabajo (Frameworks): Los marcos de trabajo son conjuntos de herramientas y librerías que proporcionan una estructura para el desarrollo de aplicaciones. Al seleccionar un framework es crucial considerar versiones que reciban actualizaciones de seguridad de forma activa y que cuenten con un ciclo de vida de soporte adecuado. Esto asegura la protección continua de las aplicaciones desarrolladas con ellos.

La lista de frameworks recomendados son (Las versiones se encuentran en el documento de Stack Tecnológico):

- Java: SpringBoot última versión
- Python: Django y Flask última versión
- Php: Laravel, CodeIgniter última versión

c.- Bases de Datos: Las bases de datos son tecnologías utilizadas para almacenar y gestionar datos. La elección de la base de datos depende de las necesidades de almacenamiento y consulta de datos.

La lista de motores de bases de datos recomendados es:

i.- Relacional, donde se recomienda la utilización de los siguientes motores:

- PostgreSQL 9+ o superior
- MySQL 5.7+ o superior
- Oracle última versión

ii.- No relacional, donde se recomienda la utilización de los siguientes motores:

- MongoDB 4+ o superior
- Redis 5+ o superior
- Elasticsearch 5.5+ o superior

d.- Librerías: Las librerías son conjuntos de funciones y clases reutilizables que facilitan tareas específicas en el desarrollo, permiten a los desarrolladores aprovechar funcionalidades existentes sin tener que reinventar la rueda. Es crucial considerar la frecuencia de las actualizaciones de seguridad y el nivel de soporte de la comunidad al elegir librerías para un proyecto. Las librerías bien mantenidas son menos propensas a tener vulnerabilidades sin parchar.

La lista de librerías recomendadas es:

i.- Bibliotecas Gráficas:

- Bootstrap versión 5.x o superior
- NPM

ii.- Scripts

- ReactJS 18.x o superior
- JQuery 3.x o superior

e.- **Plataformas en la Nube:** Las plataformas en la nube, como Amazon Web Services (AWS), y Google Cloud Platform, ofrecen servicios y recursos para hospedar, desplegar y escalar aplicaciones. Son esenciales para la implementación de soluciones en entornos escalables y flexibles.

La definición de qué herramientas utilizar sobre los ambientes cloud deberán definirse particularmente evaluando cada solución.

Como norma general el Ministerio prefiere los desarrollos agnósticos a la marca, por lo que no recomienda el uso de tecnologías nativas de cada nube.

En este contexto, la Arquitectura de Referencia la utilización de plataformas Cloud, debe incorporar **la seguridad desde el diseño**. Esto implica la **definición clara de controles de seguridad específicos para el entorno cloud**, considerando aspectos como la **gestión de identidades y accesos (IAM)** robusta y con el principio de mínimo privilegio, la **configuración segura de los recursos cloud** (instancias, almacenamiento, bases de datos, redes), la **implementación de cifrado en tránsito y en reposo** para proteger la confidencialidad de los datos, la **segmentación de la red y el uso de firewalls virtuales** para controlar el tráfico, la **monitorización y el registro centralizado de eventos de seguridad** para la detección temprana de incidentes, y la **implementación de mecanismos de respuesta a incidentes** específicos para la nube.

Dada la preferencia del Ministerio por soluciones agnósticas a la marca, las herramientas de seguridad seleccionadas deberían, en la medida de lo posible, ser **servicios nativos de la nube configurables de manera segura o herramientas de terceros interoperables**, evitando la dependencia de tecnologías propietarias que dificulten la portabilidad entre proveedores cloud. La **evaluación particular de cada solución** debe incluir un análisis exhaustivo de los riesgos de seguridad específicos del entorno cloud y la aplicación, alineándose con las directrices detalladas en "Política de Seguridad para Entornos de Nube Pública" del Ministerio de Salud.

f.- **Herramientas de Desarrollo y Gestión:** Estas incluyen herramientas para la construcción, depuración, prueba y administración de aplicaciones.

La elección de las tecnologías adecuadas debe basarse en factores como los requisitos del proyecto, las restricciones técnicas y las metas de escalabilidad y seguridad. Las tecnologías seleccionadas influyen significativamente en la eficiencia y el éxito del desarrollo y la implementación de soluciones basadas en la arquitectura de referencia.

Existe una lista de herramientas actuales en el stack tecnológico del Ministerio donde se incluyen tecnologías recomendadas para encolamiento, servidores de aplicaciones, registro de eventos, servidores web, entre otros. Para tener el listado completo consulte la guía de Implementación de SW.

4.- MARCOS DE TRABAJO Y LINEAMIENTOS PARA DISEÑO DE ARQUITECTURA DE SOLUCIONES

El conjunto estructurado de enfoques, principios y directrices que guían el proceso de diseño y construcción de soluciones tecnológicas proporcionan un conjunto de mejores prácticas y pautas para asegurar que las soluciones sean efectivas, escalables, seguras y alineadas con los objetivos del proyecto y las necesidades del cliente. Los aspectos importantes que se deben incluir son los siguientes:

4.1.- Principios Arquitectónicos

Los Principios Arquitectónicos son fundamentos y pautas que orientan el diseño de la arquitectura de soluciones tecnológicas. Deberán estar presentes para tomar decisiones de diseño que aseguren la creación de sistemas eficaces, flexibles y sostenibles a lo largo del tiempo. Los principales Principios Arquitectónicos que se deben considerar:

a.- **Modularidad**: Este principio promueve la división del sistema en módulos independientes y autónomos. Cada módulo se encarga de una funcionalidad específica y puede ser desarrollado, probado y mantenido de manera independiente. La modularidad facilita la escalabilidad, el mantenimiento y la reutilización de componentes.

b.- **Reutilización:** Fomenta la creación de componentes y servicios que puedan ser utilizados en múltiples partes del sistema o incluso en diferentes proyectos. La reutilización reduce la duplicación de esfuerzos, acelera el desarrollo y mejora la consistencia y la calidad del código.

c.- **Separación de Responsabilidades:** Este principio aboga por la asignación clara de tareas y responsabilidades a diferentes componentes del sistema. Cada componente debe realizar una función específica y no debe tener un conocimiento profundo de las operaciones de otros componentes. Esto mejora la mantenibilidad y facilita los cambios y actualizaciones.

d.- **Escalabilidad:** La arquitectura debe ser capaz de crecer en respuesta a la demanda sin comprometer el rendimiento. Los sistemas deben poder escalar horizontalmente (agregando más instancias del mismo componente) o verticalmente (mejorando los recursos de un componente existente).

e.- **Desacoplamiento:** Los componentes del sistema deben tener la menor dependencia posible entre sí. Esto permite cambios en uno sin afectar a otros, lo que mejora la flexibilidad y facilita la evolución y la colaboración entre equipos de desarrollo.

f.- **Abstracción:** Fomenta la creación de interfaces que oculten los detalles internos y presenten solo la funcionalidad esencial. Las abstracciones permiten cambios internos sin afectar a los usuarios o a otros componentes.

g.- **Coherencia y Consistencia**: Se busca mantener una estructura coherente y una lógica consistente en todo el sistema. La consistencia facilita la comprensión y reduce la complejidad.

h.- **Flexibilidad:** La arquitectura debe ser flexible para adaptarse a cambios en los requisitos y tecnologías. La flexibilidad se logra mediante el uso de patrones de diseño que permiten cambios graduales y extensiones sin rehacer toda la arquitectura.

i.- **Eficiencia:** Los principios arquitectónicos deben contribuir a la eficiencia del sistema en términos de recursos de hardware, rendimiento y consumo energético.

j.- **Seguridad:** La seguridad debe ser un principio fundamental, asegurando que los componentes y las comunicaciones estén protegidos contra amenazas y vulnerabilidades.

Estos Principios Arquitectónicos proporcionan una base sólida para la toma de decisiones en el diseño de la arquitectura de soluciones, asegurando que el sistema sea robusto, flexible y capaz de adaptarse a los cambios y desafíos tecnológicos en curso.

4.2.- Patrones de Diseño

Los Patrones de Diseño son soluciones probadas y documentadas para problemas recurrentes en el diseño de software y sistemas. Estos patrones representan soluciones a nivel de diseño que han demostrado ser efectivas para abordar desafíos comunes en el desarrollo de aplicaciones. Los Patrones de Diseño ofrecen un lenguaje común y una guía para los desarrolladores, permitiéndoles aprovechar soluciones exitosas y estandarizadas en sus proyectos.

Si bien existen distintos tipos de patrones, se deberá ajustar el uso de patrones a la solución requerida, manteniendo la simpleza y la estandarización como premisa.

Se recomienda fuertemente utilizar el tipo de patrón adecuado y deberá ser justificado el uso en cada caso.

4.3.- Metodologías de Desarrollo

Las Metodologías de Desarrollo son enfoques sistemáticos y estructurados utilizados para planificar, diseñar, construir, probar y entregar software y sistemas. Estas metodologías proporcionan un marco de trabajo para organizar y gestionar el proceso de desarrollo de manera eficiente y efectiva.

Si bien existen diferentes metodologías concernientes al desarrollo, se busca desde un punto de vista arquitectónico, ajustar a las necesidades del desarrollo requerido, en palabras sencillas, no es necesario realizar infinitas iteraciones para un mantenedor de datos, por lo que la recomendación siempre será ajustar a la naturaleza de lo que se busca solucionar.

4.4.- Lineamientos de Seguridad

Los Lineamientos de Seguridad son un conjunto de principios, reglas y pautas diseñados para establecer una base sólida de ciberseguridad que garantice la protección de los activos y datos del Ministerio, así como para mitigar los riesgos de seguridad cibernética y mantener la integridad, confidencialidad y disponibilidad de la información. Para fortalecer la postura de ciberseguridad del sector salud, es **imperativo** que cada Institución y Establecimientos de Salud implementen un **Modelo de Seguridad por Capas.** Este enfoque integral, escalable y estructurado es fundamental para la protección robusta de la información sensible, los sistemas críticos que soportan la operación y la infraestructura tecnológica subyacente, frente a la creciente sofisticación de las amenazas cibernéticas.

Este modelo debe fundamentarse en el principio de **seguridad y privacidad por defecto y desde el diseño,** establecido en la Ley 21.663 sobre le Marco de Ciberseguridad, lo que implica que todos los sistemas informáticos, aplicaciones y tecnologías de la información deben concebirse, implementarse y gestionarse tomando como base la seguridad y la privacidad de los datos personales que procesan como pilares fundamentales desde su inicio. Al integrar la seguridad y la privacidad en cada etapa del ciclo de vida de los sistemas, se asegura una protección más robusta y proactiva, complementando así la estrategia de defensa en profundidad inherente al Modelo de Seguridad por Capas. A continuación, se detallan los aspectos clave de los Lineamientos de Seguridad establecidos en el modelo:

4.4.1.- Protección de Datos:

- **Confidencialidad:** Asegurar que la información solo esté disponible para personas autorizadas. Mediante controles de acceso basados en roles (RBAC - Role-Based Access Control) y atributos (ABAC- Attribute-Based Access Control), que la información solo sea accesible por usuarios y sistemas debidamente autenticados y autorizados. Esto se implementa a través de cifrado robusto (AES-256 o superior) en

DEPARTAMENTO TIC VISADO

reposo y en tránsito (TLS 1.2 o superior), minimización de datos y anonimización/seudonimización cuando sea apropiado.

- **Integridad:** Garantizar que los datos no sean alterados por personas no autorizadas y que los cambios sean registrados y rastreados. Utilizando mecanismos de control de versiones, sumas de verificación (checksums) y firmas digitales. Técnicamente, se deben implementar registros de auditoría (logs) detallados e inmutables para rastrear cualquier modificación, así como validaciones de entrada y controles de integridad referencial a nivel de base de datos y aplicación.
- **Disponibilidad:** Asegurar que los datos y sistemas estén disponibles cuando sean necesarios. Mediante arquitecturas resilientes y tolerantes a fallos, incluyendo redundancia de componentes, balanceo de carga y mecanismos de conmutación por error (failover). Se deben implementar estrategias de backup y restauración periódicas y probadas, así como planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP).

4.4.2.- Control de Acceso:

- **Autenticación:** Verificar la identidad de los usuarios antes de otorgar acceso a sistemas y datos. Utilizando mecanismos robustos como autenticación multifactor (MFA), uso de contraseñas complejas y políticas de rotación, e idealmente, autenticación basada en certificados o biometría. Técnicamente, se deben implementar protocolos seguros como OAuth 2.0 y SAML 2.0 para la autenticación y federación de identidades.
- **Autorización:** Definir qué recursos y datos pueden acceder los usuarios autorizados, mediante la implementación de listas de control de acceso (ACLs), RBAC y ABAC, aplicadas consistentemente en la capa de aplicación y la infraestructura.
- **Auditoría:** Registrar las actividades de los usuarios y eventos del sistema para su posterior revisión. Se deben utilizar herramientas de gestión de logs (SIEM) para el análisis, correlación y alerta de eventos sospechosos.

4.4.3.- Gestión de Riesgos:

- **Evaluación de Riesgos:** Identificar y evaluar amenazas y vulnerabilidades para determinar los riesgos potenciales. Se deben realizar pruebas de penetración (pentesting) periódicas, análisis de vulnerabilidades automatizados, y revisiones de seguridad del código fuente (SAST/DAST).
- **Mitigación de Riesgos:** Implementar medidas de seguridad para reducir los riesgos a un nivel aceptable. Esto debe Incluir la implementación de sistemas de prevención de intrusiones (IPS), firewalls de última generación (NGFW), herramientas de detección y respuesta de endpoints (EDR), y la aplicación de parches de seguridad de manera oportuna.

DEPARTAMENTO VISADO

4.4.4.- Seguridad en la Infraestructura:

- **Firewalls:** Filtrar el tráfico de red para prevenir accesos no autorizados. Implementar firewalls perimetrales e internos con reglas estrictas de filtrado de tráfico basadas en el principio de mínimo privilegio para controlar el acceso a la red y entre segmentos. Se deben configurar listas blancas (whitelisting) y listas negras (blacklisting) de direcciones IP y puertos, así como inspección profunda de paquetes (DPI).
- **Antivirus y Antimalware:** Proteger contra amenazas de software malicioso. Implementar soluciones antivirus y antimalware actualizadas en todos los endpoints y servidores para detectar, prevenir y eliminar software malicioso. Técnicamente, se deben configurar análisis en tiempo real y programados, así como actualizaciones automáticas de firmas.
- **Actualizaciones y Parches:** Establecer un proceso robusto de gestión de parches para identificar, probar e implementar las actualizaciones de seguridad para todos los sistemas operativos, aplicaciones y librerías de manera oportuna, minimizando la ventana de exposición a vulnerabilidades conocidas. Se recomienda utilizar herramientas de gestión de parches automatizadas.

4.4.5.- Criptografía:

- **Cifrado:** Proteger los datos mediante la conversión en un formato ilegible, que solo puede ser descifrado por usuarios autorizados. Aplicar algoritmos de cifrado fuertes y estándares de la industria (AES-256 para datos en reposo, TLS 1.2 o superior para datos en tránsito) para proteger la confidencialidad de la información sensible almacenada y transmitida. Además de implementar una gestión de claves criptográficas segura.
- **Firmas Digitales:** Verificar la autenticidad de los datos y garantizan que no hayan sido alterados. A través de la utilización de firmas digitales basadas en criptografía de clave pública para verificar la autenticidad e integridad de los datos, asegurando el no repudio, como el uso de certificados digitales válidos y confiables.

4.4.6.- Gestión de Incidentes de Seguridad:

- **Preparación:** Establecer planes de respuesta a incidentes (IRP) para responder a incidentes de seguridad, incluyendo la atribución de roles y responsabilidades, procedimientos de comunicación y pasos de contención, erradicación y recuperación.
- **Detección:** Monitorear sistemas y redes para identificar posibles incidentes. Implementar mecanismos de monitoreo continuo de seguridad (SIEM, IDS/IPS, EDR) para identificar actividades anómalas y posibles incidentes en tiempo real.
- **Respuesta:** Actuar de manera coordinada para mitigar el impacto de los incidentes y recuperar la normalidad. Ejecutar los planes de respuesta a incidentes de manera coordinada y eficiente para contener la amenaza, erradicar la causa raíz, recuperar

los sistemas afectados y aprender de la experiencia para mejorar los controles de seguridad. Utilizar herramientas forenses y de análisis de malware cuando sea necesario.

4.4.7.- Sensibilización y Formación:

- **Conciencia en Seguridad:** Entregar información y educar a los empleados sobre las mejores prácticas de seguridad y la importancia de proteger la información deberá ser parte del proceso. Se debe implementar un programa continuo de concienciación en seguridad para educar a todos los funcionarios sobre las mejores prácticas de seguridad, riesgos cibernéticos comunes (phishing, malware, ingeniería social) y sus responsabilidades en la protección de la información. Se pueden utilizar plataformas de aprendizaje en línea y simulaciones de ataques.

4.4.8.- Cumplimiento Normativo:

- **Regulaciones:** Cumplir con leyes y regulaciones de seguridad cibernética y privacidad de datos aplicables. A través de la implementación de controles específicos para cumplir con normativas tales como la Ley de Protección de Datos Personales, Ley Marco de Ciberseguridad, Ley de Derechos y Deberes de los Pacientes, entre otras.

La implementación de Lineamientos de Seguridad es esencial para prevenir ataques cibernéticos, filtraciones de datos y otras amenazas a la seguridad de la información. Los que son esenciales para construir soluciones resilientes y proteger los activos de información del Ministerio y del Sector Salud contra las crecientes y sofisticadas amenazas cibernéticas. Estos lineamientos deben ser **adaptados y detallados específicamente para cada solución construida**, considerando su contexto y riesgos particulares.

4.5.- Lineamientos de Cumplimiento

Los Lineamientos de Cumplimiento son un conjunto de directrices y reglas establecidas por el Ministerio para asegurar que sus operaciones, procesos y actividades cumplan con regulaciones, leyes, estándares de la industria y políticas internas relevantes. Estos lineamientos están diseñados para garantizar que el Ministerio opere de manera ética, legal y en conformidad con los requisitos establecidos. Se deberá poner particular atención a:

4.5.1.- Regulaciones y Normativas:

- **Cumplimiento Legal:** Asegurar que la organización cumpla con las leyes y regulaciones aplicables al sector salud y gobierno además de las regulaciones existentes en el territorio nacional y en el País donde se aloje la infraestructura (cloud).
- **Normativas de la Industria:** Se refiere a los estándares y regulaciones específicos del sector salud.

4.5.2.- Políticas Internas:

- **Políticas de la Organización:** Establecer las normas internas y expectativas en áreas como el uso de tecnología, la seguridad de la información y el comportamiento ético.
- **Políticas de Privacidad:** Definir cómo se manejan y protegen los datos personales de pacientes, empleados y otros.

4.5.3.- Protección de Datos:

- **Privacidad de Datos:** Establecer cómo se recopilan, almacenan y utilizan los datos personales de los individuos, en cumplimiento con regulaciones como el Reglamento General de Protección de Datos.

4.5.4.- Seguridad de la Información:

- **Gestión de Riesgos de Seguridad:** Asegurar que se implementen medidas de seguridad adecuadas para proteger la información sensible y prevenir brechas de seguridad.

4.5.5.- Informes y Auditorías:

- **Documentación:** Mantener registros y documentación que demuestren el cumplimiento de las regulaciones y políticas.
- **Auditorías Internas y Externas:** Permitir evaluar y verificar el cumplimiento y la efectividad de las medidas de cumplimiento.

4.5.6.- Adaptación y Actualización:

- **Cambio en Regulaciones:** Los Lineamientos de Cumplimiento deben ser revisados durante el periodo de construcción de cualquier solución, permitiendo estar al día con el cumplimiento de cada hito.

Los Lineamientos de Cumplimiento son esenciales para garantizar que el Ministerio opere de manera ética y legal, manteniendo la confianza de los usuarios, los empleados y las partes interesadas. Además de cumplir con las regulaciones y normativas, estos lineamientos pueden contribuir a una mayor eficiencia, seguridad y calidad en las operaciones.

4.6.- Lineamientos de Rendimiento

Los Lineamientos de Rendimiento son un conjunto de pautas y directrices establecidas para garantizar el rendimiento óptimo de los sistemas, aplicaciones y procesos del Ministerio. Estos lineamientos se enfocan en maximizar la eficiencia, la velocidad y la capacidad de respuesta de los sistemas tecnológicos, garantizando una experiencia satisfactoria para los usuarios y minimizando la carga en los recursos tecnológicos. Se deberá tener en cuenta lo siguiente:

4.6.1.- Establecimiento de Objetivos:

Definir metas de rendimiento específicas para los sistemas y aplicaciones, como tiempos de respuesta, velocidad de procesamiento y capacidad de usuarios concurrentes.

4.6.2.- Diseño Eficiente:

Desarrollar sistemas y aplicaciones utilizando principios de diseño que minimicen la sobrecarga y optimicen los recursos, como la minimización de consultas de bases de datos y la reducción de llamadas de red.

4.6.3.- Optimización de Código:

Identificar áreas de código que puedan ralentizar el rendimiento y optimiza los algoritmos y procesos para lograr ejecuciones más rápidas.

4.6.4.- Gestión de Carga:

Implementar estrategias para manejar momentos de alta demanda, como la escalabilidad automática en la nube o la distribución de la carga de trabajo en servidores.

4.6.5.- Monitorización y Análisis:

Supervisar constantemente el rendimiento de los sistemas y las aplicaciones para identificar cuellos de botella y puntos problemáticos.

4.6.6.- Ajuste y Optimización Continua:

Realizar ajustes regulares en función de los datos de monitorización y las pruebas de rendimiento para mantener y mejorar el rendimiento con el tiempo.

4.6.7.- Almacenamiento y Memoria:

Optimizar el uso de recursos de almacenamiento y memoria para minimizar la latencia y mejorar el rendimiento de lectura y escritura.

4.6.8.- Redes y Comunicación:

Minimizar la latencia y mejora el rendimiento de las comunicaciones utilizando técnicas como la compresión de datos y la caché de contenidos.

4.6.9.- Tiempos de Respuesta:

Se debe asegurar que los sistemas y las aplicaciones respondan a las solicitudes de los usuarios en un tiempo aceptable, mejorando la satisfacción del usuario.

4.6.10.- Pruebas de Rendimiento:

Realizar pruebas rigurosas para evaluar el rendimiento en diferentes escenarios, como cargas de trabajo pesadas y picos de demanda.

4.6.11.- Optimización de Base de Datos:

Se debe asegurar que las bases de datos estén optimizadas para consultas rápidas y eficientes, mediante índices y optimización de consultas.

Los Lineamientos de Rendimiento son esenciales para garantizar que los sistemas tecnológicos sean capaces de manejar las demandas actuales y futuras del Ministerio y los usuarios. Un rendimiento eficiente no solo mejora la experiencia del usuario, sino que también puede ahorrar costos al reducir la necesidad de hardware adicional y tiempos de inactividad.

4.7.- Lineamientos de Integración

Los Lineamientos de Integración son un conjunto de directrices y mejores prácticas diseñadas para facilitar la conexión y la interoperabilidad efectiva entre sistemas, aplicaciones y componentes del Ministerio. Estos lineamientos aseguran que los diferentes elementos tecnológicos puedan trabajar juntos de manera fluida, lo que permite compartir datos y funcionalidades de manera eficiente y coherente. Se deberá tener en consideración lo siguiente:

4.7.1.- Estandarización:

Establecer y ajustarse a los estándares y protocolos para la comunicación y el intercambio de datos entre sistemas, asegurando que todos los componentes sigan un enfoque coherente.

4.7.2.- Interfaces Claras:

Definir interfaces bien documentadas y robustas que especifican cómo los sistemas interactúan entre sí.

4.7.3.- APIs y Servicios Web:

Utilizar APIs y servicios web para permitir la comunicación y la integración entre sistemas heterogéneos.

4.7.4.- Formatos de Datos:

Establecer formatos de datos estándar para asegurar que la información se pueda intercambiar y comprender de manera consistente.

4.7.5.- Middleware:

Utilizar el middleware proporcionado para simplificar la comunicación entre aplicaciones, como sistemas de mensajería y buses de servicios.

4.7.6.- Integración en Tiempo Real:

Permitir la integración de datos y procesos en tiempo real, asegurando que la información esté actualizada y precisa en todos los sistemas.

4.7.7.- Automatización:

Utilizar herramientas y soluciones de automatización aprobadas por TIC para facilitar la configuración y la gestión de la integración entre sistemas.

4.7.8.- Gestión de Identidad:

Se debe asegurar que los sistemas puedan compartir y verificar la identidad de los usuarios de manera segura, mediante soluciones de autenticación y autorización.

4.7.9.- Sincronización y Migración de Datos:

Definir procesos y estrategias para sincronizar y migrar datos entre sistemas, manteniendo la coherencia, la integridad y ajustándose a los estándares definidos.

4.7.10.- Pruebas de Integración:

Realizar pruebas rigurosas para garantizar que la integración entre sistemas funcione según lo previsto y que los datos se transfieran correctamente.

4.7.11.- Monitorización y Mantenimiento:

Supervisar constantemente la salud y el rendimiento de las integraciones, incluyendo health checks para identificar problemas y realizar ajustes cuando sea necesario.

Los Lineamientos de Integración son fundamentales para garantizar que los sistemas y aplicaciones del Ministerio puedan colaborar de manera efectiva y que los datos puedan moverse sin problemas entre diferentes componentes.

4.8.- Consideraciones de Infraestructura

Las consideraciones de infraestructura son factores clave que deben tenerse en cuenta al diseñar, implementar y mantener la base tecnológica del Ministerio. Estas consideraciones son esenciales para asegurarse de que los sistemas, aplicaciones y recursos tecnológicos funcionen de manera eficiente, segura y confiable. Se deberá considerar los siguiente:

4.8.1.- Escalabilidad:

Diseñar las soluciones para poder crecer o reducirse según las demandas cambiantes de la organización.

4.8.2.- Rendimiento:

Optimizar la solución para ofrecer un rendimiento adecuado, asegurando que los recursos sean aprovechados de la mejor manera posible.

4.8.3.- Seguridad:

No modificar innecesariamente las medidas de seguridad existentes en la infraestructura. Se deberá proteger los activos y datos de la organización contra amenazas cibernéticas y acceso no autorizado.

DEPARTAMENTO TIC VISADO

4.8.4.- Cumplimiento:

Asegurar que se cumpla con las regulaciones que el área de infraestructura provea.

4.8.5.- Almacenamiento:

Diseñar una estrategia de almacenamiento que permita un acceso rápido y seguro a los datos, al mismo tiempo que garantiza su respaldo y recuperación.

4.8.6.- Redes:

Diseñar el intercambio de información para que se ajuste a los requerimientos de red definidos, así como a los protocolos establecidos.

Estas consideraciones de infraestructura son esenciales para asegurarse de que la base tecnológica del Ministerio sea robusta, segura y capaz de cumplir con los objetivos y las necesidades del negocio.

4.9.- Evaluación de Tecnologías

La evaluación de tecnologías es un proceso crítico que implica analizar y comparar diferentes soluciones tecnológicas para determinar cuál es la más adecuada para satisfacer las necesidades y los objetivos del Ministerio. Esta evaluación puede aplicarse a hardware, software, herramientas, plataformas y otros componentes tecnológicos. En este apartado se revisará particularmente lo relativo a software:

4.9.1. Identificación de Requisitos:

Comprender claramente los requisitos y las necesidades de la solución para determinar qué características y funcionalidades son esenciales en la tecnología a evaluar.

4.9.2. Consideraciones de Costos:

Evaluar los costos asociados con la adquisición, implementación, capacitación y mantenimiento de la tecnología a lo largo de su ciclo de vida, considerando licencias y demás.

4.9.3. Evaluación de Riesgos:

Evaluar los riesgos potenciales asociados con la tecnología, como problemas de seguridad, falta de soporte o dificultades de integración.

4.9.4. Demos y Presentaciones:

Generar demos y presentaciones de la tecnología que se quiere incluir para obtener una comprensión más profunda de cómo se adapta a las necesidades.

4.9.5. Análisis de Costo-Beneficio:

Evaluar los beneficios potenciales en relación con los costos y los riesgos. Esto implica considerar el impacto positivo en el negocio y requerimientos adicionales.

Si bien es posible incorporar el uso de nuevas tecnologías al stack tecnológico del Ministerio, se deberá justificar el uso de cualquiera que no se encuentre ya definido previamente.

5.- RECOMENDACIONES PARA LA ACTUALIZACIÓN DEL DOCUMENTO

5.1.- Evaluación de Nuevas Tecnologías

Regularmente, evaluar nuevas tecnologías y soluciones emergentes para determinar si se alinean con la visión y los objetivos del Ministerio, y si pueden aportar valor a la arquitectura existente.

5.2.- Retroalimentación de Usuarios

Recoger comentarios y retroalimentación de los usuarios y partes interesadas sobre el rendimiento y la eficacia de la arquitectura actual. Esto puede ayudar a identificar áreas que necesitan mejoras.

5.3.- Revisión de Requisitos

Actualizar los requisitos de negocio y tecnológicos para asegurar que la arquitectura esté alineada con los cambios en la estrategia y las necesidades de la organización.

5.3.1.- Adaptación a Cambios en el Negocio

Ajustar la arquitectura para reflejar cambios en la estructura organizativa, nuevos productos o servicios, y cambios en la dirección estratégica.

5.3.2.- Actualización de Estándares y Lineamientos

Revisar y actualizar los estándares y lineamientos para reflejar las mejores prácticas actuales y garantizar la coherencia en el diseño y la implementación de soluciones.

5.3.3.- Revisión por Pares y Auditorías

Realizar revisiones por pares y auditorías periódicas para garantizar la calidad y la efectividad de los ajustes realizados.

6.- REFERENCIAS

Referencia / Estándar	Descripción	Aplicación
ISO/IEC 42010	Define principios y estructuras para describir arquitecturas de sistemas.	Base para documentar arquitecturas de forma estandarizada.
TOGAF (The Open Group Architecture Framework)	Marco para desarrollar arquitecturas empresariales alineadas al negocio.	Arquitectura de referencia institucional, interoperabilidad y alineamiento estratégico.
Archimate (Open Group)	Lenguaje de modelado para representar arquitecturas.	Visualización de relaciones entre componentes tecnológicos, aplicaciones y procesos.
COBIT Framework	Gobernanza y gestión de TI alineada con los objetivos de la organización.	Control y trazabilidad de decisiones arquitectónicas y cumplimiento normativo.
NIST SP 800-160 Vol. 1 y 2	Ingeniería de sistemas seguros; integra ciberseguridad desde el diseño.	Diseño seguro de infraestructuras críticas
AWS / Azure / GCP Well-Architected Framework	Buenas prácticas para arquitecturas en la nube.	Evaluación y mejora continua de arquitecturas cloud
ISO/IEC 25010	Modelo de calidad de productos de software.	Evaluación de atributos como seguridad, mantenibilidad, eficiencia.
ISO/IEC/IEEE 42030	Evaluación formal de arquitecturas.	Análisis estructurado de riesgos, cumplimiento y desempeño.
HL7 / FHIR	Estándares de interoperabilidad clínica y de salud.	Integración entre sistemas clínicos