LINEAMIENTO TECNICO PARA LA OPERACIÓN DEL RESUMEN DIGITAL DE ATENCION EN SALUD

MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL

Versión 1.0
Bogotá, octubre 31 de 2023

TABLA DE CONTENIDO

1. PROPÓSITO

Presentar las directrices sobre la operación de la interoperabilidad de datos de la historia clínica y el Resumen Digital de Atención en Salud relacionados con la arquitectura TI, el mecanismo de conexión segura y el mecanismo de autenticación y acceso al mecanismo de interoperabilidad de la IHCE.

2. ALCANCE

Apoyar a las secretarias de salud del orden departamental y distrital para realizar la operación del RDA e implementar el Resumen Digital de Atención en Salud en los prestadores de servicios de salud en su territorio. Para el efecto, la arquitectura tecnológica dispuesta por el Ministerio de Salud y Protección Social para la interoperabilidad de la historia clínica electrónica - IHCE incluye los siguientes componentes:

- Enviar RDA
- Consultar RDA
- Obtener RDA

Este lineamiento debe sirva como lineamiento para que las secretarias de salud y las instituciones prestadoras de servicios de salud, desarrollen las acciones necesarias para integrarse al mecanismo de interoperabilidad nacional.

3. DOCUMENTOS DEL SIGI ASOCIADOS

Ninguno

4. DEFINICIONES (SI APLICA)

IHCE: Interoperabilidad de Historia Clínica Electrónica
IPS: Instituciones Prestadoras de Servicios de Salud
RDA: Resumen Digital de Atención
VPN: Red privada virtual.
MSPS: Ministerio de Salud y Protección Social
API: Interfaz de programación de aplicaciones, es un conjunto de reglas y protocolos que permite que diferentes componentes de software se comuniquen entre sí.
API Gateway: Es un componente en la arquitectura de software que actúa como intermediario entre las aplicaciones clientes y los servicios backend, permitiendo la gestión centralizada, la seguridad, el enrutamiento y otros aspectos relacionados con las API.
API Key: Es una clave de acceso que se le entrega a los prestadores de salud para que se puedan autenticar a la plataforma tecnológica de IHCE.
Firewall: Es una herramienta de seguridad informática diseñada para proteger una red de servidores y/o estaciones de trabajo o un sistema de información al controlar y filtrar el tráfico de red entrante y saliente.

5. INTRODUCCION

El presente documento ha sido realizado con el fin de especificar los detalles tecnológicos para la operación territorial de la IHCE, con el objeto de apoyar a las entidades territoriales y las instituciones prestadoras de salud, en el desarrollo de los componentes que van a hacer parte de Interoperabilidad de la Historia Clínica Electrónica - IHCE.

6. ARQUITECTURA TECNOLOGICA - IHCE

El modelo de integración al mecanismo de interoperabilidad de IHCE requiere que los prestadores de servicios de salud incorporen el Resumen Digital de Atención en Salud como formato de intercambio, el cual es sujeto a la operación que se debe realizar, así: enviar, consultar y obtener:

- Enviar RDA

  El proceso realizado es el siguiente:

  1. La institución envía el RDA (Resumen Digital de Atención en Salud) de la persona a través de la secretaria de salud departamental o distrital, a través de la URL https://ihce.ihcecol.gov.co
  2. El documento RDA llega a la plataforma tecnológica del IHCE del MSPS a través del dispositivo de seguridad perimetral – Firewall.
  3. En la plataforma el documento RDA es recibido por el componente API Gateway, quien valida el API Key y lo redirecciona a la secretaria de salud departamental o distrital correspondiente.
  4. Se realizan validaciones del RDA como la construcción de la estructura, los datos del paciente, la información del profesional de salud y del prestador de servicios de salud.
  5. Si el RDA no pasa la validación de estructura y/o datos del paciente, el documento es rechazado. El prestador de servicios de salud debe ajustarlo y volverlo a enviar.
  6. Si la validación del RDA es exitoso, realiza la creación en el repositorio correspondiente. Al prestador de servicios de salud le envían un mensaje con la operación realizada, el número de la transacción y fecha.
  7. Una vez creado el RDA se realiza la indexación en la infraestructura datos nacional para que pueda ser consultado por la secretaria de salud departamental o distrital y los prestadores de servicios de salud.

- Consultar RDA

  El proceso realizado es el siguiente:

  1. La institución realiza la consulta de los RDA existentes para un paciente a través a través de la URL https://ihce.ihcecol.gov.co.
  2. La solicitud de consulta del RDA llega a la plataforma tecnológica del IHCE del MSPS a través del dispositivo de seguridad perimetral – Firewall.

3. En la plataforma la consulta del RDA es recibida por el componente API Gateway, quien valida el API Key y lo redirecciona a la infraestructura de datos nacional.
4. La infraestructura de datos nacional le remite al prestador de servicios de salud las referencias de los RDA con la información del paciente y le permite seleccionarlos para obtener la información.

- Obtener RDA

  El proceso realizado es el siguiente:

  1. El prestador debe seleccionar la referencia del RDA que requiere visualizar. Solo permite verlos.
  2. Con esta información, el prestador tiene acceso a los diferentes RDA del paciente que se encuentren en la infraestructura de datos nacional.

Los componentes anteriormente mencionados, están configurados en la infraestructura tecnológica de IHCE dispuesta por el MSPS, para ser accedidos por los prestadores de servicios de salud, esta se encuentra compuesta así:

- Infraestructura Seguridad perimetral

  Hace referencia a las medidas de seguridad y estrategias implementadas para proteger la infraestructura tecnológica y las aplicaciones desplegadas de amenazas externas, en ese orden de ideas, se tiene implementado los siguientes componentes:

  - Firewall

    Solución implementada en alta disponibilidad para proteger la plataforma de interoperabilidad y los datos de IHCE, empleando reglas y políticas de seguridad, basándose en criterios como direcciones IP, puertos, protocolos y contenido.

  - WAF (Web Applications Firewall)

    Solución implementada en alta disponibilidad para detectar y prevenir ataques dirigidos a vulnerabilidades específicas que pueda tener la plataforma de interoperabilidad – IHCE, como inyecciones SQL, cross-site scripting (XSS), cross-site request forgery (CSRF) y otros tipos de ataques.

  - Balanceador de Cargas

    Solución implementada en alta disponibilidad para distribuir el tráfico de red de forma equitativa entre los servidores de la plataforma de interoperabilidad IHCE, para mejorar la eficiencia, la disponibilidad y el rendimiento del sistema de información.

- Infraestructura TI Servidores

  Hace referencia al conjunto de hardware, software, redes y recursos para instalar, configurar y desplegar la plataforma de interoperabilidad – IHCE, teniendo en cuenta su evolución continua. El Ministerio de Salud y Protección Social dispuso de tres (3) ambientes distribuidos así: desarrollo, preproducción y producción,

  A continuación, se brinda una descripción de los componentes tecnológicos dispuestos por el MSPS para el despliegue y puesta en producción de la plataforma IHCE

  - API Gateway

    Componente en la arquitectura de software que actúa como intermediario entre las peticiones realizadas a través de las secretarias de salud y la infraestructura TI del Ministerio de Salud y Protección Social.

    Cuando una solicitud es realizada por la secretaría de salud, esta es recibida por el API Gateway y a través del API Key es direccionada a la secretaria de salud correspondiente.

  - Almacenamiento RDA

    Dentro de la arquitectura TI implementada por el Ministerio de Salud y Protección Social, las solicitudes realizadas por el prestador de servicios a través de la secretaria de salud tendrán dentro de la infraestructura de datos nacional un repositorio de cada territorio exclusivo para la recepción y gestión de las solicitudes. La identificación se realiza a través del API Key. Tiene los siguientes componentes:

    - Componente territorial

      Servicio encargado de procesar la entrada del RDA, realiza validaciones y acciones que permiten distribuir los datos de un RDA en múltiples servidores.

    - FHIR

      Servicio encargado de almacenar los recursos FHIR relacionados a RDA, diagnósticos, medicamentos y el contexto de estos.

  - Infraestructura nacional

    Es implementada y administrada por el Ministerio de Salud y Protección Social, dispone de los componentes necesarios que el mecanismo de interoperabilidad requiere para realizar los procesos de recepción, validación e identificación de los RDA, este nodo está compuesto por:

    - Paciente FHIR

Servicio encargado de almacenar la información relacionada de los pacientes obtenida de cada RDA.

- Almacenamiento FHIR

  Servicio encargado de almacenar los documentos que permitan saber la ubicación de la información de cada RDA, departamento y paciente, además, se encarga del almacenamiento de profesionales, organizaciones (Departamentos) y organizaciones (Prestadores).

- Validador FHIR

  Servicio encargado de validar la estructura de los recursos relacionados al RDA, utilizando los perfiles construidos para cada recurso.

- Validador fuentes de información nacional

  Servicio encargado de realizar operaciones con servicios externos como: Tabla Evolución, RETHUS y REPS. Adicionalmente, valida la existencia de pacientes, profesional de salud y el prestador de servicios de salud.

  Otra tarea relacionada es el almacenamiento de los registros de Logs de las operaciones que presenten errores.

- Terminológico

  Servicio encargado de disponer información de las terminologías como IUM y CIE-10.

- Fuentes de información nacional

  Son fuentes de datos que dispone el Ministerio de Salud y Protección Social para validar información registrada en el RDA, estas fuentes son:

  - Tabla Evolución

    Fuente de información del paciente, el cual se emplea en la validación del RDA, esto con el fin de revisar la existencia del paciente que recibe el registro de atención.

  - RETHUS

    Fuente de información del profesional de la salud, esto con el objetivo de revisar la existencia y el estado del profesional que realiza el registro de atención al paciente.

- REPS

  Fuente de información de la entidad prestadora de salud, esto con el fin de revisar el estado del prestador donde se realiza el registro de atención al paciente.

7. ARQUITECTURA TERRITORIAL

Dentro del modelo de integración al mecanismo de interoperabilidad de IHCE, para que los prestadores de servicios de salud de los diferentes territorios a nivel nacional puedan enviar, consultar y/o obtener un RDA, lo deben realizar a través una secretaria de salud departamental o distrital y este realiza el envío de la solicitud al Ministerio de Salud y Protección Social, para esto, dentro de su arquitectura tecnológica debe tener como mínimo los siguientes componentes:

- Territorio

  Conectividad hacia el Ministerio de Salud y Protección Social a través de los siguientes mecanismos:

  - Mecanismo de Conexión VPN

    En la primera fase del proyecto este es el medio de conexión definido, esto, como medida de transitoriedad, mientras se finaliza la configuración de la plataforma tecnológica requerida para implementación del mecanismo de conexión X-Road

  - Mecanismo de Conexión X-Road

    En una siguiente fase y una vez las entidades cumplan satisfactoriamente los prerrequisitos necesarios para activar este mecanismo de conexión, se realizará migración correspondiente.

- Prestadores de servicios de salud

  Conectividad hacia la secretaría de salud a través de los siguientes mecanismos:

  - Mecanismo de Conexión VPN

    En la primera fase del proyecto este es el medio de conexión definido, esto, como medida de transitoriedad, mientras se finaliza la configuración de la plataforma tecnológica requerida para implementación del mecanismo de conexión X-Road

  - Mecanismo de Conexión X-Road

En una siguiente fase y una vez las entidades cumplan satisfactoriamente los prerrequisitos necesarios para activar este mecanismo de conexión, se realizará migración correspondiente.

Adicionalmente, deben desarrollar un sistema de información con los lineamientos definidos por el Ministerio de Salud y Protección Social que les permita:

- Conexión y autenticación al sistema de información web provisto por MSPS
- Enviar RDA
- Consultar RDA
- Obtener RDA

8. CONFIGURACIÓN Y CONEXIÓN SEGURA TERRITORIAL

En aras de establecer la conexión desde las instituciones prestadores de salud a los entes territoriales y, desde este al MSPS garantizando la integridad y confidencialidad de la información del RDA (Resumen Digital de Atención), se enuncian las siguientes recomendaciones:

- Mecanismo de Conexión X-Road

- Entidades Territoriales a MSPS

  Se debe realizar la implementación y configuración de la plataforma X-Road de acuerdo con los lineamientos brindados por MINTIC

  Una vez la entidad tenga configurado el nodo de X-Road se deberá conectar al nodo configurado en el MSPS para acceder a los servicios RDA.

- Instituciones Prestadoras de Salud a la secretaria de salud

  De acuerdo con la infraestructura tecnológica a nivel de seguridad perimetral que disponga la IPS, se emiten las recomendaciones.

  - Firewall: Establecer una conexión segura entre la infraestructura tecnológica de las dos entidades, a través de una VPN Site to Site (IPSec), con las siguientes configuraciones:

    - Negociación Fase I
      - Emplear como mínimo dos protocolos de encripción con cifrado AES128 y AES256.
      - Realizar la autenticación con un algoritmo mínimo SHA256.
      - Definir mínimo dos (2) grupos de autenticación que indican como descomprimir el tráfico.

    - Negociación Fase II

- Especificar direcciones IP específicas de origen y destino.
- Realizar la autenticación con un algoritmo mínimo SHA1

o Políticas de seguridad
- Definir horario de conexión para los usuarios
- Restringir el acceso solo desde la dirección IP autorizadas

- Cliente - Sitio: Cuando la entidad no cuenta con un equipo de seguridad perimetral (Firewall), se debe realizar la configuración con las siguientes características:

o Políticas de instalación mínima en las estaciones de trabajo (Antivirus)
o Implementar una VPN SSL
o Mecanismo de autenticación con usuario, contraseña y token
o Configurar el certificado de seguridad con un algoritmo mínimo SHA265
o Configurar un puerto TCP diferente al estándar
o Restringir el acceso solo desde la dirección IP y usuarios de red autorizadas
o Definir un horario de conexión para los usuarios.
o Definir los servicios que se van a acceder

➢ Mecanismo de Conexión VPN

- Entidades Territoriales a MSPS

Las secretarias de salud departamental o distrital para el establecimiento de la conexión con MSPS debe tener como mínimo un equipo de seguridad perimetral (Firewall) robusto que permita configurar las dos fases de negociación para establecer una comunicación segura.

Establecer una conexión segura entre la infraestructura tecnológica de las dos entidades, a través de una VPN Site to Site (IPSec), con las siguientes configuraciones:

- Negociación Fase I
o Emplear como mínimo dos protocolos de encripción con cifrado AES128 y AES256.
o Realizar la autenticación con un algoritmo mínimo SHA256.
o Definir mínimo dos (2) grupos de autenticación que indican como descomprimir el tráfico.

- Negociación Fase II
o Especificar direcciones IP específicas de origen y destino.
o Realizar la autenticación con un algoritmo mínimo SHA1

- Políticas de seguridad
o Definir horario de conexión para los usuarios
o Restringir el acceso solo desde la dirección IP autorizadas

- Instituciones Prestadoras de Servicios de Salud a l Nodo Territorial

  De acuerdo con la infraestructura tecnológica a nivel de seguridad perimetral que disponga la IPS, se emiten las recomendaciones.

  - Firewall: Establecer una conexión segura entre la infraestructura tecnológica de las dos entidades, a través de una VPN Site to Site (IPSec), con las siguientes configuraciones:

    - Negociación Fase I
      - Emplear como mínimo dos protocolos de encripción con cifrado AES128 y AES256.
      - Realizar la autenticación con un algoritmo mínimo SHA256.
      - Definir mínimo dos (2) grupos de autenticación que indican como descomprimir el tráfico.

    - Negociación Fase II
      - Especificar direcciones IP específicas de origen y destino. Realizar la autenticación con un algoritmo mínimo SHA1

    - Políticas de seguridad
      - Definir horario de conexión para los usuarios
      - Restringir el acceso solo desde la dirección IP autorizadas

  - Cliente - Sitio: Cuando la entidad no cuenta con un equipo de seguridad perimetral (Firewall), se debe realizar la configuración con las siguientes características:

    - Políticas de instalación mínima en las estaciones de trabajo (Antivirus)
    - Implementar una VPN SSL
    - Mecanismo de autenticación con usuario, contraseña y token
    - Configurar el certificado de seguridad con un algoritmo mínimo SHA265
    - Configurar un puerto TCP diferente al estándar
    - Restringir el acceso solo desde la dirección IP y usuarios de red autorizadas
    - Definir un horario de conexión para los usuarios.
    - Definir los servicios que se van a acceder

9. MECANISMO DE AUTENTICACION, ACCESO A LA PLATAFORMA Y PRUEBAS

Para garantizar el acceso a la plataforma tecnológica por parte de los prestadores de salud, se deben realizar las siguientes actividades:

- Configuración exitosa de la VPN site to site entre el MSPS y el nodo territorial.
- Verificación exitosa de la comunicación entre la plataforma tecnológica IHCE del Ministerio de Salud y Protección Social y el nodo territorial.

- Configuración exitosa de la VPN site to site entre el nodo territorial y el prestador de salud.
- Verificación exitosa de la comunicación entre la plataforma tecnológica IHCE del Ministerio de Salud y Protección Social y el prestador de salud.
- La secretaria de salud debe validar y gestionar los prestadores de salud de la región que van a hacer uso de la plataforma de interoperabilidad de la IHCE, remitiendo el código REPS de las entidades al MSPS.
- El MSPS realizará la creación y configuración de las API-KEY en la plataforma tecnológica de IHCE.
- El MSPS entregará al nodo territorial los API-KEY creados para cada prestador de salud.
- El prestador de salud realizará la configuración del API-KEY en el software que tienen dispuesto para interactuar con la plataforma tecnológica de IHCE.
- El prestador de salud realizará la validación de mensajes (Bundle), el cual debe cumplir con lo definido en los lineamientos brindados por el MSPS.
- El prestador realizará pruebas de envío de registro, consulta y obtención del RDA desde el sistema de información que tienen para interactuar con la plataforma IHCE.

10. RECOMENDACIONES Y/O CONTINGENCIA

Con el ánimo de garantizar la interoperabilidad de la historia clínica electrónica – IHCE con los nodos territoriales y las instituciones prestadoras de salud – IPS, se realizan las siguientes recomendaciones:

- Secretaria de Salud departamental o distrital de salud

  - Disponer de un enlace de datos dedicado en alta disponibilidad para garantizar la conexión VPN site to site o X-Road con el Ministerio de Salud y Protección Social.

  - Disponer de infraestructura TI relacionada con seguridad perimetral en alta disponibilidad para garantizar la conectividad entre la secretaria de salud y el MSPS.

  - Cuando se realice la implementación del mecanismo X-Road, se debe implementar la infraestructura TI en alta disponibilidad para garantizar la prestación del servicio.

- Prestador de servicios de salud

  - Disponer de un enlace de datos dedicado en alta disponibilidad para garantizar la conexión VPN site to site o X-Road con la secretaria de salud.

  - Disponer de infraestructura TI relacionada con seguridad perimetral en alta disponibilidad para garantizar la conectividad entre el nodo y el prestador de salud.

  - Cuando se realice la implementación del mecanismo X-Road, se debe implementar la infraestructura TI en alta disponibilidad para garantizar la prestación del servicio.

- Desarrollar, configurar y desplegar un sistema de información requerido para interactuar con la plataforma tecnológica de IHCE.

- Realizar la configuración de la infraestructura tecnológica para la interoperabilidad de la historia clínica en alta disponibilidad para garantizar la prestación del servicio.