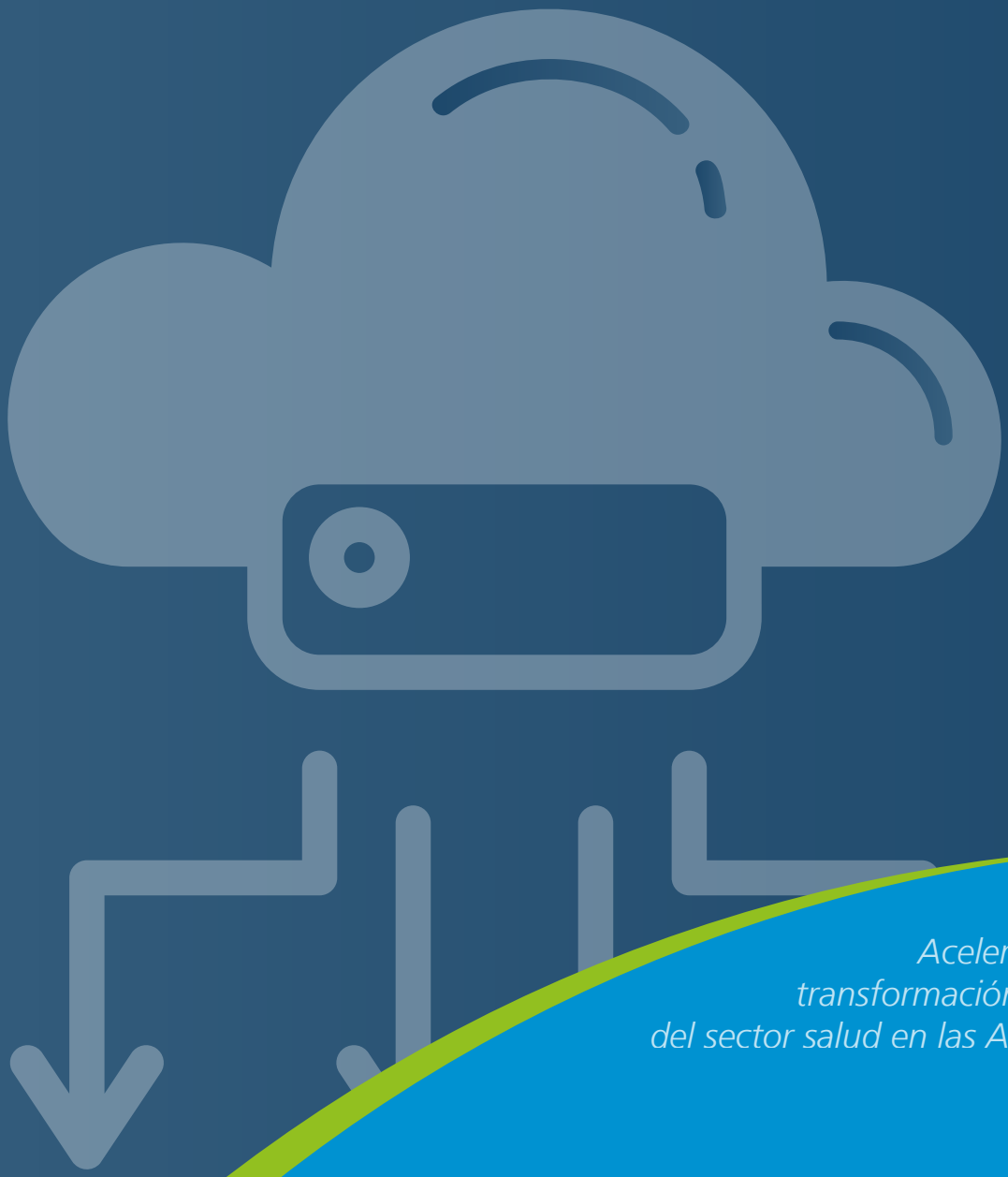


Acelerando la transformación digital del sector salud en las Américas

ALL-IN-ONE

Telesalud para atención primaria en salud con foco en la enfermedades no trasmisibles

Requerimientos básicos de seguridad y conectividad

OPS
Organización Panamericana de la Salud
Organización Mundial de la Salud
Región de las Américas

ALL-IN-ONE

Telesalud para atención primaria en salud con foco en la enfermedades no trasmisibles

Requerimientos básicos de seguridad y conectividad

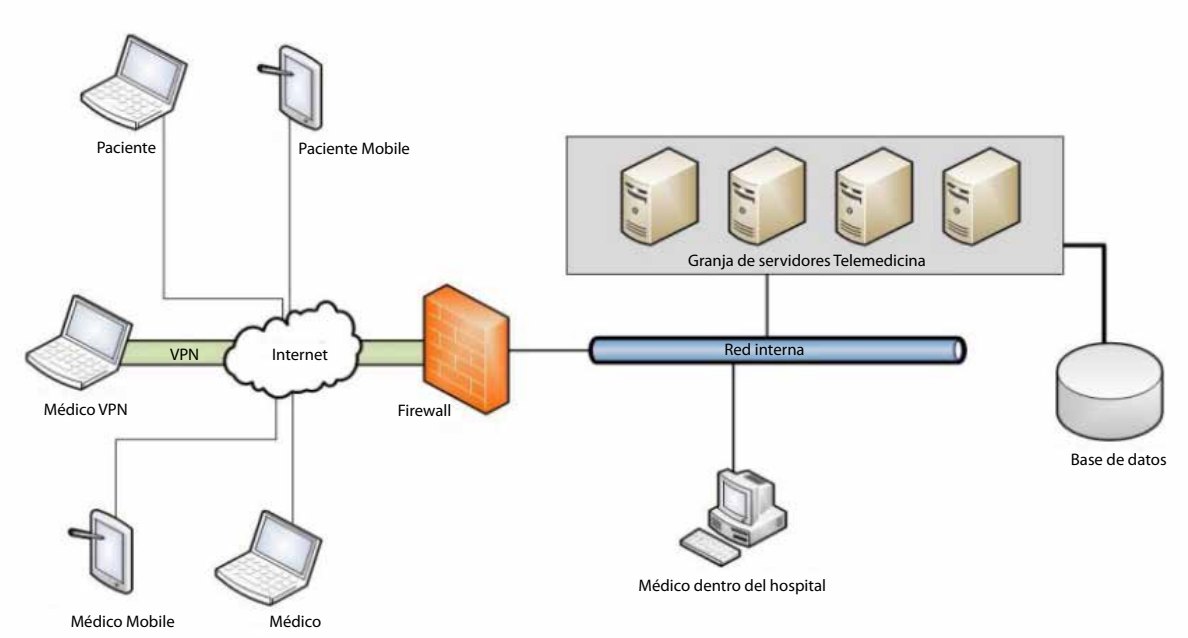
OPS Organización Panamericana de la Salud
Organización Mundial de la Salud
Región de las Américas

Contenidos

Requerimientos básicos de seguridad y conectividad

El servicio de telesalud se basa en el concepto de servicio por lo que es necesario tener en cuenta tanto la calidad del servicio como la seguridad de los datos, ofreciendo el mejor rendimiento y poniendo especial foco en la seguridad de la infraestructura.

Imagen 1. Generalidades de la telemedicina



En la imagen 1 se muestran los distintos casos de uso estudiados para que la telesalud sea un servicio flexible, es decir, no existan lugares físicos sino que las personas puedan tener su consulta virtual desde cualquier lugar, incluidos los médicos, que ya no necesitan estar en un consultorio dentro del hospital.

En el esquema general de telesalud, todas las conexiones provenientes de internet (zona insegura) deben pasar por firewalls y se analiza en todo momento la conexión, evitando de esta manera que se exploten vulnerabilidades en la plataforma.

Analizando la complejidad de este tipo de servicios, se evidencia que la mayor parte de las conexiones provienen de la zona insegura (internet) debido a que este servicio rompe con el paradigma de que el médico debe estar dentro de un hospital (y por ende en su red segura), ubicando tanto a medico como paciente en cualquier lugar del mundo.

Para lograr un correcto balance entre seguridad y rendimiento, se recomienda instalar una granja de servidores que trabajen simultáneamente dentro de la red para garantizar la alta disponibilidad, y un esquema de firewalls encargados de analizar las conexiones Todos los dispositivos que se conectan desde internet son considerados inseguros, aún aquellos que ingresan mediante VPN . BORRAD OR entrantes y salientes, configuradas con estrictos perfiles de seguridad de acuerdo a la aplicación publicada en internet.

El mismo analiza la aplicación en busca de vulnerabilidades o ataques, bloqueando cualquier intento de intrusión o explotación de vulnerabilidad.

En todos los casos las conexiones provenientes de internet se tratan como inseguras sin excepción, aun aquellas en las cuales un médico pueda estar conectado por VPN, debido a que no podemos determinar el nivel de seguridad de los dispositivos (nivel de actualizaciones de sistemas operativos, parches de seguridad, antivirus, etc.).

Dentro de la LAN, un médico puede realizar teleconsultas desde las pc de escritorio que existen en los consultorios. Aquí la seguridad se complementa con sistemas operativos actualizados, parches de seguridad al día, antivirus con soporte, esquema de actualizaciones programadas y políticas de uso tanto de la pc como de internet.

Existe también la posibilidad de que un paciente que está dentro del hospital realice teleconsultas (ej. una visita de un paciente internado que tiene una consulta programada), debido a un sistema de Wi-Fi de invitados, el cual al no tener contacto con la LAN, puede tratar al dispositivo del paciente de la misma forma que en los casos descritos anteriormente.

Un volumen de datos habitual es en promedio 680 Gbit de tráfico diario tomando como periodo de atención de 08:00 am a 20:00 pm, teniendo como promedio un tráfico superior a los 15 Mbit/s solo dedicados a este servicio.

Se recomienda que los enlaces de internet sean redundantes y contingentes, al igual que los Firewall y la infraestructura interna, de manera de disminuir al mínimo el downtime, aun en los casos de actualizaciones de software, firmware, etc.

Política de Privacidad

La solución está basada en 2 soluciones de opensource OpenEMR para el registro médico electrónico, y Jitsi Meet para la videoconsultas.

OpenEMR

Es un software de registro médico electrónico y gestión de práctica médica de código abierto. La política de privacidad de OpenEMR destaca su compromiso con la protección de la privacidad y el cumplimiento de las regulaciones de privacidad como la HIPAA. Se enfoca en la seguridad de la información del paciente y describe cómo se manejan los datos dentro del sistema. Cuenta con licencias por CC 3.0 BY1. Para una evaluación detallada de la privacidad y el cumplimiento con la HIPAA.

Jitsi (meet.jit.si)

Es una solución de videoconferencia de código abierto. La política de privacidad de meet.jit.si, actualizada por última vez el 21 de agosto de 2023, describe cómo 8x8, Inc., el principal contribuyente a la solución de videoconferencia de Jitsi.org, procesa la información personal para proporcionar el servicio de meet.jit.si. Esta política cubre qué información personal se procesa y por qué, cómo se utiliza esta información y cómo contactar al oficial de protección de datos de 8x8. Además, se asegura de que no están en el negocio de vender información personal a terceros y que utilizan la información para entregar y mejorar el servicio de meet.jit.si.

Seguridad y cifrado

Con respecto a los puntos de cifrado y seguridad cada uno de los softwares incluyen las siguientes características:

OpenEMR proporciona varias medidas de seguridad para proteger los datos de los pacientes y cumplir con las regulaciones como la HIPAA. Algunas de las características de seguridad incluyen:

- **Cifrado de documentos**: OpenEMR utiliza la biblioteca PHP mcrypt para el cifrado y descifrado de documento.
- **Contraseñas seguras:** Se recomienda el uso de contraseñas fuertes y únicas, así como la expiración de contraseñas.
- **Autenticación multifactor:** Para una capa adicional de seguridad.
- **Configuraciones de red y servidor:** Se sugiere abrir solo el puerto 443 (https) y considerar un firewall que solo permita tráfico a través de este puerto.
- **Hardening de Apache:** Se recomienda solo permitir https y desactivar el acceso directo a ciertos directorios.

Jitsi Meet es una solución de videoconferencia que también se enfoca en la seguridad y privacidad de sus usuarios. Las características de seguridad incluyen:

- **Cifrado de extremo a extremo (E2EE):** Jitsi Meet ofrece E2EE como una capa adicional de seguridad sobre el cifrado de transporte siempre presente3.
- **Salas efímeras:** Las salas de reuniones solo existen mientras la reunión está activa, lo que significa que no hay conexión con reuniones anteriores que puedan haber tenido el mismo nombre.
- **Generador de nombres de sala:** Para evitar accesos no deseados, se usan nombres de sala generados aleatoriamente que son difíciles de adivinar.
- **Soporte de navegador:** El cifrado de extremo a extremo está disponible en ciertos navegadores, pero no en todos.

OPS
Organización Panamericana de la Salud
Organización Mundial de la Salud
Región de las Américas
www.paho.org