**Requisitos para unirse al dominio Ruta Panamericana para la Salud Digital (PH4H ) de la Red de Confianza administrada por la OMS**

En el marco del proyecto de la Ruta Panamericana de la Salud Digital (PH4H), se invita a los países de ALC a sumarse a la red mundial de confianza de salud digital [[1]](#footnote-2)administrada por la Organización Mundial de la Salud (OMS) y a su dominio específico para la PH4H .  Esta red es de participación voluntaria, totalmente gratuita y disponible para los estados miembros de las Naciones Unidas, y por consiguiente para los estados miembros de la Organización Panamericana para la Salud (OPS). La red de confianza de la OMS es una plataforma de código abierto, basada en estándares sólidos y transparentes, que establece el primer componente básico de la infraestructura de salud pública digital.

Las redes de confianza regionales y mundiales se utilizan mucho hoy en día para certificar y verificar la procedencia de la información, como un pasaporte o un sitio web. La red de confianza de la OMS está diseñada para proporcionar la infraestructura de salud digital necesaria para la resiliencia en futuras respuestas a epidemias y pandemias y para ofrecer una mejor salud a todos al permitir el uso de historiales médicos personales digitales para la continuidad de la atención. De esta manera, facilita la validación de documentos de manera electrónica. Esto aumenta la seguridad de los documentos clínicos y acelera la adopción de servicios médicos digitales.

Los Estados miembros participantes envían voluntariamente claves públicas a un directorio gestionado por la OMS, de modo que se comparten de forma fiable con otros Estados miembros. Estas claves públicas pueden utilizarse para verificar que las credenciales sanitarias firmadas digitalmente (por ejemplo, tarjetas de vacunación, historiales médicos) han sido emitidas por una autoridad reconocida en la red de confianza.

A continuación, se detallan los requisitos técnicos y administrativos que deben completar los Estados miembros para unirse a la red.

Registro de País

1. **Clonar Repositorio de País Participante:** Es necesario crear un repositorio privado en GitHub para compartir las llaves criptográficas[[2]](#footnote-3) del país con la OMS. Para facilitar la creación de este repositorio privado, se recomienda [clonar este repositorio plantilla](https://github.com/WorldHealthOrganization/tng-participant-template) que contiene instrucciones y ejemplos de las llaves criptográficas que se compartirán.
2. **Generar llave PGP[[3]](#footnote-4):** Para garantizar la seguridad de este repositorio y la información compartida, deberá usarse una llave PGP para firmar el contenido del repositorio. [Esta página](https://docs.github.com/en/authentication/managing-commit-signature-verification/generating-a-new-gpg-key) describe cómo generar y usar la llave PGP en el repositorio GitHub. [Este video](https://github.com/WorldHealthOrganization/smart-trust/releases/download/v1.1.1/1.2.full-video.v2.mp4) demuestra el proceso de generación de la llave PGP y como obtener el ID de la llave.
3. **Enviar carta de intención**: Es necesario completar una carta de intención (versión [en Inglés](https://smart.who.int/trust/Letter_of_Application_DDCC.docx)) y enviarla a través de la oficina OPS del país. Esta carta debe ser presentada por la autoridad de salud nacional reconocida por la OPS y debe incluir el URL del repositorio GIthub privado y el ID de la llave PGP creados en el punto anterior.

Pruebas de integración

1. **Generar certificados para pruebas**: El repositorio [contiene scripts](https://github.com/WorldHealthOrganization/tng-participant-template/tree/main/scripts/certgen) para generar los certificados que se compartirán con en el repositorio. Antes de ejecutar la generación de certificados, asegúrese de modificar la [plantilla de país](https://github.com/WorldHealthOrganization/tng-participant-template/blob/main/scripts/certgen/DN_template.cnf) con los valores que correspondan.
2. **Registrar certificados de País:** Una vez generados los certificados, deberán ser guardados en el repositorio privado dentro de una nueva carpeta “onboarding/PH4H”, para luego actualizar el repositorio en línea.
3. **Compartir repositorio con la OMS**: Debido a que el repositorio de país es privado, es necesario invitar al usuario de la OMS para que tenga acceso a los certificados. Asegúrese de agregar con derecho de lectura al usuario [TNG-BOT-DEV](https://github.com/tng-bot-dev).

**Sobre la gestión de certificados**

* La OMS ofrece varias recomendaciones para la gestión de certificados incluyendo el uso de curvas elípticas[[4]](#footnote-5) y evitar el uso de certificados autoafirmados[[5]](#footnote-6) en ambientes de producción. Estas sugerencias son deseables y altamente recomendables, pero en ningún caso son requisitos obligatorios exigidos por la OMS para integrarse a la red de confianza.
* Si el país cuenta con una autoridad certificadora[[6]](#footnote-7) que cumple con los requisitos de la legislación nacional se recomienda el uso de certificados emitidos por esta autoridad. Si su país no cuenta con dicha infraestructura, pueden igualmente utilizarse certificados auto-firmados para unirse a la red de confianza de la OMS.
* Independientemente de la forma en que se generen los certificados, es responsabilidad de la Autoridad de Salud del país velar por el resguardo y la seguridad de la llave privada con que se firman los documentos que se entregan a los usuarios de servicios de salud.
* De ser necesario, un Estado miembro puede compartir múltiples llaves de validación en la red de confianza de la OMS. Esto es necesario si la Autoridad de Salud utiliza diferentes llaves para firmar diferentes documentos que necesitan ser validados dentro del país o por otros Estados miembros.

**Sobre el Dominio de Confianza PH4H**

* La OMS implementa sobre la red de confianza la creación de documentos estandarizados y guías de implementación de servicios de salud alineadas con las [guías SMART](https://www.who.int/teams/digital-health-and-innovation/smart-guidelines). A estos proyectos se les conoce como Dominios de Confianza. En América latina y el Caribe, la OPS y el BID impulsaron la creación del dominio [PH4H](https://build.fhir.org/ig/WorldHealthOrganization/smart-ph4h/) para armonizar y validar entre países sus documentos clínicos y servicios digitales de salud. Los países de la región están invitados a unirse a la red de confianza a través del dominio PH4H.
* El dominio de confianza PH4H permite validar documentos clínicos en su país y entre los países de la región. Además, como miembro de la red de confianza de la OMS, cada país puede validar la firma electrónica de sus documentos médicos dentro y fuera de su territorio nacional.
* Si bien la red de confianza de la OMS permite validar la firma electrónica de documentos médicos entre países, o a nivel regional, es necesario acordar casos de uso y conjuntos mínimos de información que permitan a la entidad receptora del documento usar la información que se le entrega. Estos acuerdos son parte del trabajo dentro del dominio de confianza PH4H que requiere de la participación y consenso de los países de la región.

Para cualquier consulta sobre el proceso de adhesión a la red de confianza y al dominio PH4H, favor escribir al correo [gdhcn@racsel.org](mailto:gdhcn@racsel.org)

1. <https://www.who.int/initiatives/global-digital-health-certification-network> [↑](#footnote-ref-2)
2. https://www.cloudflare.com/es-es/learning/ssl/what-is-a-cryptographic-key/ [↑](#footnote-ref-3)
3. https://www.fortinet.com/lat/resources/cyberglossary/pgp-encryption [↑](#footnote-ref-4)
4. https://es.wikipedia.org/wiki/Curva\_el%C3%ADptica [↑](#footnote-ref-5)
5. https://www.entrust.com/es/resources/learn/what-is-a-self-signed-certificate [↑](#footnote-ref-6)
6. https://www.ssl.com/es/art%C3%ADculo/%C2%BFQu%C3%A9-es-una-autoridad-certificadora-ca%3F/ [↑](#footnote-ref-7)