



UAI

Universidad Abierta Interamericana

Jitsi como solución de videoconferencia para el Ministerio Público Fiscal de la Nación Argentina

Alumno: Gustavo Oscar Ripamonti

Profesora de trabajo final: Dra. Marcela Samela

Tutora técnica: Dra. Claudia Pons

Trabajo Final de carrera presentado para obtener el título de
Licenciatura en Gestión de Tecnología Informática

Junio 2023

Resumen

El objetivo de la presente Propuesta de Intervención en el Campo Profesional es unificar y estandarizar el medio por el cual se realizan las videoconferencias, a través de la implementación del sistema de código abierto (open source) Jitsi Meet. La misma surge con la finalidad de solucionar la problemática evidenciada durante la aparición de la pandemia Covid-19, al respecto de la utilización de una gama heterogénea de equipos y programas destinados a la realización de videoconferencias dentro del Ministerio Público Fiscal de la Nación Argentina. A la fecha, estos equipos y programas no son completamente seguros, efectivos, suficientes y/o generan costos altos para cumplir con la demanda de las diferentes áreas que integran este organismo. Para la implementación del trabajo, se realizó un relevamiento teórico que permite ordenar la información necesaria, para luego utilizarla como base durante el desarrollo técnico. Se completarán 8 fases de pruebas, comenzando desde la instalación y pasando por entornos físicos, virtuales y por último su aplicación en contenedores. Las fases están divididas en diferentes hitos a corroborar en cada una de forma incremental, hasta alcanzar un nivel de funcionalidad completo, pero dentro de un entorno no productivo. Finalmente, se copiará ese entorno a la estructura productiva para la puesta en marcha definitiva. Asimismo, recurriendo a herramientas de gestión de proyectos, se ordenan los recursos humanos y técnicos, además de establecer el cronograma de la duración total del proceso. Se espera que la propuesta resuelva la problemática anteriormente expuesta, logrando estandarizar, securizar y reducir los costos de efectuar videoconferencias, además de obtener un mayor control de los recursos técnicos utilizados para ese fin y proporcionar un mejor servicio a los usuarios.

Palabras clave: videoconferencia, protocolo, código abierto, infraestructura de redes, almacenamiento.

Abstract

The objective of this Proposal for Intervention in the Professional Field is to unify and standardize the means by which videoconferences are carried out, through the implementation of the open source system Jitsi Meet. It arises with the purpose of solving the problem evidenced during the appearance of the Covid-19 pandemic, regarding the use of a heterogeneous range of equipment and programs destined to carry out videoconferences within the Public Prosecutor's Office of the Argentine Nation. To date, these equipment and programs are not completely safe, effective, necessary, and/or generate high costs to meet the demands of the different areas that make up this organization. For the implementation of the work, a theoretical survey was carried out that allows ordering the necessary information, to later use it as a base during the technical development. 8 phases of tests will be completed, starting from the installation and going through virtual and physical environments and finally its application in containers. The phases are divided into different milestones to check each one incrementally, until reaching a full functionality level, but within a non-productive environment. Finally, this environment will be copied to the productive structure for the final start-up. Likewise, using project management tools, human and technical resources are ordered, in addition to establishing the schedule of the total duration of the process. It is expected that the proposal solves the problems exposed above, managing to standardize, secure and reduce the costs of videoconferences, in addition to obtaining greater control of the technical resources used for this purpose and providing a better service to users.

Keywords: videoconference, protocol, open source, networking, storage.

Dedicatoria

A mis padres, que siempre están y estarán conmigo y a los amigos que me dan su aliento.

Contenido

RESUMEN	2
ABSTRACT	3
DEDICATORIA	4
CAPÍTULO 1.....	9
DENOMINACIÓN DEL PROYECTO	9
NATURALEZA DEL PROYECTO.....	9
JUSTIFICACIÓN	9
MARCO INSTITUCIONAL.....	12
OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS	13
COMPONENTES O RESULTADOS	14
RESUMEN	15
CAPÍTULO 2.....	17
ACCIONES A REALIZAR.....	17
CONFORMACIÓN DEL ACTA DE CONSTITUCIÓN DEL PROYECTO	17
RECOPILACIÓN DE INFORMACIÓN TÉCNICA DISPONIBLE	18
SOLICITUDES A ÁREAS INTERVINIENTES	24
FASE 1 - INSTALACIÓN Y FUNCIONAMIENTO EN ENTORNO DEV FÍSICO.....	25
FASE 2 - ENTORNO DEV SOBRE VMWARE.....	26
FASE 3 - SECURIZACIÓN DE VIDEOCONFERENCIAS	27
FASE 4 – MÓDULO DE GRABACIÓN.....	29
FASE 5 – INSTALACIÓN DE JIBRI EN DOCKER	30
FASE 6 – AUTOMATIZACIÓN DE ENVÍO DE GRABACIONES	31
FASE 7 – ADECUACIÓN DE JITSY Y PUBLICACIÓN EN UAT	33
FASE 8 – IMPLEMENTACIÓN EN ENTORNO PRODUCTIVO	34
RESUMEN	35
CAPÍTULO 3.....	36
DETERMINACIÓN DE CRONOGRAMA	36
CAPÍTULO 4.....	37
DETERMINACIÓN DE RECURSOS	37
RESUMEN	41
CAPÍTULO 5.....	42
FACTORES DETERMINANTES DE ÉXITO	42

FACTORES EXTERNOS.....	43
RESUMEN	45
CAPÍTULO 6.....	46
EVALUACIÓN DEL PROYECTO	46
COSTOS EVITABLES	46
CRITERIOS DE EVALUACIÓN DE FASES DE PRUEBA	46
RESULTADOS ESPERABLES PARA LA FASE 1.	46
RESULTADOS ESPERABLES PARA LA FASE 2.	46
RESULTADOS ESPERABLES PARA LA FASE 3.	47
RESULTADOS ESPERABLES PARA LA FASE 4	47
RESULTADOS ESPERABLES PARA LA FASE 5	48
RESULTADOS ESPERABLES PARA LA FASE 6	49
RESULTADOS ESPERABLES PARA LA FASE 7	49
RESULTADOS ESPERABLES PARA LA FASE 8	50
RESUMEN.....	50
CAPÍTULO 7.....	51
CONCLUSIONES	51
ACRÓNIMOS	52
REFERENCIAS	56
ANEXO A. ORGANIGRAMA MPF.....	60
ANEXO B. ACTA DE CONSTITUCIÓN DEL PROYECTO.....	61
ANEXO C. ARQUITECTURA JITSI	63
ANEXO D. INSTALACIÓN Y CONFIGURACIÓN DE NGINX	64
ANEXO F. JURISDICCIONES	68
ANEXO G. AUTENTICACIÓN	69
ANEXO H. REGISTRO DE PASSWORD.....	71
ANEXO I. TURN.....	74
ANEXO J. INSTALACIÓN DE JIBRI	76
ANEXO K. DOCKER.....	80
ANEXO L. APLICACIONES DE SOPORTE	84
ANEXO M. INSTRUCTIVOS.....	91
ANEXO N. ARCHIVOS PARA APLICACIONES.....	102

Índice de Figuras

FIGURA 1	14
FIGURA 2	15
FIGURA 3	21
FIGURA 4	22
FIGURA 5	42
FIGURA 6	44

Índice de Tablas

TABLA 1	11
TABLA 2	19
TABLA 3	36
TABLA 4	37
TABLA 5	37
TABLA 6	38
TABLA 7	38
TABLA 8	39
TABLA 9	40

Capítulo 1

Denominación del Proyecto

El proyecto se denomina “*Jitsi como solución de videoconferencia para el Ministerio Público Fiscal de la Nación Argentina*”, ya que es el software libre que se seleccionó para reemplazar los sistemas actuales de videoconferencia.

Jitsi es uno de los sistemas de código abierto más utilizados¹ de hoy en día, gracias a su versatilidad y a su constante crecimiento y mantenimiento, proporcionado originalmente por la empresa Atlassian y actualmente en manos de 8x8 .

Se plantea como desafío para el año 2024 implementar este sistema de código abierto que favorezca la reducción de costos en compras y mantenimiento en soluciones de terceros dentro del Ministerio Público Fiscal de la Nación Argentina y que, así mismo, dada la sensibilidad de la información que ha de manejarse permita un alto grado de seguridad en las comunicaciones.

Naturaleza del Proyecto

El presente Trabajo Final se fundamenta en el procedimiento para instalar y adecuar el sistema de videoconferencias Jitsi, alojándolo en la estructura informática local, obteniendo así administración y mantenimiento propio del software, dotando al Ministerio de una mejora en los canales de comunicación con otras dependencias, organismos públicos y/o empresas.

Por otra parte, ejecución de este plan, incluye una estandarización, no solo del medio por el cual se realizan las videoconferencias, sino del procedimiento por el cual se accede al recurso.

Se establecen como destinatarios de este proyecto todos los integrantes del Organismo que necesiten realizar una comunicación con video y audio de forma segura.

Justificación

Tras la aparición de la pandemia de Covid-19 en marzo de 2020² y las medidas sanitarias impuestas de trabajo remoto, quedó al descubierto la carencia de criterios y de recursos para llevar adelante este modelo de trabajo. Es inevitable que, para el funcionamiento del aparato judicial, no sean tomadas declaraciones y corroboradas las identidades de los participantes en las causas que se tramitan dentro del MPF.

¹ Basado en <https://hashdork.com/es/open-source-conferencing-platform/>.

² Resolución oficial del organismo <https://www.mpf.gov.ar/resoluciones/pgn/2020/PGN-0023-2020-001.pdf>

Jitsi cuenta con múltiples aristas que hacen rica su aplicación y desarrollo dentro del entorno del Ministerio, proporcionando una mejora en los servicios de comunicación para los usuarios, con funcionalidades que facilitan la labor del personal de las fiscalías (Real Academia Española., s.f., definición 2).

La elección se realizó utilizando dos métodos de recopilación de información indicados dentro del PMBOK, los cuales son el Análisis de Alternativas y el Análisis de Hacer o Comprar (Project Management Institute, Inc., 2021).

Análisis de Alternativas

Dentro del mercado de posibles aplicaciones de videoconferencia, fueron seleccionados los 3 competidores que se utilizaron en distintas ocasiones de manera eventual dentro del MPF. En la Tabla 1 se observa la comparativa entre Jitsi, Zoom de Microsoft, Meet de Google y Big Blue Button. Si bien tanto Zoom como Meet son alternativas pagas, de todas formas, se consideran para evaluar que las prestaciones técnicas de las alternativas Open Source sean suficientes o similares a las de las alternativas comerciales.

Uno de los aspectos deseables de la implementación de la solución de VC es que implique el menor costo posible, pero esto no es necesariamente una limitante al momento de tomar una decisión, también debe considerarse el costo/beneficio al respecto al tiempo que lleva la implementación de cada una de las alternativas. Al respecto de esta decisión trata el punto “Análisis de Hacer o Comprar”.

Análisis de Hacer o Comprar

Antes de comenzar con el desarrollo del proyecto, es importante determinar finalmente si se va a optar por una solución paga o no, teniendo en cuenta lo visto en el punto Análisis de Alternativas. A continuación, se indican cinco puntos de vista que se tomarán como base para complementar el análisis y que servirán de apoyo a la hora de tomar una decisión (Bara, 2016):

Las restricciones del presupuesto. El MPF intenta evitar hasta las últimas consecuencias la contratación de servicios que requieran de erogaciones periódicas, sobre todo aquellas que son con base en moneda extranjera, como lo es para el caso de las analizadas en el ítem anterior.

La rentabilidad. La instalación de Jitsi en servidores propios logra reducir los costos de proveer un servicio de videoconferencia, ya que utiliza infraestructura existente.

Tabla 1*Análisis de alternativas*

Características	Jitsi Meet	Zoom	Google Meet	BigBlueButton
Precio	Gratis	Gratis por 40 minutos con publicidad y pago	Pago, sin opciones corporativas gratis	gratis
Hosting	Self + Cloud	Solo cloud y suscripciones	Solo cloud y suscripciones	Self + Cloud
Usuarios	Hasta 75, escalable	Hasta 100 participantes free/ hasta 500 pago	Hasta 500 participantes	Hasta 150 participantes
Llamadas de audio	Si	Si	Si	Si
Videoconferencia	Si	Si	Si	Si
Agenda	Si	Si	Si	Si
Grabación de sesión	Local	Local + (desde 1GB hasta ilimitado en planes de pago)	Desde 30GB hasta ilimitado	Local o plan del host
Calidad de video	1280×720, 640×360, y 360×180	1080p y 720p	720p y 360p	1280x720, 640x480 y 320x240
Conectividad necesaria	3,5Mbps	6Mbps	3,2 Mbps	2,5Mbps (media a 640p)
Filtros de fondo	Si	Si	Si	Si

Nota. Comparativa de aplicaciones de videoconferencia de elaboración propia, realizada para facilitar la lectura.

El punto de vista de la organización. La inquietud original acerca de poseer un servicio de videoconferencia proviene de la Dirección de Tecnología en conjunto con la jefatura de la Secretaría General de Administración y RRHH.

La necesidad. Es de mediano plazo, no hay exigencias inmediatas.

Estrategia a largo plazo. La tendencia general es conseguir la auto-provisión de servicios que impacten en áreas de información sensible.

Hasta el momento se utilizó únicamente BigBlueButton como alternativa de software libre, y en vistas que el mismo proporcionó resultados aceptables, se instruyó al área de Planificación de Recursos y Proyectos Tecnológicos buscar alternativas similares, haciendo hincapié en que aquellos que resulten seleccionados, sean capaces de brindar seguridad durante la comunicación y no dependan de servidores externos.

Si bien BBB cumple con las condiciones de seguridad y gratuidad, se escogió Jitsi principalmente gracias a una característica superadora, la cual es su escalabilidad en cuanto a necesidad inicial de recursos de hardware.

Marco Institucional

El Marco Institucional es importante para reconocer la cultura organizacional en la que se desarrollará el proyecto, ya que este se verá afectado en su curso por distintos aspectos de la misma, haciendo foco en normas, políticas, métodos y procedimientos, la percepción del liderazgo, las jerarquías y sus relaciones de autoridad, y por último pero no menos importante, en los entornos operativos (Project Management Institute, Inc., 2013).

El Ministerio Público Fiscal de La Nación (ver organigrama en el Anexo A) es, según la propia definición en su sitio web (Ministerio Público Fiscal de la Nación, 2022):

...parte fundamental en la administración de justicia, compuesta por el Poder Judicial (integrado por jueces, juezas, funcionarios, funcionarias, empleados y empleadas) y los Ministerios Públicos: Fiscal y de la Defensa. En su conjunto, conforman las tres partes fundamentales en un proceso judicial. Asimismo, el Ministerio Público Fiscal es un órgano independiente dentro del sistema de administración de justicia.

El rol que les corresponde a los y las fiscales que conforman el MPF tiene fines y objetivos muy claros: defender los intereses generales de la sociedad.

En palabras simples, el MPF nuclea a todas las fiscalías que se desempeñan en causas de competencia federal. También cooperan con sus pares de cada distrito, provincia o jurisdicción.

Como toda organización de hoy en día, el MPF tiene como sustento para su funcionamiento un trasfondo informático, de la envergadura adecuada para manejar la gran

estructura de interconexión de dependencias y el volumen de información que atraviesa por las mismas.

La puesta en marcha de este proyecto depende del área de Planificación de Recursos y Proyectos Tecnológicos, parte integrante de la Dirección General de Desarrollo Organizacional y Nuevas Tecnologías. Se puede observar su estructura completa en la Figura 1.

La Dirección General de Desarrollo Organizacional y Nuevas Tecnologías tiene como misión principal el desarrollo, implementación y mantenimiento de las aplicaciones institucionales, como así también, la gestión y mantenimiento de la infraestructura de red y de comunicaciones del MPF.

Mediante la provisión de infraestructura informática y de comunicaciones, y software específico para la actividad judicial y administrativa, la Dirección brinda los servicios imprescindibles para la operatoria de las fiscalías y dependencias de la Procuración General de la Nación, con el objeto de facilitar la operatoria de tales destinos, todo ello con el soporte técnico correspondiente.

Objetivo General y Objetivos Específicos

A continuación, se describe la serie de objetivos planteados para el Trabajo Final.

General

Implementar un sistema de videoconferencias basado en Jitsi para empleados del MPF.

Específicos

Presentar proyecto a áreas no técnicas superiores para impulsar el desarrollo.

Verificar el entorno de hardware y software necesario para el normal funcionamiento del sistema de VC.

Identificar y delimitar puntos de articulación con las áreas de Seguridad Informática, Operaciones e Infraestructura, a fin de proporcionar las configuraciones y recursos adecuados acerca de la privacidad, almacenamiento y comunicación respectivamente.

Implementar entornos de pruebas que emulen distintos escenarios de la aplicación.

Ofrecer configuraciones específicas y bien delimitadas, para facilitar la implementación de las áreas técnicas.

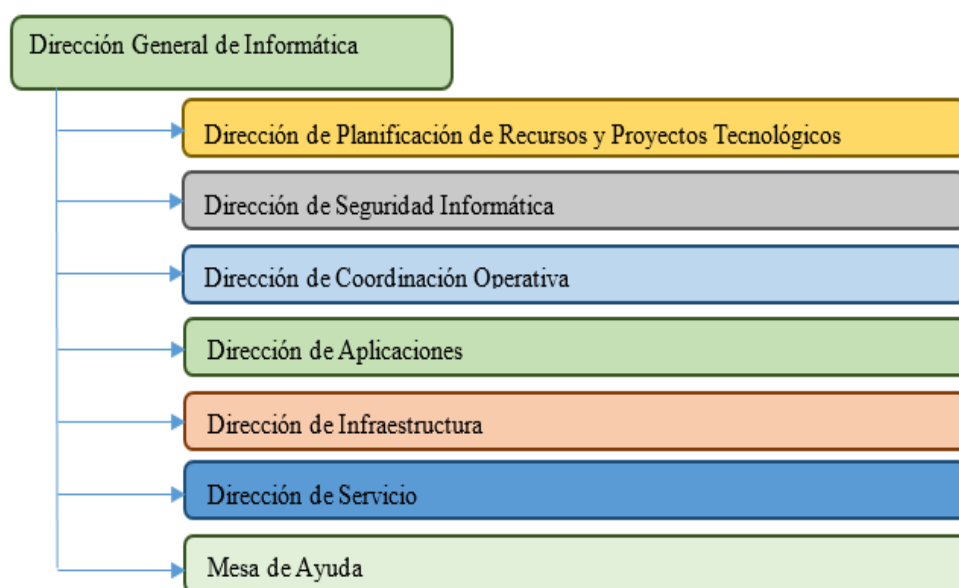
Confeccionar material de instrucción sobre la gestión de la aplicación para el personal técnico y para los usuarios finales.

Componentes o resultados

Los objetivos planteados, son las directrices necesarias que proporcionan al desarrollo del proyecto resultados globales a los que se desea arribar de forma exitosa. La Figura 2, resume aquellos resultados esperados de la aplicación del sistema. Estos aspectos no cuentan con ninguna jerarquía en particular, ya que es necesario lograr todos puntos en el final de la implementación.

Figura 1

Organigrama de la Dirección General



Nota. Organigrama actual de la dirección, no publicado en el sitio oficial³.

La estandarización del criterio de uso de las videoconferencias implica que al fin del proyecto se ha conseguido construir herramientas útiles para establecer dentro del organismo las pautas para el uso común del sistema de VC. Justamente, este proceso de estandarización propone otro punto a alcanzarse, el cual se trata de la eliminación de sistemas de VC obsoletos, a los que pocos usuarios tienen acceso o que necesitan de diversas configuraciones particulares para hacerlos funcionar, generando demoras en la prestación del servicio y provocando que los usuarios soliciten el uso de herramientas pagas, que si bien el Ministerio dispone de las mismas para casos especiales, existe un número reducido para cubrir la demanda general. También estos sistemas dispares provocan confusión en los usuarios y traen consigo problemas de índole técnica, como pueden ser un consumo desmedido de ancho de banda o, inclusive, problemas de seguridad.

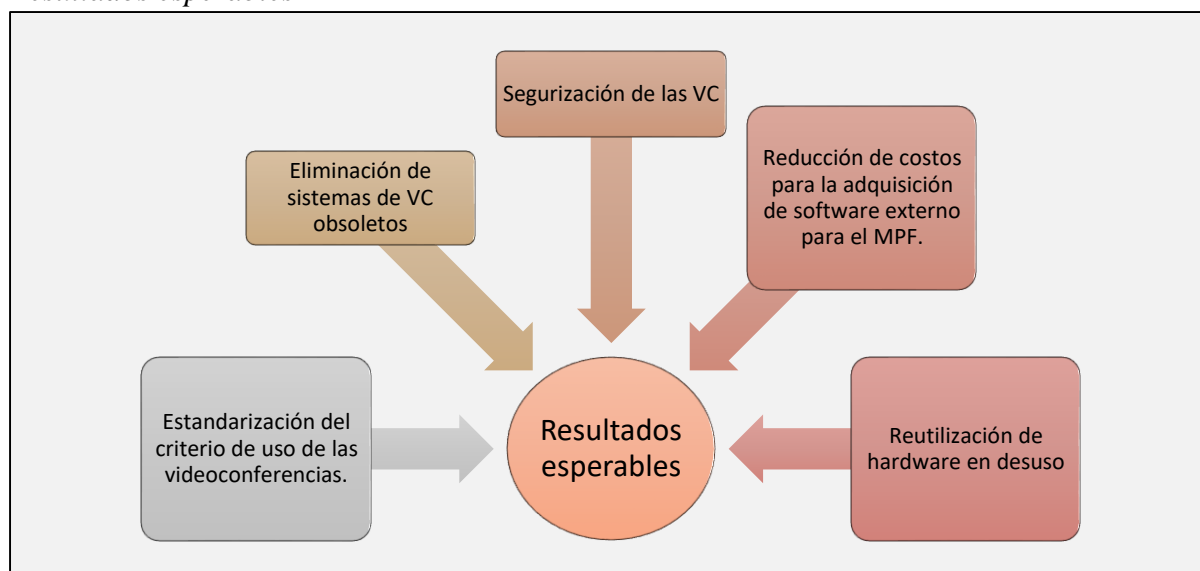
³ <https://www.mpf.gob.ar/administracion-y-rrhh/direccion-general-de-desarrollo-organizacional-y-nuevas-tecnologias/>

La segurización de las VC es otro resultado que se espera alcanzar, al proporcionar un entorno enteramente administrado por personal informático interno del Ministerio, sin la necesidad

de acceso de agentes externos ni la utilización de servicios alojados por terceros. Esta característica no apunta al desestimo total del uso de aplicaciones administradas por servidores de terceros, ya que las mismas son utilizadas en todo el mundo por la más variada gama de empresas y organismos, sino que tiende a presentarse como un factor extra a favor del uso de Jitsi. Al no utilizar aplicaciones de un proveedor externo, se cumplirá otro de los aspectos mencionados en la Figura 2, la reducción de costos en la adquisición de software externo para el MPF.

Figura 2

Resultados esperables



Finalmente, y relacionado a los costos, la implementación de este proyecto hace propicia la reutilización de hardware en desuso. Muchos servidores de bajas prestaciones que fueron reemplazados por otros fines, son útiles para la implementación, dada la escalabilidad modular en la cual se asienta Jitsi.

Resumen

En este capítulo se realizó la presentación del proyecto, a través de su descripción y justificación. Ahondando en la justificación, se seleccionaron dos métodos propuestos por el PMBOK y se desarrollaron aplicados al proyecto. También, se establecieron los objetivos a

cumplir en este trabajo, presentando un objetivo general y sus específicos complementarios. Se identificó el marco institucional para entender en qué contexto se implementará el proyecto.

En último lugar, se determinaron los resultados que se pueden esperar de la puesta en valor del proyecto.

Capítulo 2

Acciones a realizar

En el presente capítulo se establecerán las acciones específicas a realizar, utilizando la descomposición del proyecto mediante la estructura WBS (Project Management Institute, Inc., 2013), con el fin de descomponerlo en partes más simples de comprender y seguir para la implementación.

Por otra parte, se toma de la séptima edición del PMBOK, la división en fases del ciclo de vida del proyecto y la cadencia múltiple para los entregables (Project Management Institute, Inc., 2021), lo que significa que el proyecto contendrá varias versiones durante su desarrollo, con distintos niveles de funcionalidad.

Se desea aclarar que, todas las configuraciones que contengan parámetros o líneas de código, se encuentran dentro de los Anexos, con el fin de no entorpecer la lectura del documento, pero ello no implica que sean pasados por alto al momento de avanzar con las fases desarrolladas a continuación.

Conformación del acta de constitución del proyecto

En una primera instancia, se procederá a elaborar el “Acta de constitución de Proyecto” (Project Management Institute, Inc., 2013), la cual figura dentro de los documentos entregables de la guía del PMI. Si bien es un documento entregable que, a raíz de las estimaciones que deben realizarse presenta cierta complejidad para su elaboración, es igualmente una excelente herramienta para establecer un punto de inicio, acodar de antemano las responsabilidades que poseerá cada área y reflejar la interacción que habrá entre las mismas.

La comunicación del avance del proyecto a los interesados, se realizará a través de un formato push (Project Management Institute, Inc., 2021), en reuniones quincenales y a través de un correo electrónico mensual, que recopilará toda la información del estado de avance.

Es necesario destacar que, al no tratarse de una empresa tradicional, sino de un ente gubernamental, algunos de los aspectos originales que se presentan en el acta de la guía del PMI, no son aplicables; por lo tanto, los puntos que tomaremos en consideración son el Enunciado del trabajo del proyecto (SOW), el caso de negocio y los activos de los procesos de la organización (Project Management Institute, Inc., 2013).

El acta⁴ con los puntos detallados se encuentra en el Anexo B.

⁴ <https://es.scribd.com/document/392779857/Modelo-SOW-de-Adquisiciones>

Recopilación de información técnica disponible

En este punto se procede a explicar todo lo relativo a las distintas tecnologías que se deben complementar o cruzar para conseguir que se efectúe una correcta implementación del sistema de videoconferencia.

Jitsi tiene, además de la escalabilidad antes mencionada, otra característica de consideración que la hacen objeto de elección, la cual es poseer una sólida comunidad de colaboradores. Las entradas o actualizaciones realizadas dentro de un foro de cualquier software libre, dan una clara percepción del mantenimiento que tiene una aplicación, como así también evidencian del compromiso de sus desarrolladores, al momento de responder consultas o efectuar modificaciones del código fuente. Todo ello resulta útil para determinar la posible expectativa de vida del software elegido.

El primer contacto con Jitsi es a través de su página principal, la cual presenta dos vínculos que son relevantes para la implementación, Docs y Community.

Docs

Contiene la documentación básica para una primera aproximación a la herramienta, con sus requisitos técnicos y las instrucciones principales de implementación⁵. También contiene enlaces hacia otras webs de Jitsi, que amplían la información.

Community

Es acceso público y contiene de forma ordenada distintas categorías de interés, como son instalación y configuración, desarrolladores, seguridad, entre otras⁶.

La plataforma también cuenta con su repositorio en GitHub⁷, el cual contiene todos los archivos/código necesarios para realizar el deploy o configuración de Jitsi.

Para entender un poco mejor cómo es la arquitectura del software, se describen brevemente en la Tabla 2 los módulos principales, y se adjunta en el Anexo C la arquitectura completa extraída de la web oficial. Una característica positiva que presenta la utilización de Jitsi, es la capacidad con la que cuenta para instalar los distintos módulos en servidores distribuidos, lo cual se traduce en una ventaja administrativa y organizativa.

Existen también aplicaciones que son necesarias para el funcionamiento de Jitsi, pero que no forman parte del desarrollo de la solución, sino que podrían denominarse como complementarias.

⁵ <https://jitsi.github.io/handbook/docs/intro/>

⁶ <https://community.jitsi.org/>

⁷ <https://github.com/Jitsi>

A continuación, se mencionan cuáles son las tecnologías externas a Jitsi necesarias y/o recomendadas por los desarrolladores.

Tabla 2

Componentes de Jitsi

Componente	Función
Jitsi Meet	Aplicación base de la herramienta, proporciona la interfaz de acceso principal, programada con WebRTC y compatible con java.
Jitsi Videobridge (JVB)	Servidor compatible con WebRTC, el cual enruta transmisiones de video entre participantes.
Jitsi Conference Focus (jicofo)	Es el componente del servidor que administra las sesiones de videoconferencia, envía invitaciones y abre los canales de comunicación en JVB.
Jitsi Gateway to SIP (jigasi)	Es una aplicación del lado del servidor que permite el acceso de participantes SIP.
Jitsi Broadcasting Infrastructure (Jibri)	Es una serie de herramientas basadas en Chrome que permiten la retransmisión de la VC y la grabación, en formato ffmpeg.
Prosody	Servidor XMPP externo, que es utilizado por los módulos para comunicarse entre sí.

CIFS y NTFS

El primero apareció para funcionar sobre entornos de red y es un protocolo de manejo de archivos nacido en la década del 80 y desarrollado en IBM, a causa del lanzamiento de Windows 95 y con base en SMB (Visuality Systems Ltd., 2022).

NTFS aparece como sistema de ficheros con Windows NT 3.1 y en su versión 1.2 ya incorpora elementos como compresión de archivos y control de acceso a usuarios.

Nginx

Se trata de un servidor web con licencia GNU, necesario para el re direccionamiento de las solicitudes de acceso a Jitsi y la interconexión entre los módulos. En el mismo es posible establecer la configuración de acceso seguro mediante SSL (F5 Inc., 2022).

Certificado SSL

Certificado de autenticidad (VeriSign, Inc., 2022) que contiene una llave encriptada (Real Academia Española., s.f., definición 1) emitido por una entidad autorizada, que determina una relación verificable con un dominio (SolarWinds Worldwide, LLC., s.f.).

Docker

Aplicación que permite la creación de contenedores, los cuales son pequeñas máquinas virtuales (International Business Machines Corporation., s.f.), con la característica que solo se utilizan recursos básicos para lograr el funcionamiento de la aplicación que se agrega en el contenedor o “container” (Docker Inc., 2022). Cuando hablamos de recursos básicos, nos referimos a que dentro del contenedor se encontrarán los procesos y servicios estrictamente necesarios para que la aplicación que se aloje en él pueda ejecutarse con su funcionalidad plena.

En este caso particular, lo utilizaremos como medio para agregar un módulo de Jibri, permitiendo alcanzar escalabilidad y control de las grabaciones y retransmisiones.

STUN, TURN y DMZ

Ambos protocolos (STUN y TURN) forman parte del framework ICE (Olawanle, 2022) y son necesarios ya que realizan la identificación de los equipos que intervienen en la VC y redireccionan el tráfico de red en caso de que las conexiones se encuentren ocultas detrás de firewalls (SonicWall., s.f.) o de alguna configuración que enmascare su IP.

El caso del servidor STUN es el más simple, las conexiones que realiza son de punto a punto y su función principal es la de permitirle al cliente que “aprenda” (Temasys, 2022) su IP pública detrás del NAT, para poder informarla al servidor y que este a su vez envíe la información requerida.

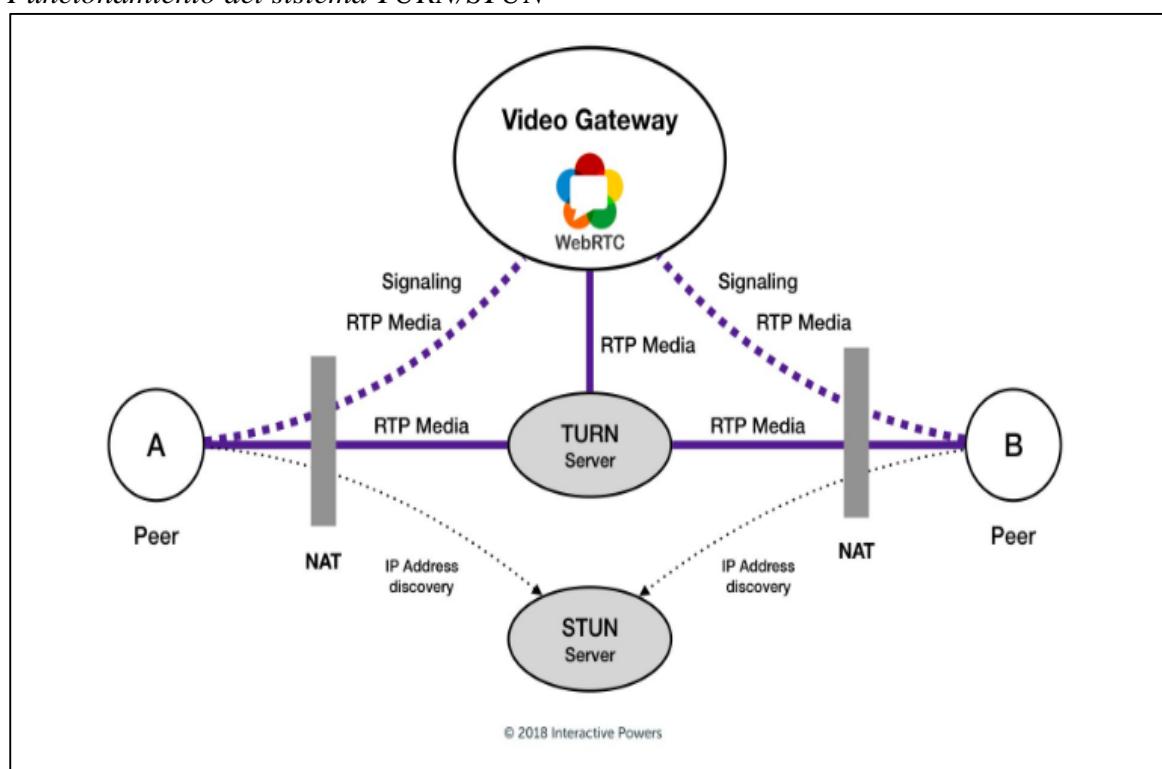
En ocasiones no es posible utilizar solo un servidor STUN al momento de contactar servidor y cliente por la infraestructura de red que puede llegar a tener cada sitio. En esos casos se utiliza TURN, tal y como se describe a continuación:

Para que la mayoría de las aplicaciones WebRTC funcionen, se requiere un servidor para retransmitir el tráfico entre pares, ya que a menudo no es posible un socket (Oracle Corporation., s.f.) directo entre los clientes (a menos que residan en la misma red local). La forma habitual de solucionar este problema es mediante un servidor TURN.⁸ (Google Developers, 2022)

En la siguiente figura se puede visualizar el funcionamiento de STUN y TURN:

Figura 3

Funcionamiento del sistema TURN/STUN



Nota. Adaptado de *ivrpowers-turn-stun-screen 005* [Imagen], por Interactive Powers, 2018, Blog Iv Powers (<https://blog.ivrpowers.com/post/technologies/what-is-stun-turn-server/>). CC BY 2.0

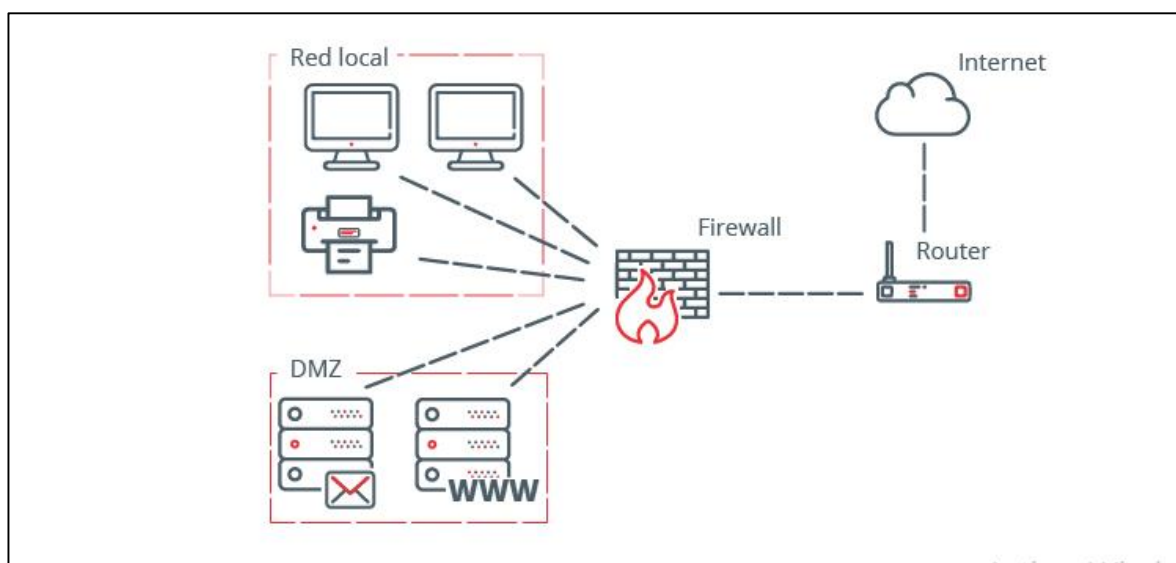
Todos los equipos que funcionan como frontera entre redes, realizan la función de traducir direcciones de red (NAT), para que la información transportada arribe a los destinos requeridos ya que cada red o subred tiene su propio direccionamiento, significando esto que inicialmente no se va a poder acceder a Jitsi desde el exterior de la red LAN del MPF.

⁸ (N. del T.) Se modificaron algunas palabras a raíz de que la traducción provista por Google era confusa en algunos sentidos.

Por otra parte, el MPF es un organismo que administra varias aplicaciones que requieren acceso desde internet, por lo tanto, cuenta con medidas de seguridad como firewalls. Pero en algunos casos solo esta medida no es suficiente para la protección de la red corporativa y para ello se configura una estructura DMZ, que se trata básicamente de la separación de la red interna con las aplicaciones o servidores que están expuestos a internet, tal como se muestra en la Figura 4.

Figura 4

DMZ



Nota. Adaptado de *DMZ.003* [Imagen], por Instituto Nacional de Ciberseguridad, Incibe.es (<https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa>). CC BY 2.0

La separación de la red interna con una DMZ es una política de Seguridad Informática y por ende no es un procedimiento que deba realizarse para este proyecto, sino que es una medida a cumplir y Jitsi debe adecuarse para funcionar de ese modo.

NXLog

Esta es una aplicación que no está relacionada de forma directa con el funcionamiento del sistema de VC, pero su uso resuelve un problema al momento del envío de grabaciones utilizando los registros de eventos o logs (Oxford University Press, s.f., definición 3) del sistema. Su principal función es la recolección de datos de diversas fuentes (NXLog Ltd, 2022).

De manera nativa durante la creación de una sala (jitsi.es, s.f.), Jitsi no devuelve mediante ninguno de sus protocolos el nombre de la misma, dado que esto no es información

relevante para la comunicación con sus módulos de apoyo, como por ejemplo lo son Jibri o Prosody, pero si es mucha relevancia para este proyecto.

VMWare/vSphere

Para realizar pruebas sobre el comportamiento de Jitsi, iniciaremos en un entorno virtualizado. El principal objetivo de dicho entorno es recrear quipos de computación físicos con la finalidad de realizar implementaciones más eficientes y seguras de software (International Business Machines Corporation, s.f.). Se utilizará la herramienta VMWare, que ya se encuentra instalada en los servidores del MPF, a través de su centralizador vSphere.

VMWare es una empresa creada en 1998 y hoy en día ofrece soluciones de virtualización en la nube (Microsoft Corporation., s.f.) o auto-administradas, como lo es en el caso de vSphere.

vSphere es un software del tipo hipervisor, siendo su tarea principal la administración de varios equipos virtuales, creados dentro de un servidor. Este software administra los recursos de las máquinas virtuales (memoria, disco, red, etc.) para adecuarlos a las necesidades de las aplicaciones que alojarán.

OwnCloud

Es un proyecto que se inició en 2010 como una utilidad de código abierto, y a partir de 2012 comenzó a funcionar como empresa, brindando servicios pagos de soporte y/o mejoras en la aplicación. Su objetivo primario es el de proporcionar espacio de alojamiento en la nube para archivos, y desde allí poder compartirlos o resguardarlos (ownCloud GmbH, 2022).

El MPF cuenta con una versión on-premise (Singh, 2020) adaptada de OwnCloud, llamada Nube, que posee las características antes mencionadas y permite al organismo no depender de servicios externos, como por ejemplo Dropbox o Google Drive, garantizando seguridad de los archivos almacenados y control sobre el dimensionamiento de la capacidad almacenamiento.

FFMPEG

Framework con licencia open source que contiene utilidades para “*decodificar, codificar, transcodificar, multiplexar, demultiplexar, transmitir, filtrar*” (FFmpeg, 2022) formatos multimedia. Además, su aplicación no se supedita a algún SO en particular, sino que es soportado por múltiples plataformas.

WebRTC

Es una API que permite las comunicaciones de audio/video o multimedia en tiempo real. Las tecnologías detrás de WebRTC se implementan como un estándar web abierto y están

disponibles como API de JavaScript normales en todos los navegadores principales. En el caso de los clientes nativos, como las aplicaciones para iOS y Android, hay una biblioteca disponible que proporciona la misma funcionalidad. El proyecto WebRTC es de código abierto y es compatible con Apple, Google, Microsoft y Mozilla, entre otros (Google Developers, 2022).

Solicitudes a áreas intervinientes

Jitsi precisa de recursos que en la organización son administrados por distintas áreas (véase Anexo A), por lo que es necesaria su colaboración para ejecutar el proyecto. A continuación, se detallan las incumbencias de cada sector a efectos de esclarecer las tareas de su competencia, la cuales fueron aceptadas previamente en el acta de constitución del proyecto.

Seguridad Informática

En primer lugar, es necesario consultarle a Seguridad Informática (SI) cuáles son los datos que se deben proveer para conseguir la comunicación de la plataforma hacia afuera de la infraestructura de red del organismo.

En segundo lugar, se solicitará la apertura de distintos puertos, los que se indicarán oportunamente en la fase pertinente. Lo mismo tendrá que hacerse para el servidor Coturn privado.

SI también debe proveer de dos IP públicas estáticas, una con el fin de realizar pruebas temporales fuera de la DMZ y otra ya en un entorno productivo con todas las barreras de seguridad. Con ello se podrá determinar el desempeño de Jitsi cuando su tráfico se vea afectado por las medidas de seguridad del organismo (transmisión de paquetes a través de proxy y firewall, por ejemplo).

Operaciones

Se le solicitará al área de Operaciones la provisión de servidores base, utilizando las especificaciones del acta, con la finalidad de iniciar la instalación de Jitsi.

También serán los encargados de habilitar los permisos de relay de emails (IONOS Cloud S.L.U., 2019), asignar equipos virtualizados con VMWare, contenedores (dockers) y cuota (Real Academia Española, s.f., definición 1) de almacenamiento en los NAS del organismo, para alojar las grabaciones de las salas del módulo de Jibri.

Asimismo, operaciones es el área encargada de la configuración de las DNS para el FQDN que le corresponde al sistema de videoconferencia, siendo en este caso el elegido “videoconferencias.mpf.gov.ar”.

Otro elemento que debe proveer esta área es el certificado de confianza para nuestro subdominio⁹.

Por otra parte, deben efectuar el alta de un usuario llamado “jibri” dentro del dominio, que funcionará tanto para el servidor de grabaciones como para acceder al NAS donde se alojarán las mismas.

Finalmente, proveerán de espacio o cuota en Nube del MPF con el objetivo de persistir y compartir las grabaciones realizadas en cada sala, aprovechando las funcionalidades de envío de archivos que son parte de la aplicación.

Infraestructura

La tarea de esta área se limitará a asignarnos espacio físico en los racks, en caso de ser necesario, para alojar servidores que provea Operaciones. Deberán también realizar las interconexiones de cableado necesarias para el equipamiento.

Aplicaciones

Principalmente se encargará de la modificación del front end de Jitsi, otorgándole el look and feel (Cambridge University Press, s.f., definición 1) definitivo. También cooperarán como área de consulta de ser necesario.

Mesa de Ayuda / Soporte

Serán los encargados de asistir a los usuarios con información sobre el uso de la plataforma, agendar las reuniones y reportar problemas y/o fallas que puedan aparecer en Jitsi. Su rol es muy importante debido a la insuficiencia de recursos técnicos, para ejecutar servicios de grabación en forma masiva, por lo que deberán efectuar un control en el uso de las videoconferencias que deban registrarse mediante grabaciones de audio y video con Jibri.

Fase 1 - Instalación y funcionamiento en entorno DEV físico.

Aspectos generales

En la primera fase se verificará el funcionamiento de Jitsi a través de una instalación básica tal y como se descarga del repositorio oficial, para corroborar el correcto funcionamiento del conjunto de aplicaciones que conforman el sistema de videoconferencia (Jitsi, Jicofo, VideoBridge y Prosody). En otras palabras, no se configurarán módulos o funcionalidades que deban agregarse por separado a la instalación básica.

⁹ No se solicita como requisito en el SOW ya que es un certificado que el organismo tramita de todas formas, como se explica en el punto 3.6.

Para esta instalación, solo se deberán realizar pruebas en una red local exclusiva, conformada por las computadoras del área de Tecnología.

También es importante para evitar los problemas que puedan llegar a ocasionarse con máquinas virtuales, realizar la instalación inicial de Jitsi sobre un servidor físico.

Es importante recalcar que el FQDN de nuestro sitio de videoconferencias es “videoconferencias.mpf.gov.ar”, ya que será requerido a futuro, no solo por la aplicación de videoconferencias para diversas configuraciones, sino que también a causa de los certificados SSL.

La instalación de Jitsi se realizará sobre Ubuntu 18.04 instalado previamente en el servidor provisto por Operaciones, siguiendo los pasos como se detallan en el sitio oficial ¹⁰. Los elementos necesarios para el armado del entorno de esta etapa se encuentran detallados en el capítulo 4.

Pruebas

Las pruebas principales a realizar en esta etapa con Jitsi son:

Nivel de coincidencia entre las instrucciones de instalación y el entorno seleccionado: Si bien las instrucciones para el entorno seleccionado se encuentran en la web oficial, debe corroborarse que las pequeñas variaciones de hardware u otras aplicaciones presentes en el servidor afecten el proceso de instalación.

Conectividad: cómo afecta la realización de una videoconferencia al ancho de banda de datos.

Calidad multimedia: como se ve y se oye efectivamente con nuestro entorno para una configuración de resolución de 720p.

Navegadores compatibles.

Fase 2 - Entorno DEV sobre VMWare

Aspectos generales

Este escenario es una réplica del planteado en la Fase 1, e incorpora los elementos solicitados en el punto “Solicitudes a áreas intervinientes”, lo cual permitirá principalmente que realicemos pruebas de comunicación con dependencias.

La implementación en este caso se realizará a través de la herramienta VMWare, realizando la virtualización en un entorno con las especificaciones que se mencionan en el Capítulo 4 – Recursos técnicos.

¹⁰ <https://jitsi.github.io/handbook/docs/devops-guide/devops-guide-quickstart>

La instalación del SO será realizada por Operaciones como para el caso anterior, y Tecnología realizará la instalación de Jitsi siguiendo los pasos de su sitio oficial.

Pruebas

En esta etapa, se replicarán las pruebas ejecutadas anteriormente en la Fase 1.

Fase 3 - Securización de videoconferencias

Aspectos generales

Uno de los puntos pilares de la presentación de este proyecto es la seguridad y el control sobre la plataforma de videoconferencias en lo relativo a la confidencialidad de información que por ella se maneja. Lo ítems que se listan debajo son aquellos que permiten establecer barreras de control específicamente sobre Jitsi.

El uso de certificados de confianza también es parte de la seguridad, pero se encuentra englobado en Solicitudes a áreas intervinientes - Operaciones, dado que es parte de una condición general que aplica a todos los sitios publicados por el organismo. Su implementación se puede encontrar en la web¹¹ y no se agrega a un Anexo o al cuerpo del presente trabajo, ya que son instrucciones específicas.

En esta etapa, se reutilizará el entorno instalado para la Fase 2.

Denominación segura de las salas

El nombre de las salas será la barrera final para proteger el acceso a las videoconferencias. Se establece que las salas deben nombrarse del siguiente modo:

“[https://videoconferencias.mpf.gov.ar/\[CÓDIGO\]_\[NOMBREDEUSUARIO\]](https://videoconferencias.mpf.gov.ar/[CÓDIGO]_[NOMBREDEUSUARIO])”

En dónde CÓDIGO es una cadena aleatoria¹² de caracteres alfanuméricos de 0 a 9 y de a hasta z incluyendo mayúsculas y NOMBREDEUSUARIO es el usuario de red del dominio. Este modo de identificar las salas tiene dos objetivos, el primero es el de evitar accesos accidentales a las salas, incluso para que el mismo usuario que hubiese realizado una VC anteriormente. En segundo lugar, al poseer la sala el nombre del usuario solicitante, se torna más simple la asociación para el envío automatizado de grabaciones.

Autenticación LDAP

La restricción en la creación de salas es uno de los controles claves a aplicar sobre Jitsi. Para lograrla, contamos con dos métodos indicados por los desarrolladores, para identificar

¹¹ <https://www.ssl.com/how-to/install-ssl-certificate-on-nginx/>

¹² No se establece para este trabajo ningún método para la generación de la cadena de caracteres, pero una web simple que realiza esta tarea es <https://pinetools.com/es/generador-cadenas-aleatorias>.

usuarios de dominio: LDAP2 y Cyrus SASL. Si bien ambas tecnologías son válidas, para nuestra implementación del sistema, se utilizarán las instrucciones de LDAP2, ya es el modo de autenticar usuarios que se encuentra presente en una mayor cantidad de versiones de Jitsi, lo que asegura estabilidad y compatibilidad con Prosody.

Por otra parte, la autenticación habilita a los técnicos de Mesa de Ayuda a asignar de permisos de acceso a usuarios del dominio, con el objetivo de iniciar una videoconferencia y ser anfitrión (Zoom Video Communications, Inc, 2021) de la misma. El usuario habilitado debe agregarse a un grupo de seguridad del dominio.

La configuración general se encuentra en el Anexo G.

Persistir contraseña de ingreso a las salas

Agregar contraseñas permite añadir un nivel extra de privacidad que evita el acceso de participantes no deseados.

Originalmente, tanto la sala como la contraseña que se establece para la misma, se eliminan al momento de finalizar la VC.

Para este proyecto, se determinó que es necesario preestablecer contraseñas a las salas, a efectos de que los usuarios posean salas seguras.

La funcionalidad de añadir contraseñas para la sala le pertenece a Prosody dentro de la estructura del sistema de VC y como se mencionó anteriormente, es un componente externo¹³ al desarrollo de Jitsi, motivo por el cual tiene sus propios elementos de configuración llamados “módulos”. Dentro de estos módulos es donde se deben colocar los parámetros para persistir las contraseñas.

La asignación de contraseña se realiza creando una sala y accediendo a la opción de seguridad, pero esto se verá más adelante, cuando se detalle el procedimiento de reserva y asignación de salas.

Las configuraciones necesarias para la implementación de dicho módulo se encuentran en el Anexo H.

Servidor TURN y STUN con NAT y DMZ

En el punto 2.2 se muestra una introducción acerca de los servidores de redireccionamiento para WebRTC y se hace referencia a la posibilidad de utilizar uno (STUN) de ellos o ambos (STUN + TURN), dependiendo de la estructura o configuración de la red. La aplicación de estos componentes del framework ICE, aportan los medios necesarios para lo

¹³ <https://prosody.im/doc>

que se puede llamar “publicación” de Jitsi, que no es ni más ni menos que asignar las rutas necesarias para que se pueda acceder al sistema de videoconferencias de forma tanto interna como externa.

La guía para la configuración del servidor TURN para Jitsi, se encuentra en el Anexo I.

Pruebas

Las pruebas de este punto son centrales para mantener segura a la plataforma. Los principales aspectos a tener en cuenta son:

Certificado de confianza: Comprobar si la plataforma funciona con HTTPS.

Denominación segura de salas: Probar la creación de salas con diversos nombres y símbolos para establecer si hay algún carácter inadmitido.

Autenticación LDAP: Verificar el acceso de usuarios del MPF.

Persistir contraseñas: Crear salas y salir, previamente estableciendo una contraseña.

STUN y TURN: Comprobar el acceso a la plataforma. El acceso fuera de la DMZ ya fue solicitado en el punto Solicitudes a áreas intervinientes – Seguridad Informática.

Pruebas con dependencias.

Fase 4 – Módulo de grabación

Aspectos generales

A lo realizado en el entorno de la Fase 3, se agrega el módulo de Jibri¹⁴ con el objetivo de grabar la VC en el caso de que el usuario lo requiera. Esta funcionalidad debe brindarse a causa de que en el ámbito donde se implementará la solución, será necesario mantener un registro audiovisual de los participantes, cuya intervención tendrá validez de declaración formal ante la ley.

Es importante que Jibri se encuentre en otro entorno diferente al de los otros módulos (Jitsi Video Bridge, Jicofo, etc.) y que de existir otras aplicaciones en dicho entorno no se utilicen dispositivos de audio y/o video.

Al configurar un módulo de Jibri para esta fase y para el presente proyecto en general, solo se podrá realizar una grabación de sala a la vez.

Jibri se integra como grabadora emulando a un participante, pero en modo oculto. Por ende, se deben agregar y modificar parámetros en Prosody, Jicofo y Jitsi Meet y también verificar que exista el usuario “Jibri” y el grupo “JIBRI” (puede ser cualquier usuario, pero por

¹⁴ <https://github.com/Jitsi/Jibri>

una cuestión de simplificación en la visualización y asignación de permisos, los utilizaremos de ese modo).

La implementación de Jibri se desarrolla en el Anexo J.

Pruebas

Los puntos a considerar para ser verificados en esta fase son los siguientes:

Grabación con dos (2) participantes sin contraseña de sala.

Grabación con dos (2) participantes con contraseña de sala.

Grabación con tres (3) o más participantes con contraseña de sala.

Grabación con tres (3) o más participantes con contraseña de sala.

Tamaño de las grabaciones.

Recursos de hardware utilizados.

Fase 5 – Instalación de Jibri en docker

Aspectos generales

En las fases previas se establece el uso de equipos físicos y la virtualización completa de un servidor, con la finalidad de verificar el comportamiento de Jitsi, además de la interacción con sus módulos adicionales.

Es necesario que a medida que se conocen las capacidades del sistema, los insumos necesarios para su implementación deban ajustarse, eliminando o reduciendo equipamiento, por esa razón en la Fase 4 se estableció una prueba para determinar el tamaño de archivo de grabación por ejemplo. Por otra parte, la reducción de recursos se encuentra limitada a causa del requisito expreso de los desarrolladores de alojar al módulo de grabaciones separado del core (The Computer Language Co Inc., s.f., definición 1).

La solución que media entre la exigencia de los desarrolladores y la limitante u optimización de recursos es la de implementar un contenedor en alojado en docker, obteniendo ventajas tales como:

Reducción de espacio físico en uso.

Escalabilidad.

Mayor control.

Robustez para el servicio de grabación.

Menor consumo de memoria, disco y procesador.

En esta fase se detendrá el servicio de Jibri instalado en el servidor durante la Fase 4 y se procederá a instalar Docker para ejecutarlo desde allí, siguiendo los pasos que se indican en el Anexo K.

Pruebas

Las pruebas necesarias para dar como cumplida esta fase son:

Funcionamiento de Docker.

Ejecución de pruebas Fase 4.

Fase 6 – Automatización de envío de grabaciones

Aspectos generales

La fase número 6 es otra de las fases clave y la que diferencia esta implementación de Jitsi, ya que marca un nivel especial de personalización.

Las grabaciones que se realizan de las VC deben ser únicamente accesibles por aquellos que oficiaron las mismas como anfitriones, a los efectos de ser confidenciales.

Por supuesto, tampoco es correcto que el usuario acceda a la ubicación real del archivo dentro de los servidores, sino que el mismo debe poseer la capacidad de auto-gestionar sus archivos mediante alguna interfaz u aplicación.

La solución propuesta integra varios aspectos técnicos que se describen en los párrafos siguientes, pero con el objetivo de facilitar la comprensión de la misma, se establece que la automatización consta del siguiente proceso:

1. Almacenamiento de archivo de video en servidor Jibri.
2. Copia del archivo al NAS del MPF.
3. Carga del archivo a la Nube del MPF.
4. Envío de mail con link de descarga del archivo de video al anfitrión, protegido con contraseña.

El medio que proporciona Jibri para conseguir un correcto ensamble de la secuencia antedicha, es la aplicación de un script (Oxford University Press, s.f., definición 5), cuya ejecución se realiza cuando se completa correctamente el guardado del archivo grabado.

Integración con otros sistemas

A causa de cómo fue originado y para su funcionamiento, Jitsi entrecruza tecnologías variadas que utiliza con distintos fines. Particularmente, se hará uso de otros protocolos como por ejemplo de almacenamiento, para cumplimentar el objetivo del proyecto y resolver aspectos que no son considerados en la instalación base de Jitsi.

NxLog

Ser anfitrión de una sala implica que a ese usuario determinado se le asignaron permisos para administrar a los participantes e iniciar una grabación, atribuciones que están reservadas

para aquellos miembros del MPF que deban tomar declaraciones a víctimas, testigos e imputados. Por ello, es de suma importancia que las grabaciones sean enviadas unívocamente al anfitrión.

Lamentablemente, jicofo no provee de una propiedad que almacene este dato y la comparta con los otros módulos, ya que para el funcionamiento de Jitsi como plataforma no es necesario.

El modo de resolver esta dificultad es instalando en el servidor de Jitsi el cliente de la aplicación utilizada por el área Seguridad Informática, NxLog. A través del servicio que ejecuta NxLog, se puede acceder a los registros o logs determinados por configuración y enviar esa información a otra ubicación, en este caso el script, para su uso.

Archivos

Los sistemas que administran el almacenamiento de archivos dentro del MPF son gestionados con software de Windows Server y un sistema de archivos NTFS, pero como se especificó con anterioridad, Jitsi funciona en un SO Ubuntu. Para sortear esa dificultad, se recurrirá al uso del protocolo CIFS, montando la unidad de red correspondiente dentro del SO que contiene Jitsi. La compatibilidad de los sistemas de archivos es absolutamente necesaria para compartir archivos de configuración y neurálgica para el proceso de envío de grabaciones.

Nube

Para conseguir la carga del video correspondiente a Nube, dentro del script de finalización de grabación de Jibri, se debe hacer uso del api que permite crear links compartidos de descarga públicos (The ownCloud developers, 2011-2023). Es necesario que sean públicos ya que puede ser necesario que el usuario destinatario del video lo comparta con individuos que no se encuentran registrados en el MPF. Los parámetros de configuración de caducidad y usuarios compartidos que se agregaron en el archivo finalize.sh, fueron provistos por Operaciones. El protocolo utilizado por Nube para la distribución de archivos es WebDav (Whitehead, 2010).

Mail

Para conseguir que el usuario obtenga el link con el video alojado en Nube, se debe transmitir el mismo vía email, pero de un modo automatizado. Como ya se dijo en párrafos anteriores, la automatización estará desarrollada en el script de finalización, pero ello no incluye a la plantilla que dará estructura al mail que se enviará.

La plantilla será creada con formato de HTML, y se agregarán los valores necesarios para el envío (link y usuario destinatario) como parámetros del script principal.

Asimismo, el uso del mail no se remitirá únicamente al envío de la notificación del link de descarga de la/las grabaciones, sino que también se informará por esa vía:

Nombre de sala incorrecto.¹⁵

Errores de carga del archivo con la grabación a Nube.

Todas las configuraciones y procedimientos pertinentes se encuentran en el Anexo L.

Pruebas

Para esta fase se establecen las siguientes pruebas, que cubren todo el proceso descrito:

Creación, copia y modificación de archivos desde Windows a Ubuntu y viceversa.

Descarga de grabación desde nube.

Envío de mails.

Finalización de las etapas de pruebas parciales

Es de vital importancia que, al finalizar esta fase, sean dados de baja todos aquellos entornos considerados de pruebas que hayan sido utilizados hasta el momento, siendo esto necesario para que no se suscite ningún inconveniente con la implementación en el entorno de pruebas de usuarios finales.

Fase 7 – Adecuación de Jitsi y publicación en UAT

Aspectos generales

La última fase de intervención técnica por parte del área de Tecnología será la presente, en la que finalmente se cederá de forma completa la administración del alojamiento de la aplicación., pero aún la configuración de Jitsi depende de Tecnología.

En esta etapa, toda la estructura de Jitsi será volcada en un entorno de pruebas administrado por operaciones, pero con toda la funcionalidad de un entorno operativo.

Aplicaciones

Cuando sean culminadas las fases de pruebas internas, es decir sin intervención de los usuarios finales, se procederá con la adecuación para la presentación y administración de la plataforma. Para ello, en primer lugar, se le solicitará a Aplicaciones que efectúe los cambios en la interfaz, tanto en la de Jitsi como en el formato que tiene el mail automatizado, agregando los colores, tipografía y logo del Ministerio.

¹⁵ No respeta el formato establecido en la Fase 3 – Denominación segura de las salas

Operaciones

Una vez modificado el look and feel, se le solicitará a Operaciones que realice la reinstalación de la plataforma en servidores y dockers UAT. Las instrucciones que deberán seguir son las establecidas en el presente proyecto, guiándose con los Anexos.

Seguridad Informática

Se deben habilitar las reglas necesarias para que Jitsi tenga acceso desde internet, con el fin de proporcionar un entorno de pruebas completo, que coincida con la implementación final.

Mesa de Ayuda

Mesa de Ayuda intervendrá a partir de este punto, asistiendo a los usuarios, entregándoles el instructivo de uso de Jitsi y a su vez agendando y preparando las salas. Ambos instructivos se encuentran en el Anexo M.

Pruebas

Ya contando con el sistema publicado hacia el exterior de la LAN, se realizarán pruebas de funcionamiento teniendo en cuenta los siguientes puntos:

Conferencia con dos (2) participantes de alguna de las dependencias de la Fase 2.

Conferencia con tres (3) o más participantes de alguna de las dependencias de la Fase 2.

Grabación de la videoconferencia y recepción de link de descarga de Nube.

Pruebas de gestión de salas con Mesa de Ayuda.

Fase 8 – Implementación en entorno productivo

Aspectos generales

La fase final del desarrollo del ciclo de vida del proyecto es su publicación en un entorno productivo. Se define como entorno productivo a la instalación del sistema dentro de la estructura del/los datacenter/s (Cisco Systems, Inc., s.f.) productivos de aplicaciones y al pase de la administración total de Jitsi a las áreas destinadas para el control y alojamiento de las mismas.

De aquí en adelante Tecnología solo se encargará de la verificación de actualizaciones y novedades al respecto de Jibri, pero sin intervenir en su implementación.

Seguridad Informática

El paso final es la publicación detrás de la DMZ y con la IP pública proporcionada por esta área. La modificación de la misma en la configuración será realizada ahora por Operaciones, tal como fue expresado la Fase 7.

Dirección de Informática

Se enviará una nota a la dirección, dando aviso de la conclusión de la implementación. Esta nota tiene como objetivo la difusión de la plataforma por medio de un canal formal, el cual será utilizado por el director para elevar la notificación a la Secretaría General de Administración y Recursos Humanos.

Pruebas

A tratarse de la última etapa, deberán ejecutarse las mismas pruebas que para la Fase 7.

Resumen

En el capítulo 2 se detallan las etapas necesarias para la implementación del proyecto de videoconferencia, desde la conformación del acta de constitución, pasando por la búsqueda de información acerca de las tecnologías que se utilizarán en el desarrollo y concluyendo con las fases necesarias para la implementación final de Jitsi. Se eligió la separación por fases para brindar una delimitación más clara de las actividades, conformadas desde la etapa pruebas hasta implementación final.

Capítulo 4

Determinación de recursos

El presente capítulo está destinado a la organización de los elementos de hardware que serán necesarios, con el fin de que sean visualizados de un modo más simple.

Recursos técnicos

Son todos aquellos recursos de origen informático, organizados según su fase correspondiente.

Fase 1

Tabla 4

Servidor Fase 1

Servidor Físico	
Disco Rígido	80GB
Memoria RAM	4GB
CPU	4 Cores
Sistema Operativo	Ubuntu 18.04
Interfaz de red	10/100/1000
Aplicaciones	Servidor Nginx
Equipamiento de Red	
Switch	10/100/1000
Otros	
Certificado SSL	

Fase 2

Tabla 5

Servidor Fase 2

Servidor Virtual	
Disco Rígido	80GB
Memoria RAM	4GB
CPU	4 Cores
Sistema Operativo	Ubuntu 18.04
Interfaz de red (virtual)	10/100/1000
Aplicaciones	Servidor Nginx, NXlog
Otros	
50GB de espacio reservado en un NAS	

Fase 3

La Fase 3 no presenta requisitos técnicos de configuración y/o equipamiento, a causa de que las pruebas necesarias se realizarán en el entorno montado para la Fase 2.

Fase 4

Seguridad Informática:

Para esta etapa se solicitará la apertura de los puertos establecidos en la Tabla 6 (8x8 Inc., 2022):

Tabla 6

Puertos a abrir

Puertos	
80 TCP	Para verificación/renovación de certificado SSL.
443 TCP	Para acceso general a Jitsi Meet
10000 UDP	Para comunicaciones generales de video/audio en red.
22 TCP	Si se accede al servidor mediante SSH. Por lo general este es el puerto por defecto, pero es configurable en la aplicación.

Operaciones:

Tabla 7

Servidor Fase 4

Servidor Virtual (no docker)	
Disco Rígido	80GB
Memoria RAM	4GB
CPU	4 Cores
Sistema Operativo	Ubuntu 18.04
Interfaz de red (virtual)	10/100/1000

Fase 5

Para esta fase no se requerirá ningún equipo o configuración en particular. La instalación de Docker y la posterior creación del contenedor que alojará Jibri se realizarán sobre el mismo servidor que en la Fase 4.

Fase 6

En esta fase se requerirá que Operaciones cree un usuario “jibri” dentro del AD del MPF, para que sea el mismo que accede a través de SMB desde las carpetas de Ubuntu en dónde Jibri almacena las grabaciones, al NAS de dónde finalmente serán compartidas las grabaciones.

Adicionalmente se solicitará permiso de mail relay a Operaciones también, para la IP que posee el servidor de Jibri.

Fase 7

Seguridad Informática.

Al área de seguridad informática se le requerirán los siguientes elementos y procedimientos:

Una (1) un IP pública para el acceso la plataforma, tanto interno como externo.

Una (1) IP pública para el funcionamiento de Coturn

Redireccionar el tráfico de datos a través de la DMZ para proporcionar seguridad a la plataforma.

Apertura de los puertos requeridos en la Fase 4.

Operaciones.

Tabla 8

Servidor Fase 8

Servidor Virtual	
Disco Rígido	80GB
Memoria RAM	4GB
CPU	4 Cores
Sistema Operativo	Ubuntu 18.04
Interfaz de red (virtual)	10/100/1000
Aplicaciones	Servidor Nginx, NXlog
Otros	
50GB de espacio reservado en un NAS ¹⁶	

Se le debe solicitar a Operaciones la instalación de Jitsi y de Jibri dentro de un entorno UAT.

Para realizar el procedimiento de forma adecuada, deberán remitirse a los Anexos desde I hasta L inclusive, en los cuales figuran todos los pasos de forma ordenada.

Finalmente, deberán asociar el DNS “videoconferencias.mpf.gov.ar” a la IP brindada.

Aplicaciones.

El área de aplicaciones accederá a los archivos de UI de la aplicación y modificará los puntos establecidos en el Anexo N.

Fase 8

¹⁶ Esta capacidad puede variar luego de la implementación, conforme se utilice la plataforma y/o se realicen distintas configuraciones de audio y video.

Operaciones

Se deben repetir los recursos establecidos para la fase anterior, pero en un entorno productivo, tanto para Jitsi (en servidores de aplicaciones) como para Jibri (en los administradores de contenedores).

Recursos humanos

Para tener una idea clara de quien será responsable en cada una de las acciones establecidas en el Capítulo 2, se utilizará una herramienta RAM. Las herramientas RAM están definidas en el PMBOK como tablas o matrices en las cuales se ilustra la relación entre actividades y miembros del proyecto (Project Management Institute, Inc., 2013), siendo en este caso las áreas completas.

Matriz RACI

La herramienta RAM seleccionada para este proyecto es la matriz RACI de alto nivel (Project Management Institute, Inc., 2013), de modo que sea simple la visualización de que responsabilidad ostentará cada sector. Que la Matriz sea de alto nivel refleja lo dicho anteriormente al respecto de la utilización de áreas completas para la asignación de actividades, en lugar de individuos. La Tabla 9 refleja la distribución final.

Tabla 9

Matriz RACI

Acciones a realizar	Tecnología	Seguridad Informática	Operaciones	Aplicaciones	Mesa de Ayuda
Conformación del acta de constitución del proyecto	R	I	I	I	I
Recopilación de información técnica disponible	R	I	I	I	I
Fase 1 - Instalación y funcionamiento en entorno DEV físico.	A	I	R	I	I
Fase 2 - Entorno DEV sobre VMWare	A	I	R	I	C
Fase 3 - Securitización de videoconferencias	A	R	I	I	I

Acciones a realizar	Tecnología	Seguridad Informática	Operaciones	Aplicaciones	Mesa de Ayuda
Fase 4 – Módulo de grabación	R	C	C	I	I
Fase 5 – Instalación de Jibri en docker	R	I	R	I	I
Fase 6 – Automatización de envío de grabaciones	R	I	C	I	I
Fase 7 – Adecuación de Jitsi y publicación en UAT	A	R	R	R	I
Fase 8 – Implementación en entorno productivo	R	C	R	I	I

Nota. Referencias: R-Responsable, A-Autorizante, C-Consultado, I-Informado.

Resumen

El capítulo 4 abarca los recursos que se necesitan para el desarrollo del proyecto, tanto técnicos como humanos. Los recursos técnicos están separados siguiendo las fases establecidas en el Capítulo 2.

Los recursos humanos también continúan con el sistema de fases del Capítulo 2, pero la distribución se realiza mediante una herramienta llamada Matriz RACI, en la cual se asignan distintos niveles de responsabilidades entre las áreas intervinientes para cada fase.

Capítulo 5

Factores Determinantes de Éxito

Se procederá en los siguientes puntos, a la determinación de variables, elementos, decisiones o causas que puedan intervenir en el desarrollo del proyecto.

Factores Internos

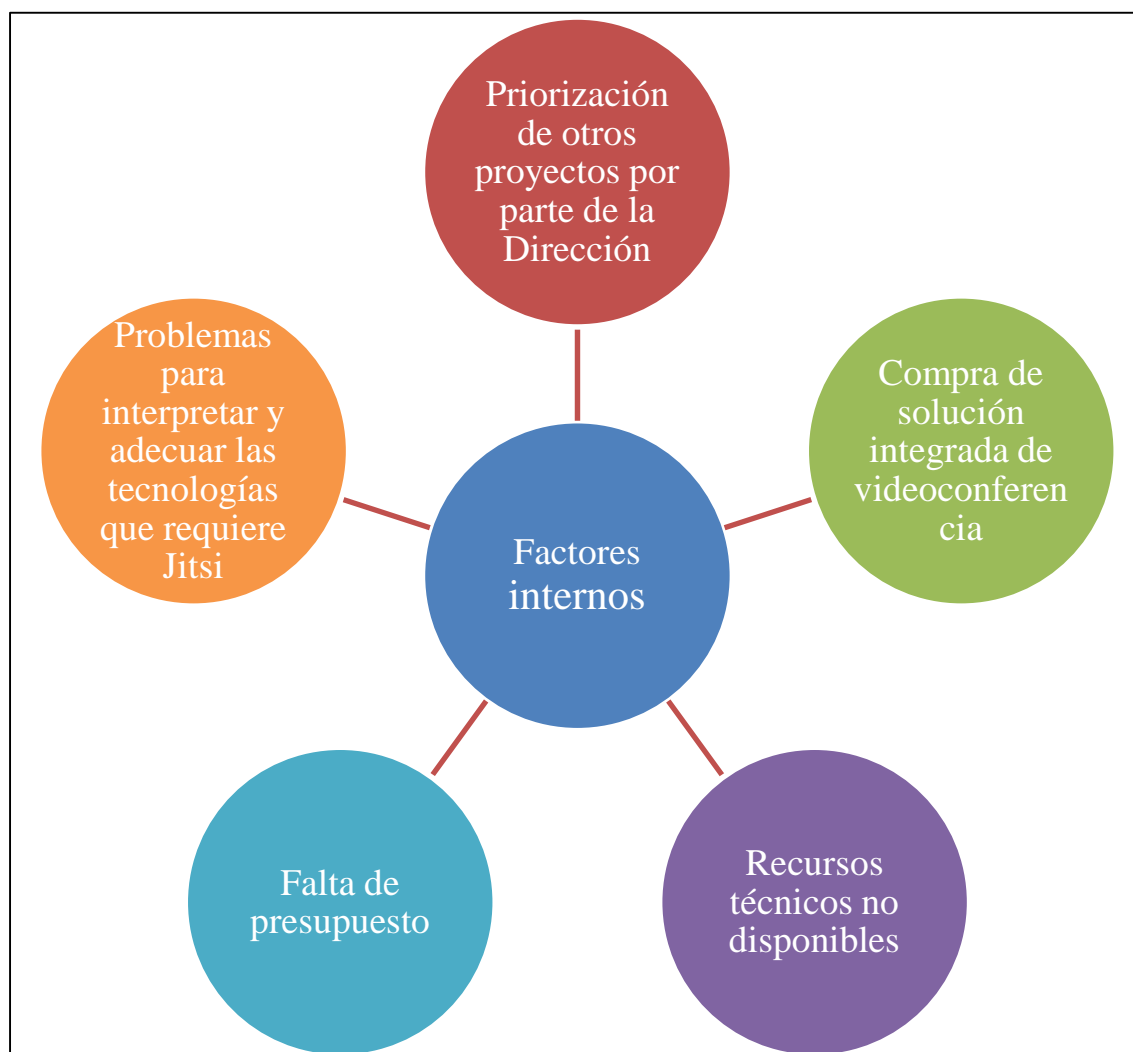
En la Figura 5 se pueden observar los factores internos a tener en cuenta para la evolución del proyecto.

Priorización de otros Proyectos por Parte de la Dirección

Se cuenta con otros proyectos en curso, como por ejemplo la implementación de un nuevo sistema de tickets para Soporte, y se debe establecer que la ejecución de este proyecto reviste de mayor urgencia.

Figura 5

Factores Internos



Problemas Para Interpretar y Adecuar las Tecnologías que Requiere Jitsi

Al tratarse de un sistema de código abierto, es posible que las tecnologías para las cuales fue diseñado no sean las mismas que administran las áreas informáticas del ministerio, como por ejemplo aplicaciones y comandos específicos de Ubuntu o lenguajes de programación.

Compra de Solución Integrada de Videoconferencia

Es posible que dadas las prestaciones iniciales propuestas para el sistema de videoconferencia basado en Jitsi, la Secretaría General de Administración y Recursos Humanos decida la adquisición de licencias de sistemas pagos para áreas puntuales y no para todo el MPF.

Recursos Técnicos No Disponibles

Los equipos de hardware destinados a la infraestructura se encuentran en un proceso de renovación y aquellos que se adquirirán ya cuentan con un objetivo determinado. Si bien se estableció que Jitsi no requiere de servidores de vastas especificaciones, tampoco se pueden utilizar equipos informáticos muy antiguos.

Falta de Presupuesto

Este punto se relaciona con los dos anteriores. El presupuesto para la adquisición de equipos destinados exclusivamente a este proyecto es prácticamente nulo y esto hace necesario seleccionar entre la compra de software pago para usuarios específicos o administrar con el presupuesto disponible los recursos tecnológicos con los que ya se cuenta.

Factores externos

Podemos ver reflejados en la Figura 6 los factores determinantes provenientes del exterior del organismo.

Cambios en la licencia de Jitsi

Los desarrolladores pueden cambiar su política de licenciamiento al ser los autores intelectuales sin previo aviso y establecerla como una aplicación paga, lo que significaría la necesidad de reiniciar el proyecto basado en otro sistema de videoconferencias.

Cambio de Procurador General

La modificación de la autoridad máxima del organismo puede traer aparejada un cambio en cuanto a las directivas de trabajo y procedimientos, además de una posible modificación del personal jerárquico.

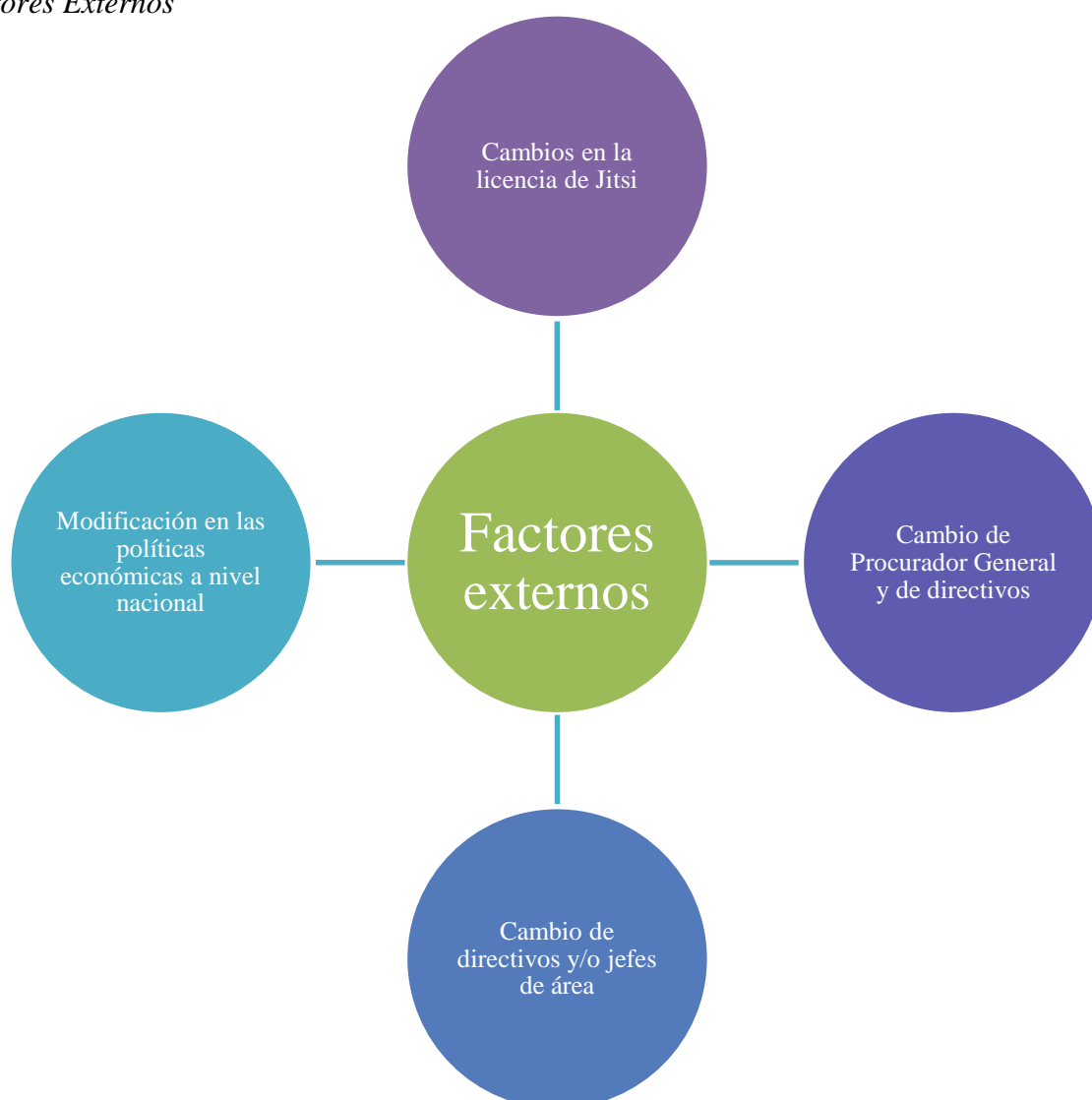
Cambio de Directivos o Jefes de Área

Esto puede suceder aún si no se modifica al Procurador y provocar la cancelación total o retraso del proyecto, ya que al bajar de estratos jerárquicos se tiene mayor control de los trabajos en curso.

Modificación en las Políticas Económicas a Nivel Nacional

Figura 6

Factores Externos



Como el proyecto depende en cierta medida del proceso de renovación del parque informático y mayoritariamente los precios para la adquisición del equipamiento se encuentran en moneda extranjera, si se produjesen variaciones del tipo de cambio o apareciesen restricciones con la importación, podrían producirse importantes retrasos o la cancelación del proyecto.

Resumen

En este capítulo se presentaron los aspectos internos y externos que pueden afectar el desarrollo o inclusive determinar la cancelación del mismo. Los internos son aquellos que provienen directamente de la estructura del MPF y los externos son aquellos que provienen de la administración nacional o del contexto económico.

Capítulo 6

Evaluación del Proyecto

Costos evitables

Dentro de los Capítulos 1 y 4 se enumeran las alternativas pagas para cubrir la demanda de VC, como así también se determinan los recursos que son requeridos para la ejecución del proyecto. Sin embargo, es importante remarcar al momento de realizar la evaluación del general del mismo, que los costos evitables son mínimos, dada la composición de la solución tecnológica (sustentada en equipos ya presentes en la organización y en software open source) y en la mano de obra requerida (las tareas de implementación no afectan el desempeño normal de las áreas involucradas).

Criterios de evaluación de fases de prueba

A continuación, se presentan los resultados que deben obtenerse de la aplicación de las distintas fases de pruebas, para considerar como viable o exitosa la implementación del sistema Jitsi.

Resultados Esperables Para la Fase 1.

Nivel de coincidencia entre las instrucciones de instalación y el entorno seleccionado.

Se espera que utilizando la guía oficial actualizada no se presenten problemas al momento de instalación y ejecución.

Conectividad. No se deben detectar incrementos significativos de consumo en el ancho de banda.

Calidad multimedia. Se debe oír sin distorsión o ruidos de fondo. En cuanto al video debe observarse acorde a la resolución seleccionada, sin pixelado.

Navegadores compatibles. Comprobar el funcionamiento de la plataforma tanto para Chrome como para Firefox y Edge, en sus últimas versiones

Las pruebas detalladas anteriormente deberán hacerse efectivas para una videoconferencia de dos (2) participantes y repetirlas para tres (3) o más.

Resultados Esperables Para la Fase 2.

Nivel de coincidencia entre las instrucciones de instalación y el entorno seleccionado.

Se espera que utilizando la guía oficial actualizada no se presenten problemas al momento de instalación y ejecución.

Conectividad. No se deben detectar incrementos significativos de consumo en el ancho de banda.

Calidad multimedia. Se debe oír sin distorsión o ruidos de fondo. En cuanto al video debe observarse acorde a la resolución seleccionada, sin pixelado.

Resultados Esperables Para la Fase 3.

Certificado de confianza. Ingresar a la plataforma y comprobar que el navegador muestra correctamente la URL con HTTPS, sin dar errores de confianza.

Denominación segura de salas. Crear salas con el formato establecido, utilizando caracteres aleatorios¹⁷.

Autenticación LDAP. Ingresar a la plataforma y autenticarse con un usuario válido. La plataforma debe reconocer las credenciales.

Persistir contraseñas. Jitsi debe solicitar la contraseña que se configuró con anterioridad al reingresar a una sala.

STUN y TURN. Debe ser posible establecer conexiones punto a punto (Felipe, 2021) o P2P (STUN) y de más de tres (3) participantes (TURN) por fuera de la LAN del MPF.

Pruebas con dependencias. Se realizarán en conjunto con agentes de Soporte de distintas jurisdicciones, siendo elegidas dos dependencias por cada una de ellas (a excepción de La Matanza ya que no se encuentran sus fiscalías habilitadas) lo que totalizaría el número de 32 dependencias. Para una mejor comprensión acerca de las jurisdicciones, véase el Anexo F. La Tabla 5 muestra que dependencias son las seleccionadas.

Resultados Esperables Para la Fase 4

Grabación con dos (2) participantes sin contraseña de sala. El sistema debe permitir la grabación sin contraseña sin emitir mensajes de error y la grabación debe almacenarse correctamente en la ruta establecida.

Grabación con dos (2) participantes con contraseña de sala. El sistema debe permitir la grabación sin contraseña sin emitir mensajes de error y la grabación debe almacenarse correctamente en la ruta establecida. La reiteración de esta prueba se realiza con la finalidad de verificar que los módulos de Prosody estén configurados correctamente.

Grabación con tres (3) o más participantes sin contraseña de sala. Ídem que la prueba realizada con dos participantes, pero sirve para descartar problemas con el servidor de Coturn.

¹⁷ Se sugiere nuevamente utilizar <https://pinetools.com/es/generador-cadenas-aleatorias>.

Grabación con tres (3) o más participantes con contraseña de sala. Ídem anterior, con el objetivo de establecer si Coturn y Prosody provocan algún problema/error al ejecutarse en conjunto.

Tamaño de las grabaciones. Realizar una grabación de 1 minuto de duración para todos los casos anteriores, y establecer un tamaño promedio, dividiendo la suma del tamaño total por los 4 modos de grabación.

Recursos de hardware utilizados¹⁸. Realizar una grabación de 1 minuto para los casos de los cuatro primeros puntos e identificar: recursos utilizados antes de la grabación, recursos utilizados durante de la grabación y recursos utilizados posteriormente a la grabación.

Resultados Esperables Para la Fase 5

Funcionamiento de Docker. Se deberá, luego de la instalación ejecutar el comando `docker run hello-world`, con el objetivo de establecer la instalación exitosa de Docker y el funcionamiento de su servicio.

Ejecución de pruebas Fase 4 con Jibri en docker.

Tabla 5

Jurisdicciones Seleccionadas

Jurisdicciones	Dependencia 1	Dependencia 2
Bahía Blanca	Fiscalía General ante la Cámara Federal de Apelaciones de Bahía Blanca	Fiscalía Federal Nº 2 de Bahía Blanca
Capital Federal	Fiscalía en lo Criminal y Correccional Federal Nº 5	Fiscalía Nacional en lo Criminal y Correccional Nº 36
Comodoro Rivadavia	Fiscalía Federal de Comodoro Rivadavia	Fiscalía Federal de Ushuaia
Corrientes	Fiscalía Federal de Paso de los Libres	Fiscalía Federal Nº 1 de Corrientes
Córdoba	Fiscalía Federal de La Rioja	Fiscalía Nº 3 ante los Tribunales Orales en lo Criminal Federal de Córdoba
General Roca	Fiscalía Federal de General Roca	Fiscalía Federal de Zapala
La Plata	Fiscalía Nº 1 ante los Tribunales Orales en lo Criminal Federal de La Plata	Fiscalía Federal de Pehuajó
Mar del Plata	Fiscalía Federal Nº 1 de Mar del Plata	Fiscalía Federal de Dolores
Mendoza	Oficina de Derechos Humanos de Mendoza	Fiscalía Federal de San Juan

¹⁸ Se recomienda utilizar el comando `htop`, <https://www.ubuntu18.com/install-htop-ubuntu-18/>

Paraná	Fiscalía Federal de Paraná	Fiscalía ante el Tribunal Oral en lo Criminal Federal de Concepción del Uruguay
Posadas	Fiscalía Federal de Eldorado	Fiscalía Federal Nº 1 de Posadas
Resistencia	Fiscalía Federal de Resistencia	Jurisdicción de Derechos Humanos de Formosa
Rosario	Fiscalía Federal Nº 3 de Rosario	Fiscalía Federal Nº 2 de Santa Fe
Salta	Sede Fiscal Descentralizada San Ramón de la Nueva Orán	Unidad Fiscal Jujuy
San Martín	Fiscalía Federal de Moreno	Fiscalía Nº 1 ante los Tribunales Orales en lo Criminal Federal de San Martín
Tucumán	Fiscalía Federal Nº 1 de Santiago del Estero	Fiscalía Federal Nº 1 de Tucumán

Resultados Esperables Para la Fase 6

Creación, copia y modificación de archivos desde Windows a Ubuntu y viceversa. Se debe verificar que los archivos de las grabaciones realizadas se encuentren tanto en la ubicación configurada en el contenedor de Jibri como en el NAS.

Denominación segura de salas. Crear salas con nombres que no respeten el formato establecido en el punto Denominación segura de las salas, realizar dos (2) grabaciones de al menos un (1) minuto y esperar recibir el mail con la notificación de este evento.

Carga de grabación a Nube. Solicitar a Operaciones que deshabilite temporalmente el usuario de Nube otorgado, con el objeto que se produzca un error. Realizar dos (2) grabaciones de al menos un (1) minuto y esperar recibir el mail con la notificación de este evento.

Descarga de grabación desde nube. Realizar dos (2) grabaciones de al menos un (1) minuto y esperar recibir el mail con el link y la contraseña de descarga de la grabación.

Resultados Esperables Para la Fase 7

Conferencia con dos (2) participantes de alguna de las dependencias de la Fase 3.

Conferencia con tres (3) o más participantes de alguna de las dependencias de la Fase 3.

Grabación de la videoconferencia y recepción de link de descarga de Nube. Realizar dos (2) grabaciones de al menos un (1) minuto y esperar recibir el mail con el link y la contraseña de descarga de la grabación.

Pruebas de gestión de salas con Mesa de Ayuda. Se le otorgará a M. de A. el instructivo descrito en el Anexo M y se le solicitará que durante los meses establecidos en el cronograma de la Capítulo 3 para la Fase 7, gestione las videoconferencias que le sean requeridas por las dependencias de la Fase 3.

Resultados esperables para la Fase 8

Ídem resultados esperables para la Fase 7.

Resumen

En el capítulo 6 se establecen los criterios a evaluar desde el punto de vista de costos y técnicos. También se hace foco en cada una de las fases propuestas en la Capítulo 2 y cuáles deben ser sus resultados para considerar las pruebas positivas. Las fases 1 a 6 necesitan de resultados que coincidan con el funcionamiento expresado por los desarrolladores para la plataforma y con lo esperado para la infraestructura disponible. La fase 7 establece parámetros esperables en un entorno delimitado con acceso a usuarios, con el fin de obtener una visión de la plataforma en funcionamiento dentro de un ámbito real. La fase 8 insta a realizar las mismas pruebas que la fase 7, pero con el sistema implementado ya en el entorno productivo.

Capítulo 7

Conclusiones

Esta Propuesta de Intervención en el Campo Profesional, es el resultado de la recopilación de información acerca del sistema de videoconferencias Jitsi y su ensamble, comenzando desde la identificación de alternativas y la introducción a las tecnologías utilizadas, atravesando la coordinación entre las áreas y culminando en la implementación concreta de la solución, con las configuraciones y procedimientos adecuados para el MPF.

La distribución que se le dio al trabajo es intencional, ya que permite, desde una mirada rápida, comprender la composición del proceso de implementación y facilita enlazar las acciones que deben realizarse con sus resultados esperados, posibilitando pasar del Capítulo 2 al 6 sin la necesidad inmediata de mayor información. La razón principal de este formato se fundamenta en que, al momento de presentar la propuesta, sea simple para quien debe tomar una decisión, identificar cual es el punto al que se desea llegar con cada acción y que las mismas no queden encasilladas en un contenido abstracto y meramente técnico.

Luego de revisar y analizar los requisitos, tanto técnicos como humanos, que son necesarios para la realización del proyecto, se concluye que el mismo es viable y que no representa un gran esfuerzo para la organización su implementación, superando los beneficios que puede traer contar con un sistema como Jitsi, a las desventajas que pueden aparecer bajo su implementación.

Finalmente, el presente documento fue confeccionado con la intención de que sirva además como elemento de consulta para aquellos que deseen implementar Jitsi en otros entornos, para así facilitar a los interesados el camino a recorrer al efectuar la sistematización de videoconferencias, ya que la información proviene de variadas fuentes y en distintos idiomas.

Acrónimos

API	<i>Application Program Interface</i>
	Interfaz que facilita la comunicación entre programas.
BBB	<i>BigBlueButton</i>
	Software de videoconferencia Open Source.
CIFS	<i>Common Internet File System</i>
	Protocolo de manejo de archivos de multiples plataformas en base a SMB.
DEV	<i>Development stage</i>
	Escenario de pruebas de entorno sin acceso a usuarios finales.
DGDOYNT	<i>Dirección General de Desarrollo Organizacional y Nuevas Tecnologías</i>
	Bloque administrativo que agrupa las áreas pertinentes a la informática dentro de la organización.
DMZ	<i>Demilitarized Zone</i>
	Función de los enrutadores que expone a los equipos de una determinada ip por fuera del firewall.
DNS	<i>Domain Name System</i>
	Sistema que traduce las direcciones ip en FQDN y viceversa
FFMPEG	<i>Fast Foward Moving Pictures Experts Group</i>
	Códec abierto de audio y video.
FQDN	<i>Fully Qualified Domain Name</i>
	Nombre de dominio completo, por ejemplo videoconferencias.com.ar

GNU	<i>Licencia Pública GNU</i>	Tipo de licencia copyleft para desarrollos de código abierto.
GPG	<i>GNU Privacy Guard</i>	Protocolo que provee de encriptado y firma a través de un sistema de administración de claves.
HTTPS	<i>Hyper Text Transfer Protocol Secure</i>	Protocolo basado en HTTP, pero con la incorporación de certificados de autenticidad para realizar conexiones seguras.
IBM	<i>International Business Machines Corporation</i>	Compañía multinacional de hardware, software y servicios informáticos.
ICE	<i>Interactive Connectivity Establishment</i>	Framework que contiene los componentes necesarios para utilizar servidores TURN y STUN.
IP	<i>Internet Protocol</i>	Protocolo que permite la transferencia de paquetes de datos por la red
M. de A.	<i>Mesa de Ayuda</i>	Nivel 1 de soporte al usuario.
MPF	<i>Ministerio Público Fiscal</i>	Reducción del nombre del organismo, para facilitar la redacción.
NAS	<i>Network Attached Storage</i>	Dispositivo dedicado al almacenamiento de información, accesible desde la red.
NAT	<i>Network Address Translation</i>	

Enmascaramiento de direcciones ip internas para accesos externos

NTFS *New Technology File System*

Protocolo de intercambio de archivos de Microsoft.

PMI *Project Management Institute*

Organismo encargado de la investigación y estandarización de procedimientos para el desarrollo de proyectos.

RACI *Responsible (R), Accountable (A),
Consulted (C), Informed (I)*

Matriz de asignación de responsabilidades.

RAM *Responsibility Assignment Matrix*

Denominación genérica para todas las herramientas matriciales de asignación de responsabilidades.

SIP *Session Initiation Protocol*

Protocolo de señalización para comunicaciones.

SMB *Server Message Block*

Protocolo multiplataforma de manejo de archivos.

SO *Sistema Operativo*

Software que administra los recursos de un equipo informático

SOW *Statement Of Work*

Descripción narrativa de los productos, servicios
o resultados que debe entregar el proyecto.

SSH *Secure Shell*

Protocolo de comunicación/ envío de comandos a servidores.

SSL	<i>Secure Sockets Layer</i>	Estándar de seguridad para sitios web
STUN	<i>Session Traversal Utilities for NAT</i>	Protocolo que informa la ip de un dispositivo/navegador punto a punto
TURN	<i>Traversal Using Relay NAT</i>	protocolo para retransmitir tráfico de red para WebRTC.
UAT	<i>User Acceptance Testing</i>	Escenario de pruebas de entorno con acceso a usuarios finales, pero sin ser el sistema completamente funcional.
VC	<i>Videoconferencia</i>	Llamada con video vía protocolos web.
VPN	<i>Virtual Private Network</i>	Acceso a una red privada a través de internet, mediante un usuario y contraseña válido.
WBS	<i>Work Breakdown Structure</i>	Forma organizada de establecer un proyecto en entregables.
WEBDAV	<i>Web-based Distributed Authoring and Versioning</i>	Protocolo para utilizar de forma colaborativa archivos en internet
XMPP	<i>Extensible Messaging and Presence Protocol</i>	Protocolo de mensajería.

Referencias

- Cisco Systems, Inc. (s.f.). *What Is a Data Center?*
<https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html#~distributed-network>
- IONOS Cloud S.L.U. (15 de abril de 2019). *SMTP Relay: qué hay detrás del concepto*. <https://www.ionos.es/digitalguide/correo-electronico/cuestiones-tecnicas/smtp-relay/>
- Oxford University Press. (s.f.). *Oxford Learner's Dictionaries*.
https://www.oxfordlearnersdictionaries.com/definition/english/log_1?q=log
- 8x8 Inc. (2022). *Jitsi Meet*. <https://jitsi.org/>
- 8x8 Inc. (2022). *Jitsi Meet Handbook*. Self-Hosting Guide:
<https://jitsi.github.io/handbook/docs/devops-guide/devops-guide-quickstart>
- Bara, M. (18 de Enero de 2016). *OBS Business School*.
<https://www.obsbusiness.school/blog/make-or-buy-en-proyectos>
- BigBlueButton Inc. (2022). *FAQ*. BigBlueButton Open Source Web Conferencing: <https://docs.bigbluebutton.org/support/faq.html>
- Cambridge University Press. (s.f.). *Cambridge Dictionary*.
<https://dictionary.cambridge.org/dictionary/english/look-and-feel>
- Cloudflare, Inc. (s.f.). *¿Qué es una clave criptográfica?*
<https://www.cloudflare.com/es-es/learning/ssl/what-is-a-cryptographic-key/>
- Cyrus SASL. (2022). *Cyrus SASL*. What is Cyrus SASL?:
<https://www.cyrusimap.org/sasl/>
- Docker Inc. (2022). Docker.com: <https://www.docker.com/>
- F5 Inc. (2022). *Nginx*. What is Nginx:
<https://www.nginx.com/resources/glossary/nginx/>
- Felipe. (5 de octubre de 2021). *Qué es P2P y cómo funciona esta red*.
<https://hostingplus.ar/blog/que-es-p2p-y-como-funciona-esta-red/>
- FFmpeg. (2022). *FFmpeg*. About FFMpeg: <https://ffmpeg.org/about.html>
- Fiscalía General de la Nación de Colombia. (febrero de 2023). *Quiénes somos*.
<https://www.fiscalia.gov.co/colombia/wp-content/uploads/portafolio-de->

servicios-institucionales-Fiscali%CC%81a-General-de-la-Nacio%CC%81n-PUBLICADO.pdf

Google Developers. (2022). *WebRTC*. Comunicación en tiempo real para la Web: <https://webrtc.org/>

Google Developers. (2022). *WebRTC*. Servidor turn: <https://webrtc.org/getting-started/turn-server>

Instituto Nacional de Ciberseguridad. (19 de Septiembre de 2019). *INCIBE*. Qué es una DMZ y cómo te puede ayudar a proteger tu empresa: <https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa>

International Business Machines Corporation. (s.f.). *IBM Docs*. <https://www.ibm.com/docs/es/i/7.2?topic=translation-masquerade-hide-nat>

International Business Machines Corporation. (s.f.). *Virtualization*. <https://www.ibm.com/cloud/learn/virtualization-a-complete-guide>

International Business Machines Corporation. (s.f.). *What are virtual machines (VMs)?* <https://www.ibm.com/topics/virtual-machines>

jitsi.es. (s.f.). *Jitsi Meet*. ¿Cómo utilizar Jitsi Meet?: <https://jitsi.es/como-utilizar-jitsi-meet/#:~:text=Para%20utilizar%20Jitsi%20Meet%20no,dato%20personal%20para%20poder%20utilizarlo.&text=Dentro%20de%20la%20web%20s%C3%B3lo,el%20bot%C3%B3n%20%C2%ABStart%20meeting%C2%BB>

MDN web docs. (23 de febrero de 2023). What is a web server?: https://developer.mozilla.org/en-US/docs/Learn/Common_questions/Web_mechanics/What_is_a_web_server

Microsoft Corporation. (s.f.). ¿Qué es la nube? <https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-the-cloud>

Ministerio Público Fiscal de la Nación. (2022). *Ministerio Público Fiscal*. Qué es el MPF: <https://www.mpf.gob.ar/que-es-el-mpf/>

Murriales, N. (Febrero de 2019). Un espacio de promoción en el ámbito educativo. *La elección de jugar*. Ciudad Autónoma de Buenos Aires, Buenos Aires, Argentina.

- NXLog Ltd. (2022). *Modules and routes*. NXLog Documentation:
<https://docs.nxlog.co/userguide/intro/modules-and-routes.html>
- Olawanle, J. (6 de septiembre de 2022). *freeCodeCamp*. What is a Framework?
 Software Frameworks Definition:
<https://www.freecodecamp.org/news/what-is-a-framework-software-frameworks-definition/>
- Oracle Corporation. (s.f.). *The Java™ Tutorials*. What Is a Socket?:
<https://docs.oracle.com/javase/tutorial/networking/sockets/definition.html>
- ownCloud GmbH. (2022). *ownCloud*. Faq: <https://owncloud.com/faq/>
- Oxford University Press. (s.f.). *Oxford Learner's Dictionaries*.
https://www.oxfordlearnersdictionaries.com/definition/english/script_1?q=script
- Project Management Institute, Inc. (2013). *Guía de los fundamentos para la dirección de proyectos (guía del PMBOK®)* (Quinta ed.). Newton Square, Pensilvania, EE.UU.: PMI Publications.
- Project Management Institute, Inc. (2021). *Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK)* (Séptima ed.). Newton Square, Pensilvania, EE.UU.: PMI Publications.
- Real Academia Española. (s.f.). *Diccionario de la lengua española*.
<https://dle.rae.es/cuota?m=form>
- Real Academia Española. (s.f.). *Diccionario de la lengua española*.
<https://dle.rae.es/enciptar#FABu3oz>
- Real Academia Española. (s.f.). *Diccionario de la lengua española*.
<https://dle.rae.es/fiscal%C3%ADa>
- Sabino, C. (1994). *Como hacer una tesis* (segunda ed.). Caracas, Venezuela: Panapo.
- Singh, H. (13 de febrero de 2020). *Cloud vs. On-Premises Document Solutions: What Does Your Company Need?* <https://info.aiim.org/aiim-blog/cloud-vs-on-premises-document-solution>
- Solabarria, E. (2021). *Cómo hacer proyectos. Cómo hacer proyectos*. (a. p. Bolunta, Ed.) Vizcaya, Bilbao, España.
- SolarWinds Worldwide, LLC. (s.f.). *What Is a Domain Controller?*
<https://www.solarwinds.com/resources/it-glossary/domain-controller>

SonicWall. (s.f.). *What is a Firewall?* <https://www.sonicwall.com/answers/what-is-a-firewall/>

Stagnaro, D., & Da Representação, N. (2012). En carrera: escritura y lectura de textos académicos y profesionales. (U. N. Sarmiento, Ed.) Los Polvorines, Buenos Aires, Argentina.

Temasys. (2022). *Temasys*. Ice and WebRTC What Is This Sorcery? We Explain...: <https://temasys.io/guides/developers/webrtc-ice-sorcery/>

The Computer Language Co Inc. (s.f.). *PCMag*. Definition of core: <https://www.pcmag.com/encyclopedia/term/core#:~:text=A%20core%20program%20would%20be,block%20in%20a%20chip%20design.>

The ownCloud developers. (2011-2023). *ownCloud Documentation*. File Sharing: https://doc.owncloud.com/server/next/admin_manual/configuration/files/file_sharing_configuration.html

VeriSign, Inc. (2022). *Verisign*. Everything You Need To Know About SSL Certificates: https://www.verisign.com/en_US/website-presence/online/ssl-certificates/index.xhtml?loc=en_US#:~:text=SSL%20stands%20for%20Secure%20Sockets,browser%20and%20a%20web%20server.

Visuality Systems Ltd. (2022). *CIFS*. ALL ABOUT CIFS: <https://cifs.com/>

Whitehead, J. (21 de abril de 2010). *webdav.org*. Welcome to WebDAV Resources: <http://www.webdav.org/>

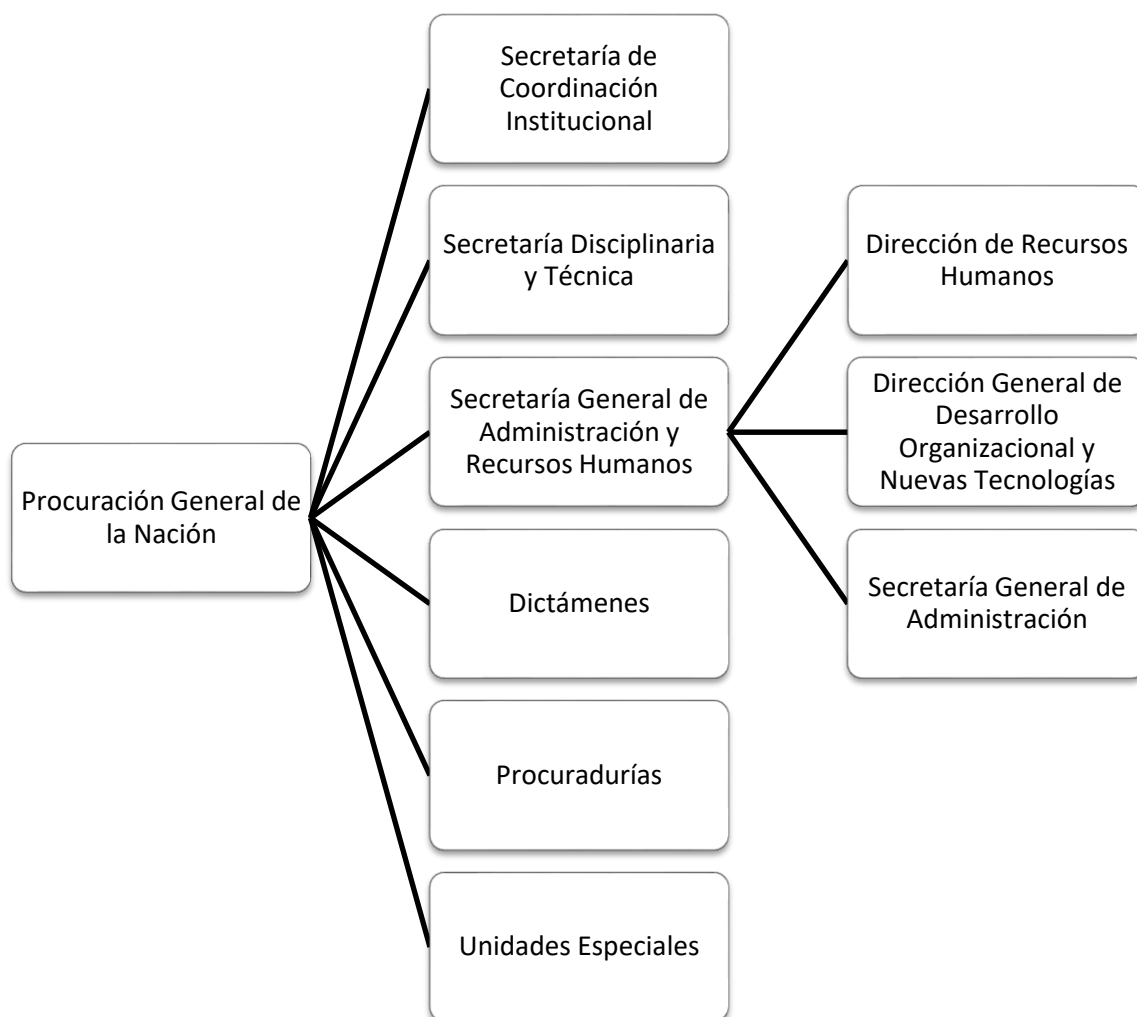
Zoom Video Communications, Inc. (22 de julio de 2021). *Roles en una reunión*. Zoom Soporte: <https://support.zoom.us/hc/es/articles/360040324512-Roles-en-una-reuni%C3%B3n>

Anexo A. Organigrama MPF

En la Figura A1 se puede observar el organigrama completo actual del Ministerio y en dónde se encuentra la Dirección de Desarrollo Organizacional y Nuevas Tecnologías.

Figura A1

Organigrama MPF



Nota: Adaptado de *Organigrama Procuración General de la Nación*, por Ministerio Público Fiscal de la Nación, 2023, MPF (<https://www.mpf.gob.ar/blog/organigrama/procuracion-general-de-la-nacion/>)

Anexo B. Acta de Constitución del Proyecto

Este documento (Tabla B1) es el acta de constitución del proyecto, tal y como se expresó en el cuerpo del trabajo. Los responsables solo están expresados por su cargo y no por su nombre propio.

Tabla B1

Acta de Constitución del Proyecto

Nombre del proyecto									
Solución de videoconferencia Jitsi para el Ministerio Público Fiscal de la Nación									
Descripción general del producto a realizar									
El Ministerio Publico Fiscal de la Nación requiere la implementación de un sistema de videoconferencia, que sea seguro, gratuito y auto-administrable.									
Se realizarán las siguientes etapas, detalladas en este documento de forma abreviada y expandidas en el cuerpo del proyecto:									
	3.1.	Conformación del acta de constitución del proyecto							
	3.2.	Recopilación de información técnica disponible							
	3.3.	Solicitudes a áreas intervinientes							
	3.3.1.	Seguridad Informática.							
	3.3.2.	Operaciones.							
	3.3.3.	Infraestructura.							
	3.3.4.	Aplicaciones.							
	3.3.5.	Mesa de Ayuda / Soporte.							
	3.4.	Fase 1 - Instalación y funcionamiento en entorno DEV físico.							
	3.4.2.	Pruebas							
	3.5.	Fase 2 - Entorno DEV sobre VMWare							
	3.6.	Fase 3 - Securización de videoconferencias							
	3.6.2.	Denominación segura de las salas							
	3.6.3.	Autenticación LDAP							
	3.6.4.	Persistir contraseña de ingreso a las salas							
	3.6.5.	Servidor TURN y STUN on-premise detrás de NAT y DMZ							
	3.6.6.	Pruebas							
	3.7.	Fase 4 – Módulo de grabación							
	3.8.	Fase 5 – Instalación de Jibri en docker							
	3.9.	Fase 6 – Automatización de envío de grabaciones							
	3.9.1.	Aspectos generales							
	3.9.2.	Integración con otros sistemas							
	3.9.3.	NxLog							
	3.9.4.	Archivos							
	3.9.5.	Nube							
	3.9.6.	Mail							
	3.9.7.	Pruebas							
	3.10.	Fase 7 – Adecuación de Jitsi y publicación en UAT							
	3.10.2.	Aplicaciones							
	3.10.3.	Operaciones							
	3.10.4.	Seguridad Informática							
	3.10.5.	Mesa de Ayuda							
	3.10.6.	Pruebas							
	3.11.	Fase 8 – Implementación en entorno productivo							
	3.11.2.	Seguridad Informática							
	1.1.2.	Pruebas							
Propósito/Objetivo									
Implementar un sistema de videoconferencias basado en Jitsi para empleados del MPF.									

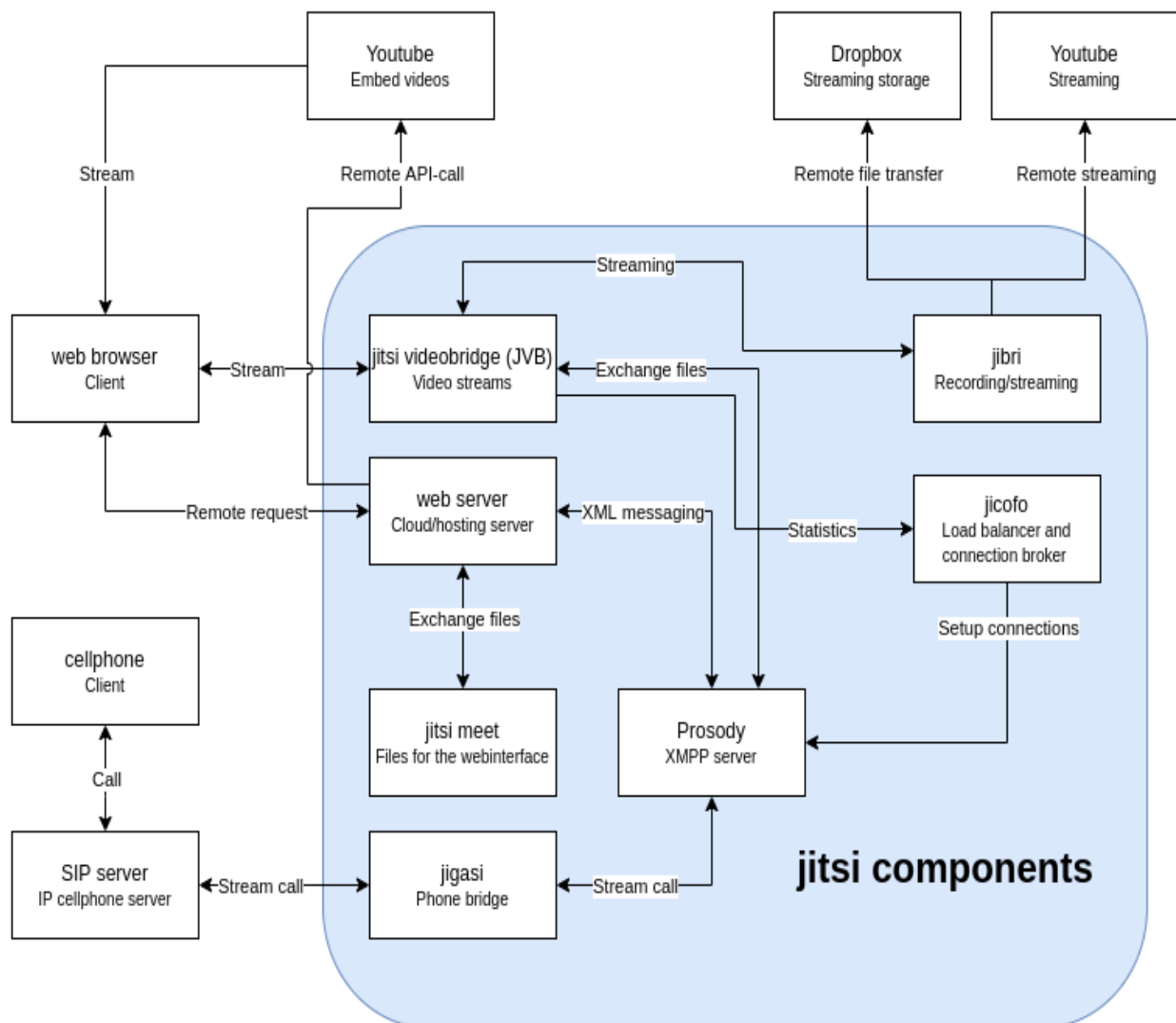
Beneficios previstos						
1. Reducción de costos						
2. Seguridad en las comunicaciones						
3. Personalización de plataforma de videoconferencia						
Tecnología requerida para el desarrollo						
<ul style="list-style-type: none">• Servidores• Infraestructura de red• Apertura de puertos TCP/UDP• Certificados SSL corporativos• Sistema operativo Ubuntu 18.04• Instalación de la aplicación NXLog y• Docker Engine						
Procesos de negocios afectados						
La implementación de esta aplicación afecta de manera positiva al proceso de funcionamiento de las fiscalías, ya que permite que se realice la toma de declaraciones de forma remota, optimizando tiempos y ayudando al cumplimiento de las medidas sanitarias.						
Interesados						
Todo el presonal del Ministerio, con especial énfasis en los agentes de las fiscalías.						
Requisitos						
<ul style="list-style-type: none">• Los jefes de las áreas técnicas implicadas deben prestar colaboración en el momento que les sea solicitado, previa coordinación.• La Mesa de Ayuda debe estar predispuesta para realizar pruebas durante la implementación y debe tener tiempo reservado para la capacitación en su uso para asistir al usuario final.• La Dirección deberá notificar a 5 dependencias de diversas áreas geograficas del territorio nacional, con el objetivo de comprobar el funcionamiento del sistema a través de las distintas rutas de telecomunicaciones• Las dependencias seleccionadas deberan poseer al menos 2 camaras web con micrófono incorporado y definición HD						
NOTA: Los requisitos establecidos en el acta serán ampliados en el punto 5 del presente.						
Entregables						
Entregable		Descripción				
FASE 1		Jitsi cerrado. Sin acceso a LAN ni accesible por usuarios.				
FASE 2		Jitsi cerrado virtualizado. Sin acceso a LAN ni accesible por usuarios.				
FASE 3		Jitsi cerrado virtualizado. Sin acceso a LAN ni accesible por usuarios, pero con mecanismos de seguridad habilitados.				
FASE 4		Jitsi securizado, abierto parcialmente, con acceso a LAN y accesible por usuarios seleccionados.				
FASE 5		Jitsi securizado, abierto parcialmente, con acceso a LAN y accesible por usuarios seleccionados. Modulo de grabación Jibri instalado.				
FASE 6		ídem Fase 5, con script de envío automatizado.				
FASE 7		Publicación de Jitsi en entorno UAT.				
FASE 8		Publicación de Jitsi en entorno PROD.				
Aprobaciones						
Rol	Nombre		Firma			Fecha
Patrocinador	Ripamonti, Gustavo					
Director del proyecto	Jefe de Tecnología					
Mesa de Ayuda	Jefe de Mesa de Ayuda					
Soporte técnico	Jefe de Mesa de Ayuda					
Seguridad Informática	Jefe de Seguridad Informática					
Telecomunicaciones	Jefe de Telecomunicaciones					

Anexo C. Arquitectura Jitsi

En la Figura C1 ubicada debajo, se muestra la arquitectura en bloques de Jitsi y sus componentes, tanto los estrictamente necesarios para propiciar el correcto funcionamiento de la plataforma, como aquellos que cumplen funciones de apoyo o aplicaciones que amplían la funcionalidad.

Figura C1

Arquitectura



Nota: Adaptado de *Architecture*, por 8x8 Inc., 2023, Jitsi Meet Handbook (<https://jitsi.github.io/handbook/docs/architecture/>). Todos los derechos reservados.

Anexo D. Instalación y configuración de NGinx

Para conseguir un correcto ruteo de las peticiones al servidor hacia Jitsi, utilizaremos NGinx como web server (MDN web docs, 2023). Para agilizar y facilitar la instalación del servidor, se detallan debajo los pasos necesarios¹⁹.

Instalar pre-requisitos:

```
sudo apt install curl gnupg2 ca-certificates lsb-release ubuntu-keyring
```

Importar una key (Cloudflare, Inc., s.f.) de firma Nginx oficial para que apt pueda verificar la autenticidad de los paquetes:

```
curl https://nginx.org/keys/nginx_signing.key | gpg --dearmor \  
| sudo tee /usr/share/keyrings/nginx-archive-keyring.gpg >/dev/null
```

Verificar que el archivo descargado contenga la clave adecuada:

```
gpg --dry-run --quiet --import --import-options import-show \  
/usr/share/keyrings/nginx-archive-keyring.gpg
```

La salida debe conter la siguiente

huella 573BFD6B3D8FBC641079A6ABABF5BD827BD9BF62 como se ve debajo:

```
pub      rsa2048 2011-08-19 [SC] [expires: 2024-06-14] \  
          573BFD6B3D8FBC641079A6ABABF5BD827BD9BF62 \  
uid                               nginx signing key <signing-key@nginx.com>
```

Si la huella es diferente, eliminar el archivo.

Para configurar el repositorio apt para paquetes nginx estables, ejecute el siguiente comando:

```
echo "deb [signed-by=/usr/share/keyrings/nginx-archive-keyring.gpg] \  
http://nginx.org/packages/ubuntu `lsb_release -cs` nginx" \  
| sudo tee /etc/apt/sources.list.d/nginx.list
```

Si desea utilizar los paquetes nginx de la línea principal, ejecutar el siguiente comando en su lugar:

```
echo "deb [signed-by=/usr/share/keyrings/nginx-archive-keyring.gpg] \  
http://nginx.org/packages/mainline/ubuntu `lsb_release -cs` nginx" \  
| sudo tee /etc/apt/sources.list.d/nginx.list
```

Configurar el repositorio para elegir los paquetes:

```
echo -e "Package: *\nPin: origin nginx.org\nPin: release o=nginx\nPin- \  
Priority: 900\n" \  
| sudo tee /etc/apt/preferences.d/99nginx
```

Para instalar Nginx usar los siguientes comandos:

```
sudo apt update \  
sudo apt install nginx
```

Debajo se muestra como debería configurarse el archivo videoconferencias.mpf.gov.ar.conf

```
server_names_hash_bucket_size 64;
```

¹⁹ http://nginx.org/en/linux_packages.html#Ubuntu


```

types {
# nginx's default mime.types doesn't include a mapping for wasm
    application/wasm      wasm;
}
server {
    listen 80;
    listen [::]:80;
    server_name videoconferencias.mpf.gov.ar;

    location ^~ /.well-known/acme-challenge/ {
        default_type "text/plain";
        root /usr/share/Jitsi-meet;
    }
    location = /.well-known/acme-challenge/ {
        return 404;
    }
    location / {
        return 301 https://$host$request_uri;
    }
}
server {
    listen 443 ssl;
    listen [::]:443 ssl;
    server_name videoconferencias.mpf.gov.ar;

    # Mozilla Guideline v5.4, nginx 1.17.7, OpenSSL 1.1.1d, intermediate
    configuration
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    ssl_prefer_server_ciphers off;

    ssl_session_timeout 1d;
    ssl_session_cache shared:SSL:10m; # about 40000 sessions
    ssl_session_tickets off;

    add_header Strict-Transport-Security "max-age=63072000" always;
    set $prefix "";

    ssl_certificate /etc/ssl/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.crt;
    ssl_certificate_key /etc/ssl/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.key;

    root /usr/share/Jitsi-meet;

    # ssi on with javascript for multidomain variables in config.js
    ssi on;
    ssi_types application/x-javascript application/javascript;

    index index.html index.htm;
    error_page 404 /static/404.html;

    gzip on;
    gzip_types text/plain text/css application/javascript application/json
image/x-icon application/octet-stream application/wasm;
    gzip_vary on;
    gzip_proxied no-cache no-store private expired auth;
    gzip_min_length 512;

```

```

location = /config.js {
    alias /etc/Jitsi-meet/videoconferencias.mpf.gov.ar-config.js;
}

location = /external_api.js {
    alias /usr/share/Jitsi-meet/libs/external_api.min.js;
}

# ensure all static content can always be found first
location ~ ^/(libs|css|static|images|fonts|lang|sounds|connection_optimization|.well-known)/(.*)$
{
    add_header 'Access-Control-Allow-Origin' '*';
    alias /usr/share/Jitsi-meet/$1/$2;

    # cache all versioned files
    if ($arg_v) {
        expires 1y;
    }
}

# BOSH
location = /http-bind {
    proxy_pass http://127.0.0.1:5280/http-bind?prefix=$prefix&$args;
    proxy_set_header X-Forwarded-For $remote_addr;
    proxy_set_header Host $http_host;
}

# xmpp websockets
location = /xmpp-websocket {
    proxy_pass http://127.0.0.1:5280/xmpp-websocket?prefix=$prefix&$args;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
    proxy_set_header Host $http_host;
    tcp_nodelay on;
}

# colibri (JVB) websockets for jvb1
location ~ ^/colibri-ws/default-id/(.*) {
    proxy_pass http://127.0.0.1:9090/colibri-ws/default-id/$1$is_args$args;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
    tcp_nodelay on;
}

# load test minimal client, uncomment when used
#location ~ ^/_load-test/([^/?&:"']+$) {
#    rewrite ^/_load-test/(.*)$ /load-test/index.html break;
#}
#location ~ ^/_load-test/libs/(.*)$ {
#    add_header 'Access-Control-Allow-Origin' '*';
#    alias /usr/share/Jitsi-meet/load-test/libs/$1;
#}

location ~ ^/([^/?&:"']+$) {
    try_files $uri @root_path;
}

```

```

    }

    location @root_path {
        rewrite ^/(.*)$ / break;
    }

    location ~ ^/([^/?&:'"]+)/config.js$
    {
        set $subdomain "$1.";
        set $subdir "$1/";

        alias /etc/Jitsi/meet/videoconferencias.mpf.gov.ar-config.js;
    }

    # BOSH for subdomains
    location ~ ^/([^/?&:'"]+)/http-bind {
        set $subdomain "$1.";
        set $subdir "$1/";
        set $prefix "$1";

        rewrite ^/(.*)$ /http-bind;
    }

    # websockets for subdomains
    location ~ ^/([^/?&:'"]+)/xmpp-websocket {
        set $subdomain "$1.";
        set $subdir "$1/";
        set $prefix "$1";

        rewrite ^/(.*)$ /xmpp-websocket;
    }

    if ($host != "videoconferencias.mpf.gov.ar") {
        return 404;
    }

    # Anything that didn't match above, and isn't a real file, assume it's
    a room name and redirect to /
    location ~ ^/([^/?&:'"]+)/(.*)$ {
        set $subdomain "$1.";
        set $subdir "$1/";
        rewrite ^/([^/?&:'"]+)/(.*)$ /$2;
    }
}

```

NOTA: por cuestiones de seguridad, se quitó el cifrado de `ssl_ciphers`.

Anexo F. Jurisdicciones

Las distintas jurisdicciones del MPF se dividen en distintas regiones geográficas y las mismas tienen asignadas agentes de Soporte Técnico que se trasladan entre cada una de ellas, resolviendo los inconvenientes informáticos que se les presentan a los usuarios, o bien cooperando con otras áreas para realizar implementaciones de procesos y/o tecnologías.

Para algunos casos, como por ejemplo Córdoba o Mendoza, las jurisdicciones no se limitan al nombre de la provincia que ostentan y pueden encontrarse dentro de las mismas fiscalías de La Rioja y San Juan respectivamente.

Las jurisdicciones se agrupan de la siguiente forma²⁰, ordenadas alfabéticamente: Bahía Blanca, Capital Federal, Comodoro Rivadavia, Córdoba, Corrientes, General Roca, La Plata, Mar del Plata, Mendoza, Paraná, Posadas, Resistencia, Rosario, Salta, San Martín y Tucumán.

²⁰ <https://www.mpf.gob.ar/mapa-de-las-fiscalias/>

Anexo G. Autenticación

Autenticación LDAP para Jitsi-meet a través de ldap2

Instalar el módulo de ldap de Prosody.

```
sudo apt-get install prosody-modules lua-ldap
```

Lo siguiente es configurar el módulo de ldap:

```
/etc/prosody/conf.avail/ldap.cfg.lua
```

```
-- https://modules.prosody.im/mod_lib_ldap.html
-- https://modules.prosody.im/mod_auth_ldap2.html
authentication = 'ldap2'

ldap = {
    hostname = 'ldap.example.com',
    bind_dn = 'cn=admin,dc=example,dc=com',
    bind_password = 'PASSWORDSECRETO',
    use_tls = true,
    user = {
        usernamefield = 'uid',
        basedn = 'ou=people,dc=example,dc=com',
        filter = '(objectClass=*)',
        -- admin?
        --namefield = 'cn',
    },
}
```

Realizar un link de la configuración al directorio de configuración:

```
ln -sf /etc/prosody/conf.avail/ldap.cfg.lua /etc/prosody/conf.d/
```

Añadir la siguiente línea a `/etc/prosody/prosody.cfg.lua`:

```
consider_bosh_secure = true
```

Para habilitar la configuración de ldap, editar

```
/etc/prosody/conf.avail/Jitsi.example.com.cfg.lua:
```

```
authentication = "ldap2"
```

Finalmente reiniciar el servicio:

```
sudo service prosody restart
```

Habilitación de hosts

Para que host autenticados puedan crear salas y los invitados ingresar a las mismas se deben seguir los siguientes pasos.

Agregar un host virtual en

```
/etc/prosody/conf.avail/Jitsi.example.com.cfg.lua:
```

Finalmente, reiniciar el navegador y los servicios:

```
sudo service prosody restart; sudo service jicofo restart
```

```
VirtualHost "guest.Jitsi.example.com"  
    authentication = "anonymous"  
    c2s_require_encryption = false
```

Anexo H. Registro de Password

Registro password obligatorio²¹.

En /usr/lib/prosody/modules/ crear módulo “mod_perpersistirpass.lua” con el siguiente contenido:

```

    local store = module:open_store("persistent_muc_passwds", "map");
module:log("info", "ingresoregpass");
if not store then
    module:log("error", "Failed to open storage.");
    return nil;
end

module:hook("muc-room-destroyed", function (event)
    local room = event.room;
    local password = room:get_password(room);

    if password then
        module:log("debug", "Room %s with pass %s about to be
destroyed", room, password);
        if not store then
            module:log("debug", "failed to open store on
destroy");
            return nil;
        end

        local now = os.time();
        store:set(room.jid, "last_used", now);
        store:set(room.jid, "password" , password);

        local store = module:open_store("persistent_muc_passwds", "map");
module:log("info", "ingresoregpass");
if not store then
    module:log("error", "Failed to open storage.");

```

²¹ Basado en <https://community.jitsi.org/t/persistent-passwords-on-self-hosted-rooms/20420/10>

```

module:log("debug", "Stored %s, %s for room %s", password, now,
if is_room_stale(last_used) then
    -- delete entry
    store:set(room.jid, "last_used", nil);
    store:set(room.jid, "password" , nil);
    module:log("debug", "deleted password for stale room %s",
room);
    return nil;
end

-- restore old pass for the mucroom
local success = room:set_password(old_pass);
if not success then
    module:log("warn", "Failed to set old password for restored
room %s.", room);
end

    module:log("debug", "Set password '%s' for restored room %s.",
old_pass, room);
    return nil;
end, 0);

function is_room_stale(last_used)
    local                                days                                =
module:get_option_number("days_to_persist_muc_passwds", 45);
    module:log("debug", "Function is_stale() called with '%s', days
is set to %s", last_used, days);
    local daysfrom = os.difftime(os.time(), last_used) / (24 * 60 *
60);
    local roomage = math.floor(daysfrom) ;
    module:log("debug", "roomage is %s days", roomage);
    if roomage then
        return roomage > days;
    end
    return false;
end
end

```


En la ruta `/etc/prosody/conf.avail/<dominio>.cfg.lua`, dentro de `Component`

`"conference.<dominio>" "muc":`

Comentar la línea `storage = "memory"`

Agregar las siguientes líneas encima de `"modules_enabled":`

```
default_storage = "memory"
```

```
storage = { persistent_muc_passwds = "internal"; }
```

```
days_to_persist_muc_passwds = 45 (indica la cantidad de días que se  
persiste la contraseña)
```

Agregar la siguiente línea: `"perpersistirpass";`

Revisar que el dominio tanto en el archivo como en el contenido a modificar sea el correcto y reiniciar los servicios Prosody, Jitsi-videobridge2 y Jicofo.

Anexo I. Turn

Configuración de servidor TURN en NGinx y Prosody

Los pasos que se presentan a continuación, son extraídos de los documentos oficiales de Jitsi y Prosody y agrupados con el fin de simplificar la configuración.

Instalar Servidor CoTurn:

```
sudo apt install coturn
```

Configurar NGinx y Prosody:

Agregar en `/etc/nginx/modules-enabled:`

```
stream {
    map $ssl_preread_server_name $name {
        Jitsi- videoconferencias.mpf.gov.ar; web_backend;
        turn- videoconferencias.mpf.gov.ar; turn_backend;
    }
    upstream web_backend {
        server 127.0.0.1:4444;
    }
    upstream turn_backend {
        server IPPUBLICA:5349;
    }
    server {
        listen 443;
        listen [::]:443;
        # since 1.11.5
        ssl_preread on;
        proxy_pass $name;
        # Increase buffer to serve video
        proxy_buffer_size 10m;
    }
}
```

Agregar en `/etc/nginx/site-available/your-conf:`

```
{
type = "turns", host = "turn-videoconferencias.mpf.gov.ar", port
= "5349", transport = "tcp"
}
```

Es muy importante no utilizar el puerto 443, ya que es el puerto TLS del servidor web. Revisar si Prosody está accediendo al puerto correcto y si resuelve el DNS

Habilitar el módulo en la lista `modules_enabled`:

```
modules_enabled = {
    -- other modules ...
    "turn_external"
}

turn_external_host = "turn.example.com"
turn_external_secret = "PASSW0r4D"
...
server {
    listen 4444 ssl;
    listen [::]:4444 ssl;
    videoconferencias.mpf.gov.ar;
    ...
modules_enabled =
{
    -- other modules ...
    "turn_external"
}
```

Generar una contraseña fuerte y colocarla como en el ejemplo en `static-auth-secret` dentro de `/etc/turnserver.conf` y en `turn_external_secret` dentro de la configuración de Prosody. Debe incluirse un dominio también dentro del parámetro `realm`:

```
realm=turn.example.com
```

En la configuración de Prosody `/etc/prosody/prosody.cfg.lua`:

Revisar si el servicio Coturn se encuentra activo:

```
sudo systemctl status coturn
```

De lo contrario:

```
sudo systemctl enable --now coturn
```

Reiniciar Prosody y Nginx

```
sudo systemctl restart Prosody
```

```
sudo systemctl restart Nginx
```

Anexo J. Instalación de Jibri

Instalación y configuración de Jibri

A continuación, se establecen los pasos necesarios para la instalación y configuración del módulo de Jibri, pero previamente se recuerda que Jibri debe encontrarse en otro SO distinto al que aloja los otros módulos que conforman Jitsi.

Instalar la última versión de Google Chrome:

```
curl https://dl-ssl.google.com/linux/linux_signing_key.pub | sudo
sh -c 'gpg --dearmor > /usr/share/keyrings/google-chrome-
keyring.gpg'
echo "deb [arch=amd64 signed-by=/usr/share/keyrings/google-
chrome-keyring.gpg] http://dl.google.com/linux/chrome/deb/ stable
main" | sudo tee /etc/apt/sources.list.d/google-chrome.list
apt-get -y update
apt-get -y install google-chrome-stable
```

Crear el archivo para políticas de administración de Chrome y agregar la siguiente línea para ocultar advertencias:

```
mkdir -p /etc/opt/chrome/policies/managed
echo '{"CommandLineFlagSecurityWarningsEnabled": false}'
>>/etc/opt/chrome/policies/managed/managed_policies.json
```

Instalar y asignar permisos a Chromedriver

```
CHROME_DRIVER_VERSION=`curl -sS
chromedriver.storage.googleapis.com/LATEST_RELEASE`
wget -N
http://chromedriver.storage.googleapis.com/$CHROME_DRIVER_VERSION
/chromedriver_linux64.zip -P ~/
unzip ~/chromedriver_linux64.zip -d ~/
rm ~/chromedriver_linux64.zip
sudo mv -f ~/chromedriver /usr/local/bin/chromedriver
sudo chown root:root /usr/local/bin/chromedriver
sudo chmod 0755 /usr/local/bin/chromedriver
```

Agregar el repositorio del sitio oficial de Jitsi para descargar la versión más actualizada de Jibri. En primer lugar, descargar la key:

```
curl https://download.jitsi.org/Jitsi-key.gpg.key | sudo sh -c
'gpg --dearmor > /usr/share/keyrings/Jitsi-keyring.gpg'
```

Agregar al archivo de orígenes (sources.list.d22) el repositorio:

```
echo 'deb [signed-by=/usr/share/keyrings/Jitsi-keyring.gpg]
https://download.jitsi.org stable/' | sudo tee
/etc/apt/sources.list.d/jitsi-stable.list > /dev/null
```

Actualizar repositorio e instalar Jibri

```
sudo apt-get update
sudo apt-get install jibri
```

Agregar al usuario Jibri a los siguientes grupos:

```
sudo usermod -aG adm,audio,video,plugdev jibri
```

Editar el archivo de configuración de Jibri con los parámetros corporativos:

```
jibri {
    .....
    api {
        xmpp {
            environments = [
                {
                    name = "yourdomain.com"
                    xmpp-server-hosts = ["1.2.3.4"],
                    xmpp-domain = "yourdomain.com"
                    control-login {
                        domain = "auth.yourdomain.com"
                        username = "jibri"
                        password = "jibriauthpass"
                        port = 5222
                    }
                    control-muc {
                        domain = "internal.auth.yourdomain.com"
                        room-name = "jibriBrewery"
                        nickname = "myjibri-1-2-3-4"
                    }
                    call-login {
                        domain = "recorder.yourdomain.com"
                        username = "recorder"
                        password = "jibrirecorderpass"
                    }
                }
            ]
            strip-from-room-domain = "conference."
            trust-all-xmpp-certs = true
            usage-timeout = 0
        }
    }
}
```

```

    }
...
}

```

Crear una entrada dentro del MUC interno, para que los clientes de Jibri sean visibles por jicofo, pero no por participantes externos en `/etc/prosody/prosody.cfg.lua`:

```

-- internal muc component, meant to enable pools of Jibri and jigasi
clients
Component "internal.auth.yourdomain.com" "muc"
    modules_enabled = {
        "ping";
    }
    -- storage should be "none" for prosody 0.10 and "memory" for prosody
0.11
    storage = "memory"
    muc_room_cache_size = 1000

```

Agregar un host virtual, que será utilizado en la sesión de Chrome, lo que permite que solo usuarios Jibri autenticados sean ocultos en la sala. Agregar lo que sigue en

```

/etc/prosody/prosody.cfg.lua:
VirtualHost "recorder.yourdomain.com"
    modules_enabled = {
        "ping";
    }
    authentication = "internal_plain"

```

Configurar las dos cuentas que utilizará Jibri:

```

prosodyctl register Jibri auth.yourdomain.com Jibriauthpass
prosodyctl register recorder recorder.yourdomain.com

```

Configurar el MUC apropiado para los controladores de Jibri, editando `/etc/Jitsi/jicofo/jicofo.conf`. Tiene que ser el mismo MUC que el configurado en `config.json`. Luego de realizar este procedimiento, reiniciar jicofo.

```

jicofo {
    ...
    Jibri {
        brewery-jid = "JibriBrewery@internal.auth.yourdomain.com"
        pending-timeout = 90 seconds
    }
    ...
}

```

Agregar en `/etc/Jitsi/meet/yourdomain-config.js`:

```

fileRecordingsEnabled: true, // If you want to enable file recording

```

```
liveStreamingEnabled: true, // If you want to enable live streaming  
hiddenDomain: 'recorder.yourdomain.com',
```

También asegurar que en la configuración de la interfaz (`/usr/share/Jitsi-meet/interface_config.js`), la matriz `TOOLBAR_BUTTONS` contiene el valor de “grabación” para mostrar el botón de grabación de archivos y el de transmisión en vivo para mostrar el botón de transmisión en vivo.

Reiniciar el sistema con `sudo systemctl restart Jibri`.

Anexo K. Docker

Instalación y Configuración de Docker.

A continuación, se establecen los pasos necesarios para la instalación y configuración de docker²³.

Actualizar el índice de paquetes “apt” e instalar paquetes que permitan el uso de repositorios sobre HTTPS:

```
sudo apt-get update
sudo apt-get install \
    ca-certificates \
    curl \
    gnupg \
    lsb-release
```

Agregar la llave GPG oficial de docker:

```
sudo mkdir -p /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo
gpg --dearmor -o /etc/apt/keyrings/docker.gpg
```

Ejecutar el siguiente comando para configurar el repositorio:

```
echo \
    "deb [arch=$(dpkg --print-architecture) signed-
by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/ubuntu \
    $(lsb_release -cs) stable" | sudo tee
/etc/apt/sources.list.d/docker.list > /dev/null
```

Instalar docker engine:

```
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io
docker-compose-plugin
```

Comprobar que funcione docker engine:

```
sudo docker run hello-world
```

Instalación y configuración de Jibri.

²³ <https://docs.docker.com/engine/install/ubuntu/>

Inicialmente, se debe proceder con la instalación tal y como se establece en el Anexo J, pero a continuación se establecen las particularidades para la implementación en contenedor^{24 25}:

Instalar el módulo necesario para asegurar que contenga las utilidades del núcleo:

```
apt update && apt install linux-image-extra-virtual
```

Configurar las interfaces de loopback, que permiten la grabación de audio y video:

```
echo "options snd-aloop enable=1,1,1,1,1 index=0,1,2,3,4" >
/etc/modprobe.d/alsa-loopback.conf
```

Configurar el módulo para su inicio automático y comprobar que se refleje correctamente:

```
echo "snd-aloop" >> /etc/modules
lsmod | grep snd_aloop
```

Crear un archivo .yaml en la ubicación /etc/user. Este archivo contendrá la configuración del contenedor:

```
nano NOMBREDEARCHIVO.yaml
```

Completar el archivo con la siguiente configuración:

```
version: '3'
```

```
services:
```

```
  Jibri:
```

```
    image: Jitsi/Jibri
```

```
    volumes:
```

```
      - ${CONFIG}/Jibri:/config
```

```
      - /dev/shm:/dev/shm
```

```
    cap_add:
```

```
      - SYS_ADMIN
```

```
      - NET_BIND_SERVICE
```

```
    devices:
```

```
      - /dev/snd:/dev/snd
```

```
    environment:
```

```
      - XMPP_AUTH_DOMAIN
```

```
      - XMPP_INTERNAL_MUC_DOMAIN
```

```
      - XMPP_RECORDER_DOMAIN
```

```
      - XMPP_SERVER
```

²⁴ <https://Jitsi.github.io/handbook/docs/devops-guide/devops-guide-docker/#recording--live-streaming-configuration>

²⁵ <https://github.com/Jitsi/Jitsi-meet/wiki/Jibri-as-Docker-connected-to-a-standard-Jitsi-Meet-installation>

```

- XMPP_DOMAIN
- JIBRI_XMPP_USER
- JIBRI_XMPP_PASSWORD
- JIBRI_BREWERY_MUC
- JIBRI_RECORDER_USER
- JIBRI_RECORDER_PASSWORD
- JIBRI_RECORDING_DIR
- JIBRI_FINALIZE_RECORDING_SCRIPT_PATH
- JIBRI_STRIP_DOMAIN_JID
- JIBRI_LOGS_DIR
- DISPLAY=:0
- TZ

```

Crear el archivo .env en la misma ubicación del punto anterior:

```

# JIBRI CONFIG
# Internal XMPP domain for authenticated services
XMPP_AUTH_DOMAIN=auth.mydomain.com
# XMPP domain for the internal MUC used for Jibri, jigasi and jvb
pools
XMPP_INTERNAL_MUC_DOMAIN=internal.auth.mydomain.com
# XMPP domain for the Jibri recorder
XMPP_RECORDER_DOMAIN=recorder.mydomain.com
# Internal XMPP server
XMPP_SERVER=mydomain.com
# Internal XMPP domain
XMPP_DOMAIN=mydomain.com
# XMPP user for Jibri client connections
JIBRI_XMPP_USER=Jibri
# XMPP password for Jibri client connections
JIBRI_XMPP_PASSWORD=long-and-difficult-password
# MUC name for the Jibri pool
JIBRI_BREWERY_MUC=Jibribrewery
# XMPP recorder user for Jibri client connections
JIBRI_RECORDER_USER=recorder
# XMPP recorder password for Jibri client connections
JIBRI_RECORDER_PASSWORD=another-long-and-difficult-password
# Directory for recordings inside Jibri container
JIBRI_RECORDING_DIR=/config/recordings
# JIBRI CONFIG
# The finalizing script. Will run after recording is complete
JIBRI_FINALIZE_RECORDING_SCRIPT_PATH=/config/finalize.sh

```

```
# When Jibri gets a request to start a service for a room, the
room
# jid will look like:
roomName@optional.prefixes.subdomain.xmpp_domain
# We'll build the url for the call by transforming that into:
# https://xmpp_domain/subdomain/roomName
# So if there are any prefixes in the jid (like Jitsi meet, which
# has its participants join a muc at conference.xmpp_domain) then
# list that prefix here so it can be stripped out to generate
# the call url correctly
JIBRI_STRIP_DOMAIN_JID=conference
# Directory for logs inside Jibri container
JIBRI_LOGS_DIR=/config/logs
DISPLAY=:0
```

Ejecutar `docker-compose -f Jibri.yml up`.

Asegurar que los botones de grabación y transmisión en vivo de la instancia de Jitsi Meet en `/usr/share/Jitsi-meet/interface-config.js` estén activados en la configuración de la barra de herramientas.

Anexo L. Aplicaciones de Soporte

En el presente Anexo, se encontrará el procedimiento de instalación de aplicaciones necesarias, en forma ordenada, para conseguir el envío de correos electrónicos automatizados con los links de descarga de grabaciones.

Preparación

Previo a realizar todas las configuraciones e instalaciones, se deben realizar los siguientes pasos:

Corroborar las rutas que se encuentran en el archivo `.env` de contenedor que ejecuta Jibri:

```
JIBRI_RECORDING_DIR=/config/recordings
JIBRI_FINALIZE_RECORDING_SCRIPT_PATH=/config/finalize.sh
JIBRI_LOGS_DIR=/config/logs
```

Instalar las siguientes aplicaciones dentro del contenedor:

OpenSSL, para crear contraseñas aleatorias, que serán las asignadas al momento de subir el video a Nube.

MailUtils, que permite el envío de mail.

Nano, editor de texto.

Para ingresar al contenedor creado y realizar todas las instalaciones indicadas anteriormente, se debe ejecutar el comando de docker:

```
docker exec -it [NOMBRE_CONTENEDOR] /bin/bash
```

Instalación y Configuración del Cliente de NxLog.

Descargar y copiar al servidor el paquete de instalación²⁶.

Descomprimir el paquete:

```
tar -xjf nxlog-5.5.7550_debian9_amd64.tar.bz2
```

Instalar el paquete descomprimido:

```
dpkg -i nxlog-5.5.7550_amd64.deb
```

Configurar NxLog editando `.../nxlog.Jitsi.conf`²⁷:

```
<Input jicofo>
Module im_file
File      '/var/log/Jitsi/jicofo.log'
Exec      $message = $raw_event;
</Input>
```

²⁶ <https://nxlog.co/products/nxlog-community-edition/download>

²⁷ La ruta puede variar, dependiendo de cada instalación. La de default es `/opt/nxlog/etc/nxlog.conf`

```

<Output NASTECNO>
Module om_file
File "/mnt/Jibrigrabaciones/JicofoJibri.log"
</Output>
<Route 1>
Path jicofo => NAS
...
<Extension _syslog>
Module xm_syslog
</Extension>

```

La configuración es tentativa, utilizando el modo de envío provisto por NxLog `om_file`, que emite un archivo, el que contiene lo capturado por el módulo `<Input>`. A través del módulo `<Output>` indicamos como se va a llamar el archivo, y mediante `<Route>`, establecemos cual es la ubicación donde queremos ubicar dicho archivo.

Archivos y unidades de red.

Eliminar todo lo que haya en `/Jibri/recordings` estando adentro de la carpeta con el comando `rm -R *`.

Crear el usuario “Jibri” y asignarle el grupo 999(grupo docker) y user id 999

```

adduser Jibri
usermod -u 999 -g 999 Jibri

```

Esto es porque el grupo docker es 999. El userid 999 es el que usa Jibri adentro del contenedor para guardar las grabaciones. El password debe ser el mismo que el registrado para el usuario Jibri proporcionado por Operaciones.

Instalar Cif Utils, para compartir archivos entre plataformas (Ubuntu/Windows)

```

sudo apt-get update
sudo apt-get install cifs-utils

```

Crear archivo en donde se encontraran las credenciales de mapeo

```

/etc/.Jibricred (puede ser cualquier nombre en lugar de .Jibricred)
username=Jibri (usuario AD q coincide con el usuario de ubuntu)
password=PASSWORD (password que coincide con el password de Jibri en Ubuntu
y Windows)
domain=dominio.com.ar

```

Asignar al archivo permisos y establecer el usuario propietario:

```

chown root: /etc/.Jibricred
chmod 600 /etc/.Jibricred

```

Editar el archivo fstab, para montar la unidad de red de Windows en Ubuntu con las credenciales de `/etc/.Jibricred`:

```
RUTA_DEL_NAS /Jibri/recordings cifs
```

```
credentials=/etc/.Jibricred,uid=999,gid=999,dir_mode=0754,file_mode=0644 0
```

```
0
```

Montar la unidad en Ubuntu y reiniciar

```
mount /Jibri/recordings
```

```
Systemctl restart
```

Archivo Finalize.sh

```
#!/bin/bash
RUTALOG="/config/enviograbaciones.log" - #Para Containers
/config/enviograbaciones.log
rutaArchivoHTML="/config/formatomailhtml.html" #Para Containers
/config/formatomailhtml.html
RUTAANFITRION="... /JicofoJibri.log" #Para leer el log de Jicofo donde está
el usuario que se loguea a la VC
RUTANAS="/config/nasrecordings/"
#NomAnfitrion=""
#FlagAnfitrion=""
cd $1 # $1 sirve para obtener la ruta a la carpeta donde se encuentra el
archivo de grabacion
NomArchivo=$(find . -type f -name "*.mp4" -printf "%f\n") #Obtener el
nombre del archivo de grabación
echo "Inicio script envio grabacion: $NomArchivo" >> $RUTALOG
#ArchivoMetadata=$(find . -type f -name "*.json") #Get NomArchivoMetadata
de la grabación (en donde se encontraría grabado el Anfitrión)
#NomAnfitrion=$(echo | jq -r .participants[].user[] $ArchivoMetadata) #Get
NomUs Anfitrion #jq -r es para obtener el resultado sin las comillas
#Copiar archivo grabación a NAS
cp -r "$1" "$RUTANAS" >> $RUTALOG 2>&1
#Verificar si el logueado coincide con la sala
NombreArchivoSinMp4=$(echo $NomArchivo | cut -d "." -f 1)
NomAnfitrionDesdeSala=$(echo $NomArchivo | cut -d "_" -f 2)
NomSala=$(echo $NomArchivo | cut -d "_" -f 1-2)
cat "$RUTAANFITRION" > "${NombreArchivoSinMp4}.log"
FlagAnfitrion=$(grep -i "$NomSala" "${NombreArchivoSinMp4}.log" | grep
$(date +"%y-%m-%d") | grep -i "AuthSession\[ID=$NomAnfitrionDesdeSala" |
grep -v "guest.")
if [ "$FlagAnfitrion" != "" ];
then
NomAnfitrion=$NomAnfitrionDesdeSala #Coincide con la sala el anfitrion
echo "$NomAnfitrion" >> $RUTALOG
fi
#Borrar el log temporal
rm "${NombreArchivoSinMp4}.log"
#subir grabacion a nube SIEMPRE
curl -fsS -u[USER]:[PASSWORD] -T "$1/$NomArchivo"
"https://nube.mpf.gov.ar/XXXX.php/dav/XXXX/Jibri/Grabaciones/$NomArchivo"
```

```

ResSubirArchivo=$?
if [ "0" != "$ResSubirArchivo" ]; #este if verifica que no se produzcan
errores HTTP ni de OwnCloud al subir el archivo
then
    echo "No se pudo subir el archivo $NomArchivo. Código error:
$ResSubirArchivo" >> $RUTALOG
    echo -e "No se pudo subir el archivo $NomArchivo a Nube. Código error:
$ResSubirArchivo" | \
    mail -a "From: Videoconferencias@mpf.gov.ar" \
        -a "Content-Type: text/plain; charset=UTF-8" \
        -s "Videoconferencias MPF: Error al subir grabación a Nube" \
        XXXX@mpf.gov.ar >> $RUTALOG 2>&1 #se envía mail a una casilla para
dar aviso
exit 0
fi
#Compartir archivo ya subido a nube, con link público con contraseña
PassNube=$(openssl rand -base64 12) #Generador de contraseña
expira=$(date -d"+7 days" '+%Y-%m-%d') #7 días a partir de que se comparte
SERVER_URI=https://nube.mpf.gov.ar
API_PATH=ocs/v1.php/apps/files_sharing/api/v1/shares
ResCompartir=$(curl -fsS --user Jibri:PASSWORD "$SERVER_URI/$API_PATH" \
    --data "path=/Grabaciones/$NomArchivo" \
    --data "shareType=3" \
    --data "permissions=1" \
    --data "name=$NomArchivo" \
    --data-urlencode "password=$PassNube" \
    --data "expireDate=$expira")
#--data-urlencode sirve para que curl no tenga problemas con caracteres
especiales
#$ResCompartir es la respuesta de owncloud en xml
ResCompartirArchivo=$?
if [ "0" != "$ResCompartirArchivo" ]; #este if verifica que no se produzcan
errores HTTP al COMPARTIR el archivo
then
    echo "No se pudo compartir el archivo $NomArchivo por error de conexión.
Código error: $ResCompartirArchivo" >> $RUTALOG
    echo -e "No se pudo compartir el archivo $NomArchivo a Nube por error de
conexión. Código error: $ResCompartirArchivo" | \
    mail -a "From: Videoconferencias@mpf.gov.ar" \
        -a "Content-Type: text/plain; charset=UTF-8" \
        -s "Videoconferencias MPF: Error al compartir grabación a Nube" \

```



```

admin@mpf.gov.ar >> $RUTALOG 2>&1
exit 0
fi
#Verificar que no haya errores de OwnCloud
StatusCode=$(echo $ResCompartir | sed -e
's/.*<statusCode>\(.*\)</statusCode>.*\/1/')
StatusCode=$(echo $StatusCode | sed 's/\&/\&/')
if [ "$StatusCode" != "100" ];
then #Hay error: Error en OwnCloud, enviar mail a admin y salir exit 0
echo "No se pudo compartir el archivo $NomArchivo por error de OWNCLOUD.
Código error: $StatusCode" >> $RUTALOG
echo -e "No se pudo compartir el archivo $NomArchivo a Nube por error de
OWNCLOUD. Código error: $StatusCode" | \
mail -a "From: Videoconferencias@mpf.gov.ar" \
-a "Content-Type: text/plain; charset=UTF-8" \
-s "Videoconferencias MPF: Error al compartir grabación a Nube -
OWNCLOUD" \
XXXX@mpf.gov.ar >> $RUTALOG 2>&1
exit 0
fi
#End Verificar Errores OwnCloud

#Obtener link de descarga
Link=$(echo $ResCompartir | sed -e 's/.*<url>\(.*\)</url>.*\/1/')
Link=$(echo $Link | sed 's/\&/\&/')

#Enviar link de grabación vía mail
if [ "$NomAnfitrión" != "" ]; #Si el anfitrión estaba en el nombre de sala
enviar al Anfitrión
then
#mandar mail a anfitrión con link de la grabación
source /config/enviarmailfinal.sh $NomAnfitrión $NomArchivo $Link
$PassNube >> $RUTALOG 2>&1 #/config/... container /Jibri/... en VMs
if [ "0" = "$?" ]; #este if verifica que si hubo un error al enviar el
mail al anfitrión
then
echo "Envío de mail exitoso a $NomAnfitrión. Grabacion: $NomArchivo"
>> $RUTALOG
fi
else #Si el anfitrión no coincide con el nombre de sala (o el nombre de
sala no tiene el formato establecido)

```

```

#mandar mail a casilla establecida con link de descarga de la grabacion
echo "Se realizó una grabación con un formato de nombre de sala
incorrecto. Grabación: $NomArchivo" >> $RUTALOG
echo -e "Se realizó una grabación con un formato de nombre de sala
incorrecto. Grabación: $NomArchivo" | \
mail -a "From: Videoconferencias@mpf.gov.ar" \
-a "Content-Type: text/plain; charset=UTF-8" \
-s "Videoconferencias MPF: Grabación sin anfitrión definido" \
XXXX@mpf.gov.ar >> $RUTALOG 2>&1
fi
exit 0
#FIN Script

```

Script Para Configuración de Mail

```

#!/bin/bash
export MAILFROM="videoconferencias@mpf.gov.ar"
export MAILTO="$1@mpf.gov.ar"
export SUBJECT="Videoconferencias MPF - $2"
export RUTALOG="/config/enviograbaciones.log"
export MAILPART=$(uuidgen)
(
  ArchivoHTML="/config/formatomailhtml.html"
  HTMLdinamico=$(cat $ArchivoHTML | sed "s,ReemplazarLink,$3,g" | sed
"s,ReemplazarPass,$4,")

```

Anexo M. Instructivos

Este Anexo está dedicado para establecer los procedimientos de uso/administración del sistema de VC, para los técnicos y usuarios²⁸.

Instructivo para Mesa de Ayuda

Este instructivo será otorgado exclusivamente al personal de Soporte/Mesa de Ayuda, con el fin de que conozcan y realicen la operatoria de la plataforma de manera correcta.

Requisitos de Hardware y Software

PC de Escritorio

Webcam con micrófono incorporado

Navegador web Google Chrome

Alcance de Videoconferencias

Internas: Con equipos dentro de la red del MPF.

Externas: Con equipos que no se encuentran dentro de la red del MPF.

Mixto: Con equipos dentro de la red del MPF y equipos externos a la red del MPF.

Participantes: Pueden haber 2 o más participantes (equipos conectados).

Grabación: Permite efectuar la grabación de la videoconferencia.

Transmisión en vivo: Permite efectuar la emisión en vivo a través de YouTube.

Participantes

Anfitrión: Es el agente del MPF que da comienzo a la videoconferencia.

Atención: Para que un usuario del MPF pueda ser anfitrión, se lo debe agregar al grupo SECVC.

Únicamente los usuarios que se encuentren en dicho grupo podrán dar comienzo a las videoconferencias.

²⁸ Las opciones y/o capturas de pantalla que se utilizaron son de la demo web de Jitsi (<https://meet.jit.si/>), y pueden estar sujetas a modificaciones, ya que la versión web puede no coincidir con la versión descargada en nuestros servidores.

Invitado: Es una persona que accede a la videoconferencia iniciada por el Anfitrión, sin necesidad de loguearse ni poseer un usuario del MPF (puede ser o no un usuario del MPF).

Recepción de solicitud

Consultar la fecha de realización de la videoconferencia a efectos de establecer la fecha de inicio y caducidad de los permisos para ser Anfitrión de la misma:

- Período de tiempo permitido por default: 2 días hábiles. Para períodos mayores solicitar autorización a Tecnología.
- Una VC puede solicitarse como máximo con un mes de anticipación.

Consultar qué usuario del MPF será el Anfitrión de la videoconferencia.

Consultar al Anfitrión si grabará la videoconferencia (aplica también para transmitir por youtube); si no va a grabar/transmitir directamente saltar al paso 4:

- Si va a grabar/transmitir, chequear en esporcalendario.mpf.gov.ar la disponibilidad, es decir comparar la cantidad de Anfitriones (si aparece el mismo anfitrión más de una vez, cuenta como uno) que hay en la agenda (grabacion/transmision). En caso de cambio a una fecha con disponibilidad, saltar al punto “Agendar la videoconferencia en el calendario con el asunto correspondiente”.
- En caso de que no se pueda cambiar la fecha, generar ticket de redmine consultando.

Agendar la videoconferencia en el calendario con el asunto correspondiente:

- “VC **RandomString_NomUsuario** NroTicket” si la videoconferencia no se grabará.
- “GRABACION **RandomString_NomUsuario** NroTicket” si la videoconferencia se grabará.
- “GRABACION PRUEBA **RandomString_NomUsuario** NroTicket” si es una prueba de grabación.
- “TRANSMISION **RandomString_NomUsuario** NroTicket” si va a transmitir por youtube.
- “TRANSMISION PRUEBA **RandomString_NomUsuario** NroTicket” para prueba de transmisión.

Proveer al usuario lo siguiente:

Link de acceso a la VC con formato:

https://videoconferencias.mpf.gov.ar/RandomString_NomUsuario

RandomString_NomUsuario corresponde al nombre de sala que tendrá la videoconferencia y es muy importante que siempre termine en _NomUsuario para la correcta provisión de la grabación.

NomUsuario: Es el nombre de usuario del Anfitrión.

RandomString: es un string aleatorio de al menos 10 caracteres que deberá generarse para cada VC solicitada, por ejemplo:

https://videoconferencias.mpf.gov.ar/mx3e8qt3eM_PLopez

Instructivo para usuarios.

El presente se otorgará a cada usuario autorizado que solicite el uso de la herramienta de videoconferencia.

Requisitos de Hardware y Software

PC de escritorio:

Webcam con micrófono incorporado.

Navegador web Google Chrome.

Notebook/Tablet con webcam y micrófono integrados.

Navegador web Google Chrome.

Celular:

Aplicación “Jitsi Meet” para Android o iOS

Alcance de videoconferencias

Internas: Con equipos dentro de la red del MPF.

Externas: Con equipos que no se encuentran dentro de la red del MPF.

Mixto: Con equipos dentro de la red del MPF y equipos externos a la red del MPF.

Participantes: Pueden haber 2 o más participantes (equipos conectados).

Grabación: Permite efectuar la grabación de la videoconferencia.

Transmisión en vivo: Permite efectuar la emisión en vivo a través de YouTube.

Participantes

Anfitrión: Es el agente del MPF que da comienzo a la videoconferencia

Invitado: Es una persona que accede a la videoconferencia iniciada por el Anfitrión, sin necesidad de loguearse ni poseer un usuario del MPF (puede ser o no un usuario del MPF).

Solicitud de Videoconferencia

Únicamente podrá dar comienzo a una videoconferencia un usuario con credenciales del MPF que posea permisos otorgados por la Mesa de Ayuda informática.

A tal efecto, se debe informar a la Mesa de Ayuda, previo a la realización de la videoconferencia, los siguientes datos:

Fecha de realización de la videoconferencia

Usuario del MPF que será el Anfitrión de la videoconferencia

La Mesa de Ayuda otorgará el permiso para ser Anfitrión y proveerá:

Un link de acceso específico para dar comienzo a la videoconferencia solicitada

Una contraseña de acceso a la videoconferencia

El permiso otorgado para ser Anfitrión de una videoconferencia, permanecerá activo por el tiempo expresado en la solicitud. Una vez finalizado este período, el permiso será revocado, debiendo solicitarlo nuevamente para próximas videoconferencias.

Reserva para Grabación de Videoconferencia

En caso de que la videoconferencia sea grabada, es imperioso que previamente se le informe a la Mesa de Ayuda Informática, a efectos de registrarlo y reservar los recursos necesarios.

Dar comienzo a Videoconferencia - Procedimiento

El Anfitrión es el único que puede dar comienzo a la videoconferencia (usuario del MPF con permisos otorgados por la Mesa de Ayuda)

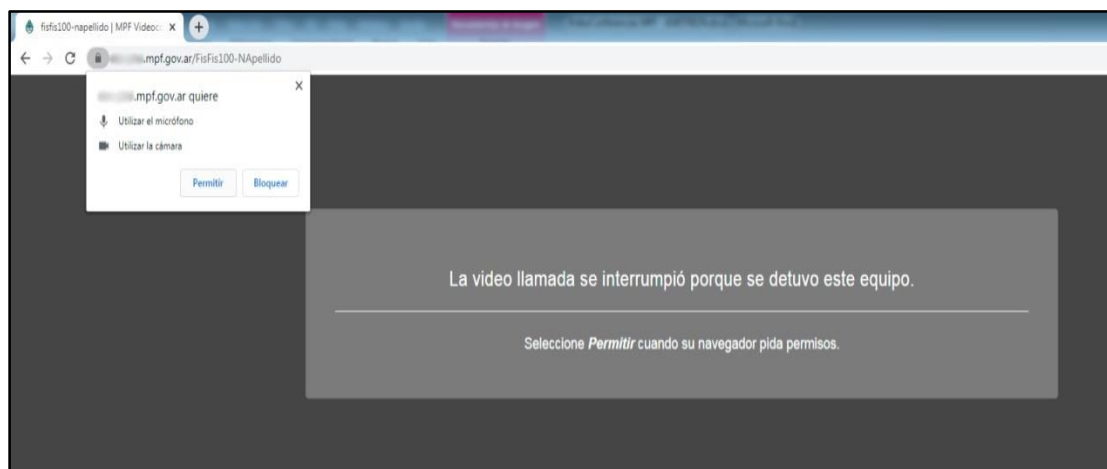
Ingresar al link de acceso a la videoconferencia provisto por la Mesa de Ayuda para dar comienzo a la videoconferencia. (En caso de ingresar al link desde un celular, el navegador web desplegará la opción para abrir la aplicación “Jitsi Meet”, o en su defecto para instalarla).

Atención: Ya sea en el navegador web Chrome o en la aplicación Jitsi Meet, siempre debe ingresarse el link de acceso a la videoconferencia.

En caso de que el navegador solicite permisos de acceso al micrófono y cámara, realizar click en “Permitir”.

Figura M1

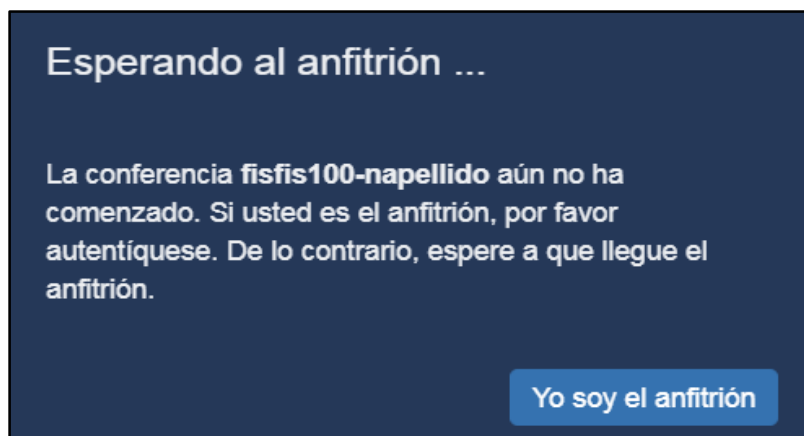
Permisos de cámara y micrófono



Realizar click en el botón “Yo soy el anfitrión”.

Figura M2

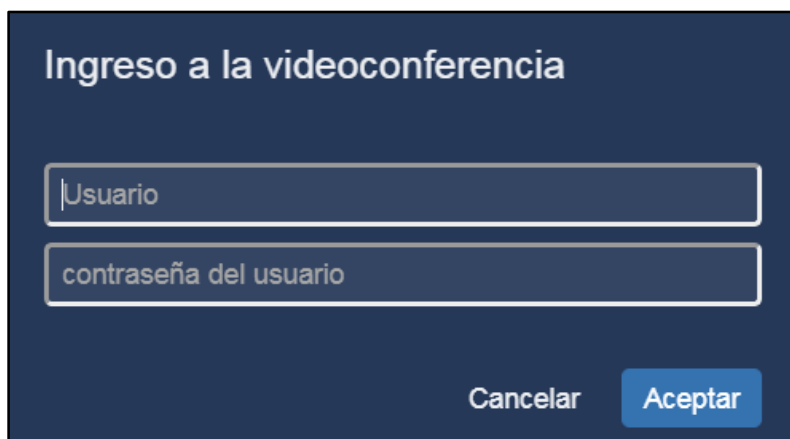
Mensaje de ingreso como anfitrión



Ingresar el usuario y contraseña de la red del MPF.

Figura M3

Cartel de credenciales de anfitrión



Ingreso a la videoconferencia

Usuario

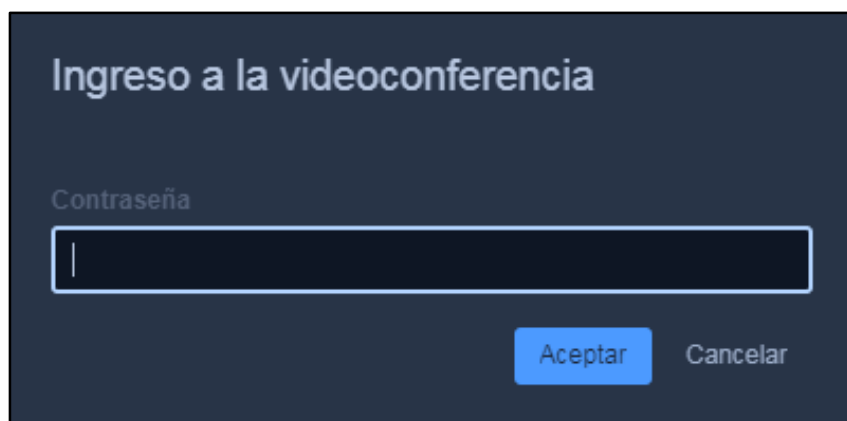
contraseña del usuario

Cancelar Aceptar

Ingresar la contraseña de acceso a la videoconferencia provista por la Mesa de Ayuda.

Figura M4

Solicitud de contraseña de sala.



Ingreso a la videoconferencia

Contraseña

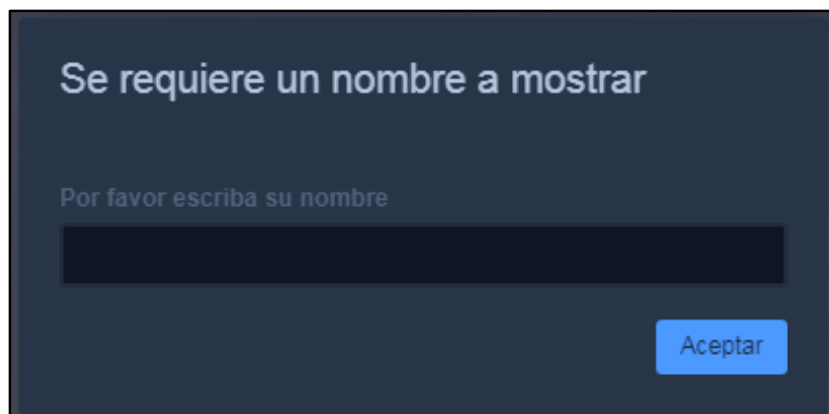
Aceptar Cancelar

Una vez realizado, inmediatamente la videoconferencia será iniciada por el servidor del MPF.

Ingresar un nombre para ser identificado por los demás participantes y realizar click en “Aceptar”.

Figura M5

Solicitud de nombre de usuario.



Se requiere un nombre a mostrar

Por favor escriba su nombre

Aceptar

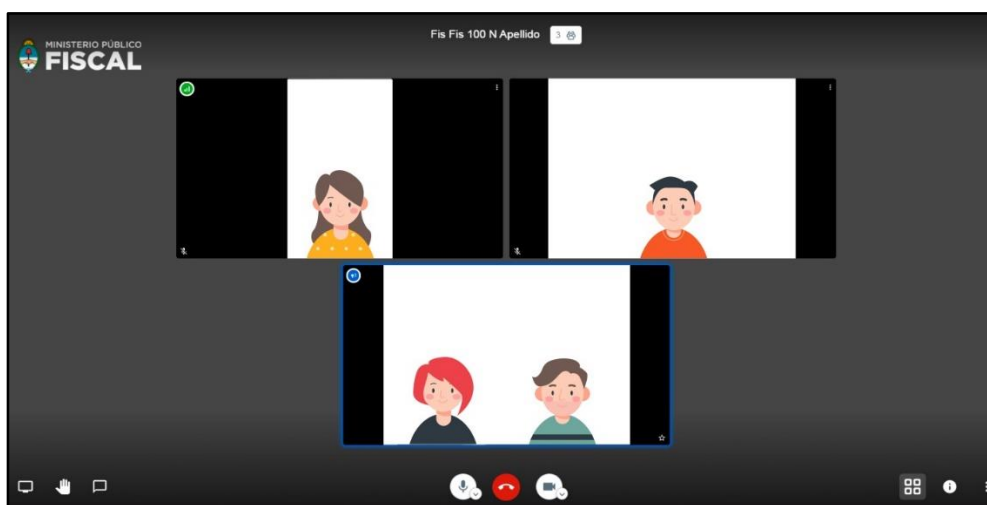
Indicar al Invitado que ingrese al link de acceso a la videoconferencia y proveerle la contraseña de acceso para que se incorpore a la misma.

Atención: El link de acceso a la videoconferencia y la contraseña de acceso a la videoconferencia pueden ser provistos a los invitados previamente a dar comienzo a la videoconferencia.

En este punto, la videoconferencia ya estará establecida con los participantes involucrados.

Figura M6

Videoconferencia iniciada.



Eliminar/Registrar contraseña de acceso a la Videoconferencia

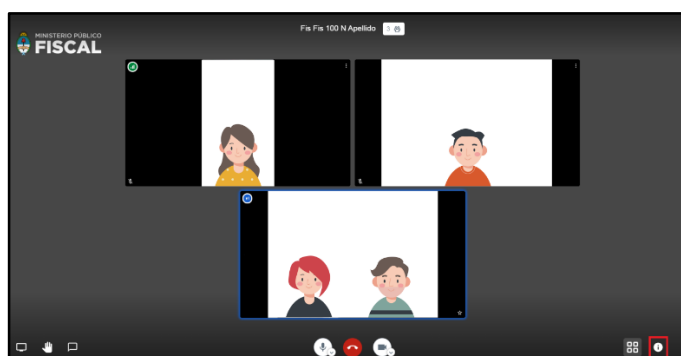
Una videoconferencia al ser iniciada ya posee una contraseña establecida; ante la necesidad de eliminarla o modificarla, se deben realizar los siguientes pasos:

Atención: Se recomienda que la videoconferencia posea una contraseña de acceso para garantizar la seguridad de la misma.

Una vez que la videoconferencia fue iniciada, se debe realizar click en el ícono ubicado en la parte inferior derecha de la pantalla.

Figura M6

Videoconferencia iniciada con contraseña establecida.



Realizar click en “Eliminar contraseña”.

Figura M7

Cuadro de informacion de sala.



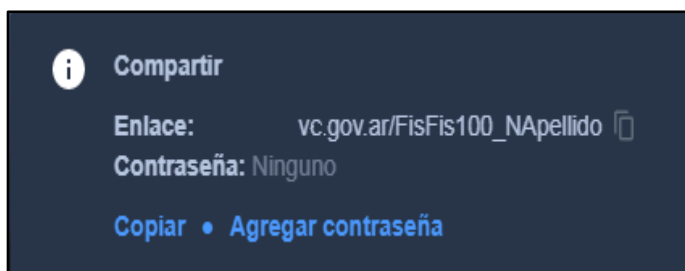
Al realizarlo, la videoconferencia ya no tendrá una contraseña de acceso

Se recomienda que la videoconferencia posea una contraseña de acceso para garantizar la seguridad de la misma.

Para registrarle una nueva contraseña se debe realizar click en “Agregar contraseña”.

Figura M8

Cuadro de informacion de sala con opción de agregar contraseña.



Ingresar una contraseña y presionar la tecla “Enter”.

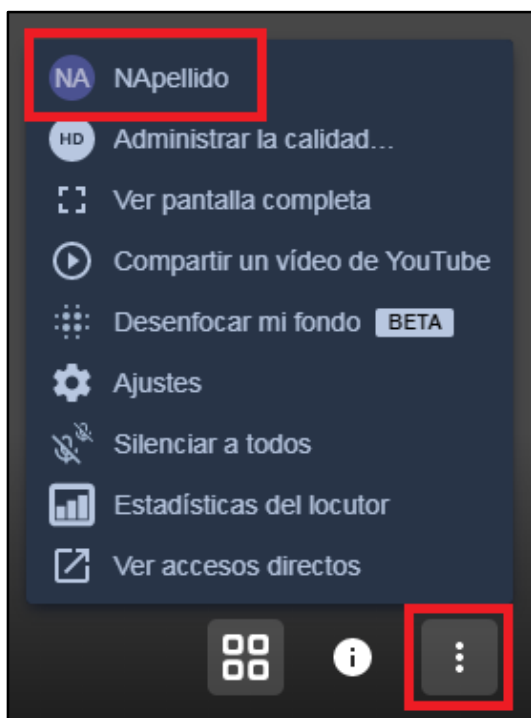
Una vez presionada la tecla “Enter”, si la contraseña se registró con éxito, debe aparecer nuevamente la opción “Eliminar contraseña”

Grabación de Videoconferencia – Visualización de participantes

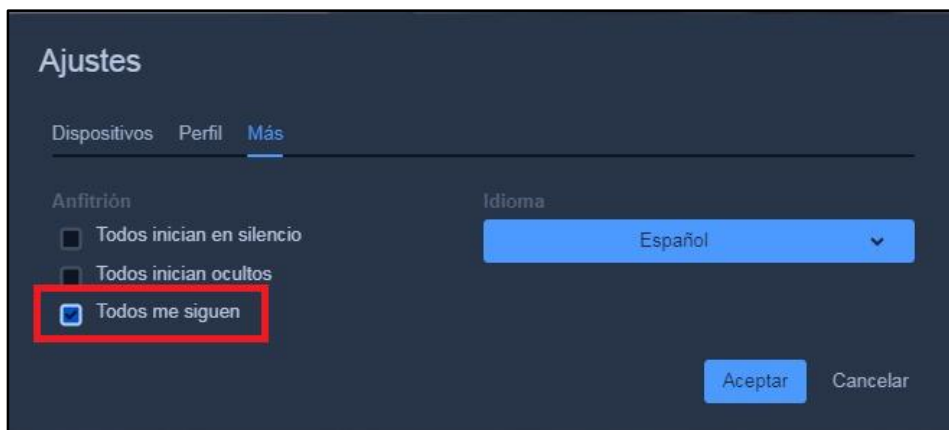
Para que en la grabación se visualicen todos los participantes en modo “mosaico” el Anfitrión debe habilitar la opción “Todos me siguen” y seleccionar la vista “mosaico” en la videoconferencia, de lo contrario la grabación se focalizará dinámicamente en el participante que hable.

Activar opción “Todos me siguen”

Dirigirse al perfil del Anfitrión y abrir el menú de opciones.

Figura M9*Menú de opciones.*

Dirigirse a la solapa “Más”, tildar la opción “Todos me siguen” y realizar click en “Aceptar”.

Figura M10*Ajustes de perfil.*

Grabación de Videoconferencia – Procedimiento

En caso de que la videoconferencia sea grabada, es imperioso que previamente se le informe a la Mesa de Ayuda Informática, a efectos de registrarlo y reservar los recursos necesarios.

Provisión de la Grabación

Al finalizar la grabación, el archivo de video será provisto automáticamente vía mail al Anfitrión desde la casilla Videoconferencias@mpf.gov.ar, a través de un link de descarga protegido mediante contraseña el cual, a su vez, puede ser reenviado a otras personas por el Anfitrión.

El link mencionado estará disponible por un plazo máximo de 7 días, por lo que las grabaciones deberán descargarse dentro de ese período.

Los archivos de grabación se resguardan en el servidor con carácter de contingencia durante 1 mes a partir de la fecha de registro de la grabación. Culminado dicho plazo, se eliminarán en forma automática y definitiva.

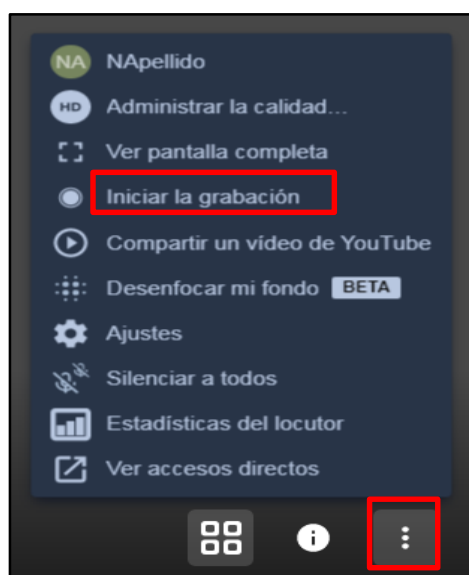
Procedimiento para grabación de la videoconferencia

Atención: Ver el apartado “Grabación de Videoconferencia – Visualización de participantes”

Realizar click en el botón de opciones y posteriormente en “Iniciar la grabación”

Figura M11

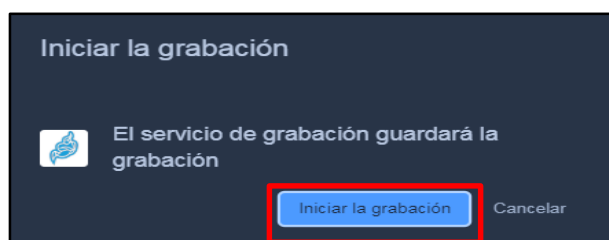
Menú de opciones - grabación.



Se deberá confirmar el inicio de la grabación realizando click en “Iniciar la grabación”

Figura M12

Iniciar grabación.

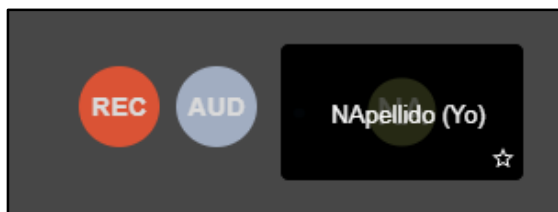


Se debe aguardar a que el sistema prepare los recursos para efectuar la grabación.

Al comenzar la grabación se escuchará una notificación por audio y se podrá visualizar el ícono “REC” en la parte superior derecha de la pantalla.

Figura M13

Grabación Iniciada.

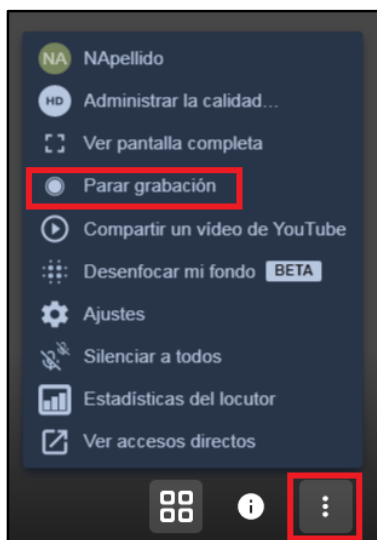


Atención: el plazo máximo de espera para que el sistema comience con la grabación es alrededor de 90 segundos, pasado ese tiempo el sistema mostrará un mensaje de que la grabación no pudo iniciarse. En este caso reintentar o comunicarse con la Mesa de Ayuda o vía mail a soporte@mpf.gov.ar.

Para detener la grabación se debe dirigir al botón de opciones y posteriormente realizar click en “Parar grabación”

Figura M14

Detener grabación.



Anexo N. Archivos Para Aplicaciones

Este Anexo contiene los archivos a editar por Aplicaciones.

Editar el archivo `[/usr/share/jitsi-meet/interface_config.js]`

APP_NAME: MPF

Agregar el ícono de pestaña `[jitsi-meet/favicon.ico]`

Agregar el logo en formato .SVG en la carpeta `jitsi-meet/images/`

Configurar el logo en `[/usr/share/jitsi-meet/interface_config.js]`

`DEFAULT_LOGO_URL: 'jitsi-meet/images/logo.svg'`

`DEFAULT_WELCOME_PAGE_LOGO_URL: 'jitsi-meet/images/logo.svg'`

Para cambiar el título y la descripción en la página de inicio, editar `jitsi-meet/lang/main.json`

Asimismo, deberán adecuar el idioma por defecto a español, ejecutando el siguiente comando:

```
cd jitsi/jitsi-meet/blob/master/lang
```

```
node update-translation.js main-es.json
```

La ejecución del comando anterior provocará que se modifique de forma automática el lenguaje de la plataforma, ya que los archivos con los diferentes idiomas, vienen incluidos en la instalación de Jitsi.