# CONVOCATORIA

# PROYECTO VPN

# Implementación de una Red Privada Virtual (VPN) para el Ámbito Académico

La **ARIU** (Asociación de Redes de Interconexión Universitaria) invita al personal de las áreas de Tecnologías de la Información (TI) de las Universidades Nacionales a presentar propuestas para el desarrollo y ejecución del proyecto **VPN**. Este proyecto busca desplegar en producción una solución de acceso remoto seguro, resistente a ataques de computación cuántica, utilizando exclusivamente herramientas de código abierto.

## 1. Objetivo del Proyecto

Diseñar e implementar una solución de acceso remoto seguro para redes universitarias que:

- Utilice criptografía resistente a computación cuántica (quantum-safe), basada en los estándares post-cuánticos del NIST vigentes.
- Integre un sistema de autenticación centralizado compatible con los sistemas de identidad institucionales.
- Sea desplegable en producción en la infraestructura de una universidad nacional, con soporte para múltiples plataformas de servidor.
- Proveer conectividad a docentes, estudiantes y personal administrativo desde dispositivos con distintos sistemas operativos.

La arquitectura, los protocolos y las herramientas a utilizar no están prescritos: su selección y justificación forman parte de la solución a presentar y serán evaluadas por el comité técnico.

Los lineamientos del proyecto para la formulación de la propuesta se encuentran en el Anexo 1.

### 1.1 Entregables

Se espera que el equipo entregue una solución completa, lista para su despliegue en producción, compuesta por:

**Del lado del servidor:**

1. Contenedor Docker con la implementación completa.
2. VM para Proxmox con la implementación completa.
3. Instalación mediante scripts parametrizados sobre GNU/Linux (al menos Debian y Ubuntu, última versión estable).

**Del lado del cliente y provisionamiento:**

4. Clientes instalables o guías de configuración para Windows, macOS y Linux.
5. Perfiles o guías de configuración para dispositivos móviles (Android e iOS).
6. Sistema de autoprovisionamiento de credenciales que permita a un usuario sin conocimientos técnicos avanzados obtener su configuración de acceso de forma autónoma.

**Documentación:**

7. Informe técnico con análisis de alternativas, justificación de decisiones de diseño y resultados de las pruebas de funcionamiento y seguridad.
8. Repositorio con guía paso a paso para el despliegue y la administración del sistema completo.

## 2. Composición de los Equipos

- Equipos **de un mínimo de 2 y máximo de 5 personas**.
- Los integrantes pueden pertenecer a la misma Universidad Nacional o a distintas instituciones.

## 3. Financiamiento e Infraestructura

**Financiamiento:** Para el desarrollo de la propuesta elegida se destinarán $15.000.000 (quince millones de pesos). Este monto se dividirá en 4 fases (25%) de revisión de avance del plazo total del proyecto.

Cumplida cada revisión de las 4 fases, se realizarán los desembolsos de manera proporcional a cada miembro del equipo de trabajo.

**Infraestructura:** Toda la infraestructura tecnológica necesaria para el desarrollo y despliegue del proyecto será soportada y provista por la ARIU, según se acuerde con el equipo y en función de las imputaciones previstas.

**Soporte y mantenimiento del producto:** Una vez finalizada la etapa de desarrollo y entrega del proyecto, la ARIU podrá, si lo considera necesario, solicitar la contratación de un servicio de

soporte y mantenimiento evolutivo y/o correctivo. Dicho servicio podrá comprender, entre otras actividades, la actualización de imágenes Docker, máquinas virtuales y scripts ante nuevas versiones del sistema operativo base o de las dependencias del sistema y la elaboración de guías de migración que faciliten la actualización de las instalaciones existentes.

La eventual contratación de este servicio no forma parte del alcance obligatorio del presente proceso y quedará sujeta a la evaluación técnica y presupuestaria que realice ARIU, así como a la disponibilidad de recursos y a los términos y condiciones que oportunamente acuerden las partes.

## 4. Criterios de Evaluación

Las propuestas serán evaluadas por un comité técnico bajo los siguientes puntajes:

**1) Por cada uno de los miembros:**

- **Antecedentes Laborales Relacionados (15%):** Experiencia comprobable en la gestión de redes, seguridad informática y administración de servidores en el ámbito universitario. Se valorará especialmente el manejo previo de protocolos VPN, sistemas de autenticación centralizada y herramientas open source, para no menos de un integrante del equipo.

- **Antecedentes Académicos (15%):** Formación de pregrado, grado o posgrado, certificaciones técnicas y participación en investigaciones relacionadas con ciberseguridad, criptografía o infraestructura de redes, a cumplir por no menos de uno de los integrantes del equipo.

**2) Por grupo de trabajo:**

- **Desarrollo de la Propuesta (40%):** Calidad y coherencia del plan de trabajo, solidez en la justificación técnica de la arquitectura elegida, tratamiento adecuado del requisito de criptografía post-cuántica, y viabilidad de los plazos propuestos para el prototipo y el producto final.

- **Entrevista (30%):** Se realizará una entrevista al grupo que presente cada propuesta con el fin de evaluar la factibilidad del proyecto presentado.

## 5. Requisitos de Presentación

Los interesados deberán entregar:

1. **Plan de Trabajo y Cronograma:** Indicando plazos para el **prototipo** y el **producto final**, tomando en cuenta las 4 fases de revisión.

2. **Aval Institucional:** Firmado por el/la/los **Rectores/Rectoras** de las universidades de origen de cada integrante.

3. **Currículum Vitae:** De cada integrante para la evaluación de antecedentes.

4. Al momento de realizar el desembolso, cumplida y aprobada la revisión de la primera fase, cada integrante del equipo de trabajo deberá presentar la constancia de inscripción en el monotributo y deberá facturar el monto percibido a la ARIU. El mismo mecanismo se utilizará para las 3 fases restantes.

## 6. Propiedad Intelectual

Todo el desarrollo deberá realizarse bajo **licencias libres** que permitan la reutilización y auditoría por parte de otras Universidades Nacionales. El equipo final deberá entregar un informe detallado y un repositorio con la guía paso a paso para el despliegue de la solución.

## 7. Cronograma y Fechas Clave

- **Periodo de Presentación:** Desde el **13 de julio** hasta el **20 de agosto.**

- **Plazos de la Propuesta:** El equipo deberá indicar en su plan de trabajo el tiempo estimado para la entrega de los siguientes entregables:

    - Un **prototipo** funcional.
    - El **producto final** (incluyendo documentación técnica y repositorio de despliegue).
    - El **informe final** con las conclusiones solicitadas.

- El **plazo máximo** de financiamiento del proyecto será de 6 meses.

## 8. Entrega y Recepción de Propuestas

- **Medio de envío:** Las propuestas deben enviarse por correo electrónico a: **proyectos@riu.edu.ar**.

- **Modalidad:** Para facilitar la gestión, **sólo un miembro del equipo** deberá enviar la documentación requerida de todos los integrantes y la propuesta técnica.

Los resultados de la convocatoria serán publicados en la página web de ARIU.

---

# ANEXO 1

# Campus Invisible

# Implementación de una Red Privada Virtual (VPN) para el Ámbito Académico

## Objetivo General

El objetivo de este proyecto es diseñar e implementar, utilizando exclusivamente herramientas de código abierto, una solución de acceso remoto seguro para redes universitarias que sea resistente a ataques de computación cuántica. La solución debe ser desplegable en producción, integrarse con los sistemas de identidad institucionales, y brindar conectividad a los distintos perfiles de usuarios universitarios desde múltiples tipos de dispositivos.

La arquitectura, los protocolos y las herramientas a utilizar no están prescritas. Su selección y justificación forman parte del trabajo a desarrollar y serán evaluadas como parte de la propuesta.

## Dirigido a

Personal de las áreas de Tecnologías de la Información (TI) de las Universidades Nacionales.

## I. Contexto y Alcance

Las redes universitarias requieren soluciones de acceso remoto que garanticen la confidencialidad e integridad de las comunicaciones frente a amenazas actuales y futuras. Los algoritmos de clave pública ampliamente utilizados hoy (RSA, ECDH, ECDSA) son vulnerables al algoritmo de Shor ejecutado en computadoras cuánticas de suficiente capacidad. Aunque dicha capacidad no existe aún, la amenaza del tipo *harvest now, decrypt later* —en la que un atacante almacena tráfico cifrado hoy para descifrarlo en el futuro— hace urgente la adopción de criptografía post-cuántica en nuevas implementaciones.

El proyecto deberá producir una solución completa que pueda ser adoptada como modelo de referencia por otras Universidades Nacionales: desde el servidor hasta el dispositivo del usuario final, pasando por el proceso de provisionamiento de credenciales y la integración con los sistemas de identidad institucionales.

# II. Requisitos de Seguridad Criptográfica

## II.1. Algoritmos post-cuánticos

La solución debe garantizar confidencialidad e integridad del canal de comunicación mediante algoritmos resistentes a ataques cuánticos. Los estándares deseables de referencia son los publicados por el NIST en 2024:

- **ML-KEM (FIPS 203):** Para el establecimiento e intercambio de claves, en reemplazo de algoritmos basados en ECDH o RSA en ese rol.
- **ML-DSA (FIPS 204):** Para firmas digitales en los componentes del sistema donde la autenticación se basa en certificados o infraestructura de clave pública (PKI).

## II.2. Criptoagilidad y elección del protocolo

Un requisito crítico del diseño es que el protocolo VPN elegido sea compatible con la integración de criptografía post-cuántica, ya sea de forma nativa o mediante un mecanismo técnicamente justificado. No todos los protocolos VPN tienen la misma capacidad en este aspecto: algunos están diseñados con un conjunto criptográfico fijo y sin mecanismos de negociación de algoritmos (ausencia de criptoagilidad), lo que puede hacer inviable o muy compleja la incorporación de PQC sin modificar el protocolo mismo. Otros protocolos, basados en TLS o en marcos negociables, ofrecen mayor flexibilidad.

Los equipos deberán analizar explícitamente este aspecto para el o los protocolos que propongan, y justificar su estrategia para integrar PQC. En caso de adoptar un enfoque híbrido —donde se combinan algoritmos clásicos y post-cuánticos en paralelo durante un período de transición— deberán justificar esta decisión y sus implicancias de seguridad. Se valorará la adopción de implementaciones estables y con soporte activo por sobre soluciones experimentales o ad hoc.

# III. Requisitos de Autenticación e Identidad

La solución debe integrarse con los sistemas de identidad institucionales de la universidad. El sistema de autenticación deberá:

- Soportar autenticación centralizada de usuarios, desacoplada del servidor VPN.

- Ser compatible con directorios institucionales (LDAP / Active Directory) y/o con protocolos de identidad federada (SAML 2.0 u OpenID Connect).
- Contemplar la gestión del ciclo de vida de los accesos: alta, baja y modificación de usuarios sin intervención manual en el servidor VPN.
- Soportar autenticación multifactor (MFA) como mecanismo configurable por el administrador.

Los equipos deberán proponer y justificar la arquitectura de autenticación completa, incluyendo la elección de protocolos, herramientas y el flujo de autenticación desde el dispositivo del usuario hasta el directorio institucional.

## IV. Requisitos de Arquitectura y Despliegue del Servidor

La solución del lado servidor debe poder desplegarse en las siguientes plataformas, a partir de los artefactos entregados:

- Contenedor Docker.
- Máquina virtual para Proxmox.
- Instalación directa mediante scripts parametrizados sobre GNU/Linux (Debian y Ubuntu, última versión estable).

La propuesta deberá contemplar además:

- **Soporte dual-stack IPv4/IPv6.** El servidor debe aceptar conexiones entrantes en ambas familias de direcciones. El túnel VPN debe ser capaz de transportar tráfico IPv4 e IPv6 simultáneamente, de modo que los dispositivos cliente con conectividad IPv6 puedan acceder a recursos de la red universitaria en ambas familias sin configuración adicional.

- **Separación de roles:** El servidor VPN y el servidor de autenticación deben poder operar como componentes independientes.

- **Alta disponibilidad:** La propuesta debe indicar qué ocurre ante la caída del nodo principal y qué mecanismos de redundancia o recuperación se contemplan, aunque no se prescribe una arquitectura específica.

- **Conectividad desde redes con NAT.** La solución debe funcionar correctamente cuando el cliente se encuentra detrás de NAT, incluyendo los siguientes escenarios, que son habituales para usuarios universitarios:

    - NAT doméstico estándar (router hogareño).

  - CGNAT (Carrier-Grade NAT) de operadores móviles, donde múltiples usuarios comparten la misma dirección IP pública.
  - Redes que restringen o bloquean el tráfico UDP (redes institucionales visitantes, redes hoteleras, portales cautivos). La propuesta deberá describir el mecanismo de fallback disponible en estos entornos.

  La propuesta deberá justificar cómo el protocolo elegido aborda cada uno de estos escenarios.

- **Monitoreo y registro:** El sistema debe generar registros de eventos de autenticación y conexión, y la propuesta debe describir cómo se accede y retiene esta información.

- **Rotación de credenciales:** El diseño debe contemplar procedimientos para la actualización y rotación de claves criptográficas sin interrupción del servicio.

# V. Requisitos de Cliente y Aprovisionamiento

Este eje es central para que la solución sea adoptable en un entorno universitario con usuarios de perfiles técnicos variados.

## V.1. Plataformas de cliente

La solución debe brindar conectividad desde dispositivos con los siguientes sistemas operativos:

| **Plataforma** | **Versiones mínimas requeridas** |
|---|---|
| Windows | 10 y 11 |
| macOS | Últimas dos versiones principales |
| Linux (escritorio) | Ubuntu y Fedora, últimas versiones estables |
| Android | Última versión y versión anterior |
| iOS / iPadOS | Últimas dos versiones principales |

Para cada plataforma, el equipo deberá entregar, según corresponda: un cliente instalable, un perfil de configuración importable, o una guía de configuración paso a paso utilizando clientes disponibles en la plataforma. La propuesta deberá justificar el enfoque elegido para cada sistema operativo.

### V.2. Provisionamiento de usuarios

Se deberá implementar un mecanismo que permita a un usuario final, sin conocimientos técnicos avanzados, obtener su configuración de acceso de forma autónoma. El mecanismo deberá:

- Autenticar al usuario antes de entregar cualquier credencial o perfil de configuración.
- Generar configuraciones específicas por dispositivo cuando la naturaleza del protocolo lo requiera.
- Minimizar la intervención del administrador en el proceso de alta de un nuevo usuario.
- Funcionar de forma segura sobre la red pública (el portal de aprovisionamiento no debe requerir acceso previo a la VPN).

## VI. Plan de Implementación

El proyecto se dividirá en cuatro fases, alineadas con los hitos de revisión y desembolso:

1. **Fase 1 — Diseño:** Análisis de alternativas tecnológicas: protocolo VPN, soporte de PQC, arquitectura de autenticación, estrategia de cliente y aprovisionamiento. Entrega: documento de diseño con todas las decisiones técnicas justificadas, que servirá de base para las siguientes fases.

2. **Fase 2 — Implementación del servidor:** Despliegue funcional del servidor VPN y del sistema de autenticación, integrados con un directorio de usuarios de prueba. Entrega: prototipo funcional del lado servidor en al menos una de las plataformas requeridas.

3. **Fase 3 — Cliente y aprovisionamiento:** Implementación de los clientes para todas las plataformas requeridas y del sistema de autoprovisionamiento. Entrega: solución completa (servidor + clientes + aprovisionamiento) funcional en entorno de prueba.

4. **Fase 4 — Hardening, pruebas y entrega final:** Revisión de seguridad de la configuración, corrección de vulnerabilidades detectadas, redacción del informe técnico y del repositorio de despliegue. Entrega: producto final listo para producción, con documentación completa.

## VII. Documentación y Recursos

El equipo deberá producir los siguientes entregables de documentación:

- **Informe técnico:** Descripción de las alternativas evaluadas en cada capa del proyecto (protocolo VPN, PQC, autenticación, cliente), justificación de las decisiones tomadas,

arquitectura final implementada, resultados de las pruebas de funcionamiento y seguridad, y recomendaciones para la adopción institucional en otras universidades.

- **Repositorio de despliegue:** Guía paso a paso para la instalación y configuración del sistema completo (servidor y clientes), incluyendo scripts, archivos de configuración comentados y procedimientos de mantenimiento habitual.

- **Revisión final con ARIU:** Para la aprobación del hito final, el equipo realizará una demostración del sistema ante el equipo técnico de ARIU, que incluirá el proceso de aprovisionamiento de un nuevo usuario y la conexión exitosa desde al menos dos tipos de dispositivos distintos.

## Perfil del Postulante

El equipo en su conjunto deberá acreditar experiencia en las siguientes áreas. No se requiere que todos los integrantes cubran la totalidad de los puntos, pero sí que el equipo los cubra colectivamente:

- Conocimiento de protocolos VPN y arquitecturas de acceso remoto seguro, con capacidad para evaluar y comparar alternativas técnicas.
- Familiaridad con criptografía de clave pública y, preferentemente, con los estándares post-cuánticos del NIST (ML-KEM, ML-DSA) y su estado de adopción en protocolos de red.
- Experiencia en sistemas de autenticación centralizada e integración con directorios institucionales (LDAP, Active Directory) y/o protocolos de identidad federada (SAML 2.0, OpenID Connect).
- Administración de servidores en entornos GNU/Linux, incluyendo configuración y hardening de servicios de red.
- Manejo de entornos de contenedores y virtualización (Docker, Proxmox).
- Experiencia en despliegue o soporte de aplicaciones en entornos con múltiples sistemas operativos (Windows, macOS, Linux, Android, iOS).
- Capacidad para producir documentación técnica clara, orientada a la adopción por parte de administradores de otras instituciones.