Nube híbrida nacional: soberana, libre, interoperable y con desarrollo local

Índice

Índice 1

Introducción 1

Visión 2

Soberanía tecnológica 3

Despliegue federal y multi actor 4

Seguridad de la información 5

Generación de empleo 6

Ahorro de divisas 6

Herramientas disponibles 7

Caso de éxito: Estonia 7

- La experiencia de Estonia 7
- Oferta de la nube pública estonia y solución tecnológica 8
- Algunas conclusiones del caso estonio 8

Elaboración del documento 9

Adhesiones personales 9

Adhesiones institucionales 11

Introducción

Recientemente la Secretaría de Innovación Pública ha convocado a un procedimiento de consulta para la concreción de una [“Nube Híbrida de Gobierno”]. El objetivo de la Consulta es recibir aportes, ideas, experiencias y recomendaciones para la definición de criterios tecnológicos que permitan la construcción de la misma.

En este marco, quienes firmamos la presente, actores de diversas organizaciones del quehacer tecnológico nacional, mujeres y hombres con décadas de experiencia profesional en tecnologías informáticas y su relación con el desarrollo nacional, apoyamos la construcción de una “Nube híbrida de Gobierno”, saludamos el llamado a Consulta y acordamos en una serie de principios que creemos fundamentales para su desarrollo y el aseguramiento de la soberanía tecnológica. Para comenzar señalamos que consideramos conveniente utilizar el término "nube híbrida nacional", más apropiado en nuestro idioma para el concepto de *hybrid gov cloud* que se encuentra en la bibliografía sobre el tema.

Este concepto nos permite pensar la importancia de la independencia tecnológica para tener un control real sobre las tecnologías y por lo tanto sobre las capacidades del Estado. Implica que el Estado debe tener control legal, intelectual y operativo de la infraestructura informática y el software (IIS) que es crítica para la gestión de políticas públicas. Sin soberanía tecnológica, el país se desprende de grados de libertad

para adoptar las políticas tecnológicas que le resulten convenientes, restricción que a su vez impacta en cómo despliega el aspecto tecnológico de sus políticas, que es cada vez de mayor preeminencia.

Consideramos que la nube híbrida nacional puede y debe ser desarrollada en base a **tecnologías libres**, interoperables, que aseguren independencia al Estado de cualquier proveedor de software o infraestructura de cómputo.

Existen en el país personas e instituciones públicas y privadas con **los conocimientos que permiten desarrollar** la nube híbrida nacional generando trabajo y desarrollo local. En base a tecnologías libres y con personal local, el Estado puede asegurar **el cumplimiento tanto de las normativas como de los más altos estándares en cuanto a la seguridad de la información y el resguardo de los datos personales de la ciudadanía**.

Como señala la convocatoria la nube pública debe **evitarse el *vendor lock-in***, es decir, las ataduras a uno o varios proveedores, asegurando mediante estándares abiertos la interoperabilidad con otras infraestructuras públicas o privadas.

Las siguientes secciones discuten distintos aspectos de las posibilidades que consideramos que se abren si la nube híbrida nacional se desarrolla bajo los principios de soberanía, software libre e interoperabilidad.

Visión

Conceptualizamos a la nube híbrida de Gobierno en base a algunos principios ordenadores y de organización.

Principios ordenadores de todo el proyecto:

- Soberanía tecnológica.
- Software libre.
- Interoperabilidad.

Principios de organización:

- **Contrataciones bajo legislación argentina y en moneda nacional**. Los servicios de la nube híbrida deben poder ser contratables mediante contratos enmarcados en su totalidad en el ordenamiento legal argentino, y pagables en moneda nacional.

- **Convivencia de múltiples proveedores de manera transparente**. Los usuarios de la nube deben contar con un conjunto de servicios que sean provistos de manera transparente por multiplicidad de proveedores. El usuario debe poder migrar sus servicios de uno a otro de manera transparente.

- **Existencia de infraestructura propia**. Entre esos múltiples proveedores es **indispensable** que la propia Arsat sea uno de ellos y que brinde servicios completamente alojados en su propio datacenter de manera de asegurar los máximos niveles de soberanía y observancia a las leyes nacionales.

- **Inclusión de otros organismos, entidades y empresas**. Otros organismos públicos y entidades (cooperativas, universidades, empresas, etc.) deben poder sumar su infraestructura a la nube híbrida de manera tal de poder gestionar sus recursos propios y los arrendados a otros actores de la nube de manera integrada, pero a su vez de poner ofrecer su capacidad de cómputo excedente para que pueda ser utilizada por otras actores del ecosistema híbrido. Para ejemplificarlo, imaginemos un organismo que brinda un servicio que en condiciones normales requiere 5 servidores y tiene momentos de pico donde son necesarios otros 5 más. Este organismo debería

poder conectar 10 servidores de su centro de cómputo a la nube, indicando que 5 son de uso dedicado a sus propias necesidades y los otros 5 pueden correr carga de trabajo de otros actores cuando el propio organismo no los utiliza. Si en algún momento su propia demanda requiere 15 servidores y no sólo 10, los adicionales son provistos de manera automáticamente por cualquiera de los otros actores que forman parte de la nube híbrida. La cantidad de servicios que haya prestado a otros y los que haya requerido de otros determinará si a fin de mes debe pagar una factura o recibir dinero.

- **Transparencia respecto a los niveles de calidad de servicio**. Los distintos actores participantes en la nube brindarán servicios con diferentes parámetros de calidad.
    - Tendrán distintos precios.
    - Garantizarán o no que sus servicios se prestan desde el país (soberanía)
    - Garantizarán distintos parámetros de red (ancho de banda, latencia, redundancia, etc.).
    - Garantizarán distinta calidad de equipamiento.

  A la hora de elegir cualquiera de los proveedores dentro de la red debería ser claro para el usuario cuáles son las características que le están siendo ofrecidas en todas estas dimensiones. Será función de Arsat certificar que los parámetros efectivamente ofrecidos coincidan con los declarados.

Soberanía tecnológica

Es importante destacar que hoy en día la implementación de casi la totalidad de las políticas públicas requiere algún soporte informático. Desde el análisis de grandes datos de salud en el contexto de la pandemia de covid, hasta de las políticas de desarrollo social como la AUH. Este nivel de informatización de la gestión del Estado sólo va a crecer en los próximos años, a un ritmo cada vez más acelerado.

Sin soberanía tecnológica el Estado se ve obligado a restringir su capacidad de decisión sobre las herramientas tecnológicas que despliega para dar respuesta a sus necesidades y a las de la ciudadanía. Esa falta de libertad para decidir tiene no sólo implicancias técnicas sino también éticas y políticas.

Un ejemplo ilustrativo de esta dificultad en la búsqueda de soberanía podría ser la necesidad de que un organismo público brinde un canal de atención mediante WhatsApp, algo que es muy razonable dado que se trata de la herramienta de comunicación favorita de gran parte de la población nacional. Sin embargo, WhatsApp es una empresa que hoy en día le pertenece a Facebook, empresa que decidió cerrarle la cuenta al presidente en ejercicio de los Estados Unidos. Sin importar la gravedad de lo ocurrido, incurrió en un acto de censura sin que mediara orden judicial. Hoy en día las opciones de repudiar ese comportamiento no utilizando la plataforma se ven limitadas.

Otro ejemplo muy claro lo brindó la posibilidad de la implementación de detección de contactos estrechos mediante emisiones de bluetooth de baja energía, tecnología que al principio de la pandemia fue presentada como la panacea contra la covid-19 y que requería ser implementada a nivel *kernel* por los sistemas operativos de los teléfonos celulares. Fue así que Google y Apple realizaron un acuerdo para implementar la tecnología y ponerla "a disposición" de los estados nacionales para que realizaran sus propias aplicaciones de salud. Resultó ser que para acceder a dicha tecnología era necesario firmar un acuerdo con estas empresas en las que los estados aceptaban que las aplicaciones no pudiesen tener ciertas funcionalidades y les daban a ambas empresas potestad de supervisión sobre el desarrollo de la propia aplicación pública, en el medio de una pandemia.

La tecnología de nube aparece en el centro de cualquier implementación tecnológica de hoy en día. Es por eso que el Estado debe asegurarse su control legal, intelectual y operativo. Una nube basada en

tecnologías libres permite que el Estado conozca todos los detalles de la tecnología que emplea y le da la posibilidad de tomar sus propias decisiones tecnológicas.

Despliegue federal y multi actor

Para el país, sumar la mayor cantidad de recursos de una manera inteligente para su disponibilización y uso es muy importante. Para ello es mandatorio que pensemos esta política pública como la posibilidad de integrar ordenadamente toda o la mayoría de la infraestructura de los grandes y medianos organismos públicos nacionales, provinciales y municipales. Estos que ya cuentan con infraestructura propia y normativa dura, en materia de tratamiento de datos, por ejemplo. Podrían sumar sus equipos actuales o de inversiones futuras en un esquema donde, por ser nube híbrida, en función de esas necesidades tener la posibilidad de migrar servicios ante determinado contexto y elegir el proveedor que mejor se ajuste a esas necesidades.

Por otro lado, una nube pública híbrida permite incorporar a las pymes y también a las cooperativas que se dedican a las telecomunicaciones y cubren una importante zona del país, especialmente, en la última milla. Estas pueden sumar sus centros de cómputos como proveedores de infraestructura en la nube y/o pensar servicios de mayor valor agregado con CDN nacionales. De esta manera, se bajan las barreras de ingreso para la participación del mundo pyme y cooperativo en esta política pública.

La nube pública híbrida es además un espacio donde **cada actor puede maximizar sus recursos digitales.**

Los **Gobiernos Provinciales y Municipales** u otros organismos públicos que no cuenten con su propia infraestructura, encuentran en la nube pública híbrida un espacio donde abaratar costos con el cumplimiento de la normativa vigente. En este sentido la Nube debe transparentar y facilitar sus servicios digitales con el fin de asegurar la igualdad de oportunidades por parte de todos los entes.

Los **centros de investigación y universidades** encuentran en la nube híbrida nacional un espacio donde escalar sus propias infraestructuras pero sobre todo un lugar donde poder desarrollar investigación con grandes procesamientos de datos. En este sentido debe pensarse la nube también como un espacio de innovación y experimentación.

Las **empresas públicas y bancos públicos** también pueden ser parte de la nube híbrida nacional aportando su experiencia utilizando servicios que mejoren y diversifiquen sus prestaciones digitales.

Las **empresas de desarrollo de software** encuentran en la nube pública una oportunidad para aportar sus conocimientos y brindar más servicios generando más trabajo local y menor erogación de divisas al extranjero.

Las **empresas nacionales de infraestructura** pueden sumar sus centros de cómputo y contar con la nube tanto como un mecanismo de compensación ante exceso de demanda como uno de generación de ingresos adicionales.

Los **sindicatos, organizaciones del mundo del trabajo** y **sus trabajadores** podrán acceder a menores niveles de informalidad y empleo en condiciones abusivas.

Seguridad de la información

En un modelo de computación en en la nube, los usuarios del servicio entregan sus datos y delegan diferentes formas de cómputo en el proveedor de la plataforma, que se responsabiliza por garantizar la confidencialidad, integridad y disponibilidad de los datos y computaciones. El Estado, al brindar o promover la existencia de un servicio de Nube Híbrida, tiene la obligación irrenunciable de velar porque el servicio provisto cumpla con estas cualidades. Estas responsabilidades sólo pueden cumplimentarse en tanto el Estado reserve para sí la capacidad de controlar cada uno de los componentes que intervengan para la provisión de los servicios.

El software libre es una herramienta fundamental para lograr estos objetivos, debido a que permite que cualquier componente de la solución sea auditado en búsqueda tanto de código malicioso como de errores y vulnerabilidades, por parte de toda la sociedad: organismos estatales, universidades públicas y privadas, organizaciones de la sociedad o incluso actores privados.

Una plataforma basada en software propietario no brinda las mismas garantías de seguridad, debido a que no puede ser validada y, por lo tanto, queda delegada la responsabilidad al proveedor, sujeta a sus propias necesidades comerciales. Incluso, en el caso de compañías multinacionales, la actividad se ve condicionada por la obligación de cumplir con normativas extranjeras, que en múltiples ocasiones se han visto obligadas a compartir la información de sus usuarios con las agencias de seguridad de sus países de origen.

Para información muy sensible, sin un alojamiento en territorio nacional bajo control nacional es muy difícil garantizar en términos reales que se cumplen esas garantías de seguridad y que el acceso a esa información sólo pueda ser autorizada por la Justicia nacional, conforme a las leyes nacionales. Cuando el alojamiento cruza la frontera, es muy difícil asegurar que no exista otro ordenamiento legal aplicable. Incluso en casos donde los proveedores presentan como garantía algunas cláusulas contractuales, estas podrían ser nulas debido a la primacía de normas de carácter superior de aquellos países donde la información está efectivamente alojada.

A modo de ejemplo, las leyes de los Estados Unidos, donde residen gran parte de los centros de cómputo que alojan y procesan datos de los servicios de nube privados, permiten, a partir de la Foreign Intelligence Surveillance Act (1978), la recolección masiva de información de países y ciudadanos extranjeros por parte de la Agencia de Seguridad Nacional de los Estados Unidos (NSA). Si bien estas leyes estaban originalmente propuestas como una herramienta de defensa contra el terrorismo, los controles sobre su aplicación fueron escasos y leyes posteriores como la Patriot Act (2001), Terrorist Surveillance Act (2007), entre otras, incrementaron la posibilidad de intervenir las comunicaciones, incluso sin la necesidad de una orden judicial. El "affaire Snowden" trajo a la luz profusa documentación que demostraba su utilización para recolección de todo tipo de información de personas no vinculadas a ningún tipo de acto delictivo y, si bien en los últimos años se han incorporado normativas que defienden los derechos de los ciudadanos a la privacidad, estas leyes se ocupan casi exclusivamente de la protección los ciudadanos locales de ese país, manteniendo las atribuciones discrecionales de varias agencias para la recolección de datos de extranjeros.

Adicionalmente, las nubes privadas acarrean gravosas consecuencias en términos de **propiedad intelectual** de los documentos y demás bienes informacionales alojados en ellas. En muchos casos, el alojamiento en nubes privadas extranjeras implica la concesión de licencias respecto de los documentos en favor de los titulares de los servicios de almacenamiento. En un contexto en el que los agentes del estado que hacen uso de estos servicios no siempre realizan una evaluación cuidadosa de los términos y condiciones que aceptan, una nube híbrida del estado debería ofrecer ventajas claras, impidiendo el

aprovechamiento legal e ilegal, con y sin fines de lucro de las obras de autoría alojadas en la nube para fines distintos de los del desarrollo nacional.

Generación de empleo

La nube híbrida nacional puede tener impactos virtuosos en la cantidad y calidad del empleo argentino al menos mediante dos mecanismos. El primero se asocia a la creación directa de empleos y consiste en reemplazar parte del masivo trabajo que realizan las plataformas extranjeras y privadas; plataformas que, en muchos casos, no respetan las condiciones de trabajo estipuladas por los marcos legales nacionales ni ofrecen remuneraciones justas.

El segundo mecanismo refiere a que, de manera indirecta, la nube híbrida de gobierno puede impulsar el crecimiento de las firmas del sector SSI argentino y así incrementar la cantidad y calidad del empleo en el sector. De hecho, pese a su sostenido crecimiento y su capacidad para generar trabajo y agregar valor, el sector se encuentra aún poco integrado con el Estado. La nube híbrida es, por ello, una excelente oportunidad para demandar desarrollos y servicios del sector SSI que a su vez, generen más empleo local e, incluso, para hacerlo priorizando a las empresas que garanticen condiciones de trabajo y remuneraciones justas para para sus trabajadores y trabajadoras.

Ahorro de divisas

Una de las ventajas del modelo de nube híbrida propuesto es que **se reduce sustancialmente la erogación de divisas o incluso en algunos casos se puede hasta evitar.** Esto encuentra su fundamento en el hecho de que:

- Si lo hacemos con herramientas open source o de código abierto, muchas veces se puede evitar tener que recurrir a soluciones pagas provistas por proveedores extranjeros bajo la modalidad de licencias.

- Dado que el hardware es ofrecido por ARSAT, y por consiguiente, adquirido en gran escala, el costo es significativamente más bajo.

- Dado que el hardware se encuentra virtualizado a través de tecnologías como OpenStack y Kubernetes, entre otras, es posible no depender de un soporte físico y, a su vez, consumir recursos sólo cuando se necesita, en lugar de hacerlo todo el tiempo. Esto a fin de cuentas se traduce en una optimización en la administración de dichos recursos.

- Un modelo de software como servicio (SaaS) permite generar sobre la base de una plataforma común una cartera de herramientas articuladas entre sí que pueden utilizarse para diversos fines en toda la organización: Recursos Humanos, Presupuesto, Patrimonio, etc. Así, se evita recurrir a soluciones externas y se optimiza el desarrollo de sistemas brindando herramientas que pueden utilizarse en todo el Estado Nacional.

- Generalmente, al adquirir software licenciado, resulta casi indispensable sumar un ítem de capacitación al presupuesto para poder hacer uso de las soluciones y éste suele ser bastante alto. Por el contrario, en un modelo como éste, el desarrollo de herramientas comunes para diversos grupos de trabajo, habilita la generación de comunidades donde el aprendizaje en el uso de las herramientas puede darse de una manera más transversal y colaborativa, atravesado por un marco de conocimiento global e integral.

- Lo anterior a su vez permite contar con consultores locales y no depender de servicios de consultoría externa que se facturan en dólares.

En conclusión, se reduce al mínimo la erogación de divisas, al concentrarse ésta únicamente en la adquisición del hardware necesario.

Herramientas disponibles

En esta sección describimos las herramientas de software libre sobre las que podría basarse una nube soberana. Se trata de herramientas maduras, con comunidades fuertes, amplias y diversas, que las respaldan. Otras experiencias en el mundo, como la de Estonia, que repasamos en este mismo documento, las usan como epicentro de sus desarrollos de nube soberana.

Si bien existe un amplio abanico, las dos herramientas más destacadas son OpenStack y Waldur, que reseñamos brevemente.

> *OpenStack es un proyecto de computación en la nube para proporcionar una infraestructura como servicio (IaaS). Reproducimos la reseña que se hace de esta herramienta en Wikipedia:*
>
> *Es un software libre y de código abierto distribuido bajo los términos de la licencia Apache. El proyecto está gestionado por la Fundación OpenStack, una persona jurídica sin fines de lucro creada en septiembre de 2012 para promover el software OpenStack y su comunidad.*
>
> *Más de 200 empresas se unieron al proyecto entre las que destacan Huawei, AMD, Avaya, Brocade Communications Systems, Canonical, Cisco, Dell, Ericsson, Groupe Bull, HP, IBM, InkTank, Intel, NEC, Rackspace Hosting, Red Hat, OVH, SUSE Linux, VMware y Yahoo!.*
>
> *La tecnología consiste en una serie de proyectos relacionados entre sí que controlan estanques de control de procesamiento, almacenamiento y recursos de red a través de un centro de datos, todos administrados a través de un panel de control que permite a los administradores controlar mientras potencia a sus usuarios proveyendo los recursos a través de una interfaz web.*
>
> *La comunidad OpenStack colabora en torno a un ciclo de lanzamiento con hitos de desarrollo de frecuencia semestral.7 Durante la fase de planificación de cada lanzamiento, la comunidad se reúne para la Cumbre de Diseño OpenStack para facilitar sesiones de trabajo para desarrolladores y armar planes a futuro*

Waldur es una herramienta opensource de *brokerage* de servicios de nube, también en el centro de la implementación de Estonia, que permite consumir transparentemente los servicios de nube de distintos proveedores y migrar entre ellos sin requerir adecuaciones específicas.

Caso de éxito: Estonia

La experiencia de Estonia

El desarrollo de una nube pública híbrida en Estonia es fruto de un largo camino de decisiones tomadas en la dirección de ser un Estado 100% digitalizado. La gran mayoría de trámites con entidades gubernamentales se puede hacer de manera digital y desde el año 2000 cada habitante tiene asociada una clave pública (PKI).

Estonia viene usando servicios de nube provistos por los principales proveedores multinacionales desde el año 2009, cuando publicaron en Amazon la página *visitEstonia.com*. En el año 2013 se hizo un relevamiento sobre el uso de los servicios de nube contratados hasta el momento por las diferentes dependencias estatales y se llegó a la conclusión de que era necesario organizarse de una manera más eficiente dado que había una dispersión grande de diferentes contrataciones. Los objetivos principales de esta reorganización no fueron abaratar costos, sino mejorar la calidad de los servicios ofrecidos a los diferentes estatales y estandarizar políticas de seguridad. Y es desde esa necesidad de reorganización que surge el proyecto de construir una nube diseñada por y para el Estado.

Ya en el año 2016 comienza el desarrollo de la nube híbrida en Estonia, liderado por la Fundación Estatal de Comunicación de la Información (en adelante **RIKS**). Se definen como “el operador de la infraestructura básica de la sociedad de la información de Estonia”. La nube híbrida fue creada en cooperación entre los sectores público y privado, un consorcio que incluye a Cybernetica AS, Dell EMC, Ericsson Eesti AS, OpenNode OÜ y Telia Eesti AS.

Además del sector gubernamental, los clientes de la Nube Nacional son gobiernos locales, proveedores de servicios vitales (ETO), empresas privadas que brindan servicios de TI al estado y proveedores de atención médica.

Oferta de la nube pública estonia y solución tecnológica

La oferta de servicios de la nube estonia es muy variada. Se apunta a cubrir la demanda que pueda tener desde una dependencia municipal hasta un ministerio que necesite infraestructura para ejecutar sus soluciones de software. Es por esto que se ofrecen servicios transversales de gestión (como correo electrónico u ofimática colaborativa), como también servicios más complejos como IaaS (*Infrastructure as a Service*, o Infraestructura como Servicio) mediante OpenStack o instancias de bases de datos Postgres. La estrategia para brindar esos servicios es, en su mayor parte, la asociación con empresas que forman parte del consorcio y que proveen los servicios a través de la nube nacional estona. Esto lo que permite es que se cumplan algunos objetivos centrales: evitar el *vendor lock-in*, la operatoria segura centralizada y el resguardo de información sensible.

Con respecto al *vendor lock-in,* la solución planteada es consumir servicios tipo IaaS/PaaS a través de un middleware desarrollado por la empresa OpenNode, empresa estonia que es responsable del liderazgo técnico. Este middleware se llama **Waldur** y permite administrar varias nubes de manera agregada y centralizada, como si fuesen una sola. Permite sumar al servicio agregado nubes privadas con OpenStack como también recursos de los proveedores internacionales más conocidos.

En lo que respecta a seguridad, la solución ha sido construida siguiendo los lineamientos del estándar **ISKE**, el estándar de seguridad nacional estonio y todo nuevo actor debe estar alineado con ese estándar. Una de las empresas pertenecientes al consorcio, Cybernetica, justamente es la encargada de acompañar en ese proceso de adopción del nivel H de los estándares ISKE (**ISKE-H**). Cabe mencionar que también construyeron un bus de información securizado llamado **X-Road** para compartir datos entre los diferentes actores que usan la nube híbrida. También son muy exigentes con el nivel de auditoría que tiene este servicio de nube, auditado por auditores externos de manera anual.

Algunas conclusiones del caso estonio

El caso estonio demuestra que la concreción de un proyecto de nube híbrida estatal es imprescindible y un objetivo ineludible si se quiere construir un Estado moderno, digitalizado, pero sin resignar soberanía tecnológica. No basta con avanzar en medidas de digitalización del Estado sin estandarización y sin las medidas de seguridad adecuadas, y en el caso de Estonia, es el Estado el que está de garante para que

esto ocurra. La presencia del Estado como garante también ayuda y genera que la unión de esfuerzos de la esfera pública con la privada se dé de manera virtuosa.

Elaboración del documento

Las siguientes personas participaron de la elaboración del documento a título individual.

- Leandro Monk, gcoop - FACTTIC
- Fernando Schapachnik, Fundación Sadosky & ICC UBA-CONICET
- Sebastian Uchitel, Director Instituto UBA/CONICET de Ciencias de la Computación.
- Pablo Vannini, gcoop - UNPAZ
- Mariano Zukerfeld- Conicet - e-TCS/Centro CTS/Umai
- Andrea Díaz, Lic en Ciencias de la Computación, UBA. Esp en Gestión de la Tecnología y la Innovación, UNSAM.
- Julián Dunayevich. Lic. en Ciencias de la Computación.
- Juan Lagostena, Ing. en Informática, docente universitario.
- Nicolás Passerini, Ingeniero en Sistemas de Información, docente universitario. Director de Seguridad de la Información en AFIP

Adhesiones personales

(en orden alfabético)

- Adriana Pintos
- Agustín Martinez Suñé,Jefe de Trabajos Prácticos - Departamento de Computación, Universidad de Buenos Aires.
- Agustina Silombra, Asociada a Cooperativa de Trabajo El Maizal
- Alejandra Martinetto, Docente investigadora de la Universidad Nacional de Luján
- Alejandro Héctor Gonzalez,Director General de Educación a Distancia y Tecnologías. UNLP
- Alejandro Otero, FIUBA -CONICET
- Alexis Soifer,Investigador de Doctorado, Departamento de Computación - Universidad de Buenos Aires
- Alexis Tcach, Asesor de directorio en sistemas de Fabricaciones militares SE
- Andres Isaac Benavides, Software Engineer TECSO
- Andrés Racket
- Antonela Isoglio, UNC, CONICET
- Ariel Caminos, MateLab
- Ariel Glikman, Ingeniero en Sistemas de Información - FRBA - UTN
- Bruno Bianchi, Departamento de Computación, FCEN, UBA
- Carlos Alberto Crespo
- Carlos chesñevar, ICIC CONICET UNS
- Carlos Damián Nuñez, Presidente Coooperativa BANTICS Ltda.
- Carlos Gustavo Nuñez, Cooperativa BANTICS
- Carlos Lombardi, Profesor Titular Ordinario, Universidad Nacional de Hurlingham
- Cecilia Galarza, Directora de CSC - CONICET
- Cecilia Kilmurray, Docente Depto Computación - UNRC
- Cecilia Perren, Docente de UNRaf

- Claudia Leonora Nogueira
- Cristian Mateos Diaz, ISISTAN-UNICEN-CONICET
- Dan Rozenfarb
- Daniel A. Rodriguez, Miembro de la Junta Directiva de The Document Foundation - LibreOffice
- Daniel Ciolek, Profesor Instructor UNQ
- Daniel Sentinelli
- Diego Garbervetsky, Profesor FCEyN. Universidad de Buenos Aires. Investigador CONICET
- Diego Milone, Investigator Principal CONICET, Profesor Titular UNL
- Enzo Catrin, TIC UncoMa
- Èrika Lopez, Unraf
- Esteban Mocskos, Profesor DC-FCEN-UBA, Investigador CSC-CONICET
- Facundo Molina, Departamento de Computación, FCEFQyN, Universidad Nacional de Rio Cuarto
- Federico Palavecino
- Federico Sodo
- Fernando Peirano, Presidente Agencia I+D+i
- Fernando Riccitelli, Director General de Sistemas de Información, Comunicación y Procesos del INTA
- Florencia Anahi Otarola, Desarrolladora de software, asociada a la cooperativa tecnológica Cambá (cargo en secretaría del concejo).
- Gabriel Alvarez, Jefe de Ingeniería
- Gabriel Glusgold
- Germán Regis, Profesor Adjunto en la Universidad Nacional de Río Cuarto
- Guillermo Oscar Bustelo, Coordinador de Patentes de Invención de la Defensa en el Ministerio de Defensa
- Guillermo Ricardo Simari, Profesor Emérito, Departamento de Ciencias e Ingeniería de la Computación, Universidad Nacional del Sur
- Hugo Haurech, FCE
- Iván Arcuschin Moreno ICC, CONICET
- Javier Alejandro Pignata, Agencia de Sistemas de la Información - GCABA
- Javier Bilatz, UNPaz - Universidad Nacional de José C. Paz
- Javier Castrillo, Consultor en Fundación Sadosky Docente en UNPAZ y UNAHUR Coordinador en Huayra Linux
- Javier Obregón
- José Daniel Daza, Antropólogo y etnógrafo digital
- José Louzao, fundador G&L Group
- Juan Augusto Maya, CSC-CONICET/UBA
- Juan Manuel Carranza
- Juan Pablo Delpino, Ingeniero en Sistemas, Director Operativo y de Tecnologia en Cooperativa de Trabajo Tecso Ltda.
- Juan Pablo Lalia
- Laura Billi, Analista de aplicaciones informáticas, Aerolíneas Argentinas
- Leandro Nahabedian, Ingeniero de datos - Practia Global
- Leonardo Fagnano, Project Manager
- Leonardo Tadei, director de Pegasus Tech Supply
- Lisandro Raviola, Docente investigador, Universidad Nacional de General Sarmiento
- Lucila Dughera, Conicet- e+tcs
- Lucrecia Odierna, Docente UNPAZ
- Marcela Gatto, Subsecretaria de Gestión Académica Bimodal, Undav
- Marcelo Báez, Profesor en Informática
- María Laura Giovannini, Docente de UNRAF. Docente de nivel medio en Provincia de Santa Fe
- Mariana ferrer, Docente
- Mariana Soengas Álvarez, Docente en UNPAZ

- Mariano Absatz, Licenciado en Ciencias de la Computación
- MAriano Camilo González Lebrero, INvestigador adjunto del CONICET/profesór adjunto de la UBA
- Mariano Cerrutti, Docente en FCEyN, UBA, estudiante de doctorado, LaFHIS
- Mariano Stampella, ANSES
- Mariano Zukerfeld, Conicet
- Martin Ales, gcoop Cooperativa de Software Libre
- Martin Vallone, Cooperativa de Trabajo Fiqus LTDA
- Matías Barbeito
- Matias Garcia, Profesor de nivel superior en UTN-INSPT y ISP Dr. Joaquín V. González, miembro de USLA, Ubuntu-ar, CaFeLug, BairesNorteLug, staff organización de FLISoL.
- Matías Hirsch, Investigador Asistente, Conicet
- Matias Kraier, tecso
- Matias roa
- Matías Romo
- Mauricio Aiello, Arquitecto de Software ne Temperies S.A
- mauro pedro tellchea garcia, virtualmind
- Mauro Theler, Docente Unraf
- Miguel Pagano, Director de la Lic. en Cs. de la Computación, FAMAF-UNC
- Nazareno Aguirre, Universidad Nacional de Río Cuarto y CONICET
- NELSON GUSTAVO SAN JOSE, Responsable Informatica Conectividad y Sistemas - UNAU
- Nicolas aliburton
- Nicolás Dimarco, Socio en Fiqus
- Nicolas dippolito, Profesor adjunto, FCEyN, UBA
- Nicolás Doallo, Presidente, Cooperativa de Trabajo Cambá Ltda.
- Pablo Ernesto Martínez López, Profesor Titular, Universidad Nacional de Quilmes
- Pablo Germán Perrone, Gerente de proyectos en Cooperativa de trabajo Tecso Ltda
- Pablo Kogan, Secretario de Extensión Facultad de Informática de la Universidad Nacional del Comahue
- Pablo Ramírez, Profesor
- Patricio Mazzaro, Ingeniero Electrico
- Pedro R. D'Argenio, Prof. Titular, FAMAF, Universidad Nacional de Córdoba Inv. Independiente, CONICET
- Ramiro Facundo Polverini Suarez, Cooperativa BANTICS
- Ricardo Medel, Fundación Dr. Manuel Sadosky, UTN FRCórdoba
- Ricardo Sánchez Peña, Inv. Superior CONICET en ITBA
- Sergio Romano, Gerente Vinculación Tecnológica, CONICET
- Silvia Coicaud, Directora de posgrados a distancia, UNPSJB
- Silvia Maria Pigñer, Silvia Maria Pigñer. Especialista en Educación
- Silvia Natalia Martínez
- Simón Emmanuel Gutiérrez Brida, Ayudante de primera en Departamento de Computación, UNRC, Río Cuarto.
- Soledad Ayala, Profesora e investigadora (UNRaf-UNQ)
- Soledad Moreno, Analista de Sistemas y metodologías de desarrollo
- Sonia Permigiani, Docente de la UNRC
- Valeria Becker, Mincyt, UNTREF
- Vera Bogdanich Espina, Microsoft
- Virginia Brassesco, Docente universitaria (UniPe, Exactas). Doctoranda Ciencias de la Computación Exactas UBA.

Adhesiones institucionales

(por orden albabético)

- bmesh hacklab
- CATEL - Cámara de Cooperativas de Telecomunicaciones
- Ciencias de la Computación - FAMAF - Universidad Nacional de Córdoba
- Club de Software Libre
- CNCT
- Cooperativa Batán de Obras y Servicios Públicos
- Cooperativa de trabajo Cambá Ltda.
- Cooperativa de Trabajo Codigo Libre LTDA.
- Cooperativa de Trabajo Fiqus LTDA
- Cooperativa de trabajo informática y telecomunicaciones 10 Ltda - IT10
- COTTIC Ltda
- El Maizal - Cooperativa de Comunicación
- FACTTIC Federación Argentina de Cooperativas de Trabajo de Tecnología, Innovación y Conocimiento
- Facultad de Ciencias Exactas y Naturales, UBA
- Facultad de Matemática, Astronomía, Física y Computación (FAMAF)
- GAIA Cooperativa de desarrollo de Software
- Gcoop – Cooperativa de Software Libre
- Instituto Superior de Ingeniería de Software de Tandil (UNCPBA & CONICET)
- Internauta, Asociación Argentina de Usuarios de Internet
- Matelab
- Nim Latinoamerica
- Nodo Tau Asociación Civil
- Observatorio de Impactos Sociales de la Inteligencia Artificial - OISIA
- Orion Pagos, de Tertium SA
- PampaSeg
- Redjar Cooperativa de Trabajo Ltda.
- Universidad Nacional de Quilmes (UNQI)