

**COPITEC**

**TRABAJO EN CONJUNTO ENTRE COMISIONES  
SOBRE EL DOCUMENTO DE CONSULTA  
“Nube Híbrida en Gobierno”  
Anexo IF-2021-19049956-APN- ONTI#JGM**

**OBJETIVO**

El presente trabajo fue realizado por la *Comisión ad-hoc* integrada por miembros de las comisiones del COPITEC de Informática, Ciberseguridad y Peritos, convocados por la Ing. Lidia Seratti, en su carácter de vicepresidenta de la entidad, en base al Documento de Consulta “*Nube Híbrida en Gobierno*”.

Autores:

- **Ing. Miguel Angel Blanco**- Miembro de la Comisión de Peritos e Informática
- **Analista Gastón Terán Castellanos** – Coordinador de la comisión de Informática
- **Ing. Pablo Croci** - Perito informático convocado por las Comisiones de Informática y Peritos
- **Lic. Patricia Delbono** - Consejera Titular y Coordinadora de la comisión de Peritos
- **Ing. Carolina Diéguez Herrera** – Representante de la Comisión de Ciberseguridad
- **Lic. Javier Vallejos** – Miembro de la Comisión de Informática

Al final del presente documento se detallan los CV de los autores.

**FUNDAMENTOS DEL TRABAJO CONJUNTO**

La Resolución de la (ex) SECRETARÍA DE COMUNICACIONES No 57/1996, aprobó, como Anexo I, el “*Reglamento General de Audiencias Públicas y Documentos de Consulta para las Comunicaciones*”, por medio del cual se regula el procedimiento denominado “*Documentos de Consulta*”.

Que de acuerdo con el requerimiento que menciona “*que conforme las políticas de participación y transparencia adoptadas por la SECRETARÍA DE INNOVACIÓN PÚBLICA, resulta oportuno someter la cuestión a consulta pública, a fin de recabar información, contribuciones, propuestas, experiencias y recomendaciones de las partes interesadas para mejorar la implementación de una “Nube Híbrida en Gobierno”, habilitando un espacio para la participación ciudadana.*”

Y considerando que es pertinente la participación del COPITEC en forma institucional, dado que su jurisdicción abarca las actividades profesionales independientes que exijan presentaciones o aprobaciones de entes nacionales o tribunales federales y de igual modo, quedan también bajo jurisdicción nacional, ejercida a través de los Consejos que comprende el Decreto Ley 6070/58, los profesionales que desempeñan tareas en relación de dependencia en reparticiones públicas y empresas del Estado, con sede física en la Capital Federal o en territorio provincial, presentamos para su análisis el siguiente Informe preliminar:

## **INFORME PRELIMINAR**

La reunión del equipo se llevó a cabo a través de la modalidad virtual, mediante la plataforma *Zoom* perteneciente al Consejo, en el día y horario citado.

Con la finalidad de generar un único documento, desde el COPITEC se decidió analizar inicialmente algunos temas relevantes, dando recomendaciones sobre los 4 aspectos/ejes del documento, que son los siguientes:

### **1 – DATOS**

1.1 TERRITORIALIDAD

1.2 - SEGURIDAD

1.3 – PRIVACIDAD

### **2 – ADMINISTRACIÓN Y GESTIÓN DE LA NUBE**

2.1 CONSOLA

2.2 APARIENCIA

2.3 ESTÁNDARES ABIERTOS Y SOLUCIONES INTEROPERABLES

### **3 - INVERSIONES**

#### **4 –VINCULACIÓN DE ARSAT CON UN PSN**

##### 4.1 TEMPORALIDAD

##### 4.2 TÉRMINOS

#### **- Conceptos Generales**

Conforme a los principales puntos considerados y analizados del documento recibido por parte de las autoridades, podemos considerar viables acciones concretas que pudiera llevar adelante el COPITEC, en las condiciones y marcos vinculares que la Dirección del COPITEC y las autoridades que eventualmente defina, teniendo en cuenta que pasar a SERVICIOS EN LA NUBE implica una inminente transformación digital.

En tal sentido y conforme a algunas estadísticas publicadas por *DELOITTE 2019*, *KPMG, 2019*, las llamadas transformaciones Digitales, no se llevan adelante sin atravesar profundas crisis organizacionales, ya sea en el sector privado o en el sector público. En este último ámbito la problemática es mayor y es aquel al que pretendemos desde el COPITEC, hacer aportes. Para entender a qué nos enfrentamos, hacemos referencia a algunos datos estadísticos que detallamos a continuación:

- Alrededor del 96% de las organizaciones estiman crítica e importante la transformación digital. En su mayoría tienen designada una dependencia o cargo responsable, para llevar adelante dicha innovación y/o modernización.

Sin embargo, es curioso entender que en un 72% se trata de administradores clásicos sin formación específica.

- La carencia de estrategias de implementaciones digitales alcanza al 64 % de estas organizaciones, es decir liderazgos con una finalidad que no dominan y para la que no se tienen planes (KPMG, 2019).
- Una significativa alerta estima que al menos el 40% de las empresas tienden a desaparecer en un término de 10 años, si no logran una adecuada adaptación que impone la tecnología en sus procesos productivos y administrativos.

Un dato más que interesante, nos dice que casi el 70% de la Administración Pública mundial se encuentra con serias deficiencias en el camino de una adecuada Transformación Digital, con relación a las organizaciones del ámbito privado (DELOITTE INSIGHTS – TECH TRENDS 2019)

### **- Información a recabar**

- *Verificar información adicional referente a:*

1. ¿ARSAT está en condiciones de cumplir con todos los requerimientos?
2. ¿Será ARSAT el único Centro de Datos que se utilizará para la nube híbrida?

- *Respuesta a la Consulta Pública – Nube Híbrida de Gobierno*

En la actualidad la nube, no es solo el repositorio o destino de nuestros datos sino una nueva forma de hacer las cosas. Por esto y con relación a esta consulta que nos parece acertada y sumamente interesante, consideramos no deben dejarse de lado los siguientes aspectos:

- *¿Quién estará a cargo de la administración?*
- *¿Quién dará soporte?*

### **- Experiencias y recomendaciones**

#### 1.- Tipo de Software a utilizar

Evaluar el tipo de contratación como servicio, más conveniente para cada caso, dado lo heterogéneo de cada una de las instituciones/ clientes que tendrá esta Nube. Seguramente, alojada físicamente en el datacenter de ARSAT y en algunos casos particulares, en casa de cliente (*“On Premises”*), con el fin de salvaguardar los datos.

#### 2.- Latencia

Evaluar si existen casos en que la latencia aún es un desafío y entonces revisar la posibilidad de hacer uso de tecnología *“Computing Edge”* vía IoT.

### 3.- Seguridad y Gobernanza

- Es deseable que el propio usuario mantenga la gobernanza de los datos.
- Implementar políticas de acceso, garantizar el cifrado adecuado (de datos tanto en tránsito como en reposo) y administrar la configuración general del servicio en la nube para satisfacer las necesidades de la organización.

Los recursos y las cargas de trabajo en la nube están expuestos a una amplia variedad de amenazas de ciberseguridad, como las filtraciones de datos, el *ransomware*, los ataques de denegación de servicio (DDoS) y los ataques de phishing. Disponer de sistemas y prácticas de seguridad en la nube es fundamental para mantener la disponibilidad de las aplicaciones vitales para la organización, proteger la información confidencial y garantizar el cumplimiento de la normativa.

Consideramos requisito mandatorio la encriptación de datos.

- Implementar el principio de mínimo privilegio
- Evaluar la necesidad de una seguridad de endpoint sólida
- Capacitación adecuada de los usuarios sobre seguridad

Se destaca la importancia que todos los usuarios de la nube sean conscientes de sus responsabilidades y conozcan los requisitos para cumplir con las políticas de seguridad de la organización

### 4.- Monitoreo

El monitoreo y evaluación continuos de actividades permite detectar anomalías de la nube y patrones preocupantes, así como a identificar riesgos y actuar para evitar futuros daños.

### 5.- Soporte / Almacenamiento

Las organizaciones deben tener un plan de respaldo que garantice que las operaciones se ejecutarán sin problemas en caso de emergencias, como la interrupción de los servicios o cortes de energía en los centros de datos. Esto incluye la implementación de

copias de seguridad basadas en imágenes que pueden crear copias de máquinas virtuales (VM) que a su vez se pueden usar para restaurar o recuperar datos.

### **- Propuestas**

Consideramos un requisito mandatorio incorporar el Análisis Forense, y la respuesta ante incidentes. Ambas disciplinas se las conoce como DFIR (*Digital Forensic & Incident Response*). Aquí el peritaje informático, y la respuesta ante incidentes, comparten con el análisis forense una disciplina central. Esto permite determinar el origen y las causas de un incidente de seguridad, y el ámbito de respuesta para mitigar el incidente y tomar medidas, a fin de evitar que vuelva a suceder. El análisis en tiempo real, (crucial para una plataforma en la nube), quedan enmarcadas en las normas ISO 27037/42/

En definitiva, proponemos elaborar un plan básico común, flexible y adaptable, que permita que todas las organizaciones del estado adquieran las capacidades y habilidades técnicas / sociales, para migrar su infraestructura a la nube.

### **- Contribuciones**

Se considera deseable que COPITEC se constituya en consultor permanente a disposición de la actividad a desarrollar vinculada a la nube, dadas las capacidades y trayectoria de la Organización y sus Matriculados.

### **- Referencias**

- <https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/11/future-of-hr-survey.pdf>
- <https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/Navigating%20a%20world%20of%20disruption/MGI-Briefing-note-Navigating-a-world-of-disruption-Jan-2019.pdf>
- [https://www2.deloitte.com/content/dam/insights/us/articles/Tech-Trends-2019/DI\\_TechTrends2019.pdf](https://www2.deloitte.com/content/dam/insights/us/articles/Tech-Trends-2019/DI_TechTrends2019.pdf)

**MIGUEL ANGEL BLANCO.**

Ingeniero Informático, Analista Universitario de Sistemas, Especialista en Criptografía y Seguridad Teleinformática, Programador Universitario, Maestrando en Ciberdefensa en la UBA y en la FIE.

Trayectoria: Desarrollo Sistemas Operativos, Proyecto Linuxmil, (2004) para empleo militar . Docente en la EST 2008-2012 - Líder Proyecto Internacional SIG de la Conferencia de Ejércitos Americanos.(2012-2017). Prestó servicios en el Comando Conjunto de Ciberdefensa. Gestión del conocimiento y la información para la toma de decisiones, desarrollo e implementación del Sistema de Gestión de Estado Mayor Conjunto, empleado en Centro de Operaciones Conjuntas, G20 y Elecciones Nacionales 2019, Implementación del Sistema criptográfico (SIFRA2) de los Agregados Militares de Defensa. (2013)- Enlace ante ARSAT del Estado Mayor Conjunto 2017-2019- Evaluador de Proyectos PIDDEF Min Def 2010-2018. Participación como ponente Internacional en múltiples eventos relacionados con el Software Libre y los Sistemas de Información Geográficos y miembro de varias asociaciones relacionadas con el Open Sources.

**PABLO PEDRO CROCI.**

Ingeniero Electrónico (UBA). Especialista en Criptografía Seguridad Teleinformática (Facultad de Ingeniería del Ejército). Maestrando en Ciberdefensa (Facultad de

Ingeniería del Ejército). Investigador Universitario (UNDEF-FIE). Participa en comisiones de peritos y ciberseguridad del Copitec. Miembro de la Comisión de Informática Forense del IRAM.

Docente de cursos de capacitación de cursos de informática Forense del COPITEC (Consejo Profesional de Ingeniería Electrónica y Computación). Docente en el posgrado de Cibercrimen y Evidencia Digital (UBA-Derecho). Docente de la materia Forensia Informática Aplicada y responsable del Laboratorio de Forensia Informática Aplicada (Facultad del Ejército Argentino –

Sede EST). Desempeño como perito informático de parte y consultor técnico judicial

**GASTÓN A. TERÁN CASTELLANOS**

Analista de Sistemas (Fundación Banco de Boston) – Lic. en Administración (UP - Universidad de Palermo) – Posgrado en Marketing (UP) Maestrando en Administración y en Comercio Electrónico e Internet (UP) Consejero suplente de la Comisión Directiva del Consejo Profesional de Ingeniería Electrónica y Computación (COPITEC) - Coordinador de la Comisión de Informática y Computación (COPITEC) – Miembro de la Comisión de Peritos (COPITEC) - Docente de cursos de informática en la Universidad de Almirante Guillermo Brown (UNAB) – Auditor interno de Procesos y Sistemas del Ente Nacional de Comunicaciones (ENACOM) - Desempeño como auxiliar de justicia (perito informático), Consultor de parte y Consultor técnico judicial.

**PATRICIA MONICA DELBONO**

Licenciada en Sistemas de Información – Posgrado de Análisis de Investigación Criminal – Perito en Sistemas Informáticos Nación, Morón y San Martín – Consejera Titular y Coordinadora de la Comisión de Peritos de COPITEC – Instructora del Curso de Practica Procesal (2009 hasta la fecha) – Instructora de los Instructores Judiciales de San Martín en el tópico *Delitos Informáticos*. Instructora de la Seminario *“Delitos Informáticos y la Prueba*

*Informática*” en el CPACF. Docente en la Diplomatura Cibercrimen y Delitos Informáticos de la UNLAM. Miembros del Comité *Científico y Académico* de los CAIF 2014 y CAIF 2018.

### **JAVIER JOSE VALLEJOS MARTINEZ**

Licenciado en Informática y Especialista en Seguridad Informática (UBA). Co fundador de Securetia S.R.L. (empresa especializada en Ciberseguridad). Profesor de materias de grado en la Universidad de Buenos Aires y Universidad de Palermo. Profesor invitado en la Maestría de Seguridad Informática de la Universidad de Buenos Aires. Instructor en la Diplomatura en Ciberseguridad impartida en la Universidad de Palermo. Dicta capacitaciones de Informática Forense y Criptografía en diversas instituciones. Participa en las comisiones de COPITEC de Informática, Peritos y Ciberseguridad.

### **CAROLINA DIÉGUEZ HERRERA**

Ingeniera Electrónica (UBA)

Actualmente, trabaja en Hewlett Packard Argentina S.R.L. como Project Engineer Specialist– Temas regulatorios para Argentina y Latinoamérica.

Participación activa en Cámaras del sector TIC.

Experiencia en reglamentaciones locales e internacionales relativas a Seguridad Eléctrica y su aplicación. Interpretación de normas, Diseño de Plan de ensayos, Atestiguamiento y Análisis de Reportes de Laboratorio. Lean Six Sigma Miembro de Comisión Ciberseguridad (COPITEC)





República Argentina - Poder Ejecutivo Nacional  
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

**Hoja Adicional de Firmas**  
**Documentación Complementaria**

**Número:**

**Referencia:** Documentación Adicional

---

El documento fue importado por el sistema GEDO con un total de 8 pagina/s.