



# III Encuentro Iberoamericano de Blockchain y Ciberseguridad RIBCI-CYTED



## **PRESENTE Y FUTURO DE LA CIBERSEGURIDAD EN EL ENTORNO AEROESPACIAL**

Dra. Ing. H. Beatriz Parra  
Mg. Ing. Bruno M. Gallo



## III Encuentro Iberoamericano de Blockchain y Ciberseguridad RIBCI-CYTED

# AGENDA

- BREVE MARCO TEÓRICO DE LA TECNOLOGÍA AEROESPACIAL
- BREVE MARCO TEÓRICO DE LA CIBERSEGURIDAD
- HALLAZGOS DE LA REVISIÓN BIBLIOGRÁFICA
- VALOR DE LA CIBERSEGURIDAD EN LAS TECNOLOGÍAS AEROESPACIALES
- VACANCIA DE LA CIBERSEGURIDAD QUE IMPACTAN EN LAS TECNOLOGÍAS AEROESPACIALES
- PROPUESTA DE LA GOBERNANZA DIGITAL
- CONCLUSIONES

# Breve Marco Teórico de la Tecnología Aeroespacial

Se entiende a la tecnología aeroespacial como el conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico aplicado a la industria aeroespacial



## Breve Marco Teórico de la Tecnología Aeroespacial (TA)

### Evolución histórica de las TA:

#### PRIMERA GENERACIÓN (1957– 1980)

- Carrera espacial entre estados unidos y la unión soviética

- Agencias espaciales

#### SEGUNDA GENERACIÓN (1981– 2000)

- Comercialización componentes aeroespaciales
- Naves espaciales reutilizables

- Tecnología innovadora

#### TERCERA GENERACIÓN (2001– presente)

- Dependencia tecnológica en internet
- Auge de las empresas espaciales privadas
- Miniaturización de los satélites
- Turismo espacial,

# Breve Marco Teórico de la Tecnología Aeroespacial (TA)

**Modelos Tecnológicos:** son estructuras conceptuales o aplicadas que describen cómo se desarrollan, organizan e integran las tecnologías utilizadas en la exploración, transporte y observación desde el espacio y en la atmósfera.

- Sistemas Espaciales
- Desarrollo Tecnológico TRL (Technology Readiness Level)
- Vehículos Aeroespaciales
- Componentes para la observación de la Tierra
- Vuelos y misiones tripuladas
- Tecnologías duales (civil + militar)

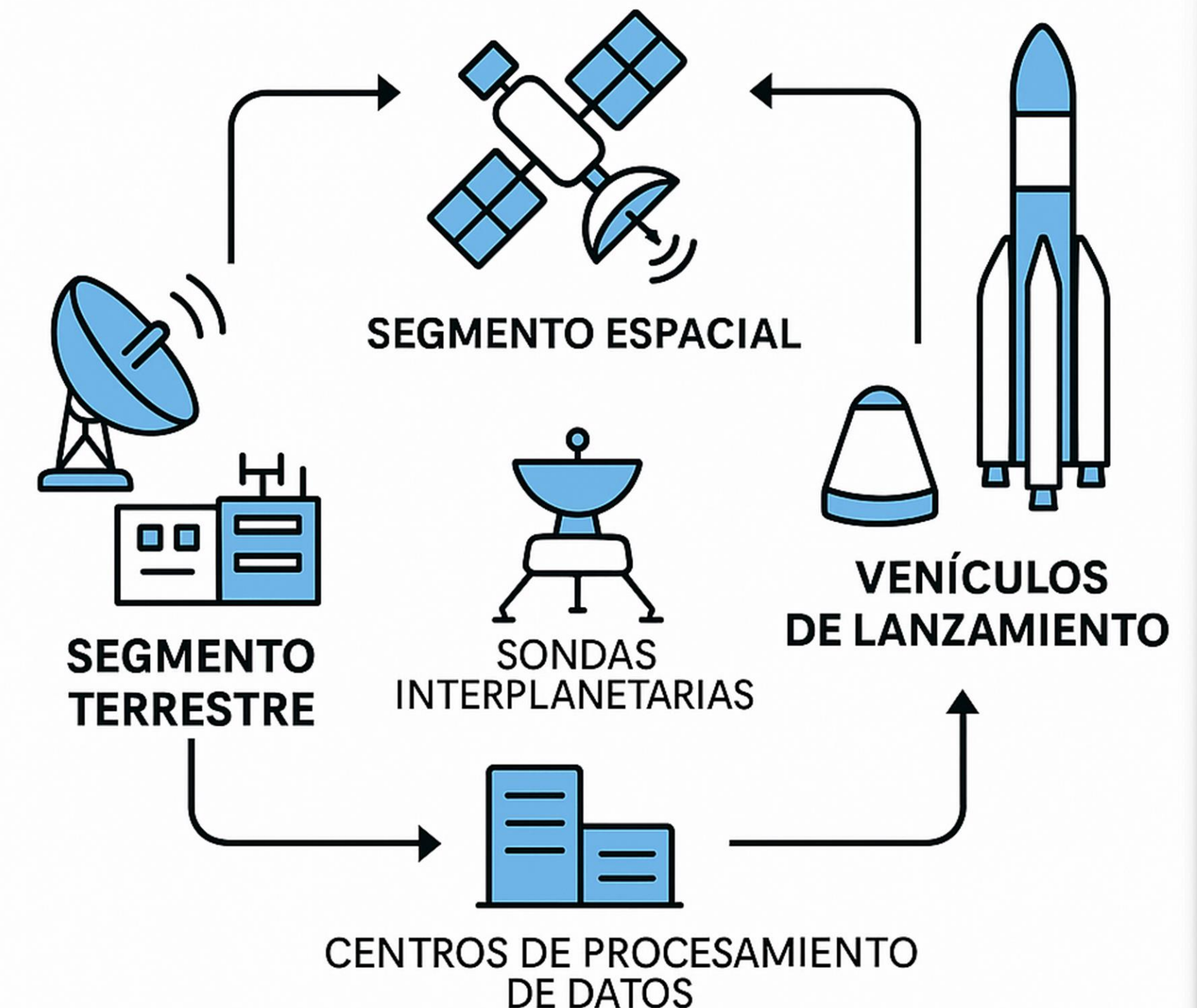


# Breve Marco Teórico de la Tecnología Aeroespacial (TA)

## Sistemas Espaciales:

- **Segmento terrestre:** estaciones de control, antenas, centros de procesamiento de datos.
- **Segmento espacial:** satélites de observación, navegación, telecomunicaciones, sondas interplanetarias.
- **Vehículos de lanzamiento:** cohetes (Falcon, Ariane, Soyuz), cápsulas (Dragon, Orion).

## MODELO DE SISTEMAS ESPCIALES

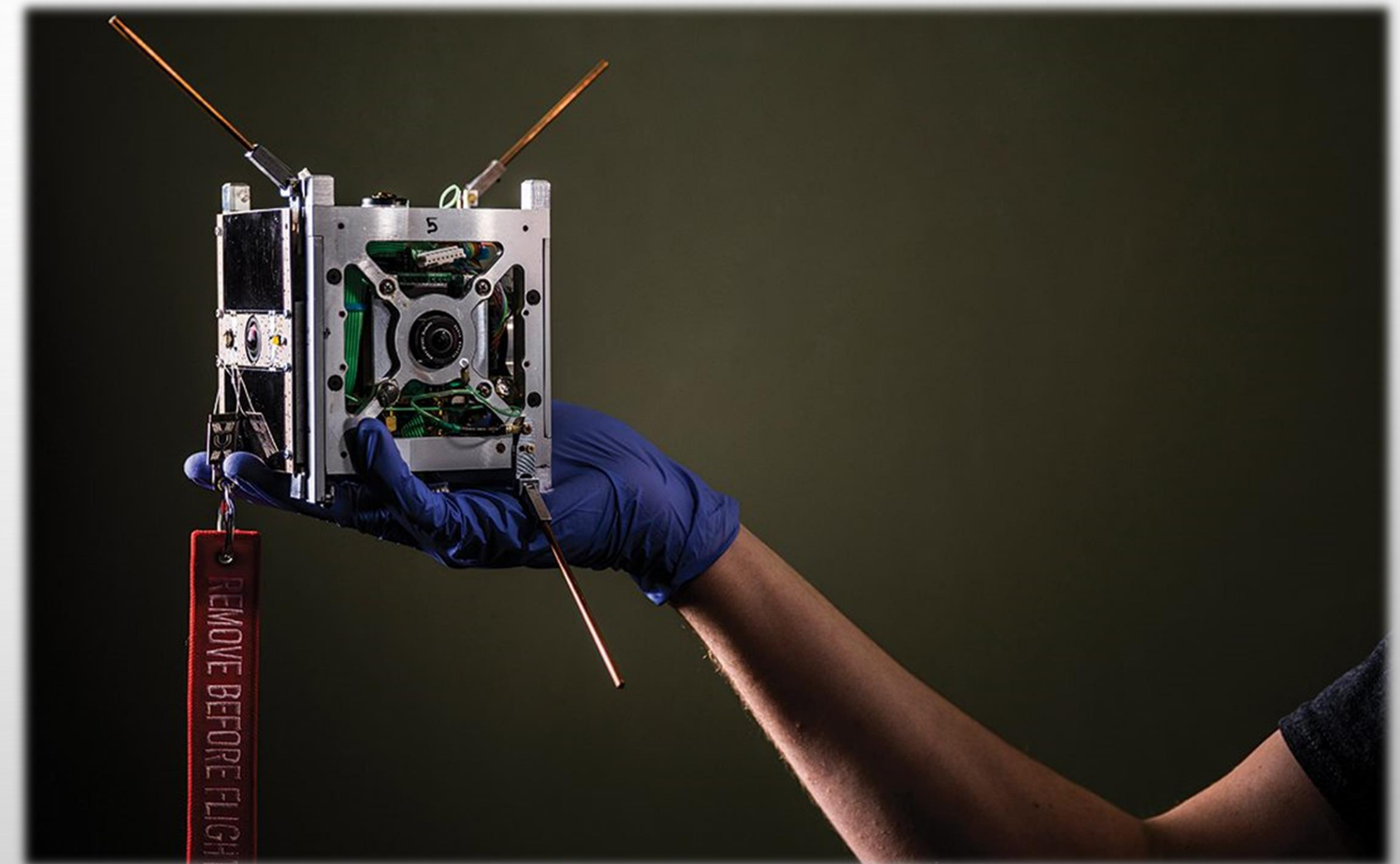




# Breve Marco Teórico de la Tecnología Aeroespacial (TA)

## Sistemas Satelitales:

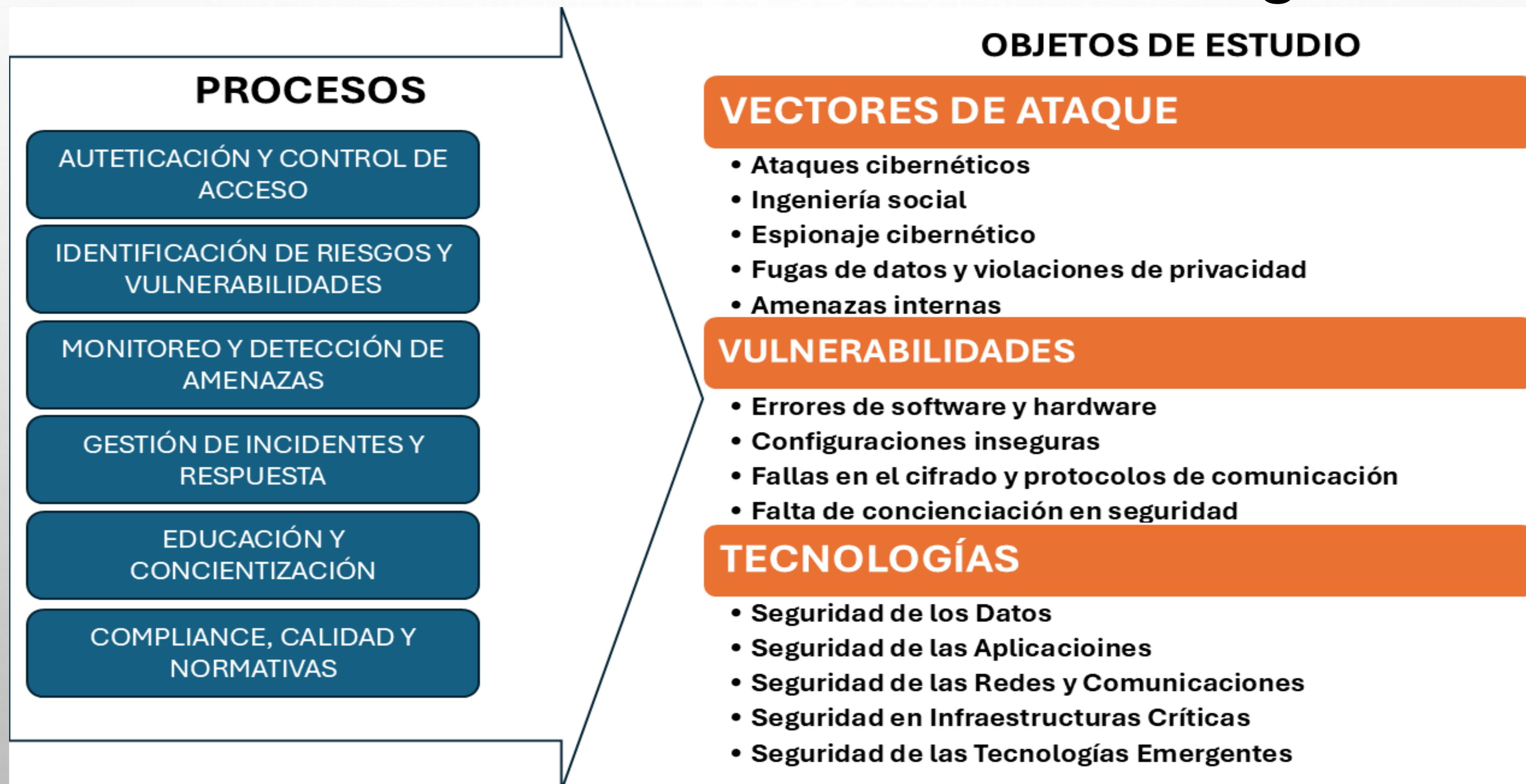
- **Estaciones Terrestres** son las instalaciones en tierra utilizadas para el control de las operaciones satelitales (telemetría, seguimiento, comunicaciones y comandos de gestión) y permiten la recopilación de datos acerca del funcionamiento y propósito del satélite.
- **Enlaces de comunicación** son de dos tipos: ascendentes (para la comunicación tierra-satélite) y descendentes (para la comunicación satélite-tierra).
- **Satélites** en sí mismos varían en diseño y propósito (comunicación, investigación, observación de la tierra, militares, etc).



Satélite CubeSats



# Breve Marco Teórico de la Ciberseguridad





# Breve Marco Teórico de la Ciberseguridad



- Acceso Indebido
- Phising
- Denegación de Servicios
- Malware
- Ransomware
- Man in the Middle

# Hallazgos de la Revisión Bibliográfica

- Acceso físico limitado a los satélites
- Adversidad del ambiente espacial y naturaleza altamente especializada
- Limitaciones de hardware y protocolos de comunicación
- Minimización de los riesgos del acceso indebido a los sistemas
- Falta de normativas internacionales unificadas (protección de datos y de la propiedad intelectual)
- Falta de colaboración en ciberseguridad entre las agencias internacionales y las naciones
- Aumento del número de satélites y constelaciones
- Acceso a la tecnología para el desarrollo de satélites pequeños
- Naturaleza de doble uso para fines civiles y militares



# Valor de la Ciberseguridad en la TA

- Se requiere incorporar la Ciberseguridad desde la fase de investigación y diseño (TRL) de los proyectos de Tecnología Aeroespacial
- Se identifican 2 factores que inciden sobre la Ciberseguridad:
  - Naturaleza global del ciberespacio que crea una plataforma para ataques sin fronteras
  - Desequilibrio de capacidades relacionadas a las TICs entre los actores del dominio espacial
- Falta de capacitación en ciberseguridad del operador del sistema
- Ausencia de sistemas con tolerancia a fallos y redundantes
- Descentralización de operaciones, múltiples ubicaciones de los centros de control y múltiples identidades al aparecer nuevos proveedores de servicios
- Necesidad de fomentar una cultura de la ciberseguridad

# Valor de la Ciberseguridad en la TA

## 2. Modelo de desarrollo tecnológico TRL (Technology Readiness Level)

Escala de madurez de tecnologías aeroespaciales, muy usada por NASA y ESA.

| Nivel | Descripción |
|-------|-------------|
|-------|-------------|

|         |                                              |
|---------|----------------------------------------------|
| TRL 1–3 | Investigación básica, pruebas de laboratorio |
|---------|----------------------------------------------|

|         |                                               |
|---------|-----------------------------------------------|
| TRL 4–6 | Validación en ambiente relevante (prototipos) |
|---------|-----------------------------------------------|

|         |                                                |
|---------|------------------------------------------------|
| TRL 7–9 | Demostración y operación en condiciones reales |
|---------|------------------------------------------------|

✓ *Ejemplo:* Un propulsor eléctrico para satélites puede estar en TRL 5 si ha sido probado en tierra en condiciones simuladas.



### Vacancias normativas y legales de la Ciberseguridad en la TA

- ***Jurisdicciones transfronterizas*** de los proyectos aeroespaciales.
- Ambigüedad y/o falta de regulaciones internacionales que permitan el abordaje de situaciones de ***ciberdelincuencia en el contexto espacial***.
- Grado de Madurez en Ciberseguridad de quienes ***toman decisiones***
- ARGENTINA:
  - Plan Espacial Nacional CONAE
  - Proyecto ARSAT (Gerencia de Ciberseguridad)
  - Ley 11.672 – Ley Nacional de Actividades Espaciales (1999)
  - Ley 27.078 – Ley Argentina Digital (2014)
  - Normativas de la ANAC
  - Regulaciones del ENACOM
  - Normativas nacionales sobre Ciberseguridad

- PROPUESTA DE UNA GOBERNANZA DIGITAL EN LAS TA
- ***Ecosistema Aeroespacial:*** todos los objetos y entidades involucrados en las actividades espaciales.
    - Agencias espaciales,
    - Gobiernos,
    - Empresas Privadas,
    - Institutos de Investigaciones,
    - Infraestructura Tecnológica Crítica,
    - Sistemas de control y operatividad,
    - Regulaciones y normativas del sector
  - ***Contexto integrado e interdependiente:*** a estudiar con visión holística.



# PROPUESTA DE UNA GOBERNANZA DIGITAL EN LAS TA

## ***LINEAS DE ACCIÓN:***

1. Trabajo Colaborativo entre todos los actores
2. Identificación de la tecnología aeroespacial como infraestructura crítica
3. Formación cruzada de RRHH
4. Definición de una infraestructura tecnológica protegida
5. Definición de regulaciones acordadas en diferentes niveles
6. Adopción de un marco metodológico integrado para la ciberseguridad de infraestructuras críticas de las TA

### CONCLUSIONES

- La mayoría de los autores rescatan la necesidad del abordaje de la ciberseguridad en los proyectos aeroespaciales.
- En Argentina falta la definición de un marco normativo y legal que permita el desarrollo de la ciberseguridad en el ecosistema aeroespacial.
- Falta de políticas internas de ciberseguridad en todas las instituciones, para generar una cultura de la ciberseguridad.
- Falta de formación continua de los profesionales de la ciberseguridad.



# III Encuentro Iberoamericano de Blockchain y Ciberseguridad RIBCI-CYTED

## BIBLIOGRAFÍA

- PARRA B., GALLO B. (2025), CIBERSEGURIDAD Y TECNOLOGÍA AEROESPACIAL: REVISIÓN DEL ESTADO DEL ARTE, XIII CONGRESO ARGENTINO DE TECNOLOGÍA ESPACIAL. 9-11 DE ABRIL, 2025. DISPONIBLE EN: [HTTPS://DRIVE.GOOGLE.COM/FILE/D/1J9EE-UGMYXVWIQZFU9CA8BZH6ZCKBV5Z/VIEW?USP=SHARING](https://drive.google.com/file/d/1J9EE-UGMYXVWIQZFU9CA8BZH6ZCKBV5Z/view?usp=sharing)
- ANSONG S., RANKOTHGE W., SADEGHI S., MOHAMMADIAN H., BIN RASHID F., AND GHORBANI A. (2025). ROLE OF CYBERSECURITY FOR A SECURE GLOBAL COMMUNICATION ECO-SYSTEM: A COMPREHENSIVE CYBER RISK ASSESSMENT FOR SATELLITE COMMUNICATIONS, *COMPUT SECUR*, VOL. 149, NO. JULY 2024, P. 104156, 2025, DOI: 10.1016/J.COSE.2024.104156.
- BOTEZATU U.E. (2023). ATTEMPTED CYBER SECURITY OF SYSTEMS AND OPERATIONS IN OUTER SPACE: AN OVERVIEW OF SPACE-BASED VULNERABILITIES” *ROMANIAN CYBER SECURITY JOURNAL*, VOL. 5, NO. 1, PP. 67-76, DOI: 10.54851/V5I1Y202306.
- DE ZOYSA S. AND SIRIWARDANA D. (2024). FINAL FRONTIER OF STRATEGIC INFORMATION WARFARE AND CYBERSECURITY CHALLENGES TO SATELLITES AND SPACE INFRASTRUCTURE. *AVAILABLE*
- FLETCHER T. N. (2023). ALIGNING CYBERSECURITY WITH BUSINESS OBJECTIVES MANAGING CYBERSECURITY THROUGH CHANGING POLICIES, MISSIONS AND CONTRACTS,” *COMM HIT SUMMIT SEPTEMBER 2023 ACHIEVING TODAY’S ADVANCED WORKPLACE*.
- FREEMAN K. (2024). THE AVIATION CYBERSECURITY CHALLENGES.
- KAVALLIERATOS G. AND KATSIKAS S., AN EXPLORATORY ANALYSIS OF THE LAST FRONTIER: A SYSTEMATIC LITERATURE REVIEW OF CYBERSECURITY IN SPACE. *INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION*, VOL. 43, NO. OCTOBER, P. 100640, DOI: 10.1016/J.IJCIP.2023.100640.
- KHAN S. K., SHIWAKOTI N., DIRO A., MOLLA A., GONDAL I., AND WARREN M. (2024). SPACE CYBERSECURITY CHALLENGES, MITIGATION TECHNIQUES, ANTICIPATED READINESS, AND FUTURE DIRECTIONS, *INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION*, VOL. 47, NO. JULY, P. 100724, , DOI: 10.1016/J.IJCIP.2024.100724.

# Gracias!

Dra. Ing. H. Beatriz Parra – [bgallo@ucasal.edu.ar](mailto:bgallo@ucasal.edu.ar)

Mg. Ing. Bruno M. Gallo - [bruno@ad-argia.com.ar](mailto:bruno@ad-argia.com.ar)

