Universidad de Buenos Aires

Facultad de Ciencias Económicas

Maestría en Ciberdefensa y Ciberseguridad

Tesis de Maestría

El impacto de la dependencia del hardware tecnológico en la Ciberdefensa y Ciberseguridad de la República Argentina

Autor: Mag. Walter R. Ureta

Director: Mag. Jorge Eterovic

Año 2021

Cohorte 2018

Declaración Jurada

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Firmado

Walter R. Ureta

DNI: 29.002.868

i Resumen

Actualmente, la República Argentina, al igual que muchos otros países, cuenta con limitadas capacidades de producción de componentes de hardware para equipos informáticos. De esta forma el país depende de la producción extranjera para satisfacer sus necesidades de equipamiento vinculado a la Ciberdefensa y Ciberseguridad de los diversos sistemas existentes en su territorio, incluidos los vinculados a activos de infraestructuras criticas o áreas sensibles del estado. Este escenario hace que no disponga de la capacidad de garantizar que los sistemas utilizados no contengan vulnerabilidades o funcionalidades ocultas a nivel de hardware.

Este trabajo realizará una revisión histórica del desarrollo de la tecnología relevante para el problema, citará ejemplos sobre las diferencias existentes entre equipamiento de defensa y seguridad convencional frente al correspondiente a sistemas que involucran sistemas electrónicos, la situación de las capacidades del desarrollo y producción en conjunto con vulnerabilidades a nivel de hardware evidenciadas en la actualidad. Finalmente aportará una conclusión sobre la posición de la República Argentina ante esta problemática y un conjunto de posibles consideraciones tendientes a reducir el riesgo existente.

Palabras clave: Hardware, Ciberdefensa, Ciberseguridad, Argentina

ii Abstract

The Argentina’s Republic, like many other countries, has got limited capabilities to produce hardware components for computers. In this way, the country depends on foreign providers to satisfy its local Cybersecurity’s equipement needs, including assets linked to critical infrastructures or government's sensible information. This scenario generates that the country has not got the capacity to warranty that its systems has not got vulnerabilities or hidden functions at hardware level.

The work of this document will cover an historical revision of the development of different technologies related to this issue, it’ll reference examples about the differences between the conventional defense and security equipment in comparison to systems that contains electronic components; the overall situation of the capacity to develop and produce technology understanding the actual risks of hardware vulnerabilities and the evidence of their existence. Finally, it’ll contribute with a conclusion about the specific situation of the Argentina’s Republic for this scenario and a set of possible considerations to reduce the existing risk.

Keywords: Hardware, Cyberdefense, Cybersecurity, Argentina

iii Dedicatorias

Este trabajo esta dedicado a aquellas personas de mente y espíritu inquietos que desde la ciencia, la investigación, la educación o la técnica generan y distribuyen conocimiento para contribuir con la prosperidad y seguridad de los habitantes de esta Nación.

iv Agradecimientos

Quiero agradecer a las autoridades y el plantel docente de esta maestría que ha generado un espacio interdisciplinario de formación en la gestión de la Ciberseguridad y Ciberdefensa. Asimismo destacar y agradecer la guía y compromiso del director de este trabajo, Jorge Eterovic, que con su experiencia y conocimiento me acompaño en este desarrollo.
Desde el plano personal, agradecer especialmente a quienes hoy forman parte de mi vida y en diferentes momentos me han apoyado para abordar y llevar adelante las diferentes etapas de esta maestría. Tampoco puedo dejar de mencionar a mi madre y padrino, que hoy no están presentes, pero me guían con el ejemplo su esfuerzo a lo largo de la vida y la confianza que han depositado en mi.

v Índice

vi Índice de tablas

vii Índice de figuras

viii Nómina de abreviaturas y términos

ABEL: acrónimo, del ingles “Advanced Boolean Expression Language”, es un lenguaje HDL desarrollado por Data I/O Corporation.

ACPI: acrónimo del ingles “Advanced Configuration and Power Interface”, o “Interfaz Avanzada de Configuración y Poder”.

AES: acrónimo del ingles “Advanced Encryption Standard”, o “Estándar de Cifrado Avanzado” es un protocolo de cifrado simétrico definido como estándar por el NIST.

ASIC: del ingles “Application-specific Integrated Circuit”, significa “Circuito integrado de aplicación especifica”.

BIOS: acrónimo del ingles “Basic Input-Output System”, cuyo significado es “Sistema Básico de Entrada-Salida” y corresponde al programa interfaz entre el firmware y el sistema operativo que se inicia al encender una computadora.

BJT: del inglés, “bipolar junction transistor”, significa “transistor de unión bipolar”.

BND: Servicio Federal de Inteligencia alemán.

CIA: Central de Inteligencia Americana.

CISC: del inglés, “Complex Instruction Set Computer”, corresponde a la arquitectura de procesador de instrucciones complejas.

CMOS: del inglés, “Complementary Metal Oxide Semiconductor”.

COIN: Acrónimo de “Contra-insurgencia”, del inglés “Counter-insurgency”, es la denominación para la variante de aviones de ataque a tierra con características optimizadas para el disponer de gran maniobrabilidad, capacidad de operación en pistas improvisadas, deterioradas y de reducida distancia.

Contactless: sistema de pago sin contacto basado en tecnología de identificación por radiofrecuencia.

CPU: del ingles “Central Processing Unit”, o “Unidad Central de Procesamiento”.

DJI: del chino: “大疆创新, Dà-Jiāng Innovations”, es un empresa líder en el desarrollo y producción de drones de uso civil a nivel mundial.

DSP: del ingles “Data Signal Processing”, significa “procesamiento de señales digitales”.

EFI: acrónimo del ingles “Extensible Firmware Interface”, es una interfaz firmware-sistema propietaria desarrollada por Intel en el año 2002 para reemplazar al BIOS.

EMV: acrónimo de "Europay MasterCard VISA", es estándar de interoperabilidad de tarjetas para la autentificación de pagos mediante tarjetas de crédito y débito.

FET: del inglés, “Field effect transistor”, significa “transistor de efecto campo”.

Fins: tiras de material microscópico que componen un transistor dentro de un circuito integrado.

FPGA: del acrónimo ingles “Field programable gate array” cuya traducción corresponde a “Campo de matrices de puertas lógicas programable”.

FPV: del inglés “First Person Viewing”. Tecnología que permite visualizar en tiempo real el video capturado desde la línea de visión frontal de un dispositivo.

FSF: del ingles, “Free Software Foundation”, es una organización creada por Richard Stallman en 1985 con el fin de promover el “Software Libre”.

GLONASS: del ruso “ГЛОНАСС, ГЛОбальная НАвигационная Спутниковая Система“, sistema de posicionamiento global de origen ruso.

Golden chip: o “integrado dorado”, es la denominación para una unidad de un modelo de circuito integrado confiable, de la que se puede afirmar que no ha sido alterada durante su producción.

GPL: acrónimo de “Licencia Publica General” , la misma fue definida por la Free Software Foundation.

GPS: del inglés “Global Positioning System”. Es un sistema de posicionamiento global basado en constelaciones de satélites.

GPT: acrónimo del ingles “GUID Partition Table”, es un estándar para la escritura de tablas de particiones de datos en medios de almacenamiento.

GPU: del ingles “Graphical Processing Unit”, o “Unidad de Procesamiento Gráfico”.

HDL: del ingles, Hardware Definition Language, o lenguaje de definición de hardware.

HF: del ingles “High Frequency”, o “Frecuencia Alta”.

IA: acrónimo de inteligencia artificial.

IDE: acrónimo de “Integrated Development Environment”, o Entorno Integrado de Desarrollo.

IoT: acrónimo; del ingles, “Internet of Things”, cuyo significado es “Internet de las cosas” y se vincula a equipos electrónicos usualmente con sensores y controles físicos inter-conectados vía internet.

ISA: del ingles, “Instruction Set Architecture”, corresponde a la arquitectura de un conjunto de instrucciones de procesamiento.

ITB: acrónimo de “Instalación de Tiro Berreta”.

JATO: del inglés “Jet Assisted Take-Off”, o “Despegue asistido por reactores”.

JFET: del ingles, “Junction field effect transistor”, significa “transistor de efecto campo de unión”.

Keylogger: es un software o hardware que de manera sigilosa registra la actividad de entrada de datos del usuario, usualmente la actividad del teclado.

LGPL: acrónimo de “Licencia Publica General Reducida” , la misma fue definida por la Free Software Foundation.

Lipo: batería recargable de polímero de iones de litio.

Machine learning: del ingles, Aprendizaje de maquina.

MOSFET: del inglés, “Metal-oxide-semiconductor Field-effect transistor”, significa “Transistor de efecto de campo metal-óxido-semiconductor”

NATO: del acrónimo en lenguaje Inglés: North Atlantic Treaty Organization. Corresponde a la alianza ínter-gubernamental de carácter militar que desde el 4 de abril de 1949 provee una defensa colectiva entre sus países miembros.

NIST: acrónimo del ingles “National Institute of Standards and Technology”, o “Instituto Nacional de Estándares y Tecnología” perteneciente a Estados Unidos con cede en Gaithersburg, Maryland.

OSD: del ingles, “Open Source Definition”, o “Definición de fuente abierta”.

OSHW: del ingles “Open Source Hardware”.

OSHWA: del ingles, Open Source Hardware Association.

OTT: del inglés “One time tape”, cuyo significado es cinta de un solo uso. Su contenido debe ser aleatorio y utilizado por una única vez.

Payload: también denominado “Carga útil”, corresponde a la lógica que realiza la acción principal sobre el sistema objetivo en un malware o software malicioso.

PCI: acrónimo del ingles, “Peripheral Component Interconnect”, cuyo significado es “Interconexión de Componentes Periféricos” y corresponde a un tipo de bus o conector para extender las capacidades de la placa principal de una computadora.

Risc-V: es un conjunto de instrucciones ISA con diseño RISC creado como hardware libre.

RISC: del inglés “Reduced Instruction Set Computer”, o “Computadora con conjunto de instrucciones reducido”.

ROM: acrónimo del ingles, “Read Only Memory”, corresponde a “Memoria de Solo Lectura”.

Root: Usuario de administración o de máximo nivel de privilegios en sistemas operativos como Unix o Linux.

Rootkit: herramienta de código malicioso con características de diseño que le brindan capacidades para permanecer oculto en un sistema.

RoT: del ingles “Root of Trust”, significa “Raiz de Confianza” y corresponde a componentes criptográficos de confianza de un sistema.

SEM: acrónimo del ingles “scanning electron microscope”, se refiere a un microscopio de barrido electrónico que permite obtener imágenes de alta resolución de pequeñas superficies en base a la interacción del electrón y la materia.

Shell: Interfaz de linea de comandos para acceder a los servicios de un sistema operativo.

SIM: acrónimo inglés de “subscriber identity module”, significa “módulo de identificación de abonado”.

STOL: del inglés”Short Take-Off and Landing”, referencia a la característica de despegue y aterrizaje corto.

System-on-chip: se utiliza para referenciar a un sistema montado en un único circuito integrado.

TPM: acrónimo del ingles “Trusted Platform Module”, o “Modulo de Plataforma de Confianza” que corresponde a la especificación ISO/IEC 11889 referida a un procesador seguro con soporte criptográfico para almacenar y gestionar claves de cifrado.

TTL: del inglés, “transistor-transistor logic”, o “Tecnología de circuitos digitales”.

UEFI: acrónimo del ingles “Unified Extensible Firmware Interface”, es una especificación estándar de interfaz firmware-sistema basado en EFI.

Verilog: es un lenguaje HDL con ciertas similitudes con el lenguaje C, fue creado por Phil Moorby en 1985 para la empresa Automated Integrated Design Systems.

VHDL: lenguaje HDL especificado por la ANSI/IEEE 1076-1993.

VHF: acrónimo del ingles “Very High Frequency”, o “Frecuencia muy alta”, utilizado para denominar a la banda del espectro electromagnético entre los 30 y 300 megahercios.

1 Introducción

La complejidad técnica de la problemática de la dependencia en hardware de origen foráneo sumada a las limitaciones del desarrollo de capacidades productivas inherentes a la industria asociada a este tipo de tecnología y el impacto económico-funcional de prescindir de ciertos avances tecnológicos en los sistemas hace que en general se omita la consideración de los problemas de seguridad a nivel de hardware en los análisis de riesgos de sistemas con componentes informáticos, inclusive en áreas sensibles de interés para la Ciberseguridad y la Ciberdefensa de una nación.

El propósito de este trabajo es comprender el estado de situación de la República Argentina para el escenario propuesto, incluyendo la factibilidad técnica de los riesgos citados en función de casos documentadas.

1.1 Hipótesis

Este trabajo perseguirá como hipótesis primaria la siguiente declaración:

> *"La dependencia en hardware de origen extranjero representa un riesgo para la Ciberdefensa y Ciberseguridad de sistemas críticos de la República Argentina."*

La misma referencia a la afirmación de que existe un problema inherente a depender de componentes físicos de sistemas informáticos de diseño y producción realizados en el extranjero.

En este contexto se plantean las siguientes preguntas de investigación que deberán ser abordadas en el desarrollo de esta elaboración:

1. ¿ Puede un sistema critico y asegurado resultar intervenido por un ciberatacante utilizando vulnerabilidades introducidas deliveradamente a nivel de hardware ?
2. ¿ Es factible el desarrollo del diseño y producción de hardware orientado a brindar soluciones confiables para sistemas críticos en el país ?
3. Ante la consideración de la posibilidad de ataques por vulnerabilidades introducidas a nivel de hardware, ¿ Existen medidas preventivas orientadas a reducir la probabilidad de éxito del mismo ?

Se desarrollaran las conclusiones vinculando los diferentes escenarios y conceptos asociados a la hipótesis principal, tomando como sustento la información elaborada en el marco teórico. Finalmente se aportaran una serie de consideraciones y buenas practicas

orientadas a reducir el riesgo que representaría el problema planteado para la Ciberseguridad y Ciberdefensa de sistemas utilizados en la República Argentina.

1.2 Objetivos

El producto de este trabajo perseguirá como objetivo principal proveer un marco teórico junto a la generación de aportes vinculados al análisis de situaciones y conclusiones que faciliten la comprensión de la problemática abordada.

De modo complementario, se buscará cumplir los siguientes objetivos específicos:

1. Demostrar que existen particularidades en las soluciones de sistemas informáticos que representan un riesgo para la Ciberseguridad y Ciberdefensa mayor al de otros tipos de componentes no informáticos.
2. Evidenciar la existencia de vulnerabilidades a nivel de hardware que han permitido comprometer sistemas informáticos.
3. Proveer de un conjunto de recomendaciones para reducir el riesgo de este tipo de expuestos.

1.3 Alcance

Este trabajo aborda la problemática de la dependencia actual de hardware con diseño y producción de origen extranjero para sistemas de información utilizados en la República Argentina. Al mismo tiempo se encuentra acotado al enfoque de sistemas críticos o sensibles utilizados en el país, en particular aquellos de interés para la Ciberdefensa y Ciberseguridad de la nación.

2 Estado del arte

Este capítulo desarrolla los eventos históricos de interés para este documento, haciendo foco en los hitos del desarrollo tecnológico de los componentes basales de los equipos informáticos de la actualidad.

2.1 Historia del transistor

La capacidad del control de corrientes eléctricas ha sido fundamental para la evolución tecnológica de los últimos siglos, pero a partir de 1920 algunos científicos enfocados en la física del estado sólido plantearon su interés en los materiales semiconductores para el control del flujo de electrones y sus posibles aplicaciones. El conocimiento desarrollado en las siguientes décadas y el interés en el potencial de sus posibles aplicaciones, tanto en el ámbito militar como civil, generó un contexto propicio para la investigación y el desarrollo de este tipo de componentes.

En el año 1945 *Bell Telephone Laboratories* de la empresa AT&T dió inicio a un proyecto en el cual se encontrarían incluidos los científicos Wiliam Shockley, John Bardeen y Walter Houser Brattain; quienes serían galardonados con el premio Nobel de Física en 1956 por sus aportes al estudio de los semiconductores y la invención del transistor. Este proyecto desarrolló un gran número de pruebas logrando en el año 1947 construir el primer transistor funcional de la historia y generando las bases del conocimiento necesario para el desarrollo de las futuras versiones de producción. Esta versión correspondía a un transistor del tipo de puntos de contacto con función de amplificador, su prototipo se construyó en base a una lámina de oro que recubría dos laterales de una cuña plástica que actuaba como aislante; esta lámina ténia un corte de 50 μm[1] y ambos segmentos se posaban con una leve presión sobre una placa de germanio que actuaría como base, permitiendo a las láminas de oro operar como emisor y colector respectivamente.

Fue este mismo prototipo el que logró amplificar la señal en una relación de uno a cien confirmando el potencial de esta tecnología que en los próximos años pasaría a ser el reemplazo de numerosos componentes utilizados en los dispositivos de la época. Como

1 **μm:** Unidad de medida correspondiente a la milésima parte de un milímetro, se denomina micrón, micra o micrómetro.

caso de referencia se encuentra la válvula de vacío, respecto de la cual el transistor disponía de estas ventajas:

- Menor tamaño
- Menor peso
- Construcción mas robusta y mejor resistencia a impactos
- Construido con componentes de estado sólido
- Menor voltaje de operación
- Requería menos potencia
- No requería entrar en temperatura o ciclos de calentamiento
- Mayor eficiencia

El dispositivo fue patentado en 1950 bajo la patente número 2,524,035[BARDEEN1950], titulada *"Three-Electrode Circuit Element Utilizing Semiconductive Materials"* y adjudicada a Bell Telephone Laboratories Incorporated.

Una versión posterior al transistor de puntos de contacto fue desarrollada por William Shockley en 1948; en este caso el dispositivo constaba de dos uniones PN con una delgada separación sobre el mismo cristal semiconductor que sería denominada BJT[2] o transistor de unión bipolar. La distribución de estas uniones, ya sea PNP o NPN, daba lugar a las tres diferentes áreas de distinto tamaño que actuarán en los roles de Base, Emisor y Colector.

A partir de este punto el interés y las diversas aplicaciones del transistor fueron tema de investigación y desarrollo de instituciones civiles y militares con la finalidad de su implementación en una amplia variedad de productos, permitiendo reducir su costo, tamaño, consumo, mantenimiento y reduciendo su costo de producción.

En paralelo al desarrollo del transistor BJT, otro tipo de dispositivo basado en semiconductores fue desarrollado. Este dispositivo se denominó FET[3] o transistor de efecto de campo. Su base conceptual fue anterior, con una primer patente registrada en el año 1925 atribuida al físico húngaro Julius Edgar Lilienfeld y otra en 1934 al alemán Oskar Heil; sin embargo ninguno de ellos pudo concretar el desarrollo de un prototipo funcional por lo que sus patentes quedaron acotadas al campo teórico por varios años. Tiempo después, en el año 1945, el físico alemán Heinrich Welker obtuvo una patente para el

2 **BJT**: del inglés, "bipolar junction transistor", significa "transistor de unión bipolar"

3 **FET**: del inglés, "Field effect transistor", significa "transistor de efecto campo"

denominado JFET[4] o transistor de efecto de campo de juntura o unión, que daría lugar al desarrollo de numerosas variantes a lo largo de décadas de evolución.

Los transistores de tipo FET disponen de tres terminales, al igual que las BJT, pero su denominación es diferente; en este caso se denominan drenaje, compuerta y fuente. En cuanto a su funcionamiento es controlado por un voltaje de entrada que no requiere corriente de polarización y su comportamiento esta determinado por la relación de voltaje entre la compuerta y la fuente, permitiendo o limitando la conducción entre la fuente y el terminal de drenaje en modo de tríodo[5] o amplificando la señal en modo de saturación.

En resumen para mediados del siglo XX se habían desarrollado dos tecnologías basadas en semiconductores que permitían controlar y amplificar señales en función de corrientes y voltajes, proporcionando componentes electrónicos de estado sólido de menor consumo, menor tamaño, menor mantenimiento con mayor durabilidad y mejor desempeño.

En 1959 el ingeniero eléctrico y físico estadounidense Jack S. Kilby presentó la solicitud de patente para un dispositivo con cuerpo de material semiconductor en el que todos los componentes de un circuito electrónico se encontraban completamente integrados en él. Esta presentación se correspondía a un prototipo real compuesto por germanio sobre el cual se integraban seis transistores que operaban como un oscilador de rotación de fase[6], dando lugar al primer circuito integrado funcional, desarrollo por el cual Kilby recibiría el premio nobel de física en el año 2000. De esta manera, lograron implementarse componentes de familias lógicas (CMOS[7], TTL[8], etc) a gran escala en una pequeña superficie para construir dispositivos de funcionalidades complejas.

Los circuitos integrados potencian las ventajas de los transistores, los mismos tienen un bajo costo de producción, con un proceso de baja incidencia de fallas de fabricación, menor consumo, menor tamaño y reducción de costo. Su producción suele realizarse

4 **JFET**: del ingles, “Junction field effect transistor”, significa “transistor de efecto campo de unión”

5 **Triodo:** es una válvula electrónica de amplificación compuesta por tres electrodos dispuestos en el interior de una envoltura de vidrio en vacío.

6 **Oscilador de rotación de fase:** es un circuito electrónico que produce una salida en forma de onda senoidal.

7 **CMOS**: del inglés, “Complementary Metal Oxide Semiconductor”

8 **TTL:** del inglés, “transistor-transistor logic”. Tecnología de circuitos digitales

mediante fotolitografiá sobre placas semiconductoras, usualmente de silicio, permitiendo disponer de una gran cantidad de componentes en un circuito de superficie reducida.

La siguiente tabla muestra la evolución del proceso de producción mediante la reducción del tamaño de un dispositivo tipo MOSFET[9] dentro de un circuito integrado:

Tamaño	Año	Tamaño	Año
10 µm	1971	130 nm	2001
6 µm	1974	90 nm	2003
3 µm	1977	65 nm	2005
1.5 µm	1981	45 nm	2007
1 µm	1984	32 nm	2009
800 nm[10]	1987	22 nm	2012
600 nm	1990	14 nm	2014
350 nm	1993	10 nm	2016
250 nm	1996	7 nm	2018
180 nm	1999	5 nm	2020

Tabla 1: Tamaños de un MOSFET en un circuito integrado

Las medidas inferiores a 5nm se enfrentan a problemas físicos que pueden afectar el correcto funcionamiento de los componentes, quizás el mas renombrado de estos problemas es el efecto de túnel cuántico donde por injerencia de la mecánica cuántica una partícula podría traspasar posiciones que la física tradicional no permitiría. Es así que, al acercarnos a puertas lógicas o fins[11] de 1nm, algunos electrones podrían atravesar la puerta lógica aunque esta se encuentre cerrada generando un comportamiento inesperado en el transistor.

9 **MOSFET**: del inglés, “Metal-oxide-semiconductor Field-effect transistor”, significa “Transistor de efecto de campo metal-óxido-semiconductor”

10 **nm**: significa nanómetro, que es la unidad de longitud equivalente a una millonésima parte de un milímetro(10^{-6} milímetros)

11 **Fins**: tiras de material microscópico que componen un transistor dentro de un circuito integrado.

2.2 Historia del microprocesador

Con el avance tecnológico aportado por los circuitos integrados se pudieron desarrollar unidades compuestas por múltiples componentes electrónicos para la realización de diversas funciones de uso frecuente, simplificando de esa manera la ejecución de operaciones complejas a un bajo costo debido a la reutilización de su diseño y los beneficios propios de la producción de este tipo de circuitos a gran escala. Este hecho dió lugar a la aparición de microprocesadores que permitían disponer de una unidad central de procesamiento que albergaba las funciones para el manejo de registros mediante operaciones aritméticas y lógicas a nivel binario. El primer dispositivo conocido fue el Intel 4004 presentado en 1971 para operaciones de 4 bits, que se componía de 2300 transistores operando a una frecuencia de 740 Khz[12], lo que era suficiente para las necesidades de la calculadora comercial Busicom 141-PF.

En los años posteriores aparecerían en el mercado otros modelos de microprocesadores que permitieron el desarrollo de novedosas computadoras para su época, algunos de ellos fueron:

- Intel 8008, presentado en 1972 fue el primer microprocesador de 8 bits con capacidad para manejar 16Kb[13] de memoria y operar a 800Khz.
- Intel 8080, del año 1974, disponía de capacidad para manejar 64Kb de memoria y operar a 2Mhz[14]. Equipó a la exitosa Altair 8800 de MITS.
- MOS 6502, de 1975, fue utilizado por exitosas computadoras personales de la época como Apple II, BBC Micro y Commodore PET.
- Zilog Z80, del año 1976, de 8 bits con operación a 1,77 Mhz fue utilizado en la exitosa computadora personal Spectrum ZX.

12 **Khz**: Kilohertz o Kilohercio, unidad de medida de frecuencia correspondiente a 1.000 ciclos por segundo.

13 **Kb**: Kilobyte, unidad de datos equivalente a 1024 (2^{10}) bytes.

14 **Mhz**: Megahertz o Megahercio, unidad de medida de frecuencia correspondiente a 1.000.000 de ciclos por segundo.

- Intel 8086, de 1978, fue el primer microprocesador de 16 bits que operaba a 4,77Mhz utilizando alrededor de 29000 transistores.
- Intel 8088, presentado en 1979, fue una versión económica el 8086 basada en un diseño de 8 bits, sin embargo fue microprocesador del IBM PC.
- Motorola 68000, de 1979, con alrededor de 68000 transistores y diseño de 16bits fue elegido para equipar Apple Macs y estaciones de trabajo Sun Unix.

Será en 1982 cuando Intel presente el 80286: un microprocesador de arquitectura CISC[15] de 16 bits con capacidad de manejar 16Mb[16] de memoria, que operaba entre 4Mhz y 25Mhz (en sus últimas versiones) y disponía de alrededor de 134.000 transistores. Este microprocesador fue producido por distintas compañías a lo largo de casi una década hasta 1991. Sin embargo, una de sus características revistió gran importancia; su conjunto de instrucciones lo hacían compatible con su predecesor y esta sería una particularidad que tanto Intel como algunos de sus competidores mantendrían en sus diseños durante las siguientes décadas.

A partir de allí, la competencia en el desarrollo y comercialización de microprocesadores tanto para uso hogareño como para usos específicos de gran magnitud o exigencia se ha sostenido generando importantes incrementos en el rendimiento de las nuevas generaciones de microprocesadores. No es de interés para este trabajo profundizar en detalle sobre las características técnicas de los mismos sino brindar al lector la noción de la magnitud de crecimiento de sus capacidades hasta la actualidad, no obstante es interesante referenciar a la denominada ley de Moore que se condice con dicha evolución. Aquel enunciado, realizado el 19 de Abril de 1965 por Gordon Earl Moore, quien fuera co-fundador de la empresa Intel, indicaba que la cantidad de transistores de un microprocesador se duplicaría cada año; sin embargo el mismo autor ajustó su enunciado en 1975 llevando el lapso de tiempo definido a dos años y posteriormente, en el año 2007, agregó un limite de aplicación que ocurriría entre los años 2017 y 2022.

15 **CISC:** del inglés, “Complex Instruction Set Computer”, corresponde a la arquitectura de procesador de instrucciones complejas.

16 **Mb**: Megabyte, unidad de datos equivalente a 1048576 (2^{20}) bytes.

El siguiente gráfico muestra la cantidad de transistores de diferentes microprocesadores producidos entre los años 1971 y 2015, estos datos se encuentran acompañados de una recta definida por la proyección de la Ley de Moore.

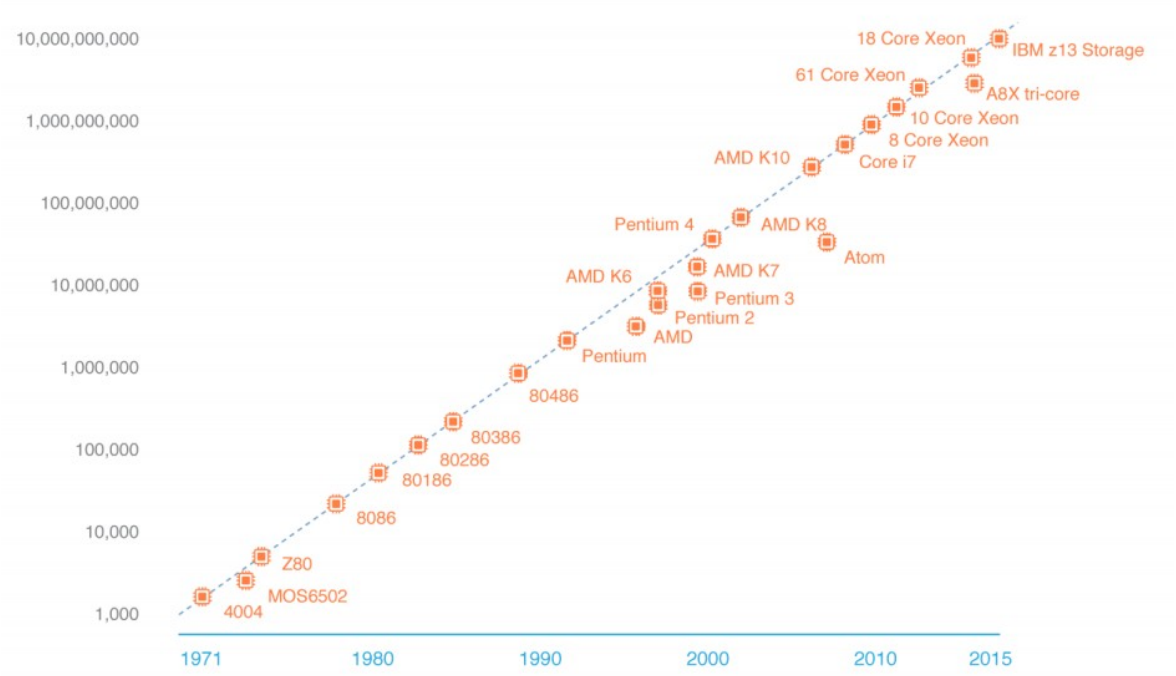


Imagen 1: Microprocessors Transistors Count 1971 – 2015 & Moore's Law

ASML Corporate Responsibilty Report 2015

Lógicamente, la complejidad de los microprocesadores actuales hace que existan diferentes aspectos que les han permitido obtener mejoras en su rendimiento y características independientemente de su cantidad de micro-transistores, entre ellas podríamos citar su arquitectura, frecuencia de funcionamiento, instrucciones con finalidades específicas, técnicas de optimización de procesamientos, etc. Pero resulta indispensable a los fines de este capítulo, identificar dos tipos de arquitecturas en las que podremos encuadrar a los procesadores utilizados en la actualidad, ellos son:

- CISC (Complex Instruction Set Computer): Esta arquitectura se caracteriza por disponer de un amplio conjunto de instrucciones con operaciones complejas entre registros en memoria o internos, haciendo uso de varios ciclos de procesamiento

por cada llamada a una instrucción. Esta arquitectura fue clave para el desarrollo de exitosos microprocesadores como el Motorola 68000, Zilog Z80 y la familia x86.

- RISC (Reduced Instruction Set Computer): Es una arquitectura de instrucciones de tamaño fijo que se ejecutan en un tiempo reducido de trabajo (usualmente un ciclo) donde solo las instrucciones de carga y almacenamiento acceden a la memoria de datos. Algunos microprocesadores de esta arquitectura son IBM PowerPC, DEC Alpha, MIPS, ARM, SPARC.

2.3 Producción de circuitos integrados

La producción de circuitos integrados a gran escala está acotada a un reducido número de empresas y organizaciones a nivel global debido a la complejidad técnica, al volumen de inversión en capital productivo y al conocimiento requerido para dicha actividad. Lo primero que debe comprenderse para abordar este tema es que hay dos grandes roles en esta industria, ellos son:

- Arquitectos: Corresponde a quienes diseñan el circuito, indicando los elementos necesarios (transistores, memoria, etc) en él y sus conexiones. En general, estas organizaciones son las mismas que los comercializan ante el usuario final.
- Fundiciones: Son las empresas que toman el diseño y lo materializan produciendo físicamente el circuito integrado.

Sin ser una tercer categoría o rol, tenemos otros actores que son fundamentales para el proceso de producción, que son las empresas que proveen a las fundiciones la tecnología de fotolitografía[17] que permite transferir diseños de patrones en una foto-máscara a otros materiales mediante la acción de agentes químicos y luz (para este caso suelen utilizarse frecuencias del rango ultravioleta); una de las principales empresas de este rubro es la holandesa ASML.

17 **Fotolitografía:** Técnica de fijar y reproducir dibujos en piedra litográfica, mediante la acción química de la luz sobre sustancias convenientemente preparadas.

Las empresas pertenecientes al primer rol mencionado (arquitectos), son mayoritarias en esta industria y de público conocimiento para los consumidores finales de productos de tecnología electrónica, entre ellas podemos citar a las principales marcas de CPUs, GPUs y dispositivos de comunicación. Algunas de ellas son: Intel, AMD, Nvidia, Broadcom, Qualcomm, Mediatek, Apple, Hitachi, Samsung, Sony, Panasonic, LG, Huahei, etc.

En contraposición las productoras o fundiciones son un número reducido de empresas no siempre conocidas por los usuarios finales pero muy afianzadas en el rubro, que de hecho suelen producir para múltiples clientes. Cabe aclarar que no todas ellas cuentan con la capacidad tecnológica para producir integrados de alta complejidad y mantenerse a la vanguardia de los mercados mas competitivos como son los de GPUs y CPUs donde actualmente se requiere fabricar diseños con una precisión de entre 20nm y 5nm, sin embargo existen una amplia cantidad de tipos de integrados que no requieren tal capacidad y pueden realizarse con tecnología mas antigua como microcontroladores, memorias, sensores, MEMS[18], integrados de uso genérico, etc.

En la actualidad se pueden identificar empresas con capacidad de producir dispositivos basados en semiconductores en los siguientes países[SEMICONDUCTORPLANTS2020]: Japón, China, Estados Unidos, Taiwan, Corea del Sur, India, Malasia, Israel, Irlanda, Rusia, Bielorrusia, Costa Rica, Méjico, Singapur, Reino Unido, Alemania, Emiratos Árabes Unidos, Holanda, Francia, Italia, Bélgica, Argentina, Austria, Hungría, Indonesia, Brasil, Tailandia, Filipinas, Corea del Norte, Australia, Polonia. Es necesario aclarar que hay una distribución de capacidades muy asimétrica, por lo que son pocos los países capaces de producir circuitos integrados de ultima tecnología y dentro de estos solo existe un número reducido de empresas que pueden hacerlo en grandes volúmenes; según el artículo *“La realidad sobre los nanómetros en procesos de fabricación de CPUs y GPUs”[AGUIRRE2017]* la porción mas representativa del mercado se ve cubierta por un reducido grupo de cuatro grandes actores, ellos son:

- Intel
- Global Foundries
- TSMC

18 **MEMS**: del inglés, “microelectromechanical systems”, refiere a tecnología electromecánica en dispositivos microscópicos.

- Samsung

En cuanto al proceso de producción convencional podría resumirse en las siguientes etapas:

1. El diseño del circuito integrado se transfiere en negativo a un filtro o máscara fotográfica.
2. Se corta una barra maciza de silicio en capas delgadas obteniendo las denominadas obleas.
3. Se trata químicamente y térmicamente la oblea para lograr una superficie limpia y uniforme.
4. Se reviste la oblea con un material foto-resistente.
5. Se proyecta un haz de luz ultravioleta hacia la oblea, pero interponiendo la máscara con el diseño en negativo, de esta forma las áreas expuestas a la luz sufrirán un cambio químico.
6. La oblea se posiciona en un torno de revoluciones fijas, donde se le aplica una solución química que elimina el material foto-resistente expuesto a la luz.
7. Se pasa la oblea a un horno para exponerla a temperaturas del rango 120-180 grados Celsius para solidificar el material foto-resistente que no fue eliminado.
8. Se expone la oblea a un agente químico, agresivo al silicio, eliminando el metal que no esta protegido por el material foto-resistente.
9. La oblea es tratada con un nuevo agente químico para remover la totalidad del material foto-resistente.
10. Se procede a los controles de conductividad y calidad de los circuitos grabados.
11. Se cortan los chips grabados en la oblea.
12. Se encapsulan con sus pines correspondientes para su disposición final.

2.4 Historia de las computadoras en la República Argentina

Es importante para este trabajo conocer algunos hitos y particularidades de los orígenes del desarrollo informático en la República Argentina, comenzando por el arribo de la primeras computadoras en la década del 60’. En aquellos años se documentó el ingreso de cinco grandes computadoras al país según informa el artículo "Continuar el camino. Cincuenta años de computación en Argentina"[SMUKLER2012]. El primero de estos fue un equipo IBM 305 RAMAC que se expuso en el sesquicentenario de la Revolución de Mayo con el fin de responder preguntas de carácter histórico. Otros dos equipos UNIVAC SS90 de la empresa Sperry Rand fueron provistos a la empresa estatal “Transporte de Buenos Aires” y un equipo IBM RAMAC 650 sería destinado a EFEA, Empresa de Ferrocarriles del Estado Argentino.

El quinto equipo, y quizás el mas paradigmático, corresponde a un Mercury II de la Empresa Ferranti, sucesora de la conocida Mark I, con entrada de datos y programas mediante cinta perforada y salida por teletipo. Este fue adquirido por la Universidad de Buenos Aires en 1958 durante la gestión del Dr. Manuel Sadosky, pero este equipo fue puesto en marcha durante 1961 debido al plazo de entrega y el acondicionamiento físico del Pabellón I de Ciencias Exactas para alojarla dado que se trataba de un equipo a válvulas, monolítico, de 18 metros de largo, mas de media tonelada de peso y que además requería gran disipación de temperatura para un correcto funcionamiento. Sobre este último punto el Dr. Sadosky enunciaba:

> *“Efectivamente, era un armatoste enorme, a válvulas. Tenía 18 metros y medio de largo, y adentro llevaba unas cinco mil válvulas. Ocupaba un gran salón. Por eso, para traerla y tener donde ubicarla, hubo que esperar hasta que se terminó de construir el primer pabellón de la Ciudad Universitaria” [CESSI2014]*

La importancia de Clementina se debe a que dio lugar no solo a que en el país se pudiera empezar a explotar la capacidad de estas nuevas tecnologías sino también a la formación de personas capacitadas para el uso de este tipo de equipos. Fue a partir de esta

incorporación que la Universidad De Buenos Aires pudo dar lugar a la creación de la carrera de Computador Científico en el año 1963 [BABINI97].

De manera contemporánea a los esfuerzos para la incorporación de Clementina a las actividades del país, la Facultad de Ingeniería de la Universidad de Buenos Aires buscaba incursionar en el aspecto del desarrollo electrónico de la mano del Humberto A. Ciancaglini, director del Departamento de Electrónica, dando lugar al desarrollo CEFIBA

(Computadora Electrónica de la Facultad de Ingeniería de Buenos Aires) entre los años 1958 y 1964. El resultado de este desarrollo no fue satisfactorio en cuanto a funcionalidad ya que para sus últimas etapas las capacidades habían quedado muy rezagadas en relación a los equipos disponibles en el mercado, no obstante el esfuerzo fue capitalizado en conocimiento y formación de recursos humanos.

En este punto de esta breve revisión histórica, es prudente a los fines de este documento, aclarar que el desarrollo de la capacidad informática de un país podría evaluarse en diferentes categorías, que si bien se encuentran relacionadas no necesariamente se superponen en conocimientos. Desde este punto de vista puedo identificar las siguientes clasificaciones:

- Desarrollo de hardware
- Desarrollo de sistemas
- Utilización y mantenimiento de sistemas

En los párrafos previos hemos visto como durante la década del 60’ el interés en el desarrollo de las capacidades informáticas del país cubría las tres categorías citadas, pero también podemos afirmar que en las siguientes décadas las capacidades del país se consolidaron en las dos últimas, enfocadas en la utilización de equipos informáticos y no tanto en la creación y fabricación de los mismos. Una clara muestra de esto surge de la cantidad de organizaciones basadas en la informática que se han desarrollado en el país, que incluyen filiales de las mas importantes empresas internacionales. Es válido aclarar que algunas de estas empresas que forman parte del conjunto de productores de hardware a nivel mundial se han inclinado al desarrollo de software por sobre el desarrollo y producción de hardware en nuestro territorio. Podemos listar algunas de ellas referenciadas por la CESSI[19][CESSI2014]: Blue Patagon, Bs. As. Software, Buffa, Bvision, C&S,

19 **CESSI**: Cámara de Empresas de Software y Servicios Informáticos de Argentina

Calipso, Cies Sistemas S.A., Cisco Systems Argentina S.A., Cognizant, Consensus, Consultores en Desarrollos Tecnológicos S.A., Consultores en Organización Asociados S.A., Cubika (GlobalLogic), Deloitte & Co S.A., E-Marketing (Competir), Elinpar, CDA, Everis Argentina, Finnegans, Accenture S.R.L., Fluxit SA, Acciona IT S.R.L., Fundación Evolución, Aeroterra , FX Informática, G.I. S.A. (Grupo Infosis), Ardison, G&L Group, Arizmendi Cómputos , Globant, Axoft , Grupo Assa, Base Global, Grupo Most, Baufest , Belatrix , Grupo Tekne, Huenei, Sia Interactive , IBM, Sisdam, Sistemas Bejerman, Sistran Consultores S.A., Sofrecom, Softland, Softlatam, Software América S.A., Soluciones Informáticas Globales S.A., Staffing IT, Synthesis, Systems Management Specialist S.A. (Grupo SMS), Liveware IS S.A., Lyracons S.A., Systems World S.A. , Maxisistemas, Tecnoap SA, Mercado Libre, Tekhne SA, MGI Accusys, Tgv, Microsoft, TPS S.A., Neoris, Unitech, Neosur, Vates, Neuralsoft, Vemn, Open Solutions, W3 Comunicacion SRL, Osi S.R.L., Worldsys S.A., Physis Informática S.R.L., Zoo Logic, Pines, Infotech, Innovision S.A., Intel, Inworx, IT Resources S.A., Jotafi S.A., Kapsch Trafficcom Argentina S.A., Latinvia, Pragma, Red Hat, Rumble S.R.L., Ryaco, Sabre International. En este listado se han omitido las entidades educativas y gubernamentales que como muestran los primeros párrafos de esta sección han sido participes pioneros en la actividad informática de la República Argentina.

Debido al ámbito de interés de este trabajo pasaremos a enfocar los siguientes párrafos en aquellos hechos históricos vinculados al desarrollo de hardware en el país; el mismo debe ser abordado con el entendimiento de que puede producirse hardware en diferentes niveles: desde el mas bajo donde encontramos la fabricación de componentes eléctricos y electrónicos básicos hasta el superior correspondiente al ensamble de componentes complejos para obtener un producto para el consumidor final. Con el fin de unificar criterios sobre este punto podemos enumerar los siguientes tipos de actividades relacionadas a la fabricación de hardware:

- Diseño y fabricación de componentes electrónicos básicos (resistencias, capacitores, inductores, etc.)
- Diseño y fabricación de componentes electrónicos basados en semi-conductores
- Diseño y fabricación de circuitos integrados

- Diseño y fabricación de circuitos electrónicos (incluidas placas y el montaje de componentes en las mismas)
- Diseño y fabricación o montaje de equipos que utilicen circuitos electrónicos (No implica diseño o fabricación de circuitos, sino el montaje de los mismos, reduciendo la producción propia de componentes utilizados a elementos de baja complejidad como gabinetes, cables, etc.)

Cabe destacar que existe una fuerte dependencia en los niveles inferiores, que si bien puede obviarse adquiriendo dichos componentes en el extranjero, esto implica establecer una relación de confianza en la calidad y funcionamiento del producto comprado al proveedor, transfiriendo la dependencia a dicha relación de confianza y las condiciones económicas y políticas para la adquisición de los componentes.

Comenzaremos esta revisión histórica enfocada a la producción de hardware en la República Argentina citando a la División Electrónica de la empresa Fate que en 1971 se avocó a la investigación y desarrollo de la calculadora electrónica Cifra 311. Esta máquina sentaría la base de conocimiento para avanzar a modelos mas complejos como la Cifra 211/221 en 1972 y la Cifra 511 para cálculo avanzado que comenzó a comercializarse en 1973. Debido a los acontecimientos históricos del país, su impacto en el gobierno y las políticas industriales, se procedió a finalizar el proyecto de la División Electrónica de Fate en agosto de 1976 y posteriormente, en el año 1978, la planta pasó a ser una filial de la empresa NEC pasando a ensamblar productos importados por la marca japonesa.

Se estima que en el periodo de 1971 a 1980 se comercializaron alrededor de 400.000 equipos de la familia Cifra de Fate, llegando a ser la mayor fábrica de calculadoras de América Latina y una de las diez mas importantes a nivel mundial. Si bien este es un caso de estudio de referencia, debido a que en este caso se investigó y desarrollaron los dispositivos solo utilizando componentes electrónicos extranjeros, hay otros casos donde empresas locales licenciaron la producción por ensamble de computadoras diseñadas en el exterior.

Telematch fue uno de estos casos, era un clon de la computadora de juegos Magnavox Odyssey 1, que comenzó a producirse en el país durante el año 1973. Otro caso fue el de la empresa EDU Games que ensambló clones de la famosa consola de juegos Atari 2600 que no se comercializó oficialmente en el país. En relación a esta marca llegó al país la

computadora Atari 65XE de manera oficial mediante un acuerdo con la empresa Sky Data S.A. pero estos equipos eran producidos en Taiwan.

La empresa Talent que se desarrollaba en la producción de televisores incursionó como licenciataria de la computadora coreana Daewon DPC 200 de norma MX1, de esta forma desde 1985 importó y ensambló en su fábrica de San Luis las computadoras que fueron conocidas como Talent MSX. Muchos componentes (no electrónicos) de estos equipos fueron fabricados en la misma planta cuyana. Es imposible evitar citar a la empresa Drean que se enfocaba en el mercado de electrodomésticos y logró en el año 1983 obtener la licencia de la empresa Commodore para producir, también en su fábrica de San Luis, la computadora hogareño Drean Commodore 64. Estos equipos comenzaron a comercializarse en el año 1985, y para el siguiente año la empresa tenía una capacidad de producción de 10.000 equipos mensuales, con la aparición del modelo Commodore 128 la empresa dejó la fabricación y pasó a operar como un importador solamente.

Según indica el artículo *"Industria electrónica Argentina. Evolución y perspectivas"* [KRAMER2012], en la década del 90 las empresas radicadas en el país que aun producían o ensamblaban hardware tendieron a reducir estas actividades incrementando la importación de ese tipo de equipos. No obstante ante la reducción de importaciones registradas entre los años 2001 y 2003, se observó una re-activación en rubros vinculados a la electrónica (no exclusivamente informáticos) que acompañado de políticas con beneficios impositivos, particularmente en Tierra del Fuego, permitió una recuperación del sector que en esta etapa se enfocó a la producción de los siguientes productos:

- Equipos de telecomunicaciones
- Equipamiento de audio y video para radiodifusión y televisión
- Armado o ensamble de televisores, equipos de video, audio y celulares
- Equipos para el procesamiento electrónico de datos y máquinas de oficina
- Básculas, balanzas de uso industrial y celdas de carga
- Sistemas de medición y control de surtidores de GNC
- Instrumentos de medición
- Sistemas para control destinados al transporte

- Sistemas para maquinaria agrícola
- Fabricación de equipos de electro-medicina
- Sistemas destinados a su utilización en automóviles
- Balanzas comerciales, cajas registradoras, impresoras fiscales y no fiscales, sistemas POS, terminales de auto-atención bancaria, máquinas contadoras y empaquetadoras de billetes y monedas, destructores y expendedores de moneda, sistemas de estacionamiento medido y tarifadores para locutorios
- Alarmas domiciliarias y porteros eléctricos
- Juegos de azar electrónicos como ruletas, traga-monedas

Como vemos este listado se enfoca en productos para el usuario final, no en componentes electrónicos; sin embargo el desarrollo de estos productos genera experiencia y conocimiento en el desarrollo de circuitos electrónicos complejos, aportando al diseño y fabricación de placas y uso de componentes electrónicos modernos. En relación a este punto el mismo documento referenciado previamente afirma:

> *"[...] El diseño de integrados es una actividad que ya se desarrolla en la Argentina, aunque todavía en forma escasa. "*

A pesar de esto, tanto instituciones educativas como organizaciones del ámbito tecnológico (por ejemplo INVAP[20] o INTI[21]), han desarrollado capacidad y conocimiento para el diseño y fabricación de integrados ASIC[22] a escala o volúmenes reducidos. Particularmente, el INTI cuenta con instalaciones y tecnología para diseñar y producir micro-dispositivos del tipo MEMS; muestra de estas capacidades es su Laboratorio de Micro y Nanoelectrónica del Bicentenario (CMNB) que dispone de microscopio de doble haz con el que han producido en pequeña escala distintos componentes como: memorias para usos satelitales, biosensores (Nanopoc[23]), leds con nano-hilos, entres otros.

---

20 **INVAP:** es una empresa argentina de alta tecnología dedicada al diseño, integración, y construcción de plantas, equipamientos y dispositivos en áreas de alta complejidad.

21 **INTI**: Instituto Nacional de Tecnología Industrial, es un organismo público de la República Argentina cuya misión es el desarrollo, certificación y asistencia técnica en tecnología industrial.

22 **ASIC**: del ingles, application-specific integrated circuit, significa circuito integrado de aplicación especifica.

Este documento no puede dejar de nombrar a la empresa Unitec Blue que produce comercialmente integrados en el país, desde la ciudad de Chascomús, sus productos están enfocados en los integrados para tarjetas SIM[24], EMV[25], Contactless[26] y prelaminadas; siendo proveedores de empresas vinculadas a las tarjetas bancarias, de transporte y seguridad.

23 **NANOPOC:** es un kit de diagnóstico para detectar, en el lugar y de manera casi instantánea, enfermedades infecciosas como el síndrome urético hemolítico (SUH), dengue, chagas y VIH.

24 **SIM**: acrónimo inglés de “subscriber identity module”, significa módulo de identificación de abonado.

25 **EMV**: acrónimo de "Europay MasterCard VISA", es estándar de interoperabilidad de tarjetas para la autentificación de pagos mediante tarjetas de crédito y débito.

26 **Contactless:** sistema de pago sin contacto basado en tecnología de identificación por radiofrecuencia.

3 La dependencia en activos tecnológicos asociados a la defensa y seguridad

Este capítulo aborda contenidos en relación diversas tecnologías y activos que pueden ser utilizados en el ámbito de la defensa. Algunos de ellos tienen relación directa con las fuerzas armadas de la República Argentina teniendo componentes de origen extranjero que han incidido negativamente en su desarrollo, uso o mantenimiento.
El propósito de este capitulo es proveer al lector del conocimiento básico sobre este tipo de elementos del ámbito de la defensa convencional a fin de poder abordar y comprender los planteos y conclusiones de este trabajo.

3.1 Pucará

En los primeros meses de 1968 la Fuerza Aérea Argentina presentó al Área de Materiales de Córdoba los requerimientos para el diseño y construcción de una aeronave de tipo COIN[27] que sería denominada IA-58 Pucará.

Se construyeron dos prototipos secuencialmente, el primero se denominó AX-2 y realizó su primer vuelo el 20 de Agosto de 1969 al mando del Mayor Roberto Starc para, luego de algunos ajustes, ser presentado oficialmente al público el 10 de Octubre del mismo año. Este primer prototipo dispuso de una motorización diferente a la utilizada en el modelo que se produciría en serie, - tema que abordaré en detalle en una sección posterior dedicada a ello -.

Meses después, el 24 de Octubre de 1970 se realizó un Festival Aéreo en el Aeropuerto de Ezeiza con motivo de los festejos del cierre de la XXIV Semana Aeronáutica y Espacial. En este evento se pudo apreciar el vuelo del prototipo AX-2 con la sorpresa de que este modelo no era el mismo avión presentado en el año anterior sino que disponía de una nueva motorización. Este hecho quedó documentado en la edición número 341 de la revista Aeroespacio publicada el 12 de Diciembre de 1970.

27 **COIN**: Acrónimo de “Contra-insurgencia”, del inglés “Counter-insurgency”, es la denominación para la variante de aviones de ataque a tierra con características optimizadas para el disponer de gran maniobrabilidad, capacidad de operación en pistas improvisadas, deterioradas y de reducida distancia.

Es así como el 28 de Noviembre de 1969 se ordenó la construcción de un segundo prototipo y la unidad AX-2 original fue reasignada como AX-01 mientras que el nuevo AX-02 ya dispondría de los motores franceses que equiparían a los futuros modelos de producción en serie; este cambio se concretó en mayo del 1970.

El prototipo AX-01 que se presentó al público el 20 de Octubre de 1969, retuvo sus motores americanos para completar pruebas y evaluaciones pero posteriormente se lo trasladó a las instalaciones de Turbomeca en Pau, Francia, abordo del Hércules C130 TC63 donde permaneció entre el 3 y el 24 de Junio de 1971 con el mismo fin. Tiempo después, el 8 de Febrero de 1972, se procedió a la instalación de los motores Turbomeca Astazou XVI-G-01 y a realizar las modificaciones pertinentes para la utilización de los mismos, dejando al prototipo AX-01 con la configuración elegida para la producción en serie.

Luego de comenzar su etapa de producción se construyeron nuevos prototipos, entre ellos el AX-03 que sería enviado a Francia en 1977 para ser exhibido en el Salón Le Bourget. Este prototipo fue dotado de componentes de aviónica adicionales que incluían dos VOR/ILS, dos ADF, dos VHF, HF, un navegador inercial Litton LTN-72, radar meteorológico Bendix RDR-160, respondedor Bendix DPR-600 y equipo de supervivencia adicional en sus asientos eyectores de tipo Martin-Baker MK AP06A.

Se realizaron pruebas preliminares en territorio argentino utilizando la ruta Córdoba, Santa Rosa, Neuquén, Bariloche, Bahía Blanca, Ezeiza, Rosario, Paraná y Córdoba, con el fin de recorrer 3200km en 8 horas. En base a la información obtenida se logró determinar que la máquina podía completar un recorrido de 4200Km a una velocidad crucero de 420 km/h.

El vuelo transoceánico se inició desde Córdoba el 14 de Mayo de 1977 a las 0830hs, realizando escalas en Recife, la Isla de Sal en Cabo Verde, Las Palmas en las Islas Canarias y Sevilla, para finalizar exitosamente su travesía en el aeropuerto de Pau el día 19 de Mayo.

El proyecto del desarrollo del IA-58 Pucará estuvo a cargo de los ingenieros aeronáuticos vicecomodoro Héctor Eduardo Ruiz y Aníbal Dreidemie. Según se conoce las prioridades utilizadas durante este proceso correspondían a estos cuatro criterios fundamentales: flexibilidad de uso, potencia de fuego, seguridad y simplicidad. El resultado fue un avión monoplano biplaza en tandem, íntegramente metálico, biturbohélice, de excelente maniobrabilidad, alta capacidad operacional en baja altura, baja servidumbre logística, de

tipo STOL[28] (300 metros de carrera de despegue y hasta 80 metros en JATO[29]), óptima flexibilidad operativa y amplio armamento ofensivo-defensivo.

Con estas características, este avión, podía ser utilizado para misiones de entrenamiento básico o avanzado, apoyo táctico, contra-insurgencia, reconocimiento ofensivo y/o fotográfico. Dado que no es de interés para este trabajo profundizar en el detalle de todas las características técnicas de esta aeronave solo citaré algunos puntos de referencia para conocimiento del lector, quien podrá extenderse a los detalles descriptos en el manual comercial de la aeronave provisto como Anexo.

- Techo operativo: 10.000 metros (32.808 pies)
- Velocidad horizontal máxima: 500 Km/h (270 nudos)
- Velocidad máxima de picada: 750 Km/h (405 nudos)
- Longitud: 14,5 metros (47,6 pies)
- Envergadura: 14,3 metros (46,8 pies)
- Altura: 5,4 metros (17,6 pies)
- Peso vacío: 4.000 kg (8.816 libras)
- Peso cargado: 6.800 kg (14.987 libras)
- Planta motriz: 2 motores turbohélices
- Capacidad de combustible interno: 1300 litros
- Alcance: 700 km (435 millas)
- Aviónica: AI, radio-faro omnidireccional VHF/LOC, sistema de aterrizaje instrumental, radiogoniómetro, baliza no direccional, giro-compás, brújula, transceptores VHF/HF, identificador amigo-enemigo, CME.
- Armamento
    - 4 ametralladoras FN-Browning M2-30 de 7,62 mm con 900 municiones cada una.

28 **STOL**: Del inglés"*Short Take-Off and Landing*", referencia a la característica de despegue y aterrizaje corto.

29 **JATO**: Del inglés "Jet Assisted Take-Off", o "Despegue asistido por reactores".

- 2 cañones: RSA-804 de 20 mm con 270 municiones cada uno. En la versión Bravo se reemplazaron por dos cañones DEFA 553, de 30mm, con 140 proyectiles para cada uno de ellos.
- 3 puntos de anclaje (2 de tipo Aero 20-AI y un Aero 7-AI central) con una capacidad total de 1.500 kg, posibilitando el uso convencional o con programador de tipo Bendix AWE1 de los siguientes elementos:
  - Bombas de propósito general FAS/Expal BK-BR y/o BRP de 125 kg y 250 kg. Bombas frenadas de 250Kg.
  - Bombas Incendiarias SITEA INC (Napalm).
  - Contenedores lanzacohetes LAU-61/A con 19× cohetes FFAR de 70 mm.
  - Coheteras ARM-657-A Mamboretá.
  - Pod de cañón de 30 milímetros, Pod de ametralladoras 7.62.
  - Tanques externos con capacidad para 300 litros de combustible.
  - Misil CITEFA MP 1000 Martín Pescador. (En la versión IA-58C).
  - Misil R.550 Matra Magic (En la versión IA-58C).
  - Cañón DEFA de 30mm adicional. (En la versión IA-58C).
  - Pod de remolque de blancos Tecnoblanc II modificado.

La etapa de producción de esta aeronave abarca el periodo entre 1974 y 1999, alcanzando un total de 107 aeronaves construidas. A lo largo de su historia se han desarrollado o planificado diferentes versiones, listadas a continuación:

- IA-58A Pucará – Principal versión de producción.
- IA-58B Pucará Bravo – Se construyó un solo prototipo en 1979 con aviónica mejorada y dos cañones automáticos DEFA de 30 milímetros.
- IA-58C Pucará Charlie - Se construyó un solo prototipo en 1985. Era una versión mono-plaza *(En base a la experiencia del conflicto de Malvinas)* se amplió su capacidad para incluir características antibuque y antihelicópteros, se le adicionó un

cañón DEFA de 30 milímetros, misiles aire-aire Matra R.550 Magic y soporte para el misil antibuque CITEFA MP1000 Martín Pescador, mejoras de blindaje y una sistema de guerra electrónica más avanzada.

- IA-58D Pucará Delta – Varios ejemplares IA-58A de la Fuerza Aérea Argentina fueron modernizados a este modelo con mejoras de aviónica y navegación satelital.
- IA-58E Pucará – Proyecto cancelado, destinado a la modernización de instrumental y motores.
- IA-58H Pucará – Proyecto cancelado, con el objetivo de desarrollar una versión destinada a la protección de fronteras.
- IA-66 Pucará II – Se construyó un solo prototipo en 1980, basado en el reemplazo de sus motores.
- IA-58 Fenix – Este es un proyecto activo, con un solo prototipo desarrollado, orientado a modernizar el sistema de armas mediante una re-motorización y equipamiento para misiones de ISR[30].

3.1.1 Motorización

Es de particular interés para este trabajo conocer los hechos vinculados a los diferentes procesos de motorización de esta aeronave, en consecuencia comenzaré referenciando al primer prototipo de Pucará que fue propulsado con dos motores turbohélices TPE-331-U-303 de la empresa norteamericana Honeywell Garrett que proveían 904 CV de potencia. Dicho motor se diseñó para uso militar en 1959 y actualmente cuenta con 18 modelos y 106 configuraciones diferentes, es ampliamente utilizado con mas de 13000 unidades vendidas en todo el mundo e incluso fue el motor seleccionado en 1965 para equipar al avión COIN Bronco OV-10, uno de los principales competidores de mercado del IA-58 Pucará. Como se indicó anteriormente el prototipo AX-01 (Originalmente denominado AX-2) retuvo estos motores hasta comienzos de 1972 donde se lo remotorizó con los mismos motores que se seleccionaron para el modelo que llegaría a la linea de producción.

30 **ISR**: Del inglés “Intelligence, Survillance and Recognition”, o “Inteligencia, Vigilancia y Reconocimiento”

El segundo prototipo, denominado AX-02, fue motorizado con turbohélices de origen francés, pertenecientes a la fábrica Turbomeca modelo Astazou XVI-G. Dicho motor fue diseñado a fines de la década del 50 y el modelo en cuestión provee una potencia de 969 CV. Es necesario mencionar que la decisión del cambio de motorización se dio luego del primer vuelo del prototipo con motor Garret buscando una solución o mejoras a inconvenientes encontrados en dicha etapa y la elección implicó cambios en la estructura para poder mantener las capacidades de vuelo y aerodinámica de la aeronave. El transcurso de los años demostraría que la elección del motor no fue adecuada en términos comerciales ya que el modelo francés tenía un mercado de repuestos, servicios y personal técnico capacitado inferior a su antecesor convirtiéndose en una desventaja ante sus competidores. A esta última situación se sumaría el hecho de que esas circunstancias precipitarían la finalización de la producción de este motor, que sumado a la falta de sus repuestos, limitó notablemente el tiempo de vida de las aeronaves construidas.

Años después, a comienzos de 1980, el proyecto denominado IA-66 abordó la problemática que ya era manifiesta sobre las desventajas de los motores franceses adoptando nuevamente motores Garret americanos, tal cual lo hizo el primer prototipo motorizado, pero en este caso se seleccionó un nuevo modelo de dicha familia, el TPE331-11-601W en conjunto con hélices Dosty Rotor de 4 palas. Al igual que en ocasiones anteriores se debieron realizar cambios en el diseño de las barquillas y bancadas para soportar la nueva motorización, quedando esta tarea a cargo de la compañía californiana Volpar Inc.. Finalmente el proyecto no prosperó y solo se construyó una unidad con esta configuración.

Durante el año 2012 y bajo la administración de Lockheed Martin Aircraft Argentina SA se avanzó en la consideración de cuatro motores para reemplazar los Astazou XVI-G. Estos modelos fueron los Garrett TPE331-12-UHR, GArret TPE331-12-B, Pratt & Whitney PT6A-60A y PT6A-62. La elección se inclinó por el Pratt & Whitney PT6A-62 con hélices Hartzell de cuatro palas de material compuesto que como ya he detallado también requeriría cambios en la estructura del avión (bancada y barquillas) que en esta ocasión serían encargados a la empresa Israel Aerospace Industry IAI. A comienzos del año 2013 se despachó el conjunto alar de la unidad matrícula A-561 con destino a Israel para comenzar con los trabajos. Sin embargo, por cuestiones burocráticas, permaneció retenida en el país hasta los primeros meses del año 2014. Meses después, en octubre del 2014, se finalizaron

las tareas sobre el conjunto alar iniciando un proceso de documentación, capacitación (para la cual se enviaron seis profesionales a las instalaciones del IAI) y construcción de piezas, utilajes y moldes. Finalmente en marzo del 2015 se procedió a trasladar el material resultante del este proceso de integración al país en el Hércules TC-100 de la Fuerza Aérea Argentina. El siguiente paso fue ensamblar el conjunto alar recibido y preparar el prototipo para su primer vuelo, hecho que tendría lugar en noviembre del 2015 proyectando la certificación del modelo para mediados del siguiente año - proceso que en los últimos meses del año 2019 aún se encuentra en curso -.

A continuación se puede apreciar visualmente la diferencia de cada motorización aplicada a este aeroplano según ha sido descripta previamente:

Imagen 2: Distintas configuraciones de motorización del Pucará

3.2 Exocet

Es un misil anti-buque subsónico[31] de origen francés desarrollado a comienzos de la década del setenta y puesto en servicio y comercialización en el año 1975, actualmente es producido por la firma MBDA.

Este misil dispone de varios modelos, componiendo una familia con los siguientes denominadores:

- MM.38 - De lanzamiento desde naves de superficie.

31 **Subsónico**: Inferior a la velocidad del sonido, estimada en 1235,52 km/h a 20 °C de temperatura, con 50 % de humedad a nivel del mar.

- AM.38 - Lanzamiento desde helicópteros
- AM.39 – Lanzamiento desde aviones. (Ejemplo: Super Etendard, Mirage F1/2000, Rafale)
- SM.39 – Lanzamiento desde naves submarinas.
- MM.40 – Lanzamiento desde superficie.

A modo de referencia podemos citar las ventajas operacionales presentadas por el proveedor en su ficha técnica[EXOCETAM39]:

• Ampliamente probado en combate

• Tipo *"Fire-and-forget"*, disparar y olvidar.

• Para atacar a distancias seguras para la aeronave de lanzamiento en todos los entornos (aguas marrones y azules) con una alta probabilidad de intercepción.

• Todos los climas,, de día y de noche.

• Garantiza una alta probabilidad de penetración en los blancos de superficies mas fuertemente protegidos.

La unidad tiene un peso de 670Kg y mide 4.69 metros de largo con un diámetro de 350 milímetros. Es impulsado con un propulsor de combustible sólido de dos etapas que le permite superar los 1.000 kilómetros por hora, con un alcance de setenta kilómetros. Su sistema de guiado, con computadora de a bordo con sistema digital avanzado automatizado de análisis de señales, está basado en un módulo inercial giroscópico para la primera fase del vuelo y un radar activo ESD ADAC en banda X para puntería en el tramo final o "*homing*"[32]. El siguiente gráfico muestra un esquema básico de la distribución de sus principales componentes.

32 Etapa de guiado automático al objetivo.

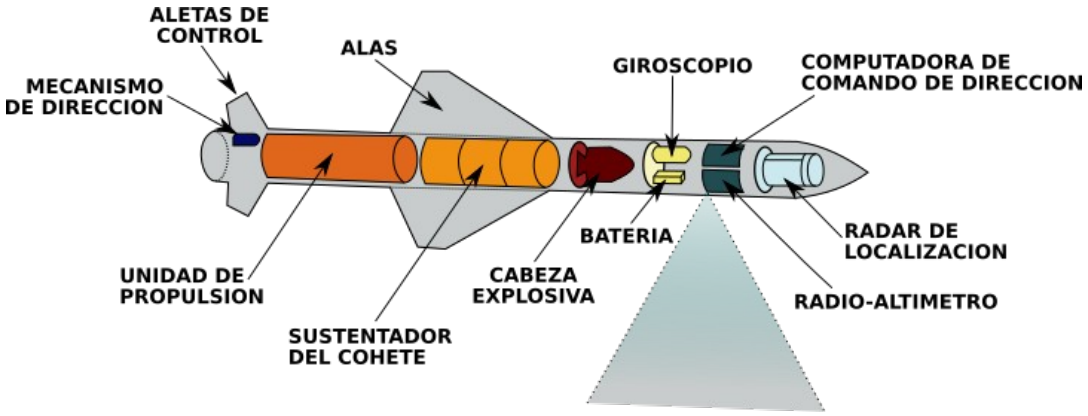


Imagen 3: Distribución de componente del misil Exocet

Este misil al ser disparado se orienta con las coordenadas del blanco para luego estabilizarse realizando un vuelo rasante a una altura cercana a los 10 metros en sus versiones originales, mientras que versiones mas actuales logran reducir esta distancia a alrededor de 3 metros. Al entrar en el área de proximidad al blanco, de alrededor de 10km del objetivo fijado, se activa su radar radar frontal que se utiliza para ajustar automáticamente la dirección del sistema de guiado para finalmente tomar una altura prefijada al momento del lanzamiento (Usualmente sujeta a las condiciones climáticas del área del objetivo). Las versiones actuales de este misil permiten finalizar el ataque con las siguientes técnicas de aproximación:

- Reducir su altura a alrededor de 3 metros para un impacto a nivel horizontal.
- Elevarse rápidamente con el fin de evitar sistemas de defensa anti-misil del objetivo para finalmente impactar desde una posición superior.

Esta descripción de componentes, capacidades y modo de operación permite comprender la complejidad de este armamento y su inherente dependencia en relación a elementos tecnológicos que incluyen software y hardware electrónico como partes críticas del mismo.

Debido al extenso periodo de producción, prestaciones y experiencias de uso en conflictos reales, el Exocet, ha sido comercializado y distribuido a un amplio conjunto de regiones. De tal forma que en la actualidad se conocen los siguientes operadores activos de este misil[WMEXO2019]:

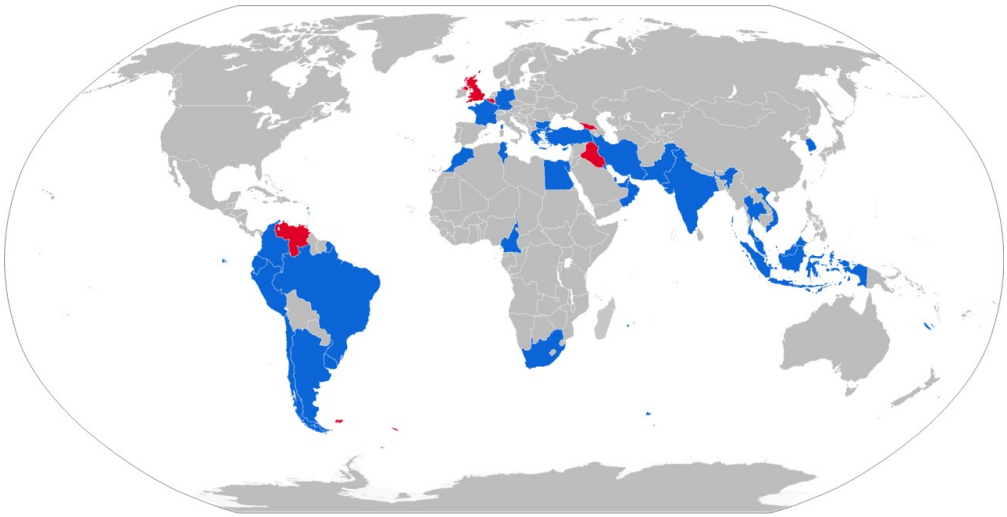


Imagen 4: Operadores del misil Exocet

- Armada Argentina: MM38, MM40 y AM39.
- Armada Real de Brunéi: MM38, MM40.
- Armada de Bulgaria
- Armada de Brasil: MM38, MM40 Block 2 y AM39, SM-39.
- Armada de Camerún: MM38, MM40 en embarcaciones P-48S (Bakassi).
- Armada Chilena: AM39, MM40 Block-2, MM40 Block-3 y SM39 para submarinos clase Escorpión.
- Armada Colombiana: MM40.
- Armada Francesa: MM38, MM40, AM39, SM39.
- Armada Alemana
- Armada Griega: MM38, MM40 Block 2/3.
- Fuerza Aérea Griega: AM39.
- Armada de Indonesia: MM38 en corveta de clase Fatahillah, MM40 Block 2 en corveta de clase Sigma , MM40 Block 3 en fragatas de clase Martadinata.
- Armada India
- Fuerza Aérea de Irán: Adquirió AM39 de Mirage F1s Iraquíes.
- Kuwait
- Libia
- Armada Real de Malasia: MM38, MM40 Block 2, MM40 Block 3 y SM39 (en submarinos clase escorpión)

- Armada Real de Marruecos: MM38, MM40 Block 2/3.
- Fuerza Aérea de Marruecos: AM39.
- Omán
- Brazo aéreo naval de Pakistán: AM39 (en Mirage-5V) y JF17 Thunder.
- Armada de Pakistán: SM39 (en submarinos clase Agosta 90B (Khalid), AM39 en aeronaves de patrullaje Breguet Atlantic.
- Armada del Perú – MM38 en corvetas de clase PR-72P, AM39 Block 2 en aeronaves ASH-3D Sea Kings y Mirage 2000P, MM40 Block 3 en fragatas clase Lupo.
- Catar
- Armada Sudafricana: MM40 Block 2 en fragatas clase Valour.
- Armada Real Tailandesa: MM38.
- Túnez: MM-40 Exocet para la embarcación de ataque rápido clase La Combattante III.
- Turquía: MM38
- Armada Popular de Vietnam: MM40 Block 3 en corveta de clase Signa.
- Armada de los Emiratos Árabes Unidos: MM40 Block 3 en corveta de clase Baynunah.
- Armada Nacional Uruguaya: MM38 en fragatas de clase Joao Belo
- Operadores que han discontinuado su utilización: Bélgica, Georgia, Irak, Reino Unido, Venezuela y Corea del sur.

3.2.1 ITB

Durante el conflicto de Malvinas, precisamente luego del 4 de Mayo de 1982 donde un misil Exocet disparado por la Armada Argentina desde un Super Etendard impactó exitosamente al portaaviones Hermes, el Estado Mayor de la Armada Argentina consideró la posibilidad de utilizar los misiles Exocet MM38 para contener los ataques de la flota británica sobre las fuerzas desplegadas en las islas. Cabe destacar, que en referencia a la anterior sección avocada a las características del misil Exocet, el modelo MM38 es una variante diseñada para su accionar en condiciones Mar-Mar lo que indica que es disparado desde una embarcación. En aquella fecha la República Argentina contaba con el sistema de lanzamiento emplazado en el destructor ARA Seguí, por lo que se decidió asignar recursos

para poder reutilizar estos recursos a fin de obtener la capacidad de utilizar los misiles desde tierra.

La ambiciosa tarea le fue asignada al entonces capitán de fragata Julio Marcelo Pérez[WPJP2019], ingeniero electromecánico (con orientación en electrónica) con posgrado en ingeniería aeroespacial, que ademas desempeñó tareas de investigación y desarrollo en el área de misiles de CITEFA[33], participó de lo proyectos de instalación de sistemas MM38 en embarcaciones de la Armada Argentina y estuvo asignado a la supervisión de la recepción de sistemas SM39 para Super-Etendard.

En conjunto con los técnicos Luis A. Torelli y Antonio Shugt se procedió al desarme y se abordó un proceso de ingeniería reversa para identificar las señales que el misil intercambia con con la unidad de control para diferentes escenarios de disparo. Sobre dicho proceso el Capitán Perez comentaba[GIONCO2019]:

> *"Cortábamos cables y probábamos señales mediante cablecitos, y estos cablecitos se juntaban con otros para simular otras señales, y éstas otras eran aplicadas con pilas, y así obteníamos, sucesivamente, indicios, marcas, signos que nos permitían reconstruir un sistema. [...] Al cabo de numerosos ensayos, llegamos a la conclusión, casi fantástica, de que sí, podíamos engañar al misil"*

Luego de esta etapa se procedió a la construcción de los siguientes componentes:

- Simulador de señales de control *(Compuesto por válvulas y potenciómetros, entre otros componentes)*
- Plataforma inercial de lanzamiento terrestre
- Carretón de transporte de misiles
- Equipo de detección de blancos
- Grupo electrógeno móvil *(Reutilizando el de un antiguo reflector antiaéreo)*

33 CITEFA: Instituto de Investigaciones Científicas y Técnicas de las Fuerzas Armadas.

Imagen 5: Sistema argentino ITB en las Calles de Puerto Argentino

Luego de varias jornadas de trabajo en Puerto Belgrano estos componentes habían dado lugar a la creación del sistema conocido como ITB, que según las propias palabras del Capitán Pérez tenía este origen[AAG2012]:

> *"Estábamos encerrados en una habitación, con dos tipos excepcionales cuyos nombres quiero recalcar: los técnicos Torelli y Shugt, y allí trabajábamos día y noche, en el más alto secreto. Nadie sabía lo que estábamos haciendo, excepto los que debían saberlo. Recuerdo que inventamos una sigla para identificar nuestro trabajo: ITB. De ese modo, para todo el mundo estábamos "en el ITB", que significaba ni más ni menos que INSTALACION de TIRO BERRETA, casi una broma. Es que resultaba casi ofensivo para la ingeniería concebir sobre todo hacer algo así, tan improvisadamente, con injertos, pedazos de cosas que conseguíamos por ahí... cablecitos... Lo cierto es que nadie podía entrar a esa habitación, y de ella salíamos alguna que otra vez para ir al buque y probar. Así experimentábamos."*

Es interesante comprender la secuencia inicial de comunicación del misil y la manera en que la solución logró resolver este intercambio de información. El sistema original se basa en tres etapas de intercambio de paquetes de datos de 64 bits; inicialmente se envía un primer paquete desde la computadora del lanzador esperando que el mismo sea devuelto

sin errores o diferencias. En una segunda etapa se enviá un nuevo paquete con algunas modificaciones y se aguarda a su correcta devolución por parte del Exocet, para finalmente entrar en una tercera etapa con el envío de un paquete cuyo contenido corresponde a la información del objetivo y configuración de lanzamiento (distancia, altura de vuelo, área de búsqueda para el homing, etc).

El Capitán Pérez y su equipo decidierón generar un paquete de datos con la información de lanzamiento correspondiente a la tercer etapa del procedimiento descripto previamente y utilizar este mismo paquete en todas las etapas con el fin de simplificar la ejecución de este intercambio de información. Dicho paquete contendría la definición del área máxima de búsqueda de blancos, para de esta forma poder concretar el disparo y según las propias palabras del Capitán Pérez[GIONCO2019]: *"Que sea lo que Dios quiera"*.

Cabe destacar que la información del blanco a utilizar era obtenida de un radar antipersonal del ejercito que utilizaba un formato de coordenadas diferente al del ITB, en consecuencia se calculaba manualmente la equivalencia de estos valores a tensiones representativas de los mismos para la ITB. Dichos niveles de tensión se ajustaban manualmente en el dispositivo de control de tiro mediante potenciómetros para programar el objetivo. Todo este proceso de obtención de coordenadas, transformación y configuración a través de tareas manuales debía realizarse con certeza y velocidad dado que los potenciales blancos podían estar en movimiento.

El sistema ITB se cargó a bordo de dos aviones Hércules C130 de la Fuerza Aérea Argentina junto al personal requerido para su operación con el fin de ser trasladado a Puerto Argentino, considerando que sólo la plataforma pesaba mas de seis toneladas y cada uno de los contenedores con su misil, alrededor de mil ochocientos kilos. Este traslado se concretó el 31 de mayo de 1982, luego de dos intentos fallidos donde los vuelos debieron cancelarse por razones de seguridad. Al arribar el apostadero Naval Malvinas se camufló, se distribuyeron los componentes y se asignaron recursos de guardia para evitar que los mismos sean advertidos por los habitantes del lugar o actividades de reconocimiento (aéreas y satelitales). Sobre este momento el Capitán Pérez decía[AAG2012]:

> *"Apenas llegamos pusimos a los dos carretones en un galpón de Puerto Argentino. Al día siguiente, el Contralmirante Otero (Jefe Naval en las islas) me asignó dos Tenientes de Fragata de Infantería de Marina para que colaboraran conmigo en el*

empleo del sistema. Ellos eran los TF IM Rodríguez Edgardo y el TF IM Abadal Mario (hoy ambos con Capitanes de Navío). A ellos se sumó el TF IM (RE) Ríes Centeno, a la sazón productor de "La Aventura del Hombre", que se encontraba con un equipo de filmación en las islas. A ellos les expliqué el funcionamiento de la ITB y como se debía proceder para efectuar un lanzamiento. Luego se sumó a Ríes Centeno el Sgto. Sánchez (Ejército Argentino) que operaría el Radar RASIT, único radar portátil disponible para que fuera el que nos proveyera de los datos del blanco, pese a que era un radar de vigilancia terrestre."

Se decidió ubicar la plataforma de lanzamiento en el camino asfaltado que atraviesa el istmo que une a la península del aeropuerto con el resto de la Isla Soledad. Dicha tarea se realizó con el amparo de la oscuridad nocturna. A partir del 1 de Junio de 1982 se comenzó a utilizar esta posición para los intentos de disparo del ITB, por lo que en cada día de operaciones se procedía con la siguiente rutina:

Hora	Tarea
1830hs	Instalación del radar y la plataforma inercial. Inicio de las actividades manuales para el posicionamiento, fijación y calibración de la plataforma.
1930hs	Hora estimada de finalización de la instalación de la plataforma inercial.
2000hs	Arribo del carretón con los contenedores de misiles y grúa autopropulsada para su instalación en la plataforma.
2030hs	Presentación y conexión del dispositivo electrónico de control de tiro y su grupo electrógeno de alimentación.

Tabla 2: Rutina de operación del ITB

En las siguientes horas se aguardaba que alguno de las buques que realizaban el asedio de artillería contra las unidades desplegadas en las islas entrara en el área de alcance del ITB, y lógicamente antes del amanecer de desarmaba el sistema de componentes para esconderlo nuevamente.

El 1 de Junio de 1982 se desplegó el operativo para el uso del ITB por primera vez, en aquella noche se realizaron dos intentos de disparos; el primero falló debido a un problema

en la ignición de misil y el segundo fue disparado pero tuvo una trayectoria incorrecta. En los siguientes días se hicieron ajustes y reparaciones menores en el ITB mientras se aguardaba el arribo de dos nuevas unidades de Exocet MM38 desde el continente. El 5 de Junio de 1982 arribó un avión Hércules C130 de la Fuerza Aérea Argentina con los dos misiles esperados para reanudar las operaciones nocturnas del ITB, a partir de ese día se preparó el sistema de armas con el procedimiento previamente descripto a la espera de un blanco factible. Días después, el 12 de Junio de 1982, se dio el escenario esperado, un buque ingresó en la zona de alcance del ITB 29.960 metros de distancia en dirección 201º 22'; el disparo fue exitoso y acertó en el blanco.

Meses después se confirmó que el buque alcanzado fue el HMS Glamorgan que recibió el impacto en la zona de popa con un resultado de 13 tripulantes fallecidos, 22 heridos y dejando a la nave fuera de servicio durante el resto del conflicto.

Imagen 6: Ubicación geográfica del ITB

Este evento fue relatado por el Capitán Pérez con las siguientes palabras[AAG2012]:

> *"Con toda premura realizamos el procedimiento y lanzamos un misil viéndolo alejarse por el brillo de la tobera en la oscuridad de la noche. Luego vimos un corto fogonazo, que después supe fue un misil Sea Cat que lanzó el buque contra el Exocet, y enseguida una explosión que iluminó todo el horizonte y se reflejó en las nubes bajas. El misil había hecho impacto en el crucero liviano Glamorgan"*

Según el documento "INVENTIVA BAJO PRESIÓN: EL LANZADOR COSTERO DE EXOCET EN LA GUERRA DE MALVINAS"[AMENDOLARA2012], al finalizar el

conflicto de Malvinas Gran Bretaña capturó el ITB de las islas y tras su análisis procedió a desarrollar una versión mejorada bajo condiciones normales dando como resultado el sistema de lanzamiento de MM38 denominado “Excalibur” utilizado para la defensa costera de Gibraltar. En paralelo trabajaron en la mejora de sus buques en base a las experiencias sufridas durante el conflicto instalando sistemas de defensa cercana anti-misiles “Phanlax”, de origen norteamericano, en portaaviones como el HMS “Illustrurius” y de clase “Invincible”, dicha estrategia sería continuada con el uso de sistemas “Goalkeeper” de origen holandés y munición mas pesada.

3.3 Drones

La invención y desarrollo del dron[34] como herramienta para múltiples tareas ha generado un aporte para diferentes actividades inclusive las relacionadas con la defensa y seguridad de las naciones. Es importante destacar que, en dicha evolución, la reducción de sus costos de producción y el desarrollo de características que simplifican el uso de los mismos han permitido la masificación del acceso a este tipo de dispositivos inclusive para la población general con fines comerciales y hasta recreativos.

Esta evolución con amplitud en diversos aspectos de su capacidad y finalidad ha dado lugar a una extensa variedad de modelos en distintas regiones del mundo. Como referencia de ello podemos apreciar algunos ejemplos en el siguiente extracto de la “Guía de supervivencia contra drones”[DSG2015]

34 **Dron:** Del inglés “*drone*”. Sustantivo, masculino. Aeronave no tripulada.

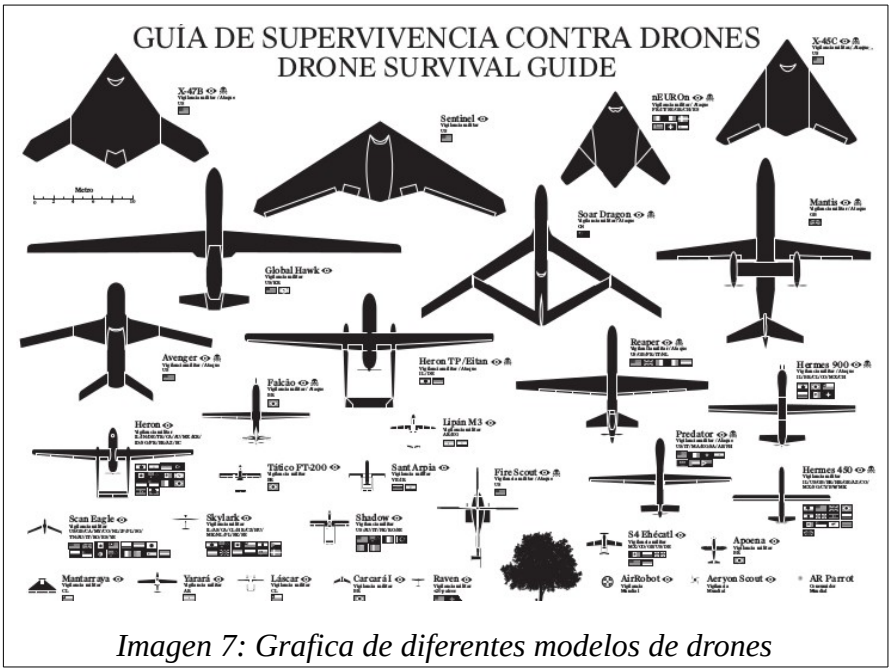


Imagen 7: Grafica de diferentes modelos de drones

La mayoría de los modelos representados en la gráfica anterior corresponden a modelos para uso militar y dada la manifiesta diferencia que se puede apreciar, aun para un lector sin conocimiento de sus particularidades, han sido clasificados por la NATO[35] en función de sus características y finalidad de uso. El siguiente cuadro muestra los detalles de dicha clasificación[STANAG4670]:

35 NATO: Del acrónimo en lenguaje Inglés: North Atlantic Treaty Organization. Corresponde a la alianza ínter-gubernamental de carácter militar que desde el 4 de abril de 1949 provee una defensa colectiva entre sus países miembros.

NATO UAS CLASSIFICATION						
Class	Category	Normal Employment	Normal Operating Altitude	Normal Mission Radius	Primary Supported Commander	Example Platform
Class III (> 600 kg)	Strike/ Combat *	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre	Reaper
	HALE	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre	Global Hawk
	MALE	Operational/Theatre	Up to 45,000 ft MSL	Unlimited (BLOS)	JTF	Heron
Class II (150 kg - 600 kg)	Tactical	Tactical Formation	Up to 18,000 ft AGL	200 km (LOS)	Brigade	Hermes 450
Class I (< 150 kg)	Small (>15 kg)	Tactical Unit	Up to 5,000 ft AGL	50 km (LOS)	Battalion, Regiment	Scan Eagle
	Mini (<15 kg)	Tactical Sub-unit (manual or hand launch)	Up to 3,000 ft AGL	Up to 25 km (LOS)	Company, Platoon, Squad	Skylark
	Micro ** (<66 J)	Tactical Sub-unit (manual or hand launch)	Up to 200 ft AGL	Up to 5 km (LOS)	Platoon, Squad	Black Widow

Imagen 8: Clasificación de UAS de la OTAN

Con un enfoque mas técnico, enfocado en su maniobrabilidad, capacidades de vuelo y generalizando la clasificación para comprender todo tipo de dron, inclusive los de uso civil, podemos establecer la siguiente tipificación:

Dron de palas móviles	De múltiples rotores	• Tricóptero • Quadcóptero • Hexacóptero • Octocóptero
	De rotor único	Helicóptero de rotor vertical principal y un segundo rotor compensatorio en posición horizontal.
Dron de ala fija	Con uno o mas propulsores en posición horizontal, correspondiendo al diseño de un aeroplano convencional.	

Tabla 3: Tipos de drones

Lógicamente la tecnología accesoria depende del tipo de aeronave comprendiendo modelos militares que pueden portar aviónica, sistemas de armas, sistemas de reconocimiento y hasta contra-medidas de defensa similares a los de aeronaves de combate convencionales.

En paralelo veremos que en el ámbito civil la tecnología hace que sea frecuente encontrar sistemas de GPS[36], FPV[37], sensores de distancia, comunicación inalámbrica de frecuencias compatibles con equipos de uso convencional como celulares, tablets o radio-controles y transmisores de video de frecuencias de 2.4 y 5.8 Ghz.

No es de interés para este trabajo documentar las diferentes características de control y automatización disponibles en este tipo de dispositivos, sin embargo es importante destacar que es frecuente que en dispositivos de comercialización convencional para uso civil, ya sea con fines recreativos como comerciales, existan controles vía software para limitar el uso del dron ante ciertas circunstancias. A modo de ejemplo del escenario citado previamente haremos referencia a productos de la empresa DJI[38], particularmente a dos de ellos, aunque los controles para limitación de uso se encuentran disponibles en toda su línea de productos. Los productos citados han sido seleccionados en función al éxito y volumen de ventas de su categoría, dichos modelos son los siguientes:

DJI - Phantom 4	Peso	Phantom 4 Pro/Pro+: 1388 grs Phantom 4 Pro/Pro+ V2.0: 1375 grs
	Medida diagonal	350mm
	Máxima velocidad de ascenso	Modo Sport: 19.7ft/s(6 m/s); Modo GPS: 16.4ft/s(5 m/s)
	Máxima velocidad de descenso	Modo Sport: 13.1ft/s(4 m/s); Modo GPS: 9.8ft/s (3 m/s)
	Máxima velocidad	45 mph (72 kph) (S-mode); 36mph (58 kph) (A-mode); 31 mph (50 kph) (P-mode)
	Sistemas de	GPS / GLONASS[39]

36 GPS: Del inglés *"Global Positioning System"*. Es un sistema de posicionamiento global basado en constelaciones de satélites.

37 FPV: Del inglés *"First Person Viewing"*. Tecnología que permite visualizar en tiempo real el video capturado desde la línea de visión frontal del dispositivo. En ocasiones los dispositivos de visualización tienen el formato de casco.

38 DJI: Del chino: *"*大疆创新*, **Dà-Jiāng I**nnovations"*, es un empresa líder en el desarrollo y producción de drones de uso civil a nivel mundial, con una cuota de mercado cercana al 70%.

39 GLONASS: Del ruso *"ГЛОНАСС, ГЛОбальная НАвигационная Спутниковая Система"*, sistema de posicionamiento global de origen ruso compuesto por 31 satelites dispuestos en 3 planos orbitales de 8 satelites cada uno dispuestos a una altitud media de 19.100km.

	posicionamiento satelital	
	Frecuencia de operación	2.400 - 2.483 GHz y 5.725 - 5.850 GHz
	Distancia máxima de transmisión	2.4 GHz: 4.3 mi (7 km, FCC); 2.2 mi (3.5 km, CE); 2.5 mi (4 km, SRRC) 5.8 GHz: 4.3 mi (7 km, FCC); 1.2 mi (2 km, CE); 3.1 mi (5 km,SRRC)
	Temperatura de operación	32° a 104° F (0° a 40° C)
	Batería	6.000 mAh LiPo[40] 2S

Tabla 4: DJI Phantom 4 - Características

40 Lipo: batería recargable de polímero de iones de litio.

DJI – Mavic 2	Peso	907 g (Mavic 2 Pro); 905 g (Mavic 2 Zoom)
	Medida diagonal	354mm
	Máxima velocidad de ascenso	5 m/s (S-mode), 4 m/s (P-mode)
	Máxima velocidad de descenso	3 m/s (S-mode), 3 m/s (P-mode)
	Máxima velocidad	72 km/h (S-mode) (nivel del mar, sin viento)
	Sistemas de posicionamiento satelital	GPS / GLONASS[41]
	Frecuencia de operación	2.400 - 2.4835 GHz y 5.725 - 5.850 GHz
	Distancia máxima de transmisión	FCC: 8.000 m; CE: 5000 m; SRRC: 5.000 m; MIC: 5.000 m
	Temperatura de operación	-10°C - 40°C
	Batería	3850 mAh LiPo[42] 4S

Tabla 5: DJI Mavic 2 - Caracteristicas

Estos dispositivos cuentan con un límite máximo de altitud y radio de operación controlado por software, básicamente se encuentran limitados a operar bajo un techo de 500 metros o 1640 pies de altura, en un área cilíndrica representada en el siguiente gráfico extraído del manual de usuario del dispositivo[DJIMAVIC2]:

41 GLONASS: Del ruso “ГЛОНАСС, ГЛОбальная НАвигационная Спутниковая Система“, sistema de posicionamiento global de origen ruso compuesto por 31 satélites dispuestos en 3 planos orbitales de 8 satélites cada uno dispuestos a una altitud media de 19.100km.

42 Lipo: batería recargable de polímero de iones de litio.

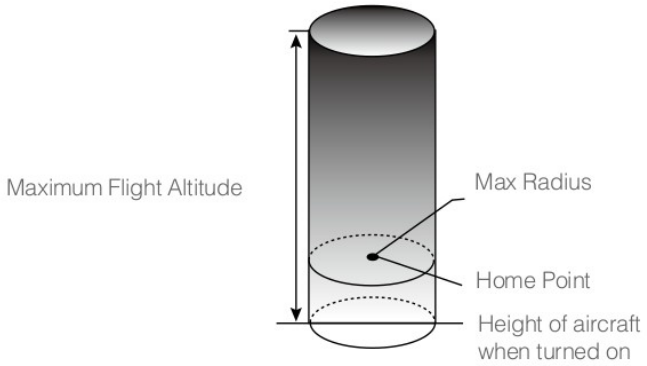


Imagen 9: Limites de altura de dron DJI

Al mismo tiempo estos modelos cuentan con zonas de vuelo vedado o *"No-Fly Zones"*, las mismas son públicas y se encuentran listadas en la página oficial del fabricante, accesible desde la url: http://www.dji.com/flysafe/no-fly . Estas áreas se encuentran divididas en dos categorías correspondientes a aeropuertos y zonas restringidas *(Ej: fronteras)*.

La siguiente gráfica muestra las limitaciones dispuestas por el software para el dispositivo en áreas de aeropuertos [DJIPHANTOM4]:

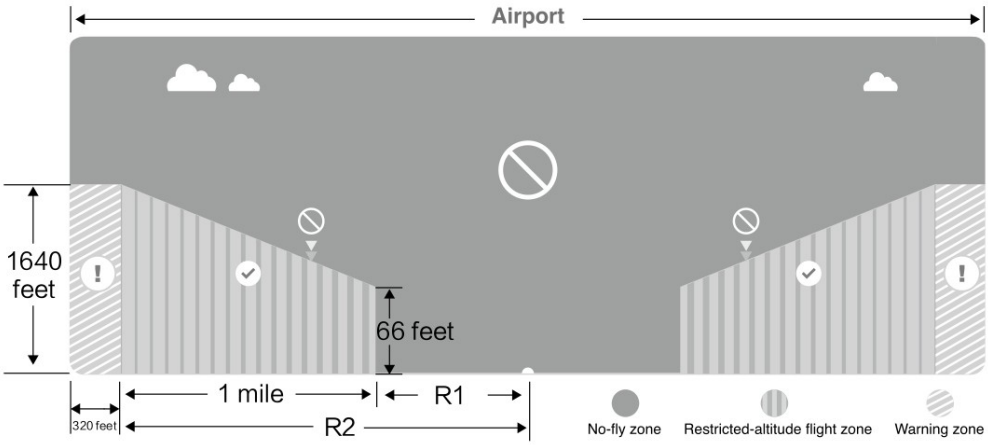


Imagen 10: Limites de operación en zonas aeroportuarias de dron DJI

En contraparte las limitaciones para la operación en zonas restringidas operan en función a la distribución representada en el siguiente gráfico :

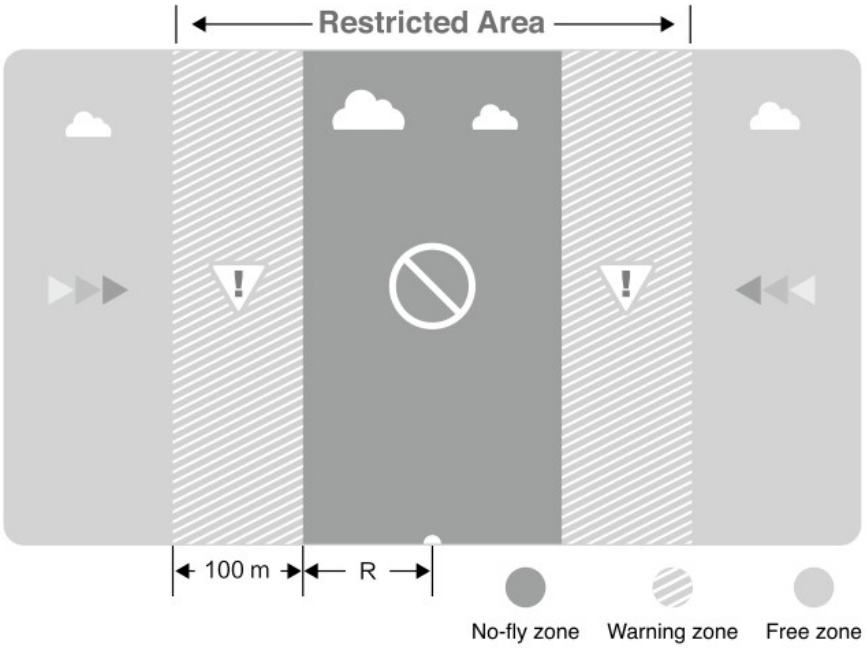


Imagen 11: Limites de operación en zonas restringidas de dron DJI

3.4 Crypto AG

La empresa de origen suizo Crypto AG que tuvo su central en la ciudad de Steinhausen ha sido un actor principal en la industria de dispositivos de comunicación criptográfica durante el último siglo. La empresa fue fundada en 1922 y a lo largo de su vida comercial, finalizada en el año 2019, se especializó en el diseño, desarrollo y producción de equipamiento para comunicaciones cifradas cubriendo diversas tecnologías desde sus comienzos con equipos mecánicos, luego con electro-mecánica y en sus últimas décadas con sistemas de cifrado electrónico.

Según indica cryptomuseum[CRYPTOMUSEUM2020], esta empresa se vio vinculada a Bundesnachrichtendienst (BND, Servicio Federal de Inteligencia alemán) y la Agencia Central de Inteligencia Americana (CIA), y a partir de 1970 estas organizaciones tomarían control de la empresa dando lugar a la operación THESAURUS que posteriormente sería renombrada como RUBICON. Este dato es de gran importancia debido a que las comunicaciones mas sensibles de numerosos países dependían de los productos de esta empresa y fue demostrado que los mismos fueron manipulados para que los organismos de

inteligencia que la manejaban dispusieran de mecanismos para poder acceder a la información cifrada que generaban sus productos y así, espiar a una gran cantidad de gobiernos. Esta situación fue expuesta públicamente a comienzos del año 2020 por una investigación *"The intelligence coup of the century"* de Greg Miller para el diario Washington Post[MILLER2020]. Esta noticia revelada fue rápidamente verificada y difundida por otros medios mundiales entre ellos la BBC[BBC2020-1][BBC2020-2].

3.4.1 CX-52

El CX-52 es un equipo de criptografía mecánica desarrollado por Boris Hagelin y producido por Crypto AG a partir de 1952 como evolución del C-52 con el fin de reemplazar en su cartera de productos a los modelos C-446 y M-209.

La máquina se basada en el uso de seis tambores de cifrado intercambiables donde cada uno tenía un número de pasos diferentes para completar su rotación. Este equipo podía ser provisto con seis tambores adicionales para ser intercambiado en función de la clave a utilizar.

El equipo tenía una interfaz de usuario simple, con entrada de clave mediante el posicionamiento los rodillos y la entrada de datos con un disco alfabético localizado en la parte izquierda del panel. Una palanca situada a la derecha del equipo daba lugar a la operación criptográfica cuya salida se observaba en el re-posicionamiento automático del disco alfabético de entrada y en la impresión de una cinta de papel de dos columnas (carácter de entrada - carácter de salida). Esta cinta era marcada para su corte de separación en la misma máquina a fin de proveer una tira de mensaje en claro y otra de cifrado.

Este equipo fue producido y comercializado en versiones civiles y militares con diversas variantes, una de ellas incluía el reemplazo de los rodillos por un lector de cinta perforada, la misma se basaba en el concepto de cinta aleatoria OTT[43] o de un solo uso, que incrementaba la seguridad del sistema y es por esta razón que esta versión particular solo fue distribuida a naciones de la NATO.

A continuación se muestran imágenes, pertenecientes a Cryptomuseum, del modelo convencional de CX-52 y el modelo OTT conectado al teclado externo (accesorio opcional):

43 **OTT**: Del inglés "One time tape", cuyo significado es cinta de un solo uso. Su contenido debe ser aleatorio y utilizado por una única vez, su reutilización afectara negativamente la seguridad del cifrado.

Imagen 12: CX-52

Imagen 13: CX-52 OTT con teclado

El interés de este documento en este dispositivo en particular radica en que la República Argentina fue uno de los países que adquirió y utilizó para comunicaciones sensibles este producto. Evidencia de esto es el decreto presidencial S 6768/1971[D6768-1971] del 31 de diciembre de 1971, donde se autorizaba la compra y utilización de estos equipos en base a la resolución de la Junta de Comandantes en Jefe en su Reunión N° 27/69, que incluía esta consideración:

> *"[…] por Resolución de la Junta de Comandantes en Jefe en su Reunión N° 27/69 ha sido establecida la utilización de máquinas criptográficas Hagelin Cryptos CX-52 Standard "A" con base eléctrica, para el tráfico clasificado en los niveles Estratégico Operacional y Estratégico Militar."*

Estos equipos comenzaron a utilizarse posteriormente al año 1972 y su utilización se prolongó aún mas allá del conflicto bélico de Malvinas, con las implicancias que esto representó para los intereses del país. Debe tenerse en cuenta que la información que ha trascendido públicamente tras el informe del Washington Post[MILLER2020] es parcial y nunca se podrá ponderar con certeza, ni cuantitativa ni cualitativamente, la información confidencial filtrada. Sin embargo, en base a la evidencia, se puede afirmar que los secretos de nivel estratégico operacional y estratégico militar del país quedaron totalmente expuestos haciendo que el esfuerzo de la nación por protegerlos se transformara en la vía para facilitarle esta información, que *per se* era sensible, a actores extranjeros tanto en tiempos de paz como de enfrentamiento con sus aliados.

4 Hardware y software de fuentes abiertas

Este capitulo desarrolla contenidos a fin de facilitar la comprensión de conceptos vinculados al software y hardware de fuentes abiertas en conjunto con una reseña de dispositivos y proyectos correspondientes a estas categorías que se encuentran disponibles en la actualidad.

Esta información sera de utilidad para que el lector comprenda las ventajas, desventajas, diferencias y potencial de estas tecnologías al momento de abordar las conclusiones.

4.1 Código Abierto y Software Libre

Es importante para este trabajo una correcta comprensión de los conceptos vinculados al acceso al conocimiento, composición y funcionamiento de productos tecnológicos. En este aspecto el ámbito del desarrollo de software ha evolucionado durante las ultimas décadas con mayor velocidad y solidez que el área vinculada al hardware, es por esto que a continuación se aborda una breve explicación de los conceptos principales del “Software Libre” y de “Código Abierto”.

4.1.1 Software Libre

Es un concepto definido por la FSF[44] basado en los criterios que debe cumplir un software para respetar la libertad de los usuarios que deberían poder ejecutar, copiar, distribuir, estudiar, modificar o mejorar el software según sus necesidades. Un punto muy importante es que esta libertad no implica que el mismo sea gratuito.

Según la FSF un programa de *“Software Libre”* cumple con estas cuatro libertades esenciales[FSF2019]:

1. Libertad de ejecutar el programa con cualquier propósito.
2. La libertad de estudiar y comprender el funcionamiento del programa y modificarlo si le fuera necesario. El acceso al código fuente es una condición necesaria para este punto.

44 **FSF**: Del ingles, Free Software Foundation, es una organización creada por Richard Stallman en 1985 con el fin de promover el “Software Libre”.

3. La libertad de redistribuir copias.
4. La libertad de distribuir copias de sus versiones modificadas a terceros. Esto permite que toda la comunidad pueda beneficiarse de estas modificaciones. El acceso al código fuente también es una condición necesaria para ello.

4.1.2 Código Abierto

El *"Código Abierto"* es un modelo de desarrollo de software basado en las ventajas de proveer acceso al código fuente del producto. La definición formal OSD[45] [OPENSOURCE2007] establece un criterio de diez puntos para que un software sea considerado de "Código Abierto", ellos son:

1. Libre distribución.
2. Acceso al código fuente.
3. Autorización para trabajos derivados.
4. Mantener la integridad del código del autor.
5. No discriminar personas o grupos.
6. No discriminar al área que los utiliza, por ejemplo no excluir el uso comercial.
7. Distribuir la licencia.
8. La licencia no debe ser especifica a un producto.
9. La licencia no debe restringir a otro software.
10. La licencia debe ser neutral en términos tecnológicos.

El articulo *"Por qué el «código abierto» pierde de vista lo esencial del software libre"[STALLMANCA2020]* explica que si bien estos puntos pueden estar alineados con las cuatro libertades planteadas por el software libre, también pueden contener limitaciones o condiciones que lo excluyan de tal condición. Por ejemplo, podría no permitir el uso de versiones modificadas para su uso privado, como es el caso de Open Watcom[46]. Otra práctica limitante es la denominada *"tivoización"* donde un dispositivo solo ejecuta programas con una firma digital especifica por lo que si bien el usuario dispone de la

45 **OSD**: Del ingles, Open Source Definition

46 **Open Watcom**: Es un IDE (Entorno integrado de desarrollo) comercial para lenguajes C,C++ y Fortran.

libertad de acceder al código y modificarlo para crear nuevos programas jamas podrá ejecutar dichas versiones, podemos encontrar ejemplos puntuales en la plataforma Android[47] y en dispositivos Tivo[48], del cual deriva el nombre de la práctica.

4.1.3 Copyleft

Según la FSF el copyleft es un método para que un programa o trabajo sea considerado *"Libre"* garantizando que las versiones modificadas que derivan de este también conserven las características de libertad. La aplicación de este concepto se realiza de la siguiente manera:

> *"Para proteger un programa con copyleft se debe declarar en primer lugar que tiene copyright. Después deben añadirse unas cláusulas de distribución, que son un instrumento legal que otorga a todo el mundo el derecho a utilizar, modificar, y redistribuir el código del programa o de cualquier programa derivado del mismo, pero solo si las condiciones de distribución no se alteran. Así, el código y las libertades se hacen legalmente inseparables."[FSFCL2019]*

4.2 Open Source Hardware Association

Los principios del Software Libre y de Fuente Abierta pueden ser llevados al campo del desarrollo de hardware en sus diferentes niveles, desde componentes hasta circuitos y accesorios físicos (conectores, gabinetes, soportes, etc) para la construcción de dispositivos tecnológicos.

De aquí surge la definición de *"Hardware de Fuentes Abiertas"[OSHW2010]*, que persigue los siguientes principios:

> *"Hardware de Fuentes Abiertas (OSHW en inglés) es aquel hardware cuyo diseño se hace disponible públicamente para que cualquier persona lo pueda estudiar, modificar, distribuir, materializar y vender, tanto el original como otros objetos basados en ese diseño. Las fuentes del hardware (entendidas como los*

47 **Android:** Sistema operativo para dispositivos móviles basado con un núcleo Linux modificado, el mismo es desarrollado por el consorcio Open Handset Alliance.

48 **TiVo:** es un grabador de video digital desarrollado y comercializado por Xperi a partir de 1999.

ficheros fuente) habrán de estar disponibles en un formato apropiado para poder realizar modificaciones sobre ellas. Idealmente, el hardware de fuentes abiertas utiliza componentes y materiales de alta disponibilidad, procesos estandarizados, infraestructuras abiertas, contenidos sin restricciones, y herramientas de fuentes abiertas de cara a maximizar la habilidad de los individuos para materializar y usar el hardware. El hardware de fuentes abiertas da libertad de controlar la tecnología y al mismo tiempo compartir conocimientos y estimular la comercialización por medio del intercambio abierto de diseños."

Esta misma definición se encuentra alineada con los principios del software de fuentes o código abierto y se extiende sobre los siguientes criterios:

- Documentación
- Alcance
- Programas informáticos necesarios
- Obras derivadas
- Libre redistribución
- Atribución
- No discriminación a personas o grupos
- No discriminación a campos de aplicación
- Distribución de la licencia
- La licencia no sera especifica a un producto
- La licencia no deberá restringir otro Hardware o Software
- La licencia será neutra en términos tecnológicos

En base a los intereses de esta definición se ha conformado una organización llamada *"Open Source Hardware Association"* que tiene por objetivo fomentar el conocimiento tecnológico facilitando el acceso a la investigación y la colaboración respetando la libertad del usuario.

Sus principales actividades incluyen la organización de la cumbre anual de hardware abierto y el mantenimiento de la certificación de hardware de código abierto, que permite a la comunidad identificar y presentar rápidamente el hardware que cumple con la definición comunitaria de hardware de código abierto. Dentro de sus actividades se encuentran las siguientes:

- Organizar conferencias y eventos de la comunidad de OSHW.
- Educar al público en general sobre el hardware de código abierto y los beneficios sociales de su uso.
- Organizar el movimiento de hardware de código abierto en torno a los valores y principios compartidos.
- Recopilar, compilar y publicar datos sobre el movimiento de hardware de código abierto.
- Proporcionan una manera simple y práctica para que los creadores indiquen que sus productos cumplen con un estándar de código abierto.

4.3 Ejemplos de hardware de fuente abierta

Existen numerosos ejemplos de hardware de fuentes abiertas de diversa complejidad, muchos de ellos se encuentran listados en la lista de dispositivos certificados de OSHWA[49] [OSHWALIST], algunos de ellos serán descriptos en las próximas secciones.

4.3.1 Arduino

Arduino es una empresa de origen italiano avocada al desarrollo de hardware y software libre. La empresa diseña y fabrica placas electrónicas basadas en microcontroladores de la empresa ATMEL, microprocesadores ARM Cortex e Intel Quarx, sus productos se distribuyen con las licencias de fuentes abiertas “Creative Commons Attribution Share-Alike”, GPL[50] o LGPL[51].

49 **OSHWA:** del ingles, Open Source Hardware Association.

50 **GPL**: acrónimo de “Licencia Publica General” , la misma fue definida por la Free Software Foundation.

51 **LGPL**: acrónimo de “Licencia Publica General Reducida” , la misma fue definida por la Free Software Foundation.

El proyecto que dio lugar a la creación del primer producto de Arduino se llamo Wiring y data del año 2003. Este proyecto desarrollado en el “Interaction Design Institute Ivrea” de Italia buscaba crear una placa electrónica de prototipado de bajo costo y fácil producción para permitir a estudiantes y profesionales crear dispositivos con capacidad de interactuar con el entorno mediante actuadores y sensores. Pocos años después, en el 2005, se comenzaría a comercializar el primer modelo basado en el microcontrolador AVR ATMega8 de la empresa Atmel.

Junto al éxito de su primer producto se incremento el desarrollo del software asociado a estos productos que incluye una IDE[52] y numerosas librerías al mismo tiempo que se amplio la familia de productos con modelos de diverso tamaño y potencia. Actualmente sus productos también incluyen versiones con microprocesadores ARM luego de una alianza del año 2017.

Arduino ha definido las dimensiones de sus productos en función de su tipo, los mas utilizados son:

- Arduino/Genuino 68.6mm x 53.4mm [2.7 in x 2.1in]
- Minima 61.5mm × 25mm [2.4in × 1.0in]
- Mega 101.6mm × 53.3mm [4in x 2.1in]
- Wearable 51mm ⌀ [2 in ⌀]
- Mini 17.8mm × 48.3mm [0.7in × 1.9in]

La siguiente tabla muestra algunos de los modelos actualmente fabricados por Arduino y sus características técnicas básicas.

52 **IDE**: acrónimo de “Integrated Development Environment”, o Entorno Integrado de Desarrollo.

Nombre	Procesador		Formato	Interfaz	Alimentación	Memoria			I/O				Año
	Modelo	Mhz			Volt.	Flash (KB)	EEPROM (KB)	SRAM (KB)	Digital I/O (pins)	Digital I/O PWM(pins)	Analog input (pins)	Analog output pins	
Arduino Uno WiFi rev 2	ATMEGA4809, NINA-W132 Wi-Fi module ECC608 (crypto)	16	Arduino	USB	5 V	48	0.25	6	14	5	6	0	2018
Arduino / Genuino MKR1000	ATSAMW25 (SAMD21 Cortex-M0+ 32 bit ARM MCU, WINC1500 2.4 GHz 802.11 b/g/n Wi-Fi, y ECC508 (crypto)	48	Minima	USB	3.3V	256	No	32	8	12	7	1	2016
Arduino MKR Zero	ATSAMD21G18A	48	Minima	USB	3.3V	256	No	32					–
Arduino 101 Genuino 101	Intel® Curie™ module dos nucleos x86 (Quark SE)	32	Arduino	USB	3.3V	196		24	14	4	6		2015
ArduinoZero	ATSAMD21G18A	48	Arduino	USB	3.3V	256	0 to 16 Kb emulation	32	14	12	6	1	2015
Arduino Due	ATSAM3X8E(Cortex-M3)	84	Mega	USB	3.3V	512	0	96	54	12	12	2	2012
Arduino Yún	Atmega32U4, Atheros AR9331	16,400	Arduino	USB	5V	32 KB, 16 MB	1 KB, 0 KB	2.5 KB, 64 MB	14	6	12		2013
Arduino Leonardo	Atmega32U4	16	Arduino	USB	5V	32	1	2.5	20	7	12		2012
Arduino Uno	ATmega328P	16	Arduino	USB	5V	32	1	2	14	6	6		2010
Arduino Mega2560	ATmega2560	16	Mega	USB	5V	256	4	8	54	15	16		2010
Arduino Ethernet	ATmega328	16	Arduino	Ethernet Serial	5V	32	1	2	14	4	6		2011
Arduino Fio	ATmega328P	8	Minima	Xbee Serial	3.3V	32	1	2	14	6	8		2010
Arduino Nano	ATmega328 (ATmega168 v3.0)	16	Minima	USB	5V	16/32	0.5/1	1/2	14	6	8		2008
LilyPad Arduino	ATmega168V o ATmega328V	8	Wearable		2.7-5.5V	16	0.5	1	14	6	6		2007
Arduino Pro	ATmega168 o ATmega328	16	Arduino	UART Serial, I2C(TWI), SPI	5V or 3.3V	16/32	0.5/1	1/2	14	6	6		–
Arduino Mega ADK	ATmega2560	16	Mega	USB	5V	256	4	8	54	14	16		2011
Arduino Esplora	Atmega32U4	16			5V	32	1	2.5					2012
Arduino Micro	ATmega32U4	16	Mini		5V	32	1	2.5	20	7	12		2012
Arduino Pro Mini	ATmega328P	8 (3.3V) /16 (5V)	Mini	Six-pin serial header	3.3V / 5V	32	1	2	14	6	6		–

Tabla 6: Modelos de dispositivos Arduino

4.3.2 BeagleBone

La Fundación BeagleBoard.org es una corporación sin fines de lucro radicada en Michigan, Estados Unidos. Se encarga de brindar educación y colaboración para el diseño y uso de software y hardware de código abierto en la informática integrada. Proporciona un foro para que los propietarios y desarrolladores de software y hardware de código abierto intercambien ideas, conocimientos y experiencias. La comunidad BeagleBoard.org colabora en el desarrollo de soluciones informáticas físicas de código abierto que incluyen robótica, herramientas de fabricación personal como impresoras 3D y cortadoras láser, y otros tipos de controles industriales y de máquinas. Sus diseños son de código abierto y los componentes están disponibles para que cualquiera pueda fabricar hardware compatible, todos estos dispositivos son compatibles con Linux y los lenguajes de programación disponibles es este sistema operativo.

A continuación se muestran los modelos actualmente comercializados y sus características técnicas:

Modelos	**PocketBeagle**	**BeagleBone Black**	**BeagleBone Blue**	**BeagleBone AI**
Procesador	AM3358 ARM Cortex-A8	AM3358 ARM Cortex-A8	AM3358 ARM Cortex-A8	AM5729 2x ARM Cortex-A15
Velocidad Máxima del Microprocesador	1GHz	1GHz	1GHz	1.5GHz
Co-procesadores	2x200-MHz PRUs, ARM Cortex-M3, SGX PowerVR	2x200-MHz PRUs, ARM Cortex-M3, SGX PowerVR	2x200-MHz PRUs, ARM Cortex-M3, SGX PowerVR	4x200-MHz PRUs, 2x ARM Cortex-M4, 2x SGX PowerVR, 2x HD video
Pines análogos	2 (3.3V), 6 (1.8V)	7 (1.8V)	4 (1.8V)	7 (3.3V)
Pines digitales	44 (3.3V)	65 (3.3V)	24 (3.3V)	72 (3.3V) (7 Compartidos con los

				análogos)
Memoria	512MB DDR3 (800MHz x 16), microSD card slot	512MB DDR3 (800MHz x 16), 4GB on-board storage using eMMC, microSD card slot	512MB DDR3 (800MHz x 16), 4GB on-board storage using eMMC, microSD card slot	1GB DDR3 (2x 512Mx16, dual-channel), 16GB on-board storage using eMMC, microSD card slot
USB	USB 2.0 480Mbps Host/Client Port, USB 2.0 on expansion header	USB 2.0 480Mbps Host/ Client Port, USB 2.0 Host Port	USB 2.0 480Mbps Host/Client Port, USB 2.0 Host Port	USB 3.0 5Gbps Host/Client Port, USB 2.0 Host Port
Interfaces de Red	add-ons	10/100 Ethernet	2.4GHz WiFi, Bluetooth, BLE	Gigabit Ethernet, 2.4/5GHz WiFi, Bluetooth, BLE
Video	SPI displays	microHDMI, cape add-ons	SPI displays	microHDMI, cape add-ons
Audio	add-ons	microHDMI, cape add-ons	add-ons, Bluetooth	microHDMI, Bluetooth, cape add-ons

Interfaces de Expansión Soportadas	3x UART, 4x PWM, 2x SPI, 2x I2C, 8x A/D converter, 2x CAN bus (w/o PHY), 2x quadrature encoder, USB	4x UART, 12x PWM/Timers, 2x SPI, 2x I2C, 7x A/D converter, 2x CAN bus (w/o PHY), LCD, 3x quadrature encoder, SD/MMC, GPMC	4x UART, 2-cell LiPo, 2x SPI, I2C, 4x A/D converter, CAN bus (w/ PHY), 8x 6V servo motor, 4x DC motor, 4x quadrature encoder	4x UART, 12x PWM/Timers, 2x SPI, 2x I2C, 7x A/D converter, CAN bus (w/o PHY), LCD, 3x quadrature encoder, SD/MMC
Sensores "On-board"	-	-	10 degree of freedom IMU (accelerometer, gyroscope, magnetometer, thermometer), barometer/thermometer	on-die temperature

Tabla 7: Características de dispositivos BeagleBone

4.4 FPGA

Es un dispositivo electrónico encapsulado programable compuesto por bloques cuya función e interconexión es configurable permitiendo definir diversos comportamientos en los mismos mediante el uso de un lenguaje de descripción de hardware o HDL[53] como VHDL[54], Verilog[55] o ABEL[56].

53 **HDL**: del ingles, Hardware Definition Language, o lenguaje de definición de hardware.

54 **VHDL**: lenguaje HDL especificado por la ANSI/IEEE 1076-1993.

55 **Verilog**: es un lenguaje HDL con ciertas similitudes con el lenguaje C, fue creado por Phil Moorby en 1985 para la empresa Automated Integrated Design Systems.

56 **ABEL**: acrónimo, del ingles, Advanced Boolean Expression Language, es un lenguaje HDL desarrollado por Data I/O Corporation.

Su nombre deriva del acrónimo ingles *"Field programable gate array"* cuya traducción corresponde a *"Campo de matrices de puertas lógicas programable"*, como su nombre lo indica estas puertas lógicas pueden configurarse en base una definición programada para hacer que el dispositivo cumpla diferentes tareas como podría hacerlo un circuito integrado de tipo ASIC[57]. Según su tecnología pueden ser de configuración volátil o de configuración persistente, en este ultimo caso se sub-clasifican en re-programables y de programación única.

En términos generales los FPGAs al igual que otros tipos de integrados se componen de tres tipos elementos:

- **Puertas lógicas** para la manipulación de bits.
- **Biestables** para el almacenamiento de bits.
- **Cables** o **enlaces** para transporte de bits.

En el caso particular de los FPGAs se pueden programar los cables o enlaces, a modo de habilitarlos o no, y de esta forma relacionar bloques de lógica, entradas y salidas para obtener el comportamiento deseado.

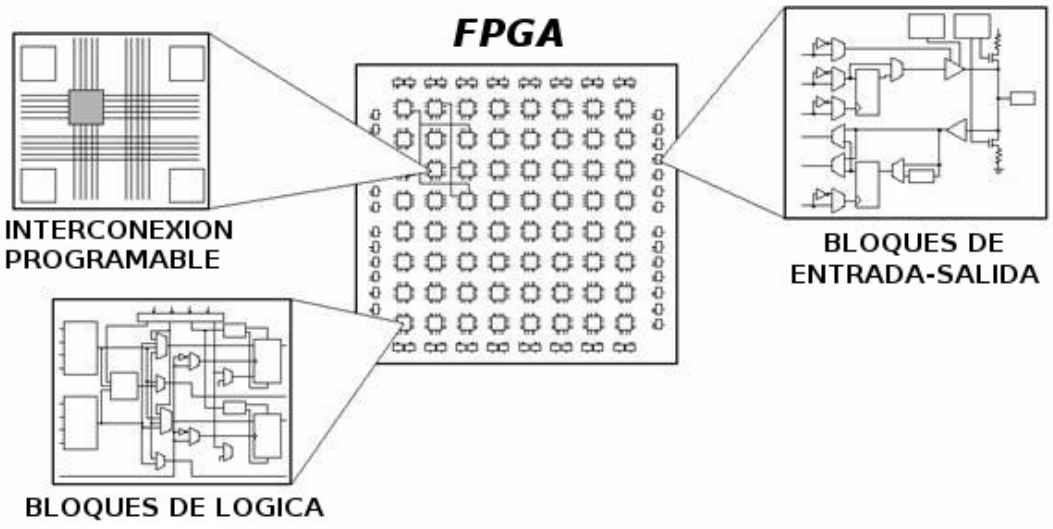


Imagen 14: Esquema de componentes de un FPGA

57 **ASIC**: del ingles, application-specific integrated circuit, significa circuito integrado de aplicación especifica.

Esta configuración da lugar a un flujo de trabajo que nace con el diseño para luego de pasar por su definición en un HDL poder llevarlo al dispositivo físico. La siguiente imagen del proyecto *"FPGA Wars"* muestra este concepto de trabajo:

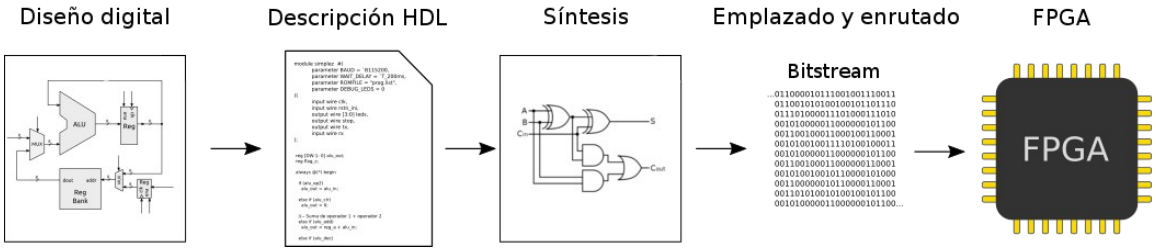


Imagen 15: Flujo de trabajo para la configuración de un FPGA

Este proceso depende de herramientas que permiten transformar la definición de HDL en las instrucciones de "*bitstream*" indicadas para que el dispositivo pueda configurarse correctamente, si bien esta tecnología con los detalles técnicos de cada modelo es cerrada en el año 2015 Clifford Wolf logró por ingeniería inversa de FPGAs Lattice iCE40 crear y liberar un conjunto de herramientas que posibilitan pasar definiciones de Verilog a *"bitstream"* para este modelo y derivados, en base a esto se creo el proyecto IceStorm[58].

Es importante identificar que tienen ventajas frente a los ASIC ya que son reprogramables, de reducido costo y tiempo para el desarrollo, y su producción es mas rápida y económica. Al mismo tiempo estas características se ven contrastadas por su menor desempeño, mayor consumo y limitaciones para la implementación de sistemas de alta complejidad.

En la actualidad existen varios productores de dispositivos FPGA como Atmel, Altera, AMD, Motorola y la empresa Xilinx quien fuera la pionera en la comercialización de esta tecnología con el modelo XC2064 de 1985.

4.5 Microprocesadores de fuente abierta

Como se indico previamente los conceptos del Software Libre y de Fuentes o Código Abierto pueden aplicarse al hardware inclusive en dispositivos electrónicos complejos

58 **Proyecto IceStorm**: Proyecto de ingeniería reversa de FPGAs iCE40, con sitio web en http://www.clifford.at/icestorm .

como son los microprocesadores, por lo que particularmente podemos encontrar iniciativas que buscan distribuir diseños para microprocesadores entre otros de ellos. A continuación se enuncian algunos ejemplos.

4.5.1 Risc-V

Risc-V es un conjunto de instrucciones ISA[59] con diseño RISC creado como hardware libre, el mismo es abierto y de distribución gratuita para que pueda ser implementado sin abonar regalías ni sufrir limitaciones en cuanto a su propósito o ámbito de aplicación.

Este proyecto esta impulsado por la “RISC-V Foundation”[60] una corporación sin fines de lucro cuyos miembros participan del desarrollo de las especificaciones del RISV-V ISA y el ecosistema de hardware y software vinculado al mismo. El proyecto original tuvo su origen el la Universidad de California en Berkeley durante el año 2010, pero la actual “RISC-V Foundation” se fundo años después durante el 2015. Un dato interesante es que cuenta con mas de trescientos miembros y su directorio incorpora representantes de Bluespec Inc., Google, Microsemi, NVIDIA, NXP, la Universidad de California y Western Digital.

El conjunto de instrucciones RISC-V, con diseño modular, consta de partes base y extensiones; el mismo ha sido desarrollado con un enfoque practico, extensible y características para el desarrollo de velocidad con bajo consumo de energía y reducidos costos. También es interesante citar que el diseño permite manejar datos de 32, 64 y 128 bits mas una variedad de sus subconjuntos permitiendo su implementación tanto para pequeños integrados como para super-computadoras. Otro aspecto a destacar es que aun no se ha desarrollado el set de 128 bits ya que el mismo se reserva para las necesidades y capacidades futuras a fin de evitar una anticipada obsolescencia. El siguiente cuadro lista los conjuntos de instrucciones de RISC-V con su denominación:

---

59 **ISA**: del ingles, “Instruction Set Architecture”, corresponde a la arquitectura de un conjunto de instrucciones de procesamiento.

60 **RISC-V Foundation**: Corporación sin fin de lucro para el desarrollo de RISV-V. Su sitio en internet es https://riscv.org/

Nombre	Descripción
Base	
RV32I	Instrucción de Entero de la base Puso, 32-bits
RV32E	Conjunto de instrucciones de base entera(embebido), 32-bits, 16 registros
RV64I	Conjunto de instrucciones de base entera, 64-bits
RV128I	Conjunto de instrucciones de base entera, 128-bits
Extensión	
M	Extensión estándar para Multiplicación de Entero y División
Un	Extensión estándar para Instrucciones Atómicas
F	Extensión estándar para punto flotante de precisión simple
D	Extensión estándar para punto flotante de precisión doble
G	Abreviatura para la base y extensiones anteriores
Q	Extensión estándar para punto flotante de precisión cuádruple
L	Extensión estándar para punto flotante decimal
C	Extensión estándar para instrucciones comprimidas
B	Extensión estándar para manipulación de bits
J	Extensión estándar para lenguajes traducidos dinámicamente
T	Extensión estándar para Memoria Transaccional
P	Extensión estándar para Empaquetado-SIMD Instrucciones
V	Extensión estándar para Operaciones de Vector
N	Extensión estándar para interrupciones de nivel de usuario

Tabla 8: Conjuntos de instrucciones de RISC-V

En la actualidad la especificación es lo suficientemente madura para permitir que existan desarrollos tanto para educación, investigación y comercialización. Un caso de referencia es la empresa SiFive que comercializa núcleos de 32 y 64 bits con arquitectura RISC-V, distribuidos en diferentes series y modelos según la necesidad; la serie 7 para alto rendimiento, series 3/5 para eficiencia y la serie 2 con consumo optimizado. Cada una de estas series presenta modelos en base a los siguientes conjuntos

- Tipo E, de núcleos embebidos de 32 bits para IA[61] e IoT[62].
- Tipo S, núcleos embebidos de 64 bits para almacenamiento y *"machine learning"*[63].

61 **IA**: Acrónimo de inteligencia artificial.

62 **IoT**: Acrónimo; del ingles, "Internet of Things", cuyo significado es "Internet de las cosas" y se vincula a equipos electrónicos usualmente con sensores y controles físicos inter-conectados vía internet.

63 **Machine learning**: del ingles, Aprendizaje de maquina.

- Tipo U, procesadores de 64 bits para ejecución de Linux, tareas de centros de datos, redes, etc.

Existen muchos otros casos de éxito en el ámbito comercial que no abordare en detalle como CloudBear[64], UltraSoc[65], Syntacore[66], Andes Technology[67]entre otros.

4.5.2 OpenRISC

Es un diseño de procesador basado en arquitectura RISC cuya especificación fue liberada y publicada bajo licencia LGPL. Este diseño se implemento en el lenguaje Verilog[68] logrando que se fabricara con éxito sobre dispositivos FPGA[69] y como circuitos integrados ASIC. Este proyecto persigue proveer lo siguiente:

- Un set de instrucciones de arquitectura RISC con características DSP[70] libre y de fuente abierta.
- Un conjunto de implementación de esta arquitectura de acceso libre y código fuente abierto.
- Un conjunto completo, libre y de código fuente abierto de herramientas de desarrollo, librerías y aplicaciones.
- Una variedad de “system-on-chip”[71] y simuladores de sistema para estos núcleos.

64 **CloudBear**: Empresa de desarrollo de procesadores con sitio oficial en https://cloudbear.ru .

65 **UltraSoc**: Empresa de desarrollo de hardware orientado a cyberseguridad con sitio oficial en https://www.ultrasoc.com .

66 **Syntacore**: Empresa de desarrollo de procesadores con sitio oficial en https://syntacore.com .

67 **Andes Technology**: Empresa de desarrollo de procesadores de 32 bits con bajo consumo con sitio oficial en https://www.andestech.com .

68 **Verilog:** lenguaje de descripción de hardware para el modelado de sistemas electrónicos.

69 **FPGA**: del ingles, “Field-programmable gate array”, o Campo de matrices de puertas lógicas programable. Es un dispositivo electrónico que puede programarse median lenguajes de descripción de hardware.

70 **DSP**: del ingles, Data Signal Processing, significa procesamiento de señales digitales.

71 **System-on-chip**: se utiliza para referenciar a un sistema montado en un único circuito integrado.

El diseño de OpenRISC[72] fue originalmente elaborado por la comunidad de OpenCores[73], esta es una organización enfocada a facilitar y promover el desarrollo de núcleos o procesadores siguiendo los lineamientos de Fuente Abierta para hardware. Para tal fin provee un portal para listar, presentar y gestionar proyectos de este tipo junto a las herramientas para acceder, administrar y distribuir el código fuente resultante.

4.5.3 J-core

Este proyecto ha desarrollado un procesador con diseño “system-on-chip” para el set de instrucciones SuperH[74] denominado J2, el mismo se encuentra implementado en VHDL[75] y disponible bajo licencia BSD, libre y de fuente abierta.

El procesador SuperH, junto con su set de instrucciones, fue desarrollado en Japón a fines de los años noventa por la compañía Hitachi, presentando un modelo de arquitectura híbrida basada en RISC pero utilizando micro-código para permitir a algunas instrucciones ejecutar múltiples ciclos de trabajo, hecho no común en la arquitectura de referencia donde las instrucciones suelen usar solo un ciclo. Muchas de patentes de la arquitectura SuperH expiraron en el año 2015 facilitando la re-implementación del procesador original denominado J2 bajo el modelo de hardware abierto y utilizando el nombre de J2.

El diseño del J2 de J-core puede ser implementado sobra placas FPGA, como Numato Mimas v2[76] o Avnet Microboard[77] basadas en Spartan-6[78], brindando capacidad para ejecutar un sistema operativo de núcleo Linux.

72 **OpenRISC:** Proyecto para el desarrollo de un procesador libre. Su sitio en internet es https://openrisc.io

73 OpenCores: Comunidad de desarrollo de hardware abierto orientada a proyectos de procesadores. Su sitio en internet es https://opencores.org

74 **SuperH**: Procesador RISC de 32 bits desarrollado por Hitachi Ltd.

75 **VHDL**: del ingles, Virtual Hardware Definition Language, significa lenguaje de definición virtual de hardware.

76 **Numato Mimas v2**: Es una placa de desarrollo que utiliza el FPGA Xilinx Spartan-6.

77 **Avnet Microboard**: Es una placa de desarrollo que utiliza el FPGA Xilinx Spartan-6.

78 **Spartan-6**: Es una familia de integrados FPGA de la empresa Xilinx construidos con tecnología de 45nm. Esta familia dispone de modelos compuestos por una cantidad de 3800 a 75000 celdas lógicas, su producción y disponibilidad esta planificada hasta al menos el año 2027.

4.6 Open Titan

En el año 2019 la empresa Google promovió la creación del proyecto OpenTitan[79], que reúne a otras grandes empresas como Lowrisc, Western Digital y otras, para el diseño y desarrollo transparente, confiable y seguro de dispositivos Root of Trust (ROT)[80] para el uso empresarial, de proveedores de plataformas y fabricantes de circuitos integrados. Algunos de las características definidas como objetivos de este proyecto son:

- Gestión independientemente
- De fuentes libres
- Seguridad a través de la transparencia
- Propiedad intelectual de alta calidad
- Arquitectura moderna
- Independencia de proveedor y plataforma

El proyecto define objetivos, requerimientos para el RoT, definiciones, practicas y características del software y hardware a utilizar, entre otros activos. El código del proyecto contiene múltiples diseños de alto nivel para sintetizarse o compilarse en diferentes objetivos como FPGAs, ASICs o herramientas de simulación.

Si bien este proyecto aun esta en una etapa temprana, el interés de este trabajo en su existencia es evidenciar la inquietud que tienen las empresas en la confiabilidad del hardware que les genera la necesidad de buscar alternativas mas transparentes en independientes como esta.

79 **OpenTitan**: Proyecto para el diseño e implementación de un RoT, con sitio disponible en https://opentitan.org .

80 **RoT**: del ingles, Root of Trust, significa Raiz de Confianza y corresponde a componentes criptográficos de confianza de un sistema, usualmente vinculados a HSM (Hardware Security Modules) para el manejo contraseñas y firmas.

5 Vulnerabilidades de hardware

Este capitulo aborda diferentes trabajos académicos o presentados en reconocidos congresos del ámbito de la seguridad informática que han demostrado en forma teórica y práctica ataques a la seguridad de un sistema informático mediante vulnerabilidades de su hardware. Estos trabajos se describen en esta tesis con el propósito de dar a conocer el estado del arte y la factibilidad técnica de este tipo de amenazas.

5.1 Mac EFI Rootkits, Loukas K (snare)

Los siguientes párrafos se basan en el trabajo de Loukas K titulado “DE MYSTERIIS DOM JOBSIVS, Mac EFI Rootkits”[LOUKAS2012] presentado en el evento de Black Hat USA 2012. Este documento expone los riesgos de la existencia de software malicioso que puede afectar a una computadora infectando su sistema de arranque previamente a la carga del sistema operativo y en algunos casos persistiendo la amenaza en integrados de memoria del hardware del sistema central en lugar de los dispositivos de almacenamiento del equipo.

Si bien este documento hace foco en sistemas Mac toma referencias históricas de casos que también involucraron a computadoras de tipo PC, citando virus que infectaban el MBR para pasar a casos mas complejos como CIH/Chernobyl (que inutilizaba el equipo corrompiendo su BIOS[81]), o pruebas conceptuales como IceLord y Rakshasa que podían almacenar el código malicioso en el mismo BIOS para persistir en el sistema y alterar el proceso de inicio convencional, de esta forma podían mantenerse activos aun luego de que se reinstalaran los sistemas o se reemplazaran sus dispositivos de almacenamiento.

Este trabajo ha sido seleccionado para ser incluido en este capitulo debido a que no solo se extiende en la teoría sino que abarca demostraciones de prueba de concepto sobre el tema tratado, y esto fue elaborado sobre la referencia de su autor a otros documentos y presentaciones que expusieron conocimiento sobre la tecnología y técnicas utilizadas, particularmente su autor cita a los siguientes trabajos:

81 **BIOS**: acrónimo del ingles “Basic Input-Output System”, cuyo significado es “Sistema Básico de Entrada-Salida” y corresponde al programa interfaz entre el firmware y el sistema operativo que se inicia al encender una computadora.

- “Implementing and Detecting a PCI Rootkit” de John Heasman fue presentado en el evento BlackHat del año 2007. Este trabajo se basa en la capacidad de persistir un código RootKit[82] en el BIOS mediante ACPI[83].

- “Persistent BIOS Infection” de Anibal L. Sacco y Alfredo A. Ortega, el mismo fue presentado en la conferencia CanSecWest del año 2009. Su contenido se enfoca en el sistema BIOS, cubriendo desde su historia, estructura de funcionamiento y particularidades técnicas de su proceso de actualización o flashing enfocado en la infección con persistencia en el este.

- “Attacking Intel® BIOS” fue elaborado por Rafal Wojtczuk y Alexander Tereshkin para Invisble Thing Labs, el mismo se presentó en el evento BlackHat USA del año 2009. En este caso se estudia un ataque particular a un BIOS Intel, sobrecargando procesos de la carga de imagen del inicio del equipo permitiendo saltar protecciones criptográficas del proceso de escritura del del BIOS para completar una persistencia del código malicioso.

- “Hardware Backdooring is practical” de Jonathan Brossard, presentado en el evento de BlackHat 2012. Debido a que dentro de este mismo capitulo se abordará en detalle este trabajo me limitaré a indicar que este trabajo demostró que es posible y práctico implementar una puerta trasera permanente a nivel de hardware, la prueba de concepto se conoció con el nombre de Rakshasa[84].

Para poder abordar este trabajo se debe tener en claro que el denominado BIOS data de mediados de 1970, el mismo define la interfaz de firmware[85] que se ejecuta al encender una computadora. Es el BIOS el que permitía que la computadora pueda revisar sus componentes críticos al iniciar, gestionar el inicio de un sistema operativo desde los periféricos de almacenamiento y proveer una capa de abstracción para la interacción con

82 **Rootkit:** herramienta de código malicioso con características de diseño que le brindan capacidades para permanecer oculto en un sistema.

83 **ACPI**: acrónimo del ingles “Advanced Configuration and Power Interface”, o Interfaz Avanzada de Configuración y Poder.

84 **Rakshasa**: su significado corresponde a un tipo de demonio humanoide presente en la mitología Hindú y Budista.

85 **Firmware**: también denominado “soporte lógico inalterable” corresponde al programa de mas bajo nivel que controla el hardware.

los dispositivos de hardware. Luego de mas de dos décadas de uso, en el año 1998, la compañía Intel procedió a trabajar en el diseño de un reemplazo para el BIOS que brindara una solución a las diversas limitaciones que este presentaba, de esta iniciativa surgiría EFI[86], que posteriormente y bajo el control del Consorcio Unificado de EFI, creado en el año 2015, daría lugar al actual estándar de UEFI[87].

La siguiente lista muestra algunas de las principales características de UEFI:

- Soporte de ejecución en 32 y 64 bits.
- Soporte del estándar GPT[88] o *"Tabla de particiones GUID"*.
- Compatibilidad y emulación del antiguo sistema BIOS.
- Independiente de la arquitectura y controladores de la CPU.
- Diseño modular.
- Controladores disponibles en **UEFI Byte Code**, independientes del microprocesador.
- Entorno amigable y flexible Pre-Sistema Operativo.
- Extensiones incorporadas desde dispositivos no volátiles conectados.
- Soporte de ACPI[89].
- Soporte de SMBIOS[90]

A diferencia del antiguo BIOS la especificación de UEFI ha sido diseñada para permitir la extensión del firmware cargando imágenes de aplicaciones y controladores UEFI, de esta

86 **EFI**: acrónimo del ingles "Extensible Firmware Interface", es una interfaz firmware-sistema propietaria desarrollada por Intel en el año 2002 para reemplazar al BIOS.

87 **UEFI**: acrónimo del ingles "Unified Extensible Firmware Interface", es una especificación estándar de interfaz firmware-sistema basado en EFI.

88 **GPT**: acrónimo del ingles "GUID Partition Table", es un estándar para la escritura de tablas de particiones de datos en medios de almacenamiento basado en el modelo de LBA (Logical Block Addressing) con compatibilidad con BIOS MBR y capacidad de registro para 128 particiones por unidad.

89 **ACPI**: acronimo del ingles "Advanced Configuration Power Interface", cuyo significado es Interfaz Avanzada de Configuración y Energía.

90 **SMBIOS**: significa "System Management BIOS", es una especificación de estructuras de datos y métodos para acceder a la información del BIOS de una computadora, la misma data de 1999.

forma estos componentes externos también pueden acceder al los servicios de inicio y tiempo de ejecución. El siguiente gráfico, perteneciente a la especificación, muestra la secuencia de inicio convencional y la relación entre el gestor de inicio y los binarios UEFI durante este proceso.

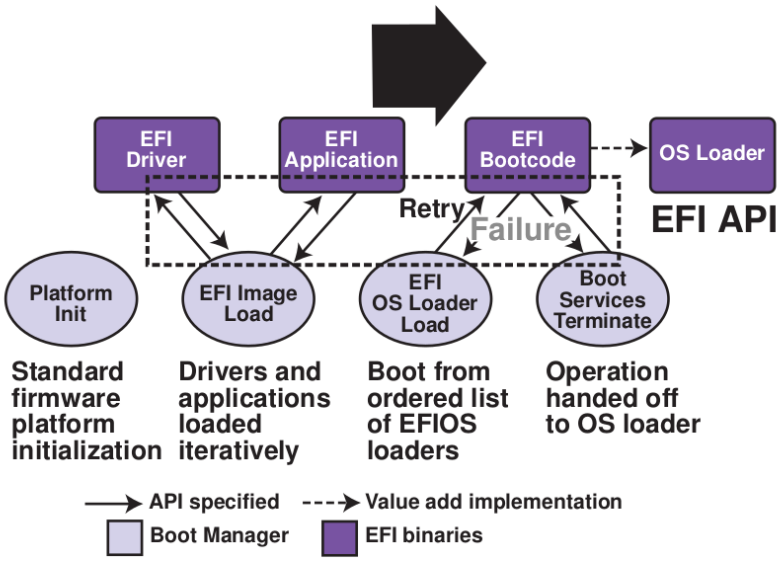


Imagen 16: Secuencia de inicio UEFI

Esta breve introducción a las capacidades de ejecución de lógica en el proceso de inicio UEFI requiere un mínimo conocimiento de la arquitectura de parte de ella. Esta arquitectura consta de siete áreas como indica el siguiente grafico extraído de la especificación de la plataforma inicialización de UEFI:

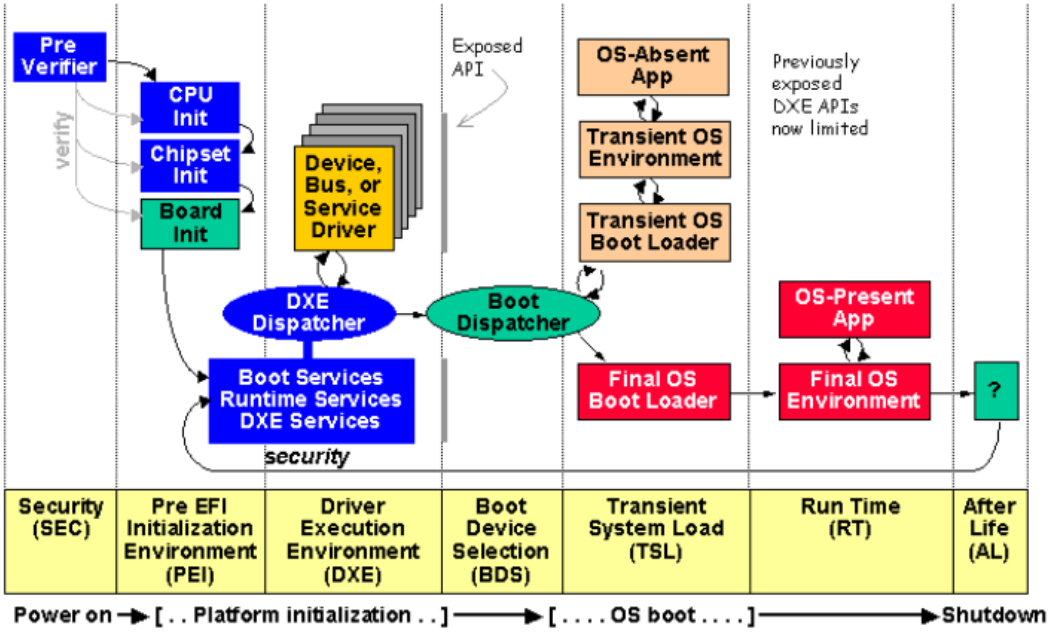


Imagen 17: Fases de la Arquitectura de Firmware de la Plataforma de Inicialización UEFI

A continuación se resume la función de cada una de estas etapas o fases:

- Security (SEC): La etapa de *"Seguridad"* consta de un reducido conjunto de ordenes y se encarga de verificar los recursos para el inicio del equipo.
- Pre-EFI Initialization Environment (PEI): En la etapa de *"Pre-inicializacion del entorno EFI"* se inician los principales recursos de hardware del equipo para posteriormente proceder a la ejecución de servicios EFI (de arranque, tiempo de ejecución, de controladores...) disponiendo de dichos recursos críticos.
- Driver Execution Environment (DXE): En la etapa del *"Entorno de ejecución de controladores"* se completa la inicialización de servicios y se cargan los controladores EFI desde sus diferentes orígenes.
- Boot Device Selection (BDS): La etapa de *"Selección de dispositivo de arranque"* se selecciona el dispositivo que contiene el "boot loader" o "cargador de arranque" del sistema operativo a utilizar.

- Transient System Load (TSL): En la etapa de “Carga transitoria del sistema” se procede a intentar ejecutar el “boot loader” o “cargador de arranque” seleccionado en la etapa previo o los componentes alternativos.
- Run Time (RT): La etapa de “Tiempo de ejecución” corresponde a la actividad del sistema operativo y sus aplicaciones.
- After Life (AL): En la etapa de “Luego de la vida”, corresponde a la transición del control del sistema operativo al firmware para la gestión del fin de la actividad en el sistema.

Aclarados estos conceptos se puede proceder a abordar los principales puntos del trabajo “DE MYSTERIIS DOM JOBSIVS, Mac EFI Rootkits”[LOUKAS2012], donde se plantean en forma teórica y con los detalles técnicos correspondientes a cada caso dos ataques factibles para un equipo Apple basado en UEFI, ellos son:

- Ataque a FileVault[91]: El ataque planteado se basa en la implementación de un keylogger[92] que permita capturar la clave de cifrado del disco para posteriormente escribirla en un archivo o transferirla vía red. La forma citada en el trabajo es la implementación del keylogger como un controlador EFI vinculado al protocolo de entrada de texto simple que utilizando la función “ReadKeyStroke” que informa el valor de cada tecla presionada. Dado que la carga de este componente malicioso sería realizada por EFI antes de la selección y ejecución del arranque, al momento que la lógica de FileVault solicite la contraseña del cifrado del disco al usuario el keylogger en cuestión estaría ejecutándose y podría capturar el valor de la misma para posteriormente comunicarla al atacante.
- Parcheo del Nucleo del sistema operativo: En este caso el objetivo es alterar el núcleo del sistema operativo a cargarse en el sistema utilizando en controlador EFI para concretar esta alteración. Al igual que en el caso anterior se toma ventaja de la capacidad de poder disponer del código malicioso en ejecución en una etapa previa del arranque del sistema operativo, con la particularidad que en este escenario se debe realizar la modificación del núcleo cuando este es cargado en memoria por

91 **FileVault**: corresponde a la implementación de cifrado de disco completo de la empresa Apple.

92 **Keylogger**: es un software o hardware que de manera sigilosa registra la actividad de entrada de datos del usuario, usualmente la actividad del teclado.

EFI con el fin de posteriormente ser ejecutado. En el trabajo referenciado se han demostrado los detalles técnicos de implementaciones a modo de prueba de concepto alterando el comportamiento del comando "*kill*".

Ambos casos expuestos se basan en la capacidad de extensión del estándar UEFI para concretar los ataques pero inicialmente no se detalla la manera en que estos controladores UEFI que actúan como vectores del ataque conteniendo la lógica maliciosa logran persistirse para poder estar disponibles en el inicio del sistema. Este punto es aclarado en el trabajo referenciado con tres diferentes opciones:

- Dispositivo de arranque: Dado que la especificación de UEFI define la existencia de una partición llamada ESP[93] al inicio de la tabla de particiones con la finalidad de controladores EFI y cargadores de arranque, se puede alterar los datos ubicados allí. En el caso expuesto en el trabajo referenciado no seria posible ya que la implementación de Apple no utiliza este espacio con esa finalidad, por lo que la alternativa es modificar el "*Mac OS X bootloader*" en el archivo "*boot.efi*" .
- ROM[94] de expansión PCI[95]: Esta opción se denominaba "option-ROM" en el antiguo sistema BIOS, básicamente es la carga de una lógica para ampliar capacidades desde una memoria de tipo ROM montada en un dispositivo, por ejemplo una placa de red o de video. Como se explicó previamente la carga de los controladores EFI es previa a la ejecución del gestor de arranque del sistema operativo por lo que constituye otro punto de persistencia adecuado para introducir el código malicioso. Dado que la especificación de UEFI es amplia en cuanto al soporte de tipos de dispositivo esto podría ocurrir tanto en una placa conectada directamente a la placa madre por PCI o por algún otro dispositivo externo que se conecte a un bus de la placa. Este ultimo es el caso de los dispositivos del puerto

93 **ESP**: acrónimo del ingles. "EFI System Partition", cuyo significado es "Partición del Sistema EFI".

94 **ROM**: acrónimo del ingles, "Read Only Memory", corresponde a "Memoria de Solo Lectura" en este contexto se aplica a memorias físicas de tipo EEPROM o Flash que tienen la particularidad de ser persistentes.

95 **PCI**: acronimo del ingles, "Peripheral Component Interconnect", cuyo significado es "Interconexión de Componentes Periféricos" y corresponde a un tipo de bus o conector para extender las capacidades de la placa principal de una computadora.

Thunderbolt[96] de las computadoras Mac, que mediante este sistema se conectan al bus PCI express, en el trabajo referenciado se utilizó uno de estos dispositivos para la demostración de la prueba de concepto denominada *"evil maid"* donde un controlador malicioso se alojó en un adaptador ExpressCard SATA y en un adaptador de red para alterar el arranque del equipo.

- EFI Firmware Flash: Esta opción corresponde a modificar el código de la implementación EFI para incluir el código malicioso dentro de el, y luego sobre escribir el almacenado en la memoria EEPROM o Flash de la placa madre del equipo.

5.2 Hardware backdooring is practical, Jonathan Brossard

A continuación se explican los principales puntos del trabajo *"Hardware backdooring is practical"*[BROSSARD2012] de Jonathan Brossard. Como fundamentos para dar origen a su trabajo cita diferentes fuentes periodísticas y documentales en referencia a la posibilidad de que un país pudiera disponer de métodos para el espionaje cibernético a nivel internacional, entre ellos el informe *"Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage"*[NORTHROP2012].

En concreto, el trabajo referenciado aborda los aspectos críticos , tanto teóricos como técnicos, asociados a la posibilidad de desarrollar un programa a modo de puerta trasera con características superiores al común de este tipo de desarrollos, para ello este software debía cumplir con los siguientes objetivos:

- Persistencia, aun ante acciones de restauración o recuperación del sistema.
- Características furtivas, evitando alojar código malicioso en el equipo.
- Portabilidad e independencia del sistema operativo.

96 **Thunderbolt**: Es una interfaz de hardware diseñada por Apple e Intel para la conexión de dispositivos externos a una computadora. En sus versiones 1 y 2 el formato físico del conector era Mini Display Port y a partir de la versión 3 es de tipo USB-C.

- Acceso remoto con posibilidad de actualizaciones remotas.
- Disponer de un mecanismo de infección negable y no atribuible.
- Capacidad de cruzar los perímetros de la red.
- Capacidades de redundancia en su operación.
- Características que le permitan no ser detectable por software antivirus.

En base a los puntos descriptos Jonathan Brossard procedió con el diseño de un software para la prueba de concepto que demostrará la factibilidad del planteo de su trabajo, este software fue denominado como Rakshasa[97].

El diseño en cuestión se baso en componentes de fuentes abiertas para facilitar la portabilidad y la reducción del esfuerzo de desarrollo en base a la reutilización de código, su autor estima que este diseño podría ser efectivo con alrededor de 230 modelos de placas principales de computadoras. Al mismo tiempo que se obtenía otra ventaja asociada a uno de los objetivos propuestos, que es la dificultad de detección o identificación del código malicioso. Esto se debe a que gran parte del código de este software malicioso correspondía a software convencional regularmente utilizado en distintos firmware de BIOS reduciendo así la posibilidad de identificar la amenaza y de esta forma también la atribución de un ataque conducido por el mismo. Algunos de estos componentes claves en el diseño son Coreboot, SeaBios y iPXE que le dan la capacidad de escribir la memoria física EEPROM o Flash tanto de la placa principal como de sus dispositivos conectados grabando un nuevo BIOS o ROMs de PCI alterados para su propósito. De forma conexa a la capacidad de poder modificar estos componentes críticos para el inicio del sistema se obtiene la posibilidad de ejecutar payloads[98] o rutinas con fines específicos, como puede ser un versión modificada de Kon-Boot[99], desde ubicaciones remotas ya sea a través de la red convencional o inclusive mediante interfaces de red inalámbricas dando lugar a evitar dispositivos de seguridad perímetrales. La posibilidad de conexión a redes habilita la gestión remota de este software, la posibilidad de actualización y adaptación a cada equipo

97 **Rakshasa**: su significado corresponde a un tipo de demonio humanoide presente en la mitología Hindú y Budista.

98 **Payload**: también denominado “Carga útil”, corresponde a la lógica que realiza la acción principal sobre el sistema objetivo en un malware o software malicioso.

99 **Kon-Boot**: es un software para evitar la comprobación de contraseñas en Windows y MacOS.

objetivo gracias a una librería de componentes de gran tamaño ubicada en un servidor externo y la posibilidad de prescindir de la persistencia del código malicioso en el sistema objetivo ya que el mismo puede obtenerse vía red cuando sea necesario, reduciendo así la evidencia de la infección y la posibilidad de atribución.

Debido a que el hardware de base actual y particularmente los microprocesadores disponen de diversas tecnologías que dificultan el control irrestricto de los recursos del sistema este software malicioso debió deshabilitar muchas características de modo de retrotraer las protecciones del entorno de hardware a las disponibles en la década del 90 y así poder afectar la seguridad de cualquier sistema operativo. Entre estas características que el autor del trabajo logro controlar se encuentran:

- La remoción de micro-código de actualización en el CPU.
- Deshabilitar el ASLR[100].
- Remover las protecciones anti-SMM[101].
- Remover el bit NX (No execution – No ejecutable) que imposibilita la ejecución de ordenes en áreas de memoria de datos.
- Habilitar todos los mapeos como modificables en el ring0[102].
- Bootkiting basado en el payload de Kon-boot.

Una implementación de Rakshasa fue desarrollada en base a los puntos anteriormente descriptos y se exhibió en una demostración a modo de prueba de concepto durante el evento BlackHat de las Vegas del año 2012, en dicha ocasión se inicio una maquina virtual con un BIOS alterado con Rakshasa. Durante esa ejecución se demostró que luego de iniciar el equipo infectado se podían observar en un analizador de tramas de red distintas conexiones mediante las cuales se obtenían de servidores externos los archivos que le

100 **ASLR**: acrónimo del ingles *"Address Space Layout Randomization"*, que significa *"Aleatoriedad de la Disposición del Espacio de Direcciones"*. Es un técnica de gestión de asignación de memoria orientada a la seguridad, la misma tiene por fin dificultar que un atacante salte de manera controlada posiciones de memoria desde una función vulnerable con el fin de ejecutar lógica propia.

101 **SMM**: acrónimo del ingles *"System Management Mode"*, o *"Modo de Gestión del Sistema"* también vinculado a la protección *"Ring-2"*. Es un modo de operación del microprocesador enfocado en la gestión del hardware.

102 **Ring-0**: Nivel de protección de acceso o privilegios asociados al núcleo del sistema, de mayor privilegio en el modelo. Ring-1/2, corresponden a los controladores de dispositivos y Ring-3 a aplicaciones, siendo este ultimo el de menor privilegio.

permitían ejecutar un bootkit que finalmente habilitaba el acceso a todos los usuarios del equipo en modo de administrador. Por cuestiones éticas los autores decidieron no publicar el código de este programa malicioso pero tanto la profundidad de los detalles técnicos sobre la manera en que resolvieron e implementaron los desafíos planteados en el diseño como la demostración de las capacidades de su implementación conceptual sostuvieron su hipótesis de la factibilidad de este tipo de desarrollos y sus capacidades potenciales.

Finalmente cabe destacar que un software malicioso con estas características podría evadir antivirus, la protección que proveen TPMs[103] y cifrados completos de unidades de almacenamiento. Ademas que de lograr identificar algún comportamiento sospechoso que de indicios de una infección las medidas mas drásticas de resolución como la restauración de copias de seguridad, el borrado de las unidades del sistema, la reinstalación del sistema operativo, el reemplazo de la unidades de almacenamiento o inclusive de partes del hardware podrían ser inútiles. Lo que nos lleva a pensar en una gran cantidad de escenarios que incluyen a aquellos donde las infecciones podrían darse incluso antes de adquirir el hardware o simplemente al adicionar algún nuevo componente de hardware infectado a un sistema existente.

5.3 Stealthy Dopant-Level Hardware Trojans

El trabajo titulado *"Stealthy Dopant-Level Hardware Trojans"*[BECKER2014] se enfoca en demostrar que se pueden introducir cambios e nivel físico en los circuitos integrados durante su proceso de producción y que los mismos podrían evadir técnicas de detección existentes ademas de generar comportamientos planificados y ajenos al diseño original.

Existen diferentes razones que motivan la inquietud de investigar la viabilidad de este tipo de "ataques" de bajo nivel y los riesgos que representan ante el actual concepto de ciberguerra[104]. Una referencia explicita que el autor hace en su trabajo es sobre reportes de *"Defense Science Board"* del Departamento de Defensa de los Estados Unidos que ya en el año 2005 citaban esta preocupación. Pocos años después, durante el 2010, la empresa

103 **TPM**: acrónimo del ingles *"Trusted Platform Module"*, o *"Modulo de Plataforma de Confianza"* que corresponde a la especificación ISO/IEC 11889 referida a un procesador seguro con soporte criptográfico para almacenar y gestionar claves de cifrado.

104 **Ciberguerra**: "Acciones de una nación-estado para penetrar computadoras o redes de otra nación con propósito de causar daño o interrupción a los mismos." [CLARKE2010]

VisionTech fue acusada de vender integrados con alteraciones que fueron distribuidos a empresas vinculadas al área de defensa para su utilización en sistemas críticos como frenos de trenes de alta velocidad, sistemas de radar para seguimiento en aviones F-16 y sistemas de control balístico para misiles entre otras posibles aplicaciones.

Existen formas de detectar alteraciones o "troyanos"[105] en circuitos integrados, para introducir al lector en las mismas podemos clasificarlas de la siguiente manera:

- Pre-fabricación: En este caso las modificaciones se realizan en el diseño, usualmente en HDL, ya sea por herramientas utilizadas durante su creación o por acciones de empleados no confiables. En este caso las técnicas de detección se basan en pruebas funcionales y reemplazo o redundancia de componentes.
- Post-fabricación: Para esta clasificación que se refiere a alteraciones introducidas fuera del diseño, particularmente durante la fabricación física del integrado, podemos realizar la siguiente sub-clasificación de los métodos de detección:
    - Con "*Golden chip*"[106]: En este caso se puede recurrir a algunas técnicas como las siguientes:
        - Ingeniería reversa óptica, este es un proceso de pruebas destructivo, donde se extraen las capas del integrado y se las fotografiá con SEM[107] para posteriormente comparar dichas fotos con las mascaras de producción del integrado de referencia o "*Golden chip*". Con este método se puede identificar la existencia de uniones o transistores ajenos a la implementación de referencia. Este es un método costoso en términos de tiempo y recursos, complejo en su ejecución y destruye el integrado bajo prueba.
        - Comparación de canales laterales de información, en este caso se comparan alteraciones en el comportamiento de mediciones no funcionales del

105 **Troyano**: denominación para un componente con algún comportamiento malicioso que se oculta al usuario detrás de una funcionalidad normal o esperada.

106 **Golden chip**: o *"integrado dorado"*, es la denominación para una unidad de un modelo de circuito integrado confiable, de la que se puede afirmar que no ha sido alterada durante su producción.

107 **SEM**: acrónimo del ingles *"scanning electron microscope"*, se refiere a un microscopio de barrido electrónico que permite obtener imágenes de alta resolución de pequeñas superficies en base a la interacción del electrón y la materia.

integrado durante la ejecución de casos de prueba en el integrado a evaluar y el *"Golden chip"*. Para este escenario se consideran las alteraciones de tiempos, consumo, emisiones electromagnéticas, frecuencias, etc. Si bien no es un método de detección destructivo tampoco es certero ya que se pueden omitir variables en el análisis o las variaciones podrían resultar imperceptibles o dentro de un rango aceptable.

- Sin "Golden chip": Para este caso debe recurrirse a la ejecución de pruebas funcionales sobre el integrado.

El método de implantación del troyano presentado por el autor del trabajo referenciado se basa en técnicas de ofuscación de diseño utilizadas actualmente en la industria de fabricación de semiconductores. Técnicamente se trata de aplicar diferentes polaridades de dopante en zonas particulares del área activa del componente a afectar, para así controlar su comportamiento de una forma predecible y sin alterar la estructura del mismo.

Como ejemplo se presenta el caso de un inversor compuesto por un transistor p-MOS y otro n-MOS unidos por su terminal de drenaje. La siguiente imagen muestra un diagrama que representa el inversor original y el alterado, este último se modificó para que tenga una salida constante por V_{DD} independientemente de su entrada.

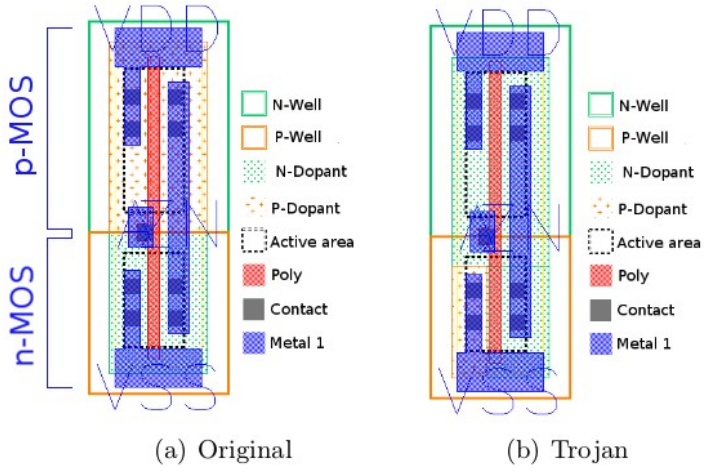


Imagen 18: Componente inversor (original y alterado)

Se puede apreciar que se dopó negativamente la totalidad del p-MOS dejándolo vinculado al área de dopaje negativo del n-MOS, y ademas se dopó positivamente la conexión de

origen o “source” del n-MOS dejándola aislada. El resultado final altera el comportamiento del dispositivo pero, como se ve en el diagrama, conserva la misma estructura de los componentes metálicos haciendo que la modificación se imperceptible en comparaciones basadas en imágenes de la estructura.

El trabajo presenta dos casos de estudio donde se ha aplicado esta técnica, ellos son:

- Intel’s Ivy Bridge RNG[108]: el troyano aplicado al diseño de este dispositivo es capaz de reducir el nivel de seguridad del numero aleatorio producido de 128 bits a un nivel seleccionado. Inclusive luego de estos cambios pasa el BIST[109] y puede generar números aleatorios para pasar el conjunto de pruebas del NIST[110] para números aleatorios.
- Side-channel Trojan: En este caso se utilizo la técnica para establecer un canal lateral oculto en una implementación de cajas-S[111] de AES[112] que potencialmente podría manipular el consumo para filtrar valores de la clave utilizada.

Este trabajo se destaca por los detalles técnicos y los casos presentados que son de potencial aplicación para funciones muy sensibles en la seguridad de un sistema. Deja en evidencia la posibilidad de implementar comportamientos maliciosos en el hardware desde su etapa mas temprana, la creación de los circuitos integrados. Destacando también que esta técnica resulta muy difícil de detectar y aun así los intentos requieren de un esfuerzo y capacidades técnicas muy importantes.

108 **Intel’s Ivy Bridge RNG**: es un dispositivo criptográfico para generación de números aleatorios ajustado a las definiciones de NIST SP800-90, FIPS 140-2, y ANSI X9.82.

109 **BIST**: acrónimo del ingles “*Built In Self Test*”, con significado “*Auto-evaluación incorporada*”. Corresponde a un conjunto de pruebas definidas dentro del diseño e implementadas en el dispositivo.

110 **NIST**: acrónimo del ingles “*National Institute of Standards and Technology*”, o “Instituto Nacional de Estándares y Tecnología” perteneciente a Estados Unidos con cede en Gaithersburg, Maryland.

111 **Caja-S**: es una componente de algoritmos de cifrado simétrico, utilizado en su lógica para reducir la relación del texto plano con su correspondiente valor cifrado.

112 **AES**: acrónimo del ingles “*Advanced Encryption Standard*”, o “Estándar de Cifrado Avanzado” es un protocolo de cifrado simétrico definido como estándar por el NIST.

5.4 God Mode Unlocked – Hardware Backdoors in x86 CPUs

Los siguientes párrafos describen el trabajo de Christopher Domas titulado *"GOD MODE unlocked: Hardware backdoors in x86 CPUs"[DOMAS2018]* que fuera presentado en el evento BlackHat del año 2018. Dicho trabajo plantea la existencia de una puerta trasera para ejecutar instrucciones en la arquitectura de procesadores x86, y posteriormente avanza con una investigación técnica para demostrar la existencia de la misma en un modelo del microprocesador VIA C3.

Su investigación incluyó el relevamiento de patentes relacionadas a microprocesadores que daban indicios de la existencia de mecanismos acordes al planteo que posibilitarían la ejecución de instrucciones evitando los controles de seguridad, una clara referencia es la siguiente traducción de un extracto de la patente US8341419[PARKS2012]:

> *"Además, acceder a algunos de los registros de control internos puede permitir al usuario eludir los mecanismos de seguridad, por ejemplo, permitir el acceso al anillo 0 desde el anillo 3. Adicionalmente, estos registros de control pueden revelar información que los diseñadores de procesadores desean conservar como propia. Por estas razones, los diversos fabricantes de procesadores x86 no hacen pública la documentación a descripciones para la dirección o función de alguno de los MSR de control."*

Cabe destacar que la investigación realizada involucró conceptos de otras patentes vinculadas al tema, entre las cuales su autor enuncia las siguientes: US8341419, US8880851, US8296528, US9292470, US9317301, US9043580, US9141389 y US9146742.

En consecuencia, la peligrosidad de esta puerta trasera se basa en la capacidad de disponer de un microprocesador de tipo RISC dentro de la arquitectura CISC de x86 al que se denomina DEC[113] o *"núcleo embebido profundamente"*. Este núcleo puede ejecutar instrucciones en modo de Ring-0 evitando los controles de seguridad de los niveles superiores, es importante tener en cuenta que el modelo de seguridad de anillos esta basado

113 **DEC**: acrónimo del ingles *"Deeply Embedded Core"*, cuyo significado en español es *"Nucleo Embebido Profundamente"*.

en aplicar diferentes protecciones para el acceso a los recursos siendo de Ring-0 el de mayor privilegio y reduciendo el acceso a medida que se incrementa el nivel del anillo. La siguiente grafica representa el modelo:

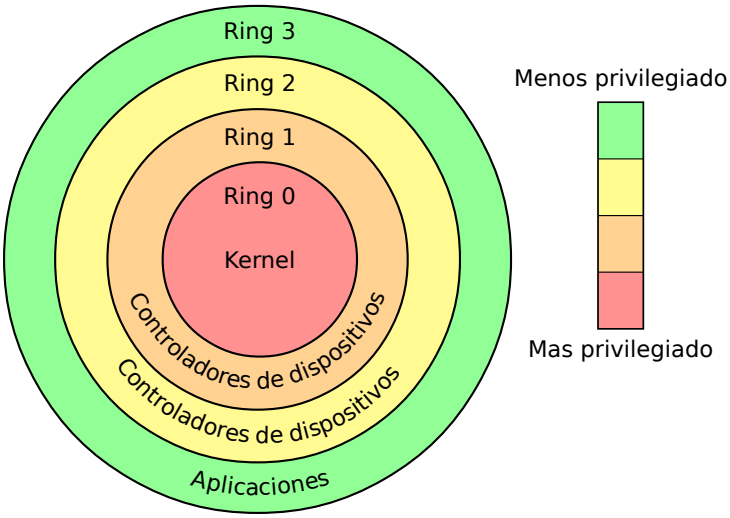


Imagen 19: Modelo de dominios de protección jerárquica por anillos

El trabajo en referencia despliega los detalles de los procedimientos utilizados para descubrir las instrucciones vinculadas al DEC e implementar un software para escalar privilegios utilizando esta puerta trasera. No esta en la incumbencia de esta tesis analizar o facilitar al lector la comprensión de las actividades técnicas realizadas en el trabajo dado que esto requiere que el lector también tenga conocimientos sólidos de la arquitectura de un microprocesador y el lenguaje ensamblador, sin embargo es de incumbencia para este capitulo enumerar los hitos alcanzados por el autor del trabajo para lograr implementar dicho software, ellos son:

- Identificar el "*registro de configuración global*" que se utiliza para activar el DEC. Se determino que para el caso de estudio el bit 0 del MSR[114] en la dirección 1107h estaba asociado a la activación del DEC.
- Identificar la "*instrucción de lanzamiento*" que permite activar el DEC RISC. Se identifico a la instrucción 0f3f con esta función.

114 **MSR**: acrónimo del ingles "*Model Specific Register*", cuyo significado es "*Registro Especifico del Modelo*" es un espacio de memoria utilizado a modo de registro por el microprocesador.

- Identificar la “*función puente*” que permite enviar las instrucciones RISC al DEC. Se determino que la instrucción “*bound*” tenia esta función.
- Implementar un programa que utilizando el DEC modifique las credenciales de un proceso para escalar privilegios. El autor realizo una implementación a la que denomino “*esc*” que luego de activar el DEC enviaba instrucciones al mismo para escalar privilegios con la siguiente lógica:

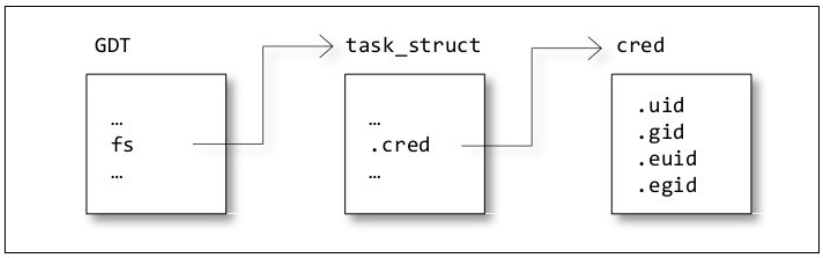


Imagen 20: Lógica para acceder a las credenciales del proceso

Con este fin diseñó el siguiente pseudo-código, que posteriormente sería escrito en instrucciones de lenguaje ensamblador y procesadas por un ensamblador, diseñado y construido para este caso, a fin de obtener su representación binaria en 32 bits. Es esta representación la que se utiliza con la instrucción “*bound*” para ejecutar las sentencias en “*Ring-0*”.

```
gdt_base = get_gdt_base();
descriptor = *(uint64_t*)(gdt_base+KERNEL_SEG);
fs_base=((descriptor&0xff00000000000000ULL)>>32)|
((descriptor&0x000000ff00000000ULL)>>16)|
((descriptor&0x00000000ffff0000ULL)>>16);
task_struct = *(uint32_t*)(fs_base+OFFSET_TASK_STRUCT);
cred = *(uint32_t*)(task_struct+OFFSET_CRED);
root = 0
*(uint32_t*)(cred+OFFSET_CRED_VAL_UID) = root;
*(uint32_t*)(cred+OFFSET_CRED_VAL_GID) = root;
*(uint32_t*)(cred+OFFSET_CRED_VAL_EUID) = root;
*(uint32_t*)(cred+OFFSET_CRED_VAL_EGID) = root;
```

Tabla 9: Pseudo-código para la modificación de las credenciales del proceso

A continuación se presenta una versión resumida del código del programa en lenguaje C, debido a que se removieron varias lineas de instrucciones para el DEC no es funcional, se incluye solo para que el lector pueda visualizar la estructura y las funciones utilizadas en el mismo.

```
#include <stdlib.h>
```

```
int main(void) {
    /* Desbloqueo de la puerta trasera al DEC */
    __asm__ ("movl $payload, %eax");
    __asm__ (".byte 0x0f, 0x3f");

    /* Modificación de la memoria del nucleo */
    __asm__ ("payload:");
    __asm__ ("bound %eax,0xa310075b(,%eax,1)");
    /*En este espacio hay otras 18 instrucciones para el DEC*/
    __asm__ ("bound %eax,0xe0108dfd(,%eax,1)");

    /* Ejecución de un shell */
    system("/bin/bash");

    return 0;
}
```

Al compilar y ejecutar la versión original de este programa se puede apreciar el efecto que produce, dado que es ejecutado por un usuario normal y devuelve un shell[115] en sesión del usuario root[116] con máximos privilegios en el sistema. A continuación se muestran la salida de la ejecución:

```
delta:~/rosenbridge/esc/bin$ whoami
delta
delta:~/rosenbridge/esc/bin$ ./escalate
bash-4.1# whoami
root
bash-4.1#
```

Tabla 10: Salida de la ejecución del programa para escalar privilegios

Si bien el programa implementado para la prueba de concepto demuestra la existencia de la puerta trasera a nivel de hardware en el procesador VIA C3 y logra explotar su uso para escalar privilegios en un caso concreto, el trabajo también aporta un gran valor en el detalle de su investigación y los procedimientos técnicos utilizados para identificar las posiciones de memoria e instrucciones que posibilitan el uso de DEC RISC sentando las bases y facilitando herramientas para extender el trabajo a otros modelos.

115 **Shell**: Interfaz de linea de comandos para acceder a los servicios de un sistema operativo.

116 **Root**: Usuario de administración o de máximo nivel de privilegios en sistemas operativos como Unix o Linux.

6 Resultados y conclusiones

6.1 Conclusiones

Para abordar la problemática de la dependencia en el hardware de origen extranjero de la República Argentina debemos comenzar con algunas consideraciones sobre su posición en el mercado de la fabricación de productos basados en semiconductores que como ya he comentado en este documento es bastante particular, dichas consideraciones se listan a continuación:

- Cantidad de organizaciones con capacidad de producción: En este aspecto solo se puede referenciar una empresa privada llamada Unitec Blue, a la que se suman un pequeño conjunto de entidades tanto educativas como de aplicación tecnológica especifica como INVAP y el INTI.
- Capacidad industrial instalada para la producción en grandes volúmenes: Este punto, vinculado al anterior, acota las posibilidades del país dado que solo una empresa de origen privado produce en volumen productos de uso genérico para su comercialización. El resto de las organizaciones con tecnología en el área carece de capacidad productiva o interés en la producción a gran escala.
- Capital humano: Históricamente la República Argentina ha desarrollado la formación de recursos vinculados a la computación, lógicamente esto se ha dado desde el arribo de las primeras computadoras al país. Sin embargo a lo largo de estas décadas el área de software sufrió un crecimiento notablemente mayor que las carreras vinculadas al hardware, particularmente aquellas afines a la ingeniería electrónica. Este escenario se vincula con la disponibilidad de profesionales del área en el país y asimismo tiene coherencia con la reducida cantidad de empresas de este rubro. Cuantitativamente podemos entender la situación al visualizar que durante el año 2017 se graduaron solo 839 personas en todo el país, y ninguna provincia supero los 200 egresados, los siguientes gráficos evidencian la situación:

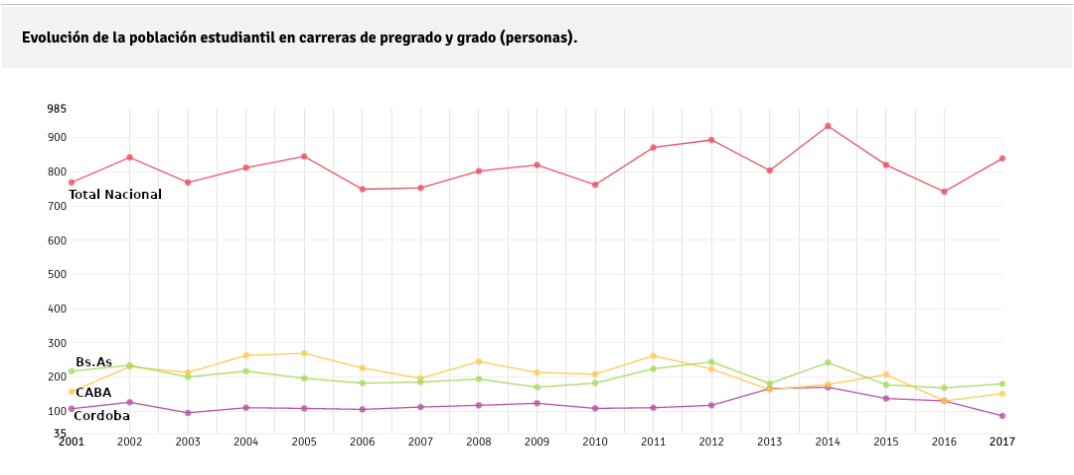


Imagen 21: Cantidad de egresados de Ingeniería Electrónica a nivel nacional, mas valores de las tres jurisdicciones con mayor volumen de egresados.

Otro dato de interés es la proporción de graduados del área de Ingeniería Electrónica provistos por entidades públicas en relación a las privadas.

Imagen 22: Proporción de egresados Publico-Privado

Los puntos presentados son coherentes al desarrollo histórico de la industria en el país, que si bien en épocas tempranas de las computadoras tuvo un desarrollo importante, el cual se pudo apreciar con los logros de los productos de Fate, posteriormente devino en un contexto que enfoco a la industria nacional del hardware al licenciamiento y ensamble. Este hecho tuvo como consecuencia la reducción de la capacidad productiva para la

fabricación de dispositivos basados en semiconductores y un acotado mercado laboral para el área de ingeniería enfocada en este tipo de productos que se traslada al volumen de profesionales graduados.

La situación previamente descripta no solo implica la limitación de la independencia para progresar en la generación de tecnología en cuanto a componentes físicos de sistemas informáticos y electrónicos, sino que también genera una situación de dependencia en actores externos para la utilización de diferentes tecnologías, especialmente cuando hablamos de dispositivos de uso masivo de producción a mediana y gran escala. Existen otros escenarios que de manera directa o indirecta muestran como el manejo de una tecnología puede limitar el progreso en otras áreas de un país, un ejemplo concreto es la industria aeroespacial, para el caso de nuestro país es representativo el ejemplo del desarrollo de misiles entre 1960 y 1990, donde se incluyen los proyectos Condor y Condor II[DELEON2015]. Dicho desarrollo tecnológico se vio discontinuado afectando a la capacidad de obtener independencia tecnológica en esta área y sus aplicaciones derivadas. Como resultado la República Argentina que cuenta con capacidades concretas y demostradas para el desarrollo de satélites depende de empresas o gobiernos extranjeros para su ubicación en orbita, al igual que para abastecerse de armamento avanzado o de mediano y largo alcance basado en este tipo de propulsores, sin importar que durante varios años del siglo XX se invirtió y avanzó en el desarrollo de esta tecnología en el país.

Otro aspecto a considerar es la relación entre la capacidad de producir o disponer de los componentes de un sistema y la capacidad de decisión sobre su tiempo de vida o periodo de utilización, este punto se vincula al concepto de obsolescencia programada o planificada[117]. En términos prácticos, la imposibilidad de ser un país productor de componentes de hardware tecnológicos hace que se dependa de proveedores externos, dependiendo de la planificación que estos actores hacen sobre el ciclo de vida de los mismos; esto implica no solo de su obsolescencia por falta de comercialización sino también por falta de componentes para reemplazo, reparación y actualizaciones de fallas, esta ultima es muy común en sistemas informáticos y dispositivos electrónicos complejos debido al uso de software en los mismos.

117 **Obsolescencia planificada**: *"El ciclo de vida del producto es acortado, entonces se reduce el tiempo que le toma al consumidor comprar el próximo producto de esa linea."*[KEEBLE2013] .

En los últimos párrafos he planteado los siguientes escenarios de dependencia aplicables a sistemas complejos:

- Dependencia en desarrollo y acceso a la tecnología.
- Dependencia del ciclo de vida o sumisión a la planificación de obsolescencia.

Me parece indispensable citar ejemplos de estos escenarios con sistemas o activos para la defensa convencional que se vieron afectados por situaciones de dependencia como las citadas.

El primero de estos escenarios corresponde a los misiles MM-38 y AM-39 utilizados durante el conflicto de Malvinas, claramente el país no estaba en posición de producir este tipo de armamento, avanzado para ese momento, por lo que tanto la disponibilidad de los mismos y del equipamiento complementario para su utilización estaba sujeto a su fabricante, de origen francés. La República Argentina había adquirido catorce unidades de sistemas de armas Dassault Breguet Super Étendard en conjunto con catorce misiles Exocet AM-39, dicha versión del misil francés esta diseñada para ser disparada desde el aire y se ofrecía con el modelo de avión en cuestión. Esta combinación permitía disponer de un misil "*Fire and Forget*"[118] anti-buques de largo alcance cuya distancia de operativa de 70 kilómetros se incrementaba debido al alcance y velocidad del sistema de armas que lo portaba, en este caso un caza-bombardero con una velocidad máxima de 1100Km/h y 1820 kilómetros de alcance[119] (850 kilómetros de radio de acción[120] efectivo), que ademas podía operar desde portaaviones y reabastecerse de combustible en vuelo. Con este sistema de armas se obtenía una capacidad de ataques a buques considerables que podía cubrir grandes distancias y ejecutar ataques en corto tiempo y con menor riesgo, dado que el sigilo y la capacidad de escape de una caza-bombardero es notablemente superior a los buques que portaban misiles con características similares como era el caso de MM-38.

Sin embargo, solo arribaron al país cinco unidades con un misil AM-39 para cada uno de ellos entre 1980 y 1981, el resto de las unidades no llegarían hasta el fin del conflicto en 1982. Sin lugar a duda esta situación de dependencia afecto negativamente la capacidad de

118 **Fire and Forget**: del inglés, disparar y olvidar. Tipo de misil que una vez configurado el objetivo y disparado no requiere de control o seguimiento alguno.

119 **Alcance**: distancia máxima de operación en vuelo lineal.

120 **Radio de acción**: distancia máxima de operación con retorno al punto de salida o inicio del vuelo.

la República Argentina durante el conflicto, dado que se utilizaron la totalidad de los misiles disponibles (solo cinco sobre los catorce adquiridos) con una alta tasa de efectividad. En paralelo se dio otra situación que muestra los efecto de este escenario de disponer de sistemas con tecnología avanzada cuyo desarrollo y construcción es íntegramente extranjero, de los cinco aviones disponibles durante el conflicto solo se utilizaron cuatro en operaciones viéndose obligados a desensamblar el quinto con el fin de utilizar sus partes como repuestos para las otras cuatro unidades debido a la imposibilidad de obtener las piezas del proveedor.

En resumen este ejemplo muestra el impacto de la dependencia tecnológica en los dos aspectos citados, primero es la limitación en la cantidad de unidades del sistema de armas disponibles debido a que la empresa dejo de proveer tanto los mismos hasta después del conflicto limitando la disponibilidad en un momento critico o en el momento en que resultaban necesarios. El segundo se corresponde a la dependencia del ciclo de vida o mantenimiento, en este caso particular el ciclo de vida del producto se vio temporalmente afectado para este comprado especifico y por un periodo de tiempo funcional a los intereses del país que producía el sistema de armas. Básicamente, sobre los cinco aviones Super Etendard disponibles en el país solo se pudieron utilizar cuatro, el 80%, dado que ante el nivel de exigencia en su uso bajo las condiciones reales del conflicto bélico se necesitaban repuestos que no eran provistos, de no haber utilizado una unidad para abastecerse de repuestos las otras cuatro habrían visto limitadas sus características y funcionalidades, o algunas de ellas no habrían podido seguir operando.

La situación previamente descripta fue la que dio lugar a la búsqueda de alternativas para reducir el impacto negativo en las capacidades de ataque a buques durante el conflicto, y allí se forjó la idea que finalizaría con la creación del ITB o *“Instalación de Tiro Berreta”* que permitió utilizar misiles MM-38 desde una plataforma terrestre, cuyos detalles han sido descriptos en el capitulo dos de este documento. El trabajo del Ingeniero Pérez y su equipo fue admirable y reconocido local e internacionalmente, especialmente por las condiciones en las que se llevo a cabo y los resultados obtenidos; aquí se debe resaltar la importancia de la inversión en conocimiento y el valor del desarrollo del capital humano para afrontar situaciones de adversidad e in-equidad en el desarrollo tecnológico.
Al mismo tiempo es necesario para este análisis plantear el interrogante sobre si esto podría llevarse adelante con tecnologías actuales, entendiendo que hoy en día existen y se

comercializan al público en general plataformas electrónicas de IoT que con facilidad pueden manejar sistemas de criptografía y protocolos mucho mas complejos que el utilizado en aquellas primeras versiones de MM-38, por lo que es lógico suponer que las versiones actuales como el MM-40 Block 3 dispondrían de mayor complejidad y seguridad en sus comunicaciones.

En linea con el planteo previo se puede abordar un segundo interrogante relacionado a la dependencia en el acceso a la tecnología en la actualidad dado que no necesariamente debe ser una limitación de acceso físico. Un hipotético caso a plantear basado en la dependencia es que en la actualidad y con las capacidades electrónicas disponibles es muy fácil que un dispositivo como el MM-40 Block 3, con capacidades de manejar señales electromagnéticas como el radar activo y el GPS, pueda tener comportamientos no declarados iniciados por un agente externo o condiciones preprogramadas de forma tal que disponer físicamente y controlar el dispositivo no implique que pueda ser utilizado sin limitaciones, tal cual ocurre en drones comercializados al público en general como los modelos de DJI descriptos en el capitulo dos que no vuelan en zonas prohibidas definidas por el fabricante (Por ejemplo, zonas de aeropuertos). Sobre este hipotético escenario podríamos tener misiles que operan con normalidad cuando se utilizan en las practicas pero se desvíen e impacten antes del blanco si el objetivo se encuentra en una zona sensible para los intereses del país que lo produce, o por ejemplo los buques de este país podrían disponer de contra-medidas particulares para estos misiles que en lugar de utilizar métodos convencionales como intentar confundir sus sensores con señuelos o inhabilitarlos por jamming[121] simplemente envíen solo una señal determinada que desvié levemente el curso hacia el terreno para un impacto previo a su posición. Lo interesante de este caso es que los usuarios del misil pagarían por dicho armamento y no advertirían la situación, salvo que tengan acceso al diseño de la electrónica y la construcción de la unidad, inclusive si entraran en conflicto con el país proveedor o alguno de sus aliados ya que en condiciones de conflicto real seria imposible peritar o analizar la causa del disparo fallido; este escenario ademas del beneficio económico le daría al país proveedor la certeza de que ese equipamiento no podría ser usado con efectividad en su perjuicio.

121 **Jamming**: también denominado “interferencia intencionada” es una técnica por la cual se transmiten señales de forma deliberada para perturbar la transmisión de otra señal.

Me resulta de interés este escenario hipotético que acabo de describir debido a que muestra como con el avance de la tecnología, particularmente la evolución de la electrónica y los sistemas de información, hace que la disponibilidad física de un elemento que cumple su función no solo genere una dependencia en un actor externo sino que también puede exponer al usuario a una situación aun mas comprometida y asimétrica frente a quien maneja esta tecnología haciendo que este usuario no sea consciente de la situación e inclusive que pague por ello. Este mismo escenario pero en una situación real se dio cuando la República Argentina compro equipos Hagelin Cryptos CX-52 para el tráfico clasificado en los niveles Estratégico Operacional y Estratégico Militar que se utilizaron desde 1972, e inclusive durante el conflicto de Malvinas, haciendo que el esfuerzo económico y humano para adquirir y operar estos equipos resultara perjudicial para los intereses de la Nación debido a que en lugar de incrementar la seguridad de las comunicaciones facilito la filtración de los estas a terceros inclusive durante periodos bélicos con las consecuencias que esto implicó.

Otro caso real para ejemplificar una situación de dependencia en activos de defensa convencionales es el del IA-58 Púcara; este es el único avión diseñado íntegramente en la República Argentina, que fue fabricado en serie en el país, utilizado activamente en conflictos bélicos reales y que logró formar parte de unidades de vuelo en otros países. En la actualidad ya no existe ningún país que continúe utilizando este sistema de armas, los últimos países en desactivarlos fueron la República Oriental del Uruguay el 17 de marzo de 2017 y posteriormente la República Argentina el 17 de septiembre de 2019. Y ambos casos comparten al menos una característica vinculada directamente con la dependencia del ciclo de vida en un factor externo, básicamente ninguno de los dos países planifico el reemplazo de estas aeronaves como suele realizarse cuando las unidades alcanzan su limite de horas de vuelo o el modelo es reemplazado por otro en su función, sino que debieron tomar la decisión de desactivarlos sin reemplazo alguno debido a la imposibilidad de seguir cumpliendo con los mantenimientos programados y requeridos de las unidades por la falta de repuestos, particularmente aquellos asociados a sus motores Turbomeca Astazou XVI-G de origen francés cuya producción cesó hace varias décadas sin licenciamientos para la fabricación de sus componentes.

En este punto debo hacer algunas aclaraciones para el mejor abordaje de este tema por el lector; primero, la motorización no fue el único aspecto a considerar para el fin del ciclo de

vida de este sistema de armas pero si fue crítico e inevitable dado que en la aeronaves, a diferencia de los vehículos terrestres de uso civil, existen esquemas de mantenimiento preventivo y programado estrictos que implican controles, verificaciones y revisiones[122] de sus componentes de forma obligatoria. Desde principios de la década del noventa la aeronave dejo de modernizarse, ofrecerse en el mercado (con los niveles de disponibilidad de equipamiento, unidades, repuestos y servicios que esta industria demanda) acompañado del posterior desmontaje de su linea de producción de unidades y repuestos. Y en este punto debemos aclarar que en las industrias, y particularmente las lineas de montajes de vehículos complejos, detener la producción y desensamblar una linea de montaje suele ser un punto irreversible dado que las mismas disponen de gran cantidad de elementos únicos, construidos o configurados específicamente para esa tarea en un modelo particular (herramientas, andamiaje, matriceria, etc.) sin considerar el conocimiento asociado al diseño, la técnica de producción y el desarrollo del recurso humano (especialmente cuando el mismo no se avoca a nuevas producciones, quedando cesante o realizando otros tipo de labores).

En resumen, este ejemplo muestra el impacto de la dependencia en el ciclo de vida de un producto, algunos hechos resultantes de esta situación para ambos países involucrados:

- Desde el punto de vista técnico, muchas unidades de aviones militares que no han llegado al fin de su ciclo de vida han tenido que ser desactivadas en forma temprana, sin posibilidad de aprovechar el resto de la vida útil de esta plataforma.
- Desde el punto de vista funcional, ninguno de los dos países se encontraba en condiciones de reemplazar las unidades con otras de características similares, y en consecuencia las funciones que estos podían desempeñar quedan vacías en sus esquemas de defensa.
- Desde el punto de vista económico, independientemente del valor residual de la amortización planificada, estos activos pasaron de ser unidades activas en condición de combate a desperdicios o elementos de deposito dado que no pueden ser vendidos por su situación ni fraccionados para repuestos ya que tampoco existen compradores que operen este modelo. Como datos para el lector, es

122 **Revisiones:** Dependiendo su tipo y categoría, implican el control y/o reemplazo de componentes basado en el tiempo de vida y no en su estado a fin de garantizar el correcto funcionamiento de la unidad.

frecuente en la industria aeronáutica avocada al ámbito militar reservar la comercialización de modelos de ultima generación al país que lo produce y eventualmente aliados estratégicos o países que invierten y/o participan en la producción del mismo, pero con el correr de los años y a medida que la tecnología del modelo se hace mas accesible o entra en desuso es común que estos países reemplacen dichas unidades y que las mismas se vendan a países con menor capacidad de desarrollo y presupuesto en esta área. De esta forma el vendedor obtiene un beneficio económico por estos activos que aun son operativos pero que él no utilizara, al mismo tiempo que abre oportunidades de negocio para la fabrica de estas unidades ya que las mismas necesitaran mejoras, repuestos, mantenimientos y otros servicios durante el tiempo que el nuevo comprador las utilice. Por lo tanto, la posibilidad de venta de sistemas de armas usados es concreta en este rubro que actualmente también considera compradores del sector privado, ejemplos de esto son Draken International[123], Tactical Air Support[124] o Blue Training[125] que cuentan con sistemas de armas propios.

Al igual que en el ejemplo anterior, correspondiente a los misiles AM-39 y MM-38, también es necesario reconocer que la situación de los motores se advirtió en etapas tempranas, inclusive al momento de iniciar la producción cuando se sabía que el motor francés seleccionado era antiguo y con una proyección de producción muy limitada en el tiempo, quizás factores externos o políticos influyeron en la decisión. Lo concreto es que como se detallo en el capitulo dos la Fabrica Militar de Aviones y las gestiones que la sucedieron, abordaron varias veces proyectos de motorización que no prosperaron en nuevas unidades ni se implementaron para las unidades existentes debido a que los motores aun tenían muchas horas de vida útil por delante, por lo que al pasar el tiempo y tornarse insostenible la disponibilidad de partes del motor Turbomeca Astazou XVI-G para su mantenimiento se inicio un último proyecto de remotorización que por numerosas demoras no llego a estar homologado a tiempo para ser considerado por los últimos países que operaron este sistema de armas, pero aun así pudo concretarse en una unidad que demostró una vez mas la factibilidad de re-motorizar esta aeronave. De esta situación me interesa

123 **Draken International**: Empresa con sitio web disponible en http://www.drakenintl.com .

124 **Tactical Air Support**: Empresa con sitio web disponible en https://tacticalairsupport.com .

125 **Blue Training**: Empresa con sitio web disponible en https://blueairtraining.com .

rescatar la importancia de contar con elementos desacoplados en un sistema, como en este caso la unidad motriz, que sumado a la propia capacidad técnica y el conocimiento permitieron realizar varias veces reemplazos del mismo en el diseño sin depender exclusivamente de un proveedor extranjero *(En el último proyecto IAI realizo las tareas de ingeniería y el prototipo, pero de haber prosperado las re-motorizaciones del resto de las unidades se habrían concretado en FadeA)*.

El último caso de ejemplo, citado previamente, corresponde a activos para el manejo de información cifrada particularmente a las maquinas CryptoAG o Hagelin Cryptos modelo CX-52 que la República Argentina adquirió para proteger el tráfico clasificado de niveles Estratégico Operacional y Estratégico Militar a partir de 1972. En este caso la dependencia no limito el acceso a la tecnología ni tampoco el ciclo de vida del producto, mas todo lo contrario la falta de desarrollo nacional en esa área genero la dependencia que a diferencia de los otros ejemplos se encontró con un interés externo en facilitar el acceso a esta tecnología por el mayor periodo posible, con diferentes beneficios. Por un lado el vendedor se beneficio con una venta con beneficios económicos y oportunidades de negocio futuras o asociadas a dicha operación, y en paralelo se aseguró que las comunicaciones de datos sensibles del ámbito de la estrategia operacional y militar del país se transmitirían con sus equipos; décadas después se confirmó que esta firma tenía en su nómina personas vinculadas a agencias de inteligencia de diferentes países, con lo cual conocían perfectamente como esta maquina realizaba sus cifrados y estos grupos tuvieron la libertad de manejar el diseño de dichos equipos para facilitar el acceso a la información que manejaban facilitando la posibilidad de enfocarse en el acceso a un dominio de datos acotado y de un alto valor estratégico. El resultado final fue la filtración sistemática de datos sensibles de la República Argentina durante los años en que estos equipos fueron utilizados, dicha situación fue expuesta y publicada en investigaciones periodísticas durante el comienzo del año 2020[BBC2020-1][BBC2020-2], los perjuicios son imposibles de cuantificar dado que inclusive se filtraron datos durante el conflicto bélico de Malvinas con las consecuencias que esto implicó para los intereses y los ciudadanos de la República Argentina. En resumen, este ejemplo muestra como la dependencia tecnológica también puede ser utilizada para tomar ventajas económicas y estratégicas, obteniendo injerencia en las capacidades o la información sensible de un país.

Existe otro elemento que no puede omitirse al analizar la dependencia en sus diferentes enfoques, el mismo es transversal a los escenarios citados y corresponde a la formación del recurso humano en el conocimiento y habilidades requeridas para el manejo de la tecnología. Los activos tecnológicos complejos sin importar su naturaleza (mecánicos, informáticos, electrónicos, etc.) suelen requerir de la capacitación de aquellas personas que los utilizan. Cuando la disponibilidad del recurso humano o el ciclo de vida útil de los mismos depende de un factor externo se generan situaciones forzadas de erogación de recursos que no necesariamente estarán planificadas y cubiertas en termino de capacidades y disponibilidad para la asignación de los recursos requeridos, tanto humanos como económicos.

El objetivo de los párrafos previos que detallan consideraciones sobre conceptos y ejemplos concretos de dependencia tecnológica de la República Argentina llevan por objetivo acercar al lector a algunos planteos sobre estas situaciones al apreciarlo con elementos físicos reales y escenarios pasado con resoluciones y consecuencias concretas. A partir de aquí pasaré a enfocarme en analizar como situaciones de dependencia de estos tipos impactan en el quinto dominio[126] donde encontramos elementos de alto valor pero en muchos casos intangibles. Traslademos esto al ámbito de estudio de esta tesis, la ciberdefensa de la República Argentina, considerando que la OTAN[127] define en el MC 0571 el concepto de ciberdefensa como *"La aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques"* y en linea con esta definición la resolución 1380/2019 del Ministerio de Defensa de la República Argentina establece:

> *"Entiéndase por CIBERDEFENSA a las acciones y capacidades desarrolladas por el MINISTERIO DE DEFENSA, EL ESTADO MAYOR CONJUNTO y las FUERZAS ARMADAS para anticipar y prevenir ciberataques y ciberexplotación de las redes nacionales que puedan afectar al Ministerio de Defensa y al Instrumento Militar de la Defensa Nacional, como así también a las Infraestructuras Críticas operacionales soporte de los Servicios Esenciales de interés para la Defensa o a Infraestructuras operacionales soporte de*

126 **Quinto dominio**: Dominio o dimensión de combate u operación reconocido por la OTAN y ejércitos de distintos países. El conjunto esta definido en tierra, mar, aire,espacio e información.

127 **OTAN**: acrónimo, Organización del Tratado del Atlántico Norte.

procesos industriales de fabricación de bienes sensibles para la Defensa o que posibiliten el acceso a los activos digitales estratégicos adjudicados a su custodia."[RESOL-2019-1380-APN-MD]

De aquí se desprende que la incumbencia abarca la infraestructura de comunicación, que para este caso también comprende los equipo de manejo de datos, y los activos intangibles como el software y la información propiamente dicha; este ultimo componente es el de mayor valor en el contexto actual.

En párrafos anteriores de este capitulo he abordado la problemática de la dependencia y mostrados casos antiguos vinculados a activos de defensa convencional de la República Argentina, pero al enmarcar este análisis dentro del ámbito de la ciberdefensa debemos destacar que los activos físicos que permiten el procesamiento y transmisión de datos dependen de componentes electrónicos que actualmente se basan en tecnologías que permiten crear componentes de muy pequeño tamaño que se integran en complejos sistemas haciendo difícil su ingeniería reversa. En consecuencia disponer físicamente de un dispositivo no garantiza el conocer y garantizar su funcionalidades internas a menos que se tenga acceso al diseño y un adecuado seguimiento del proceso de producción del mismo, esta situación da como resultado el hecho de que la esperada o correcta ejecución y manejo de información esta sujeta inevitablemente a quienes diseñan y los producen los dispositivos que la soportan. Es necesario destacar que la afirmación previa no limita el correcto funcionamiento a este escenario, también existen otras situaciones que pueden incidir en los sistemas y sus datos, que de hecho constituyen gran parte de los escenarios de los ciberataques como por ejemplo los problemas de configuración, defectos de software, defectos de utilización del sistema, etc.

Sobre este concepto asociado a la dificultad de conocer todos los comportamientos de un equipo informático debemos sumar otro factor de riesgo para la ciberdefensa en el contexto actual, y es la proliferación de equipos interconectados a través de redes publicas o en redes privadas que no se encuentran totalmente aisladas de redes externas. Podemos asociar este planteo al caso del CX-52, que he abordado previamente, en el mismo el dispositivo operaba cifrando mensajes que luego se comunicaban por diversos canales, sin embargo en la actualidad la criptografía ha extendido su integración con dispositivos o sistemas de diferente nivel donde muchos de ellos se encuentran integrados a las comunicaciones. Algunos ejemplos son los dispositivos que implementan protocolos de

comunicación inalámbrica, sistemas para cifrado de correo electrónico o mensajería, dispositivos para generar VPNs o túneles de cifrado. Sin lugar a duda muchos organismos e infraestructuras de incumbencia para la ciberdefensa nacional utilizan dispositivos con estas características, es de interés para el contexto de la hipótesis de este trabajo plantear la factibilidad de que en forma análoga al caso descripto de la empresa Crypto AG estos dispositivos podrían cumplir su función y al mismo tiempo generar una situación latente de compromiso o exposición. Tomando como base la información provista en el capítulo anterior sobre diversas formas de crear comportamientos maliciosos, limitaciones u ocultar capacidades en el hardware podemos enunciar como factibles las siguientes situaciones hipotéticas:

- Un dispositivo podría dejar de funcionar o alterar sus funciones ante una señal externa.
- Un dispositivo podría ante una actualización de hardware o software tomar provecho de la comunicación para extraer o alterar datos sin ser advertido.
- El dispositivo podría funcionar de manera deficiente restringiendo las capacidades esperadas del funcionamiento.

Esta situación representa un riesgo concreto y no menor, al punto que los países que operan como principales actores en el ámbito tecnológico se encuentran actualmente considerando esta situación en casos como la infraestructura de comunicaciones 5G y la provisión de componentes de hardware para sistemas de uso aeroespacial como los de posicionamiento global entre otros.

En cuanto al aspecto de recursos humanos debo aclarar que al comenzar este capitulo se hizo referencia a los formación de profesionales del área de hardware pero al enfocar el análisis en la ciberdefensa debemos redireccionar la atención a un grupo mas amplio que también incluye a quienes se ven involucrados en su operación. No solo la formación y disponibilidad de recursos es un tema de gran importancia para satisfacer las necesidades del caso, sino también los siguientes escenarios que no pueden ser ignorados:

- La necesidad de actualización continua en la formación de los recursos humanos, debido al cambio de tecnologías y productos utilizados, definidos por factores externos como el mercado, proveedores de activos adquiridos u otras

organizaciones que forman parte de las infraestructuras criticas de la Nación con autonomía sobre los sistemas utilizados para sus operación o negocio.

- La existencia de recursos con formación y experiencia en sistemas y componentes utilizados en áreas civiles y comerciales que atraviesan periodos de demanda de personal capacitado y que disponen de buenas capacidades para su remuneración. Este escenario es propicio para que la rotación de personal asignado a la cibedefensa sea un riesgo no menor y concreto.

Esto nos lleva a que la ciberdefensa en el marco de las condiciones de la República Argentina, como otros países con igual o menor desarrollo en la capacidad de producción de hardware, este influenciada por las siguientes situaciones adversas vinculadas al hardware y el tipo de sistemas actuales:

- Dependencia de hardware de origen extranjero, y sus implicancias en la disponibilidad y ciclo de vida del mismo.
- Limitación del conocimiento sobre las funciones y comportamientos del hardware extranjero.
- Aumento en la cantidad de equipos que requieren comunicación con redes externas.
- Capacidad de capacitación y retención del personal.

6.2 Resultados

En base a la información colectada en este documento y el criterio personal sobre la problemática y las posibles medidas de prevención para la reducción de los riesgos generados por las situaciones previamente descriptas se pueden establecer las siguientes recomendaciones:

Comprensión de la problemática de base: según lo expuesto en este documento resulta fundamental que las personas con capacidad de decisión sobre la ciberseguridad y ciberdefensa sean plenamente conscientes de las situaciones de riesgo que emanan de la dependencia en hardware cuyo desarrollo y producción es ajeno al ámbito de control.

Diversificación de hardware en los sistemas: ante la imposibilidad de disponer de hardware plenamente confiable se debería diversificar los proveedores dentro de cada área

funcional. Se debe comprender que esta decisión implica un aumento de costos vinculado a la formación y habilidades de los recursos humanos mas la complejidad de la integración y operación de estos componentes de distinto origen en un mismo sistema. Este escenario también plantea la consideración de distribuir proveedores de una misma función en una serie de diferentes capas a fin de evitar que una vulnerabilidad afecte al sistema en profundidad, como caso de ejemplo se puede referencia el uso de distintos firewalls en serie.

Consideración del aislamiento de conexiones: Si bien está demostrado que no todos los ataques basados en hardware ocurren en sistemas en linea, es claro que la comunicación de los mismos con redes internas y externas incrementan notablemente las posibilidades de ataque y mas aun la filtración de datos que es una exposición de seguridad cuyo impacto o consecuencia es irreversible; por esta razón y ante la asimetría planteada en este documento se debería considerar el aislamiento o la máxima reducción de conectividad en aquellos sistemas que requieran niveles de seguridad elevados para sus datos o operaciones, como es el caso de las infraestructuras criticas.

Open source: aquellos dispositivos de hardware con componentes de software de bajo nivel de fuente abierta permiten incrementar la confianza en estos dispositivos, por lo que deberían ser priorizados en la selección de componentes de un sistema con interés en la seguridad. No obstante cabe aclarar que esta condición en un dispositivo no lo hace mas seguro por si misma, sino que depende de que su funcionamiento y lógica sean auditados y verificados por entidades ajenas al proveedor y fuera de su ámbito de influencia, con el fin de proveer una confianza real y documentada sobre la su comportamiento y capacidades.

Open hardware: de forma asociada al punto anterior y en función de la factibilidad de diferentes tipos de ataques a nivel de hardware, algunos de los cuales han sido abordados en este documento, es recomendable la preferencia de componentes de hardware abierto para que al poder ser auditados y verificados se pueda disponer de una valoración mas objetiva y fundada para considerarlos confiables. Otro aspecto a considerar es la utilización de hardware genérico que pueda ser personalizado o programado para la función requerida independientemente del proveedor del mismo, particularmente aplica a dispositivos que puedan adaptarse a interfaces o especificaciones independientes a un único proveedor. También hemos visto que en muchos casos esto reduce notablemente la oferta e impacta en

las capacidades del hardware derivando en la afectación de su desempeño, no obstante el objetivo de las recomendaciones de esta sección del trabajo se enfocan en la seguridad del sistema por sobre otros factores.

A lo largo de este capitulo he cubierto los objetivos planteados en este trabajo, no obstante esto considero adecuado recordar que la problemática de la dependencia tecnológica ha sido históricamente crítica para los países menos desarrollados y es en este momento de la historia donde la ciberdefensa y ciberseguridad se suman a este escenario del cual la República Argentina posee y ha poseído numerosos casos; como ya hace varias décadas lo detalló el notable Dr. Bernardo Housay en estas lineas:

> *“La ciencia, la técnica y la investigación son la base de la salud, bienestar, riqueza, poder e independencia de los pueblos modernos. Hay quienes creen que la investigación científica es un lujo o un entretenimiento interesante pero dispensable. Grave error, es una necesidad urgente, inmediata e ineludible para adelantar. La disyuntiva es clara, o bien se cultiva la ciencia, la técnica y la investigación y el país es próspero, poderoso y adelanta; o bien no se la práctica debidamente y el país se estanca y retrocede, vive en la pobreza y la mediocridad. Los países ricos lo son porque dedican dinero al desarrollo científico tecnológico. Y los países pobres lo siguen siendo si no lo hacen. La ciencia no es cara, cara es la ignorancia.”*

6.3 Futuras lineas de investigación

Las futuras lineas de investigación que emanan de este trabajo incluyen los puntos enumerados a continuación:

- La incidencia de hardware de origen extranjero en la infraestructura de comunicación de datos del país.

- Análisis y comparativas de la dependencia en hardware de origen extranjero en los países de Sudamérica, tomando como referencia las consideraciones de análisis de este trabajo.
- Análisis del mercado de soluciones basadas en hardware de fuentes abiertas en la República Argentina.

7 Bibliografía y Referencias

Bibliografía

AAG2012: Aquellas armas de guerra, (2012),Misil antibuque Exocet francés,

AGUIRRE2017: Mikel Aguirre, (2017),La realidad sobre los nanómetros en procesos defabricación de CPUs y GPUs,

AMENDOLARA2012: Alejandro Amendolara, (2012),INVENTIVA BAJO PRESIÓN:EL LANZADOR COSTERO DE “EXOCET”EN LA GUERRA DE MALVINAS,

BABINI97: NICOLAS BABINI, (1997),LA LLEGADA DE LA COMPUTADORA A LA ARGENTINA,

BARDEEN1950: J BARDEEN, “Three-Electrode Circuit Element Utilizing Semiconductive Materials”, 1950

BBC2020-1: BBC News Mundo, (2020),Las revelaciones sobre cómo EE.UU. y Alemania "espiaron a decenas de gobiernos durante décadas" con una máquina suiza,

BBC2020-2: BBC News Mundo, (2020),Crypto AG : la máquina espía suiza que fue utilizada por los regímenes militares de Sudamérica para coordinar el infame Plan Cóndor,

BECKER2014: Becker, G.T., Regazzoni, F., Paar, C, (2014),Stealthy dopant-level hardware Trojans,

BROSSARD2012: Jonathan Brossard, (2012),Hardware backdooring is practical,

CESSI2014: Cámara de Empresas de Software y Servicios Informáticos- CESSI Argentina, (2014), HISTORIA DE LA INDUSTRIA INFORMATICA ARGENTINA, HISTORIA DE LA INDUSTRIA INFORMATICA ARGENTINA

CLARKE2010: Clarke, Richard A.,(2010), Cyber war,

CRYPTOMUSEUM2020: Crypto Museum, (2020), Crypto AG, MINERVA. Hagelin-Cryptos,

D6768-1971: Boletín Oficial de la Republica Argentina, (1971),Decreto S 6768/1971,

DELEON2015: PABLO GABRIEL DE LEON, El proyecto misilístico Cóndor.Su origen, desarrollo y cancelación, 2015

DJIMAVIC2: DJI,(2019), MAVIC 2 PRO/ZOOM User Manual v2,

DJIPHANTOM4: DJI,(2018), Phantom 4 Pro / Pro+ Series User Manual, Phantom 4 Pro / Pro+ Series User Manual

DOMAS2018: Christopher Domas, (2018),PROJECT: ROSENBRIDGE - Hardware Backdoors in x86 CPUs,

DSG2015: , (2015),Guia de supervivencia contra drones,

EXOCETAM39: MBDA, (2018),EXOCET AM39 Datasheet,EXOCET AM39 Datasheet

FSF2019: Free Software Foundation, (2019),¿Qué es el software libre?,

FSFCL2019: Free Software Foundation, (2019),¿Qué es el copyleft?,

GIONCO2019: Daniel Guillermo Gionco, (2019),Malvinas: el argentino que durante la guerra inventó unarma “berreta” que dejó fuera de combate al poderoso destructor Glamorgan,

KEEBLE2013: KEEBLE D., The culture of planned obsolescence in technology companies, 2013

KRAMER2012: Claudio Krämer, (2012),Industria electrónica argentina. Evolución y perspectivas,

LOUKAS2012: Loukas K, (2012),DE MYSTERIIS DOM JOBSIVS, Mac EFI Rootkits,

MILLER2020: Greg Miller, (2020),The intelligence coup of the century,

NORTHROP2012: Bryan Krekel, Patton Adams, George Bakos, (2012),Occupying the Information High Ground:Chinese Capabilities for Computer Network Operations and Cyber Espionage,

OPENSOURCE2007: Opensource.org , (2007),The Open Source Definition,

OSHW2010: Open Source Hardware Association, (2010),Hardware de Fuentes Abiertas,

OSHWALIST: OSHWA, CERTIFIED OPEN SOURCE HARDWARE PROJECTS, 2020

PARKS2012: G. G. Henry, T. Parks, Apparatus and method forlimiting access to model specific registers in amicroprocessor, 2012

RESOL-2019-1380-APN-MD: MINISTERIO DE DEFENSA, (2019),Resolución 1380/2019,

SEMICONDUCTORPLANTS2020: Wikipedia, (2020),List of semiconductor fabrication plants,

SMUKLER2012: Alejandro Smukler, (2012),Continuar el camino. Cincuenta años de computación en Argentina,
STALLMANCA2020: Richard Stallman, (2020),Por qué el «código abierto» pierde de vista lo esencial del software libre,
STANAG4670: NORTH ATLANTIC TREATY ORGANIZATION (NATO) ,(2014), UAS Tactical Pocket Guide, UAS Tactical Pocket Guide
WMEXO2019: Wikimedia, (2019),Exocet,Exocet
WPJP2019: Wikipedia, (2019),Julio Pérez (militar),

ix Anexos

Anexo A – IA-58 Pucará

CARACTERISTICAS PRINCIPALES:

Largo total	14,250 m.
Envergadura	14,500 m.
Altura	5.36 m.
Superficie alar	30,3 m2
Potencia de despegue	2 x 980 HP
Relación peso-potencia	3,47 kg/HP
Peso máximo de despegue	6.800 kg.
Planta de poder (2)	Astazou XVI-G
Asientos eyectables 0/0	Martin Baker PA-06A

INTRODUCCION

El IA. 58 PUCARA es un avión de ataque polivalente y su misión primaria el reconocimiento ofensivo sobre mar y tierra como así también el apoyo de fuego en el campo táctico, pudiendo cubrir con eficacia misiones de contrainsurgencia.

Las características y cualidades fundamentales de este avión son las siguientes

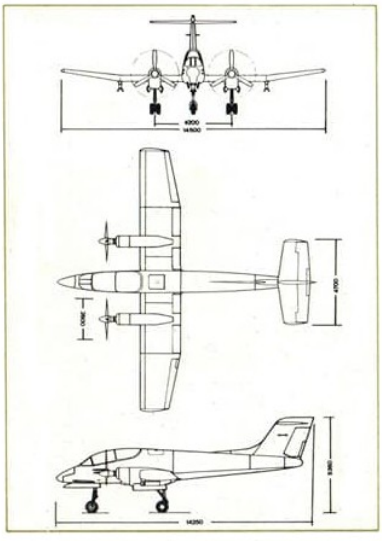
- ***Monoplano metálico.***
- ***Biturbohélice.***
- ***Excelente maniobrabilidad.***
- ***Alta capacidad operacional en baja altura.***
- ***Baja servidumbre logística.***
- ***Aterrizaje y decolaje corto.***
- ***Optima flexibilidad operativa.***
- ***Armamento ofensivo y defensivo.***

El IA. 58 PUCARA ha sido diseñado para cumplir con las siguientes misiones:

- ***Entrenamiento básico o avanzado, según el patrón de vuelo.***
- ***Apoyo táctico.***
- ***Contrainsurgencia.***
- ***Reconocimiento ofensivo.***
- ***Reconocimiento fotográfico.***

Cuenta con una tripulación compuesta por piloto y copiloto con asientos dispuestos en tandem, eyectables y regulables en altura.

El asiento del copiloto se encuentra 25 cms. más alto que el del copiloto. A esta disposición se suma el diseño especial de la nariz del avión y la cúpula totalmente de plexiglas, lo cual permite lograr una amplia visibilidad para ambos tripulantes.



DESCRIPCION

El avión IA. 58 PUCARA es un monoplano metálico, ala baja Cantilever, empenaje en T, con tren de aterrizaje retráctil. Los alerones son de perfil Frise y de construcción en dural. La estructura, de tipo monocasco, se divide en tres partes: anterior, central y posterior.

El cono delantero es desmontable y rebatible para facilitar el acceso a los distintos equipos que en él se instalan.

La cabina del avión está equipada con dos asientos Martin Baker MK-PA-06A, que permite la eyección a nivel del suelo con velocidad nula (0-0), con equipo de supervivencia marítimo-terrestre opcional para el comprador. Ambos asientos se encuentran instalados en diferentes planos para permitir la mejor visibilidad de ambos tripulantes.

El sistema de comandos de vuelo está constituido por cadena cinemática a barras y cables.

El tren de aterrizaje posee amortización mediante anillos elásticos Ring-Feder, habiéndose adoptado este sistema teniendo en cuenta aquellas pistas de condiciones precarias, desde donde puede operar el avión.

La iluminación exterior se compone de dos faros de aterrizaje (uno en cada pilón de ala), luces de posición en los extremos de alas y cola con dos niveles de intensidad: "brillante atenuado" y "destellante", también consta de un faro anticolisión de panel rodante ubicado en la parte superior del empenaje vertical.

El IA. 58 PUCARA fue concebido en base a las especificaciones de un avión de ataque de uso múltiple. Esta característica impuso la utilización de cañones y ametralladoras fijas y cargas lanzables ubicadas en los lanzadores de ala (dos) y en el fuselaje central (uno), lo que permite diferentes combinaciones y la utilización máxima de su capacidad portante lanzable.

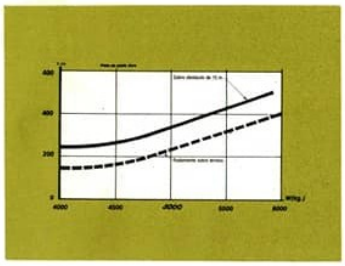
A su posibilidad de aterrizar en terrenos de muy corta extensión, se agrega la ventaja de poder utilizar cohetes de despegue tipo J.A.T.O. soportados en el pilón central. En estas condiciones y utilizando tres J.A.T.O. puede decolar en 80 m. (rodaje en tierra).

IA 58 pucará

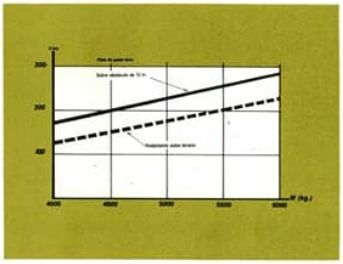
PERFORMANCES

Techo con dos motores funcionando.....10.000....(32.808 pies)
Techo con un motor funcionando .....6.000....(19.685 pies)
Velocidad horizontal máxima.....500 km/h....(270 nudos)
Velocidad máxima de picada .....750 km/h....(405 nudos)
Velocidad de pérdida sin flaps tren adentro ..125 km/h....(67,5 nudos)
Carrera de despegue .....300 m.....(984 pies)
Régimen inicial de trepada.....18 m/seg.....(3.543 pies/min.)

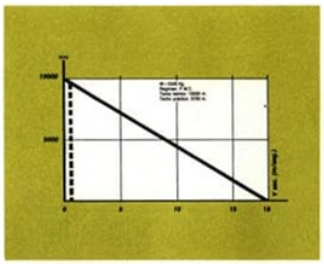
Despegue



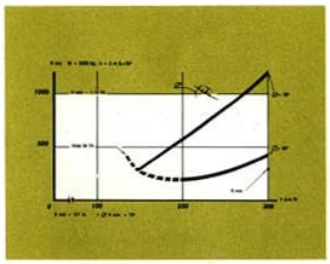
Aterrizaje



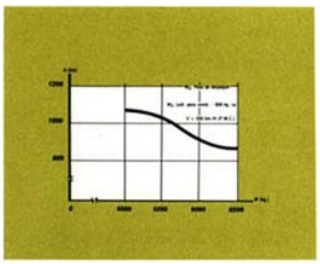
Velocidad ascensional y techo



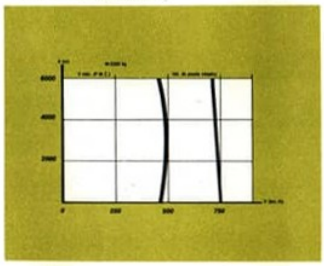
Radio de viraje



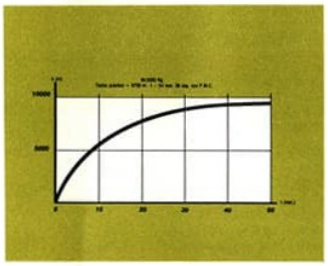
Alcance



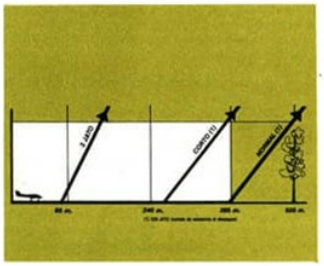
Velocidad máxima y de picada



Tiempo de ascenso



Técnicas de despegue



IA 58 pucará

ARMAMENTO

La guerra moderna ha demostrado que la aviación táctica debe estar preparada para atender rápidamente requerimientos de las fuerzas de superficie, aportar una gran potencia de fuego y disponer de un tiempo prolongado de permanencia en el aire, lo que permite efectuar su misión en forma amplia y eficaz.

La verdadera polivalencia del I.A. 58 PUCARA lo hace apto para desempeñarse en variadas tareas de combate, pudiendo operar desde cualquier tipo de pistas, ya sean semi-preparadas o improvisadas debido a sus excepcionales performances de despegue y aterrizaje corto.

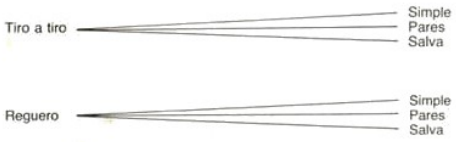
Asimismo mantiene su capacidad de combate y de reconocimiento ofensivo en cualquier configuración de armamento lanzable. Aún en la versión Ferry, o sin cargas externas y cualquiera sea su misión puede utilizar su armamento fijo constituido por:

* Cuatro ametralladoras Browning 7,62 mm. con 900 proyectiles.
* Dos cañones HS-804 de 20 mm. con 270 proyectiles. En la versión "B" estos cañones están reemplazados por dos DEFA 553, de 30 mm. y 140 proyectiles para cada cañón, lo que amplía su capacidad de tiro.

Para portar las cargas lanzables se dispone de tres pilones eyectores con una capacidad máxima total de 1.500 Kgs. Dos de ellos son pilones Aero 20 Al, fijados uno en cada ala y el otro es un Aero 7-Al ubicado en la parte inferior del fuselaje.

El disparo de las armas fijas y las cargas lanzables se efectúa desde el puesto de piloto. Para lanzar las cargas externas puede usarse el circuito convencional o utilizarse el programador Bendix AWE 1 que equipa al I.A. 58 PUCARA. Mediante este programador el piloto puede selectar:

* Cantidad de cargas a lanzar: entre 2 y 40
* Distintos modos de lanzamiento:

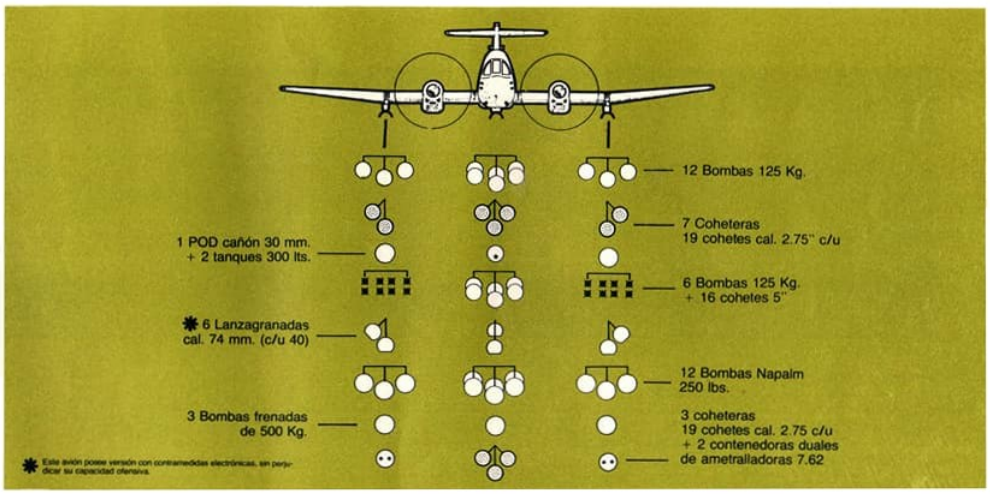


* Cadencia entre disparos: Se puede graduar entre los 20 milisegundos hasta 2 segundos, con todos los valores intermedios.

Como elemento de puntería, el I.A. 58 PUCARA cuenta con una mira reflectora simple iluminada Matra 83-A3, pudiendo regularse su depresión para lanzar las cargas portantes en cualquier ángulo de disparo.

8

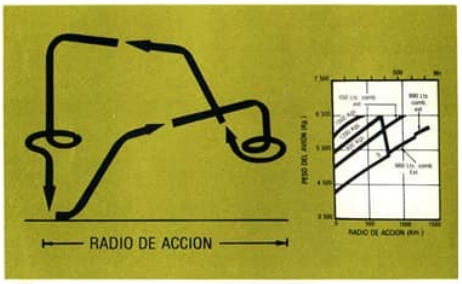
CARGA EXTERNA



9

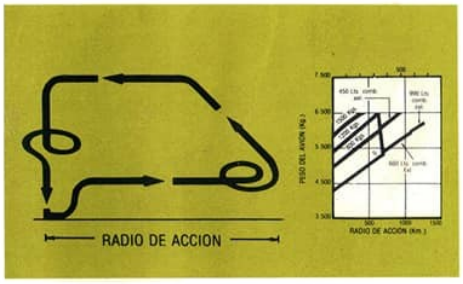
IA 58 pucará

MISIONES DE ATAQUE



ALTO - BAJO - ALTO

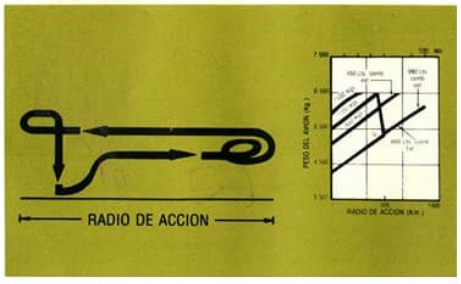
Trepada.
Altura de vuelo hacia el Blanco h = 6.000 m.
Penetración y 5 minutos sobre el Blanco a 150 m. de altura.
Trepada hasta la altura de regreso.
Regreso volando a h = 8.000 m.
Reserva: 10% del combustible inicial.



BAJO - BAJO - ALTO

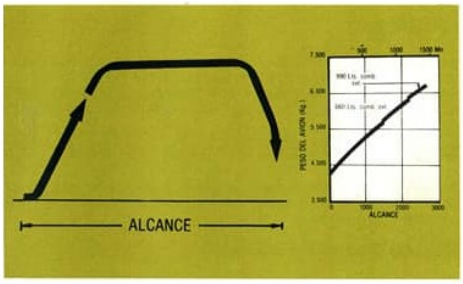
Trepada hasta h = 150 m. y vuelo hacia el Blanco a la misma altura.
Penetración y 5 minutos sobre el Blanco a 150 m. de altura.
Trepada y regreso volando a h = 8.000 m.
Reserva: 10% del combustible inicial.

NOTA:
Los valores indicados sobre las curvas corresponden a las cargas ofensivas portadas (lanzables).
En todas las misiones, cualquiera sea su configuración de cargas exteriores, se incluye a los dos cañones y las cuatro ametralladoras con su correspondiente munición.



BAJO - BAJO - BAJO

Ida y vuelta al Blanco volando a 150 metros de altura.
Penetración y 5 minutos de combate.
Reserva 10% del combustible inicial.



FERRY

Trepada hasta h = 6.000 m.
Traslado hasta el objetivo, volando a h = 6.000 m.
Reserva: 10% del combustible inicial.

IA 58 pucará

MANTENIMIENTO

GENERALIDADES

Este avión ha sido diseñado especificamente para lograr un alto índice de confiabilidad, bajo tiempo medio de reparación de averías y poco servicio programado. Los equipos y sistemas se han diseñado desde el comienzo con una alta resistencia a la fatiga. El servicio en tierra y los equipos de prueba han sido optimizados para mejor facilidad del manejo.

CONFIABILIDAD

El objetivo de la confiabilidad del diseño, consiste en lograr que el avión en servicio, complete las misiones con un mínimo de novedades de vuelo.

Esta meta ha sido conseguida con el I.A. 58 "PUCARA" debido a la robustez de su estructura, la sencillez de sus sistemas y la fácil manipulación de los mismos.

SEGURIDAD DE VUELO

Se ha puesto gran empeño en la seguridad de vuelo, con la finalidad de conseguir una mejora considerable sobre los niveles alcanzados por los tipos de avión actualmente en servicio.

FACILIDADES DE MANTENIMIENTO

La F.M.A. proveerá a los usuarios de sus aviones la Documentación Técnica necesaria para realizar un correcto mantenimiento de todos los componentes de los sistemas y equipos de sus productos.

TIEMPO DE DIAGNOSTICO DE AVERIAS Y CAMBIO DE ELEMENTOS

Siempre que sea factible, todos los sistemas usan el concepto de localización de fallas hasta el nivel de unidades fácilmente recambiables LRUs (Unidades recambiables en línea).
Cuando la proporción de defectos previstos de los componentes es de 0,1 por 1.000 horas o mayor, se presta atención especial para facilitar el mantenimiento, la reparación o el recambio de dichos elementos.

INSPECCION

Tanto la estructura primaria y secundaria como los componentes son fácilmente accesibles para la inspección visual.

FACILIDAD DE MANEJO

El requerimiento de un fácil manejo y mantenimiento fue un factor decisivo en el diseño del IA. 58 PUCARA.

El avión es fácilmente comandable, aún con un solo motor. La V.M.O. (velocidad máxima operacional) es de 405 Kts aproximadamente M-063 disponiendo un adecuado margen con respecto a la velocidad crítica de diseño (M-0.77), no presentándose por lo tanto ningún fenómeno que afecte la estabilidad, ni el control en el dominio de vuelo del avión.

Tiene una admirable capacidad de maniobra a baja altura y una amplia gama de velocidades de operación, lo que le permite cumplir misiones de combate sobre terrenos de severa configuración orográfica.

Una amplia respuesta en la recuperación de picadas a velocidades máximas y su variedad de armamenro ofensivo, lo sitúan dentro de los aviones con sistemas de armas de máxima eficacia.

COMANDOS DE VUELO

Los comandos de alerones, timón de profundidad y de dirección poseen una cadena cinemática a barras, a fin de asegurar la inmediata respuesta de los mismos.
El comando de alerones y timón de profundidad se integran por medio de un bastón de mando en cada puesto de pilotaje, con empuñadura normalizada para aviones de combate.
El comando del timón de dirección es de tipo convencional, y los pedales de cada puesto de pilotaje son ajustados longitudinalmente. Variando la inclinación de cada uno de los pedales, se frena la rueda correspondiente del tren principal.
También es posible acoplar al comando de dirección, la rueda de nariz, lo que permite efectuar virajes durante el carreteo.
Los compensadores de los comandos de profundidad, alerones y dirección, se accionan eléctricamente (con prioridad para el piloto), de la siguiente manera:

- Profundidad: con una llave en la empuñadura de los bastones de mando, la que acciona un motor eléctrico que mediante una transmisión mecánica varía la posición del trim-tab.
- Alerones: con la misma llave de los compensadores de profundidad, accionándola lateralmente.
- Dirección: con una llave ubicada en el panel izquierdo del puesto de piloto.

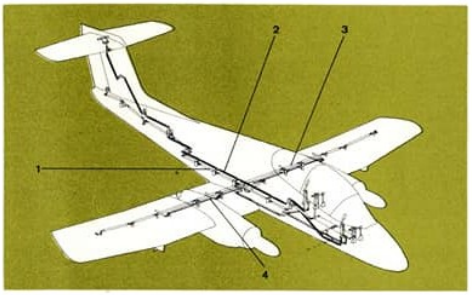
Los comandos de los compensadores de profundidad y alerones se encuentran en la parte superior de la empuñadura de los bastones, y el de dirección en el panel izquierdo del tablero principal.
El comando de accionamiento de los compensadores da preferencia a la señal del piloto sobre la del copiloto.

Los Flaps son del tipo Slotted, monolargueros, y de construcción en dural 024T, están constituidos por cuatro tramos ubicados en el ala central a ambos lados de las barquillas. Cada tramo es soportado por dos tomas fijadas con bulones.
El comando de flaps es hidráulico accionado por una electroválvula comandada en paralelo desde los puestos de pilotaje, de tal manera, que cada tripulante puede controlar la posición de los flaps (con prioridad para el piloto).

1 - Comando de Dirección
2 - Comando de Profundidad
3 - Comando de Alerones
4 - Comando de Flaps

COMANDOS DE MOTOR

Este sistema se compone de todos los elementos que hacen posible la transmisión del movimiento de comandos de los puestos de piloto y copiloto, al grupo turbopropulsor.
Este sistema es de tipo mecánico y los movimientos son transmitidos a través de barras y cables. Los mecanismos de barras se complementan con guiñoles articulados en el fuselaje que tiene por finalidad interconectar a los puestos de piloto y copiloto.
El control de potencia y paso de hélice de ambas plantas de poder, se efectúa desde 2 torres, fijadas a los paneles laterales izquierdos de ambos puestos de pilotaje.
En el diseño de los comandos se ha prestado especial atención a la accesibilidad de los mismos con el objeto de facilitar las tareas de inspección y mantenimiento.



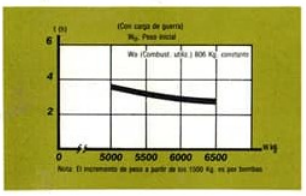
SISTEMA DE COMBUSTIBLE

El I.A. 58 "PUCARA" cuenta con un tanque doble de bodega que consta de dos cuerpos, encimados y ensunchados entre sí; ubicados inmediatamente detrás de la cabina, y un tanque autoobturable en cada ala. Estos tanques dan al avión una capacidad de 1280 litros, que pueden ser almacenados aún con carga máxima de armamento. Tal característica hace que el I.A. 58 "PUCARA" tenga una capacidad excepcional de carga de combustible, en relación con aviones de similar tamaño y misión. Utilizando los tanques externos suplementarios, la capacidad total de combustible se incrementa a 2240 litros.
La carga de combustible se realiza, en forma convencional, por las bocas ubicadas en el tanque de fuselaje. El vaciado en tierra puede efectuarse simple y rápidamente.
El sistema de comustible está diseñado de tal forma que el tanque de fuselaje alimenta por gravedad a los tanques de ala, asimismo, estos aseguran la alimentación de los motores a presión mediante bombas sumergidas; en caso de falla eventual de éstas, la alimentación se realiza por gravedad. Un circuiro auxiliar de combustible para vuelo invertido, posibilita la alimentación con el caudal y presión necesarios durante 30 segundos.
Para el control del caudal, se emplean válvulas de corte y reguladoras de probada calidad. De han instalado medidores de flujo, que permiten conocer permanentemente el régimen de consumo.
Para la determinación de la cantidad de combustible, se han incorporado a cada tanque medidores de tipo capacitivo, que permiten obtener información parcial de cada tanque de ala y fuselaje. El circuito de combustible cuenta con un sistema de filtrado y calefaccionado del fluido en concordancia con las exigencias del motor. Para ello se intercala en el sistema un precalentador (controlado por una válvula termostática) donde el combustible obtiene una temperatura estabilizada, evitando así la formación de hielo en los filtros y logrando un rendimiento óptimo de la combustión.

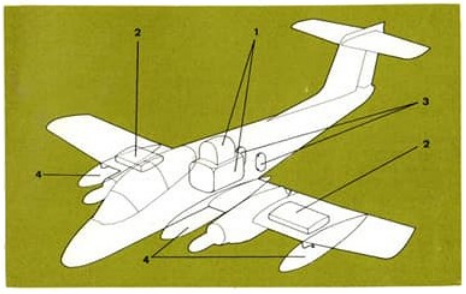
Disposición de los tanques de combustible

Posición en el avión	Número de tanques	Capacidad
Ala	2	508 Lts.
Fuselaje	2	772 Lts.
Total	4	1280 Lts.
Tanques externos ala	2	640 Lts.
Tanque externo fuselaje	1	320 Lts.
Máximo combustible		2240 Lts.

Autonomía



1 – Tanques de bodega
2 – Tanques autoobturables
3 – Acumulador de vuelo invertido
4 – Tanques externos opcionales



IA 58 pucará

SISTEMA ELECTRICO

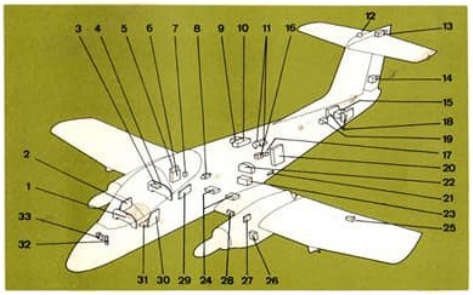
El I.A. 58 "PUCARA" cuenta con un sistema eléctrico mixto (corriente continua y alterna), para satisfacer los requerimientos de los diversos equipos del avión.
El circuito eléctrico es unifilar, con una capacidad de carga superior en un 10%, a la requerida por los distintos sistemas. Para evitar interferencias con los equipos de radio y de navegación, se han blindado los tramos de encablado correspondientes.
La alimentación de corriente continua de 24 V, es provista por una batería de tipo alcalina.
Para la generación de corriente alterna, se dispone de tres inversores estáticos. Dos de ellos proveen corriente de : 200 V., 115 V., 26 V. Uno de estos inversores es utilizado en operación normal, reservándose el otro para emergencia.
El tercer inversor produce corriente de 200 V. (onda cuadrada), para alimentar el circuito de deshielo del parabrisas blindado.
Los interruptores automáticos son del tipo de disparo libre, habiéndose graduado éstos y los fusibles, de acuerdo con los requerimientos de máxima potencia del correspondiente circuito.
Para simplificar el trazado de los circuitos y las tareas de inspección y mantenimiento, se han agrupado en paneles únicos los interruptores y los instrumentos relacionados con los mismos.
El circuito eléctrico de armamento se alimenta con corriente continua proveniente de una barra independiente. Este circuito, además de los fusibles y del seguro de empuñadura ubicado en el bastón de comando, cuenta con 3 seguros eléctricos, a saber:

- llave general de tres posiciones (ARMAMENTO - NO - J.A.T.O.).
- micro llave accionada por la rueda de nariz en posición ARRIBA.
- seguro electro-mecánico, accionado aerodinámicamente cuando el avión alcanza los 110 kts.

De esta forma se logra que el armado del avión en tierra se realice con el máximo de seguridad y se eviten los disparos accidentales durante el rodaje o en la carrera de decolaje, ya que los seguros deben estar cerrados para darle continuidad al circuito.
El circuito de eyección en emergencia de las cargas portadas por los pilones es independiente del anterior y puede ser accionado aún en la carrera de decolaje con tren abajo y antes de alcanzar los 110 kts.
El disparo de los cohetes auxiliares de despegue (J.A.T.O.), se efectúa desde la empuñadura del puesto del piloto, accionando el gatillo para disparo de ametralladoras y cañones (que cuenta con seguro de empuñadura).
La iluminación exterior del avión está compuesta por:

- Dos faros de aterrizaje (uno en cada pilón de ala).
- Luces de posición en los extremos de alas y en la cola, con dos niveles e intensidad: "brillante atenuado" y "destellante".
- Una luz anticolisión de fanal rotante ubicada en la parte superior del empenaje vertical.

1 – Tablero piloto
2 – Panel de fusibles e interruptores térmicos
3 – Alarma audible matafuego y trim
4 – Tablero copiloto
5 – Caja regulación de trim
6 – Caja de distribución C3-C4
7 – Caja control de incendio
8 – Motor actuador cupula
9 – Caja relay de armamento
10 – Caja programador de armamento
11 – Reguladores de voltaje
12 – Faro anticolisión
13 – Actuador trim direccion
14 – Actuador trim direcrión
15 – Inversor estático de 1000 VA
16 – Caja amplificador debimetro
17 – Caja automática de helice
18 – Inversor estático de 250 VA
19 – Caja comando trim
20 – Caja principal auxiliar (C-4B)
21 – Tomacorriente ficha arranque aux.
22 – Caja princ. central (C-1)
23 – Batería 24V
24 – Cajas de arranque
25 – Actuador trim alerón
26 – Caja T4
27 – Caja de resistencia
28 – Caja de interruptores micros
29 – Panel de interruptores izq. copiloto
30 – Panel de interruptores izq. piloto
31 – Panel de arranque
32 – Control de temperatura 1003 y 1004
33 – Relay



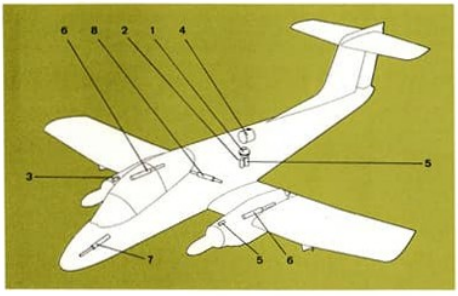
TREN DE ATERRIZAJE Y SISTEMA HIDRAULICO

El tren de aterrizaje del I.A. 58 "PUCARA" es triciclo, totalmente retráctil. Su robustez permite la operación en terrenos no preparados.
Tanto el tren principal como el delantero, son tipo semi-cantilever construidos en acero cromo-molibdeno soldado.
Los amortiguadores son del tipo "Ring feder" (anillo elástico metálico) que poseen la cualidad de requerir muy poco mantenimiento.
Las ruedas del tren principal (no orientable), son sin cámara y de media presión. En el tren delantero (orientable), la rueda es simple y de iguales características y tamaño que las del tren principal.
Los frenos actúan solamente sobre el tren principal y son del tipo a discos, con accionamiento hidráulico de doble circuito. Esta característica, asegura su eficacia en caso de emergencia.
El sistema de retracción prevé el escamoteo completo del tren hacia adelante, introduciéndose en las barquillas del motor para el caso del principal y en la parte inferior de la nariz para el delantero. En ambos casos, tapas de accionamiento automático lo ocultan totalmente.
El accionamiento del tren es hidráulico. Sin embargo, la extensión del mismo queda asegurada por la acción de la gravedad, contribuyendo a ello la presión dinámica del aire. Por otra parte el trabado del tren de aterrizaje se asegura por un sistema mecánico acumulador de energía a resorte. De esta manera la emergencia del tren es totalmente efectiva.
El sistema hidráulico del I.A. 58 "PUCARA" es convencional (200 kg./cm2 de presión). Mediante dos bombas hidráulicas accionadas por los motores, se asegura el flujo y la presión en todo el circuito. La alimentación del sistema se realiza desde un depósito que está ubicado detrás del tanque de combustible de fuselaje. El mismo asegura:

- Alimentación en vuelo normal e invertido.
- Fácil acceso para realizar los trabajos de mantenimiento.

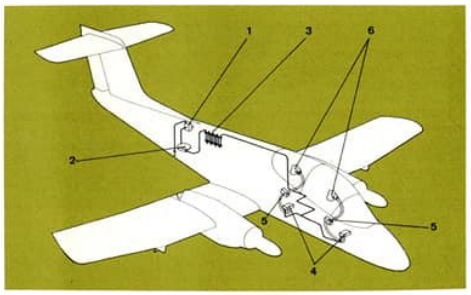
Las eventuales fluctuaciones del sistema principal son evitadas mediante un acumulador. Otros dos acumuladores, independientes entre sí, aseguran el funcionamiento de los frenos, tanto en operación normal como en emergencia.
El sistema es controlado por válvulas automáticas, que son accionadas en forma directa o remota. Mediante tres manómetros, se obtiene la indicación de la medición de presión del circuito principal y de los frenos.
Los cilindros de accionamiento y cañerías empleadas son normalizadas, existiendo en F.M.A. una probada experiencia en la utilización de dichos elementos, lo que asegura que el sistema sea simple, limpio y seguro.

1 – Acumulador de presión
2 – Acumulador de freno
3 – Acumulador de freno de estacionamiento
4 – Depósito hidráulico
5 – Bomba hidráulica
6 – Cilindro de accionamiento tren principal
7 – Cilindro de accionamiento tren delantero
8 – Cilindro de accionamiento flaps



OXIGENO

El circuito de oxígeno de avión I.A. 58 "PUCARA" se compone de los siguientes elementos:
Un convertidor, una válvula combinada de venteo, y carga, un evaporador, dos reguladores de oxígeno, dos máscaras con tubos flexibles, un indicador de cantidad y una luz de alarma falta de oxígeno.
El oxígeno líquido que pasa por el evaporador en forma de serpentín, se gasifica tomando la temperatura ambiente. El oxígeno gaseoso es conducido por las cañerías hasta los paneles reguladores de piloto y copiloto, partiendo posteriormente hacia las conexiones de los asientos, pasando por los tubos flexibles a las máscaras, según la de mando.
Además de este sistema, se dispone de una botella de oxigeno gaseoso ubicada en cada uno de los asientos piloto y copiloto accionadas estas por un mecanismo especial. Su utilización se requiere en caso de fallas en el sistema normal de oxígeno en el avión y al producirse la eyección del asiento.



1 – Boca de carga
2 – Convertidor
3 – Vaporizador de oxígeno
4 – Regulador oxígeno avión
5 – Conector de desprendimiento rápido
6 – Máscara de oxígeno

CABINA

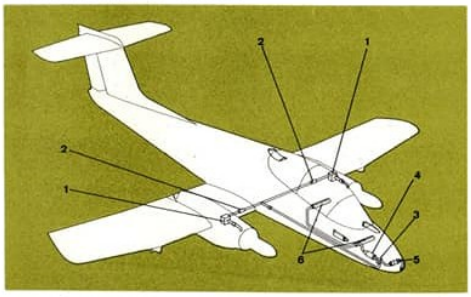
La espaciosa dimensión de la cabina del I.A. 58 PUCARA, combinada con una adecuada distribución de los equipos e instrumentos, permite que el pilotaje del avión resulte confortable.
En la cabina, los asientos eyectables del piloto y copiloto, se hallan dispuestos en tandem. El asiento del copiloto está 25 cm. más alto que el del piloto lo cual, unido al diseño de proa (que es baja y corta), y al tamaño de la cúpula de plexiglás, permite un excelente ángulo de visibilidad para ambos tripulantes. Dos espejos retrovisores, ubicados en el puesto de pilotaje, amplían la visibilidad hacia la parte posterior del avión.
Los controles de vuelo y otros equipos, están duplicados o intercomunicados.
Un sistema efectivo y completo asegura un nivel óptimo de iluminación del instrumental en todas las condiciones de vuelo.
El acceso a la cabina se realiza mediante un apoya-pie accionado automáticamente al abrir la cúpula. Esta es a su vez accionada en forma electromecánica o manual, tanto desde la cabina como desde el exterior.
El blindaje de la cabina está constituído por el parabrisas y el piso, capaces de anular el efecto de impactos directos de armas hasta calibre 7,62 mm. (0,3") desde una distancia de 150 mts.

VENTILACION Y CALEFACCION

El I.A. 58 PUCARA cuenta con un doble sistema de ventilación de cabina que permite mantener en la misma un ambiente confortable, aún en los casos en que la temperatura exterior sea del orden de los –50ºC.
Para ello, en la zona del fuselaje delantero, se han instalado tomas de aire exterior, regulables manualmente, en casos de vuelos con temperatura ambiente templada.

El sistema de calefacción toma aire caliente de la zona del compresor de motores, lo conduce a un mezclador, donde se le agrega aire exterior proveniente de tomas dinámicas. La entrada del aire frío exterior es regulable a voluntad. En este circuito se han previsto filtros, tanto para el aire caliente como para el aire frío y válvulas antirretorno para impedir el paso de aire a presión de un motor a otro, en el caso de que uno de ellos no esté operando. El aire así mezclado, ingresa en la cabina, asegurándose un renovación permanente con una ventilación regulable, ubicada en la parte posterior de dicha cabina.

1 - Válvula de corte
2 - Válvula Anti-retorno
3 - Válvula de regulación
4 - Caja mezcladora
5 - Filtro
6 - Distribuidores



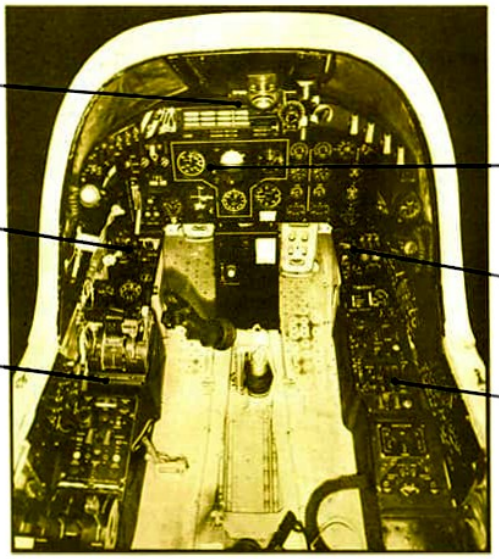
INSTRUMENTAL, EQUIPAMIENTO RADIOELECTRICO Y ALARMAS

La elección de los equipos del I.A. 58 "PUCARA", se ha efectuado con el fin de cumplir con los requisitos operativos, tanto en el campo de batalla como en áreas donde las ayudas terrestres para la navegación son limitadas.
Con respecto al instrumental de navegación, además de los instrumentos normales de vuelo, (todos ellos son indicadores) para piloto y copiloto) se han previsto dos horizontes artificiales,con plataforma giroscópica independiente ubicada cercana al centro de gravedad del avión, lo que permite mayor precisión de indicación y más larga vida del instrumento.
Cuenta con un equipo VOR/LOC/ILS y un equipo radiogoniómetro ADF (ambos con controles e indicadores en ambas cabinas), un girocompás cuya indicación se tiene a través del RMI y, complementariamente, un compás magnético.
El instrumental ha sido adecuadamente distribuido en seis tableros independientes a saber:

1) Tablero Principal Central.
2) Tablero Principal Superior.
3) Tablero Inferior Derecho.
4) Tablero Inferior Izquierdo.
5) Tablero Lateral Derecho.
6) Tablero Lateral Izquierdo.

Los mismos han sido diseñados de tal manera, que permite una perfecta lectura y rápida identificación, habiéndoselo dotado de iluminación indirecta para vuelos nocturnos, con dispositivos que atenúan, optativamente, su intensidad por sectores.

IA 58 pucará



INSTRUMENTAL

1. INSTRUMENTOS DE CONTROL DE VUELO

* Variómetro
* Altímetro
* Velocímetro
* Indicador de giros y virajes
* Horizonte artificial
* Acelerómetro

2. INSTRUMENTOS Y EQUIPOS PARA CONTROL DE LA NAVEGACION

* VOR/LOC/ILS (equipo, controles e indicadores duplicados)
* Radiogoniómetro A.D.F. (equipos, controles e indicadores duplicados).
* Compás magnético.
* Giro compás (equipo, controles e indicadores duplicados).

3. EQUIPOS DE COMUNICACIONES

* V.H.F. (equipos con controles duplicados).
* H.F. (equipos con controles duplicados).
* Intercomunicador.
* IFF (opcional).

4. INSTRUMENTOS DE CONTROL DEL SISTEMA DE PROPULSION

* Taquímetro.
* Temperatura de aceite.
* Indicador de temperatura de gases de escape.
* Indicador de torque.
* Indicador de cantidad de combustible (dobles).
* Indicador de temperatura de combustible (doble).
* Indicador de consumo de combustible.
* Indicador de paso de hélices.
* Tablero de alarma contra incendio.
* Luces de alarma:
  - Paso mínimo de vuelo.
  - Prohibición de decolar.
  - Falla en la presión de aceite.
  - Filtro de combustible saturado.
  - Falta de presión de combustible.
  - Falla de potencia.
  - Bomba de hélice.
  - Vuelo invertido.

5. INDICADORES SISTEMA HIDRAULICO

* Indicador posición de tren.
* Indicador posición de flaps.
* Manómetro triple de freno.
* Manómetro de presión hidráulica.

6. INDICADORES VARIOS

* Indicador sistema de oxígeno.
* Voltímetro C.C.
* Alarma falla C.A.
* Termómetro aire exterior.
* Indicador de compensadores.
* Luces de alarma de:
  - Circuito de armamento activado.
  - Bandera automática.
  - Arranque.
  - Robinete.
  - Bloqueo.
  - Generador.
  - Cúpula destrabada.
  - Emergencia cúpula.

IA 58 pucará

FABRICA MILITAR DE AVIONES

CORDOBA · ARGENTINA

comunicar
Belgrano 527 - CBA

FABRICA MILITAR DE AVIONES

Avda. Fuerza Aérea Argentina – Km. 5 1/2
5103 CORDOBA - R. ARGENTINA
Tel. 45011/15
Télex: AMCOR - AR 51965