

Guía de Seguridad de las TIC CCN-STIC 1654

Guía de configuración

iOS 18 (iPhone 13, iPhone 14, iPhone 14 Plus, iPhone 14 Pro, iPhone 14 Pro Max, iPhone 15, iPhone 15 Plus, iPhone 15 Pro, iPhone 15 Pro Max, iPhone 16, iPhone 16 Plus, iPhone 16 Pro, iPhone 16 Pro Max, iPhone 16e)



Noviembre 2025

Edita:



Centro Criptológico Nacional, 2025

Fecha de publicación: Noviembre 2025

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

ÍNDICE.....	2
ÍNDICE DE TABLAS	3
ÍNDICE DE FIGURAS	3
1. INTRODUCCIÓN	4
1.1 DESCRIPCIÓN DEL PRODUCTO	4
2. OBJETIVO Y ALCANCE	5
2.1 PLATAFORMAS HARDWARE	5
3. ORGANIZACIÓN DEL DOCUMENTO	15
4. FASE DE INSTALACIÓN.....	16
4.1 REQUISITOS	16
4.2 ENTREGA SEGURA DE DISPOSITIVOS	16
4.2.1 ADQUISICIÓN DE DISPOSITIVOS MÓVILES.	16
4.3 VERIFICACIÓN DEL DISPOSITIVO.	16
4.3.1 BÚSQUEDA EN EL DISPOSITIVO	17
4.4 REGISTRAR DISPOSITIVOS EN MDM	18
4.4.1 CONFIGURACIÓN DE MDM.	18
4.4.2 REGISTRAR DISPOSITIVOS MÓVILES EN LA CONFIGURACIÓN DE GESTIÓN.....	19
4.4.3 INSTALAR PERFIL DE CONFIGURACIÓN EN IOS	20
4.4.4 CONFIGURAR EL AGENTE MDM Y LAS COMUNICACIONES MDM	20
4.4.5 PREVENCIÓN ANTE LA BAJA DE UN DISPOSITIVO	21
5. FASE DE CONFIGURACIÓN	22
5.1 RESTRICCIONES GENERALES.	22
5.2 VPN.....	23
5.3 WLAN.....	25
5.4 PROTECCIÓN DE DATOS	25
5.4.1 CÓDIGO DE ACCESO	26
5.4.2 ELIMINACIÓN DE LA PROTECCIÓN DE DATOS.....	27
6. REFERENCIAS	28
7. ABREVIATURAS	29
8. ANEXO I. PERFILES DE CONFIGURACIÓN.	30
8.1 PERFIL DE CONFIGURACIÓN 1: "PERFIL DE CONFIGURACIÓN MDF PP PARA AIRPRINT"	30
8.2 PERFIL DE CONFIGURACIÓN 2: "PERFIL DE CONFIGURACIÓN DE MDF PP PARA RESTRICCIONES GENERALES"	31
8.3 PERFIL DE CONFIGURACIÓN 3: "PERFIL DE CONFIGURACIÓN MDF PP PARA RESTRICCIONES DE CONTRASEÑA"	33
8.4 PERFIL DE CONFIGURACIÓN 4: "PERFIL DE CONFIGURACIÓN MDF PP PARA VPN"	35

ÍNDICE DE TABLAS

Tabla 1. Mapeo de Soc a ISA.....	5
Tabla 2. Modelos de iPhone incluidos en la certificación	14
Tabla 3. Payloads de Restricciones.....	22
Tabla 4. Payloads para VPN.....	25
Tabla 5. WLAN Ciphersuites	25
Tabla 6. Payloads para contraseñas	26

ÍNDICE DE FIGURAS

Figura 1. Identificación del modelo.....	17
Figura 2. Identificación del modelo en el dispositivo (bandeja SIM)	17
Figura 3. Identificación del modelo en el dispositivo (conector de carga)	18
Figura 4. Entorno de Operación del TOE.....	18

1. INTRODUCCIÓN

1. El propósito de este documento es proporcionar una guía sobre cómo configurar los dispositivos iPhone 13, iPhone 14, iPhone 14 Plus, iPhone 14 Pro, iPhone 14 Pro Max, iPhone 15, iPhone 15 Plus, iPhone 15 Pro, iPhone 15 Pro Max, iPhone 16, iPhone 16 Plus, iPhone 16 Pro, iPhone 16 Pro Max, iPhone 16e con iOS 18 que han sido calificados por CPSTIC y se enumeran en el Catálogo de productos de CPSTIC (cpstic.ccn.es).

1.1 DESCRIPCIÓN DEL PRODUCTO

2. Los dispositivos iPhone 13, iPhone 14, iPhone 14 Plus, iPhone 14 Pro, iPhone 14 Pro Max, iPhone 15, iPhone 15 Plus, iPhone 15 Pro, iPhone 15 Pro Max, iPhone 16, iPhone 16 Plus, iPhone 16 Pro, iPhone 16 Pro Max, iPhone 16e con iOS 18 están destinados a ser utilizados como una solución de comunicaciones que proporciona conectividad móvil para el personal a los datos de la empresa.
3. Para esta comunicación, se requiere un dispositivo móvil Apple iPhone (modelo iPhone 13, iPhone 14, iPhone 14 Plus, iPhone 14 Pro, iPhone 14 Pro Max, iPhone 15, iPhone 15 Plus, iPhone 15 Pro, iPhone 15 Pro Max, iPhone 16, iPhone 16 Plus, iPhone 16 Pro, iPhone 16 Pro Max, iPhone 16e) y el propio sistema operativo, que se identifica como el software por su número de versión (iOS 18).
4. El producto proporciona conectividad inalámbrica e incluye soporte para agentes de administración de dispositivos móviles (MDM), conexiones de red privada virtual (VPN), cliente WLAN, Bluetooth, factores de autenticación biométrica (BAF), acceso a la red empresarial protegida, datos y aplicaciones empresariales, y comunicación con otros dispositivos móviles iPhone de Apple.
5. El sistema operativo (iOS 18) gestiona el hardware del dispositivo y proporciona las tecnologías necesarias para desplegar aplicaciones nativas (también conocidas como apps). Una aplicación nativa es una aplicación compilada para ejecutarse en una plataforma móvil específica. El TOE OS también proporciona una interfaz de programación de aplicaciones (API) denominada como marco MDM, que ofrece funciones de administración que pueden ser utilizadas por soluciones MDM de terceros, lo que permite a las empresas usar perfiles para controlar algunas de las configuraciones del dispositivo.
6. El producto puede utilizarse como un dispositivo móvil dentro de un entorno empresarial en el que la configuración del dispositivo se gestiona a través de una solución MDM.

2. OBJETIVO Y ALCANCE

2.1 PLATAFORMAS HARDWARE

8. Esta sección enumera los dispositivos cubiertos por esta certificación. Se proporcionan las características técnicas de cada dispositivo, incluida la arquitectura del conjunto de instrucciones, también conocida como microarquitectura.

Soc	ISA
A15 Biónico	ARMv8.6-A
A16 Biónico	
A17 Pro	
A18	ARMv9.2-A
A18 Pro	ARMv9.2-A

Tabla 1 Mapeo de Soc a ISA

Información del dispositivo	N.º de modelo	Celular
iPhone 13 BAF: Face ID (GEN.2) BT: 5.0 NFC: Tenedores SÁBADO: No Soc: A15 Biónico UWB: 6 GHz – 8,5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) con 2.2 MIMO Núcleo: 4387	A2482	5G (sub-6 GHz y mmWave) con MIMO 4x4 Gigabit LTE con 4x4 MIMO y LAA 5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) CDMA EV DO Rev. A (800, 1900 MHz) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2631	5G (sub-6 GHz y mmWave) con MIMO 4x4 Gigabit LTE con 4x4 MIMO y LAA 5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) CDMA EV DO Rev. A (800, 1900 MHz) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2633	5G (sub-6 GHz y mmWave) con MIMO 4x4 Gigabit LTE con 4x4 MIMO y LAA 5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n38, n40, n41, n66, n71, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA/HSPA+/DC HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2634	5G (sub-6 GHz y mmWave) con MIMO 4x4 Gigabit LTE con 4x4 MIMO y LAA 5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n30, n38, n40, n41, n48, n66, n77, n78, n79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2635	5G (sub-6 GHz y mmWave) con MIMO 4x4

		Gigabit LTE con 4x4 MIMO y LAA 5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n30, n38, n40, n41, n48, n66, n77, n78, n79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
iPhone 14 BAF: Face ID (GEN.2) BT: 5.3 NFC: Tenedores SÁBADO: Tenedores Soc: A15 Biónico UWB: 6 GHz – 8,5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) con 2.2 MIMO Núcleo: 4387	A2649	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con MIMO 4x4 5G, LTE de clase Gigabit con MIMO 4x4 y LAA
	A2881	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con MIMO 4x4 5G, LTE de clase Gigabit con MIMO 4x4 y LAA
	A2882	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n77, n78, n79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (bandas 34, 38, 39, 40, 41, 42, 46, 48, 53); UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2883	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2884	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
iPhone 14 Plus BAF: Face ID (GEN.2) BT: 5.3 NFC: Tenedores SÁBADO: Tenedores Soc: A15 Biónico UWB: 6 GHz – 8,5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) con 2.2 MIMO Núcleo: 4387	A2632	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con MIMO 4x4 5G, LTE de clase Gigabit con MIMO 4x4 y LAA
	A2885	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)

		GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con MIMO 4x4 5G, LTE de clase Gigabit con MIMO 4x4 y LAA
	A2886	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2887	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2888	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
iPhone 14 Pro BAF: Face ID (GEN.2) BT: 5.3 NFC: Tenedores SÁBADO: Tenedores Soc: A16 Biónico UWB: 6 GHz – 8,5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) con 2.2 MIMO Núcleo: 4387	A2650	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con MIMO 4x4 5G, LTE de clase Gigabit con MIMO 4x4 y LAA
	A2889	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con MIMO 4x4 5G, LTE de clase Gigabit con MIMO 4x4 y LAA
	A2890	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n77, n78, n79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (bandas 34, 38, 39, 40, 41, 42, 46, 48, 53); UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2891	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2892	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
iPhone 14 Pro Max BAF: Face ID (GEN.2) BT: 5.3	A2651	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261)

NFC: Tenedores SÁBADO: Tenedores Soc: A16 Biónico UWB: 6 GHz – 8,5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) con 2.2 MIMO Núcleo: 4387		FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con MIMO 4x4 5G, LTE de clase Gigabit con MIMO 4x4 y LAA
	A2893	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con MIMO 4x4 5G, LTE de clase Gigabit con MIMO 4x4 y LAA
	A2894	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n77, n78, n79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (bandas 34, 38, 39, 40, 41, 42, 46, 48, 53); UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2895	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A2896	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
iPhone 15 BAF: Face ID (GEN.2) BT: 5.3 NFC: Tenedores SÁBADO: Tenedores Soc: A16 Biónico UWB: 6 GHz – 8,5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) con 2.2 MIMO Núcleo: 4387	A2846	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n75, n76, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3089	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n75, n76, n77, n78, n79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3090	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n53, n66, n70, n77, n78, n79)

		FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3092	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
iPhone 15 Plus BAF: Face ID (GEN.2) BT: 5.3 NFC: Tenedores SÁBADO: Tenedores Soc: A16 Biónico UWB: 6 GHz – 8,5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) con 2.2 MIMO Núcleo: 4387	A2847	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n75, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3093	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n75, n76, n77, n78, n79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3094	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n53, n66, n70, n77, n78, n79) FDD-LTE (bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (bandas 34, 38, 39, 40, 41, 42, 46, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3096	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
iPhone 15 Pro BAF: Face ID (4.ª generación) BT: 5.3 NFC : Sí SAT : Sí SoC : A17 Pro UWB: 6 GHz-8,5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) con 2.2 MIMO	A2848	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, N40, N41, N48, N53, N66, N70, N71, N75, N76, N77, N78, N79) 5G NR mmWave (Bandas n258, n260, n261) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)

Núcleo: 4388		GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3101	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, N40, N41, N48, N53, N66, N70, N71, N75, N76, N77, N78, N79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3102	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, N48, N53, N66, N70, N77, N78, N79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3104	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, N48, N66, N70, N77, N78, N79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
iPhone 15 Pro Max BAF: Face ID (4.ª generación) BT: 5.3 NFC : Sí SAT : Sí SoC : A17 Pro UWB: 6 GHz-8,5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) con 2.2 MIMO Núcleo: 4388	A2849	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, N40, N41, N48, N53, N66, N70, N71, N75, N76, N77, N78, N79) 5G NR mmWave (Bandas n258, n260, n261) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3105	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, N40, N41, N48, N53, N66, N70, N71, N75, N76, N77, N78, N79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3106	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, N48, N53, N66, N70, N77, N78, N79) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48, 53)

		UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3108	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, N48, N66, N70, N77, N78, N79) FDD LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD LTE (Bandas 34, 38, 39, 40, 41, 42, 46, 48) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
iPhone 16 BAF: Face ID (4.ª generación) BT: 5.3 NFC : Sí SAT : Sí SoC : A18 UWB: 6 GHz-8,5 GHz Wi-Fi: Wi-Fi 7 (802.11be) con 2.2 MIMO Núcleo: 4388	A3081	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3288	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3287	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3286	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
iPhone 16 Plus	A3082	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76)

BAF: Face ID (4.ª generación) BT: 5.3 NFC : Sí SAT : Sí SoC : A18 UWB: 6 GHz-8,5 GHz Wi-Fi: Wi-Fi 7 (802.11be) con 2.2 MIMO Núcleo: 4388		TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3291	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3290	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3289	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
iPhone 16 Pro BAF: Face ID (4.ª generación) BT: 5.3 NFC : Sí SAT : Sí SoC : A18 Pro UWB: 6 GHz-8,5 GHz Wi-Fi: Wi-Fi 7 (802.11be) con 2.2 MIMO Núcleo: 4388	A3083	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3294	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261)

		FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3293	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3292	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
iPhone 16 Pro Max BAF: Face ID (4.ª generación) BT: 5.3 NFC : Sí SAT : Sí SoC : A18 Pro UWB: 6 GHz-8,5 GHz Wi-Fi: Wi-Fi 7 (802.11be) con 2.2 MIMO Núcleo: 4388	A3084	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3297	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3296	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71)

		TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
	A3295	DD-5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n66, n70, n71, n75, n76) TDD-5G NR (Bandas n38, n40, n41, n48, n53, n77, n78, n79) 5G NR mmWave (Bandas n258, n260, n261) FDD-LTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDD-LTE (Bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz) 5G (sub-6 GHz y mmWave) con 4x4 MIMO11 Gigabit LTE con 4x4 MIMO11
iPhone 16e BAF: Face ID (4.ª generación) BT: 5.3 NFC : Sí SAT : Sí SoC : A18 UWB: No Wi-Fi: Wi-Fi 6 (802.11ax) con 2.2 MIMO Núcleo: 4388	A3212	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n75, n76, n77, n78, n79) FDDLTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDLTE (bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+ (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3410	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n75, n76, n77, n78, n79) FDDLTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDLTE (bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+ (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3409	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n75, n76, n77, n78, n79) FDDLTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDLTE (bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+ (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)
	A3408	5G NR (Bandas n1, n2, n3, n5, n7, n8, n12, n14, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n53, n66, n70, n71, n75, n76, n77, n78, n79) FDDLTE (Bandas 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TDLTE (bandas 34, 38, 39, 40, 41, 42, 48, 53) UMTS/HSPA+ (850, 900, 1700/2100, 1900, 2100 MHz) GSM/EDGE (850, 900, 1800, 1900 MHz)

Tabla 2 Modelos de iPhone incluidos en la certificación

3. ORGANIZACIÓN DEL DOCUMENTO

Este documento consta de las siguientes secciones:

- a) Sección 4. Esta sección incluye aspectos y recomendaciones a considerar antes de proceder con la instalación del producto.
- b) Sección 5. Esta sección contiene recomendaciones a tener en cuenta durante la fase de configuración del producto.
- c) Anexo I. Esta sección muestra los perfiles de configuración que un usuario puede implementar en dispositivos iPhone utilizando una solución MDM.

4. FASE DE INSTALACIÓN

4.1 REQUISITOS

9. Antes de integrar los dispositivos móviles a la red, se recomienda diseñar e implementar una solución MDM, la cual ayudará al administrador a configurar y gestionar estos dispositivos. Existen diversas soluciones MDM para lograr este propósito. También se recomienda diseñar e implementar una puerta de enlace VPN siguiendo la sección “Descripción general de VPN para la implementación de dispositivos Apple” de **[¡Error! No se encuentra el origen de la referencia.]**, para asegurar la comunicación con los dispositivos.
10. Si los dispositivos utilizan certificados x509 para autenticarse en la conexión VPN, la organización debe implementar una PKI, que incluya una CA de confianza tanto para la pasarela VPN como para el dispositivo, así como un responder OCSP o una lista de revocación de certificados (CRL) para gestionar las solicitudes de verificación de revocación.

4.2 ENTREGA SEGURA DE DISPOSITIVOS

11. Los dispositivos móviles probados están destinados a usuarios autorizados de organizaciones empresariales y organismos gubernamentales.
12. El administrador de dispositivos móviles es responsable de realizar la configuración necesaria para garantizar que los dispositivos estén configurados de acuerdo con las especificaciones de la certificación.

4.2.1 ADQUISICIÓN DE DISPOSITIVOS MÓVILES.

13. Apple tiene canales dedicados para ventas a empresas y gobiernos, incluyendo operadores móviles autorizados y revendedores autorizados de Apple. Es importante destacar que estos proveedores pueden inscribir automáticamente los dispositivos en Apple Business Manager.

4.3 VERIFICACIÓN DEL DISPOSITIVO.

14. Al recibir los dispositivos móviles, se debe verificar el número de modelo para asegurar que coincida con los listados en la Tabla 2 Modelos de iPhone incluidos en la **[¡Error! No se encuentra el origen de la referencia.]**. Buscar en Configuración.
15. Para identificar el número de modelo, en la aplicación de Configuración, seleccione “General” → “Información”. A la derecha del número de modelo, encontrará el número de pieza. Toque el número de pieza para ver el número de modelo.

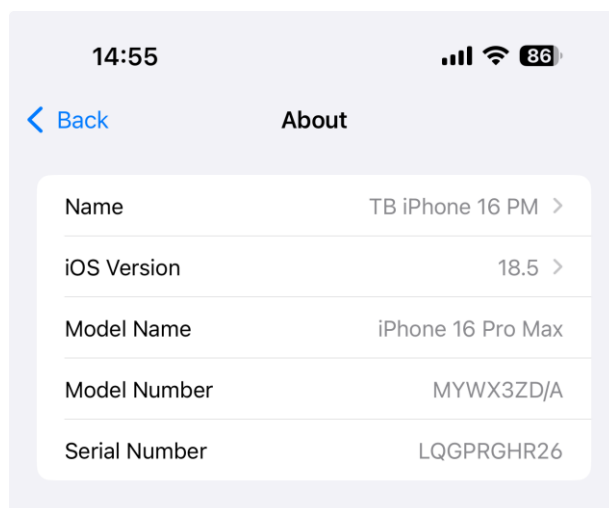


Figura 1 Identificación del modelo.

Las instrucciones se dan en esta página <https://support.apple.com/es-es/106343>.

4.3.1 BÚSQUEDA EN EL DISPOSITIVO

16. Para encontrar el número de modelo en un iPhone, podemos hacerlo de dos maneras dependiendo del modelo:

- Para encontrar el número de modelo en un iPhone 8 o posterior que tenga una bandeja SIM, retire la bandeja SIM y mire en la ranura. Asegúrese de estar en un lugar con buena iluminación para poder verlo. El número de modelo se encuentra en la parte superior, en el lado de la pantalla.



Figura 2 Identificación del modelo en el dispositivo (bandeja SIM)

- a) Los modelos de iPhone que solo admiten eSIM no tienen bandeja SIM. Para encontrar el número de modelo, búsquelo en el conector Lightning o USB-C. Asegúrate de estar en una luz brillante para que puedas verlo. Busque el número de modelo en la parte superior del conector, en el lado de la pantalla.



Figura 3 Identificación del modelo en el dispositivo (conector de carga)

Las instrucciones se muestran en esta página <https://support.apple.com/es-es/106343>.

4.4 REGISTRAR DISPOSITIVOS EN MDM

4.4.1 CONFIGURACIÓN DE MDM.

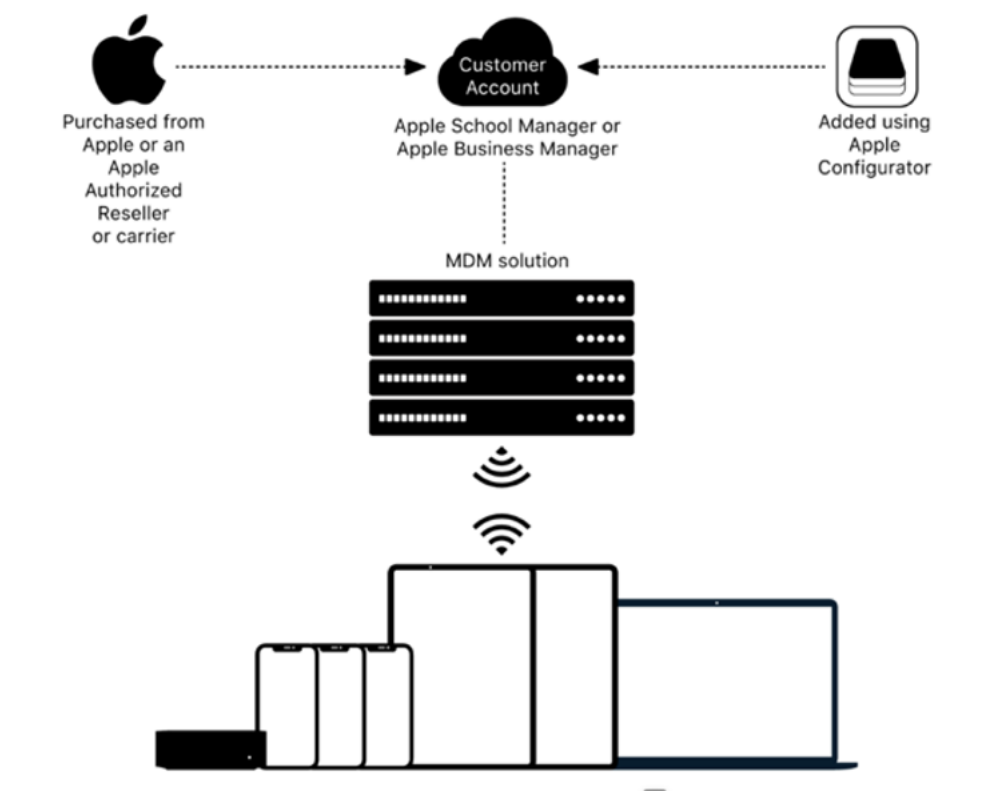


Figura 4. Entorno de Operación del TOE.

17. El entorno operativo básico para el TOE consiste en el dispositivo móvil iPhone y una solución MDM como el entorno operativo requerido para que el TOE funcione correctamente. Esto se puede ver en la Figura 4. Entorno de Operación del TOE.**Error! No se encuentra el origen de la referencia..**
18. Un usuario típico usaría el TOE directamente al interactuar físicamente con él. En este caso, el usuario utilizaría un iPhone 16 con iOS 18 o cualquiera de los modelos definidos en la Tabla 2 Modelos de iPhone incluidos en la que ejecuten iOS 18.

19. La solución MDM proporciona una forma para que el dispositivo aplique configuraciones de manera asincrónica e informe su estado a los servidores. Las capacidades de gestión de seguridad son proporcionadas a la organización a través de la solución MDM, aplicando actualizaciones de software, desplegando configuraciones y manteniendo una vista actualizada de todos los dispositivos gestionados. Solo las instancias inscritas pueden ser gestionadas por la solución MDM.
20. Se requiere que un administrador configure el TOE para que opere de acuerdo con los requisitos definidos en este documento. La configuración evaluada consiste en lo siguiente:
 - Se debe establecer un código de acceso para la autenticación del usuario.
 - Se define una política de códigos de acceso que especifica criterios de longitud mínima y complejidad.
 - Se define un número máximo de intentos fallidos consecutivos para ingresar el código de acceso.
 - Se define una política de bloqueo de sesión.
 - Especificaciones para los dispositivos permitidos de recopilación de audio y video.
21. Especificación de conexiones VPN.
 - Se define una política para el almacenamiento externo a través de un conector de dispositivo.
22. Para garantizar que los dispositivos estén configurados para cumplir con los requisitos de esta evaluación CPSTIC, los dispositivos deben configurarse en modo supervisado. Consulte: <https://support.apple.com/en-us/guide/deployment/dep1d89f0bff/web>

4.4.2 REGISTRAR DISPOSITIVOS MÓVILES EN LA CONFIGURACIÓN DE GESTIÓN

23. Los dispositivos móviles generalmente se gestionan mediante una solución MDM. El proceso para hacerlo varía dependiendo de la solución MDM elegida por la organización que despliega los dispositivos, y corresponde al administrador de dispositivos móviles determinar los pasos detallados según la solución MDM seleccionada por la organización. Los dispositivos móviles se configuran utilizando los Perfiles de Configuración especificados por el administrador de dispositivos móviles y se despliegan en los dispositivos.
24. Apple proporciona una guía y más detalles en los siguientes enlaces:
<https://support.apple.com/es-es/guide/deployment/depc0aadd3fe/web>
<https://support.apple.com/es-es/guide/deployment/dep23db2037d/web>

25. Se recomienda utilizar Apple Business Manager (ABM) para el registro en MDM. Apple Business Manager es un portal web sencillo para administradores de TI. Se integra con soluciones de gestión de dispositivos móviles (MDM) de terceros, lo que te permite comprar contenido de manera masiva con facilidad.
26. Con Apple Business Manager, puedes automatizar el registro en MDM y simplificar la configuración inicial de los dispositivos sin tener que tocarlos ni prepararlos antes de que lleguen a los usuarios. Puedes registrar automáticamente los dispositivos en tu solución MDM preferida, siempre que el dispositivo haya sido agregado a tu organización en el momento de la compra, ya sea desde Apple, un operador móvil autorizado, un revendedor autorizado de Apple o a través de Apple Configurator. Para más información, consulta: <https://support.apple.com/en-us/guide/apple-business-manager/axm7909096bf/web>
27. La Inscripción Automatizada de Dispositivos está diseñado para todos los dispositivos Apple propiedad de la organización. La Inscripción Automatizado de Dispositivos permite a las organizaciones configurar y gestionar los dispositivos directamente desde la caja. También puedes usar todas las cargas útiles y restricciones disponibles definidas por Apple, y tienes la opción de evitar que el usuario elimine el perfil de registro en la solución de gestión de dispositivos móviles (MDM). Para más información, consulta: <https://support.apple.com/es-es/guide/deployment/dep73069dd57/web>

4.4.3 INSTALAR PERFIL DE CONFIGURACIÓN EN IOS

28. Muchos aspectos de la funcionalidad de seguridad del iPhone se configuran utilizando Perfiles de Configuración que se instalan en los dispositivos móviles. Los Perfiles de Configuración son archivos XML (Extensible Markup Language) que permiten la distribución de información de configuración a los dispositivos móviles. Pueden contener ajustes para varios parámetros configurables en el dispositivo móvil.
29. La planificación de perfiles de configuración y payloads ayuda a reducir la complejidad. Para optimizar la gestión del payload, siga las prácticas recomendadas de gestión de dispositivos móviles (MDM) antes de empezar a desplegar perfiles de configuración, como se explica en <https://support.apple.com/es-es/guide/deployment/dep9a318a393/web>

4.4.4 CONFIGURAR EL AGENTE MDM Y LAS COMUNICACIONES MDM

30. Al instalar y configurar tu solución MDM, considera cómo configurarás la red, Transport Layer Security (TLS), los servicios de infraestructura, los servicios de Apple y las copias de seguridad.
31. Cuando instalas una solución MDM alojada localmente, debes configurar todos los siguientes elementos:

- Usar un nombre de dominio completamente calificado (FQDN).
 - Tener una dirección IP estática.
 - Configurar el MDM con Transport Layer Security.
 - Mantener ciertos puertos del firewall abiertos.
32. Configura y prueba cada uno de estos elementos desde el principio del proceso para garantizar un despliegue sin problemas. Si tu solución MDM es gestionada externamente o está alojada en la nube, tu proveedor de MDM podría encargarse de muchos de estos elementos en tu nombre. Para más información, consulta <https://support.apple.com/es-es/guide/deployment/dep2bcde692e/web>

4.4.5 PREVENCIÓN ANTE LA BAJA DE UN DISPOSITIVO

33. Durante el proceso de inscripción, se carga en el dispositivo móvil un Perfil de Configuración que incluye un MDM Payload y se utiliza para asociar el dispositivo móvil a un Servidor MDM. Si se elimina el MDM Payload, el dispositivo móvil dejará de estar inscrito en el servidor MDM.
34. Para evitar la anulación de la inscripción de dispositivos, la opción más eficaz es utilizar la inscripción automatizada de dispositivos, que es una función de Apple Business Manager descrita en la sección 4.4.2.
35. Para más información sobre "Volver a inscribir dispositivos en MDM", consulta: <https://support.apple.com/en-us/guide/deployment/dep26505df5d/1/web/1.0>

5. FASE DE CONFIGURACIÓN

36. Esta sección ofrece una guía más detallada sobre cómo configurar dispositivos móviles supervisados para cumplir con los requisitos de la evaluación CPSTIC.
37. Esta sección detalla los valores clave del diccionario que deben usarse o dónde ciertas opciones para el valor clave no están permitidas.
38. Para las claves de diccionario no mencionadas en este documento, consulta las políticas de seguridad de la organización que realiza el despliegue.

5.1 RESTRICCIONES GENERALES.

39. A continuación, se presentan las claves esenciales para los Payloads de Restricciones

Carga útil	Pista	Descripción
Restricciones generales		
Restrictions	<i>allowAssistant</i>	Debe fijarse en 'false'. (Se recomienda no tener Siri activado en los ajustes de CPSTIC)
Restrictions	<i>allowAssistantUserGeneratedContent</i>	Debe fijarse en 'false'. (Se recomienda no tener Siri activado en los ajustes de CPSTIC)
Restrictions	<i>allowAssistantWhileLocked</i>	Debe fijarse en 'false'. (Se recomienda no tener Siri activado en los ajustes de CPSTIC)
Restrictions	<i>allowLockScreenControlCenter</i>	Debe fijarse en 'false'.
Restrictions	<i>allowEnablingRestrictions</i>	Debe fijarse en 'false'.
Restrictions	<i>allowUSBRestrictedMode</i>	Debe fijarse en 'true'.
Restrictions	<i>allowCloudDocumentSync</i>	Debe fijarse en 'false'. Esto desactiva la sincronización de Documentos y Valores clave con iCloud.
Restrictions	<i>forceAutomaticDateAndTime</i>	Debe fijarse en 'false'. (Se recomienda no tener Siri activado en los ajustes de CPSTIC)
Configuración de TLS/HTTPS		
Restrictions	<i>allowUntrustedTLSPrompt</i>	Debe fijarse en 'false'
Restrictions	<i>forceAirPrintTrustedTLSRequirement</i>	Debe fijarse en 'true'
Bluetooth		
Restrictions	<i>allowBluetoothModification</i>	Debe fijarse en 'true'

Tabla 3Payloads de Restricciones.

5.2 VPN

40. Para las conexiones VPN que usan IKEv2, el algoritmo de integridad a utilizar lo puede seleccionar el administrador de los dispositivos móviles configurando la clave IntegrityAlgorithm en la carga útil de VPN. Es importante destacar que configurar IntegrityAlgorithm en 'SHA1-96' no está permitido en la configuración evaluada.
41. El administrador de los dispositivos móviles utiliza los VPN Payloads para configurar un sistema VPN basado en IPsec a nivel de sistema, especificar la configuración de Internet Key Exchange Version 2 (IKEv2) y definir atributos como:
 - La configuración "AlwaysOn" de la VPN.
 - El método de autenticación mediante certificado.
 - Certificados definidos por el administrador.
42. La VPN "AlwaysOn" debe habilitarse configurando la clave VPNTType a 'AlwaysOn' en el Perfil de Configuración. Cuando se selecciona 'AlwaysOn' como VPNTType para un Perfil de Configuración, la clave correspondiente ProtocolType debe configurarse como 'IKEv2'. La matriz Interfaces, que enumera las interfaces a las que se aplica una configuración específica de VPN "AlwaysOn", puede especificarse opcionalmente como 'Cellular, WiFi' (valor predeterminado), 'Cellular' o 'WiFi'.
43. IKEv2 debe configurarse utilizando las claves del diccionario IKEv2. El administrador de los dispositivos móviles debe especificar la dirección IP o el nombre de host del servidor VPN a través de RemoteAddress, el identificador del cliente a través de LocalIdentifier, el identificador remoto a través de RemoteIdentifier, el método de autenticación como 'Certificate' a través de AuthenticationMethod, y el certificado que se utilizará para la autenticación a través de PayloadCertificateUUID.
44. Se pueden configurar claves opcionales que permitan:
 - Habilitar la autenticación extendida a través de ExtendedAuthEnabled.
 - Especificar un nombre de usuario y una contraseña a través de AuthName y AuthPassword.
 - Especificar el intervalo durante el cual se mantiene viva la conexión cuando no se puede alcanzar el par a través de DeadPeerDetectionRate.
 - Especificar el Nombre Común del emisor del certificado del servidor y/o el Nombre Común de tu certificado del servidor a través de ServerCertificateIssuerCommonName y ServerCertificateCommonName.
 - Especificar los IKESecurityAssociationParameters y ChildSecurityAssociationParameters, los cuales permiten una mayor especificación de un EncryptionAlgorithm, un IntegrityAlgorithm y un DiffieHellmanGroup, tal como se describe en la Tabla 13: Claves Esenciales para la Protección de Datos.
45. Para más información, consultar: <https://support.apple.com/en-gb/guide/deployment/depae3d361d0/web>

Carga útil	Llave (Clave)	Descripción
VPN	<i>VPNType</i>	Debe fijarse en 'AlwaysOn'.
VPN	<i>OnDemandEnabled</i>	Debe fijarse en '0'.
IKEv2 Dictionary Keys		
VPN	<i>RemoteAddress</i>	Debe estar configurado Especifique la dirección IP o el nombre de host del servidor VPN de su organización.
VPN	<i>LocalIdentifier</i>	Debe estar configurado
VPN	<i>RemoteIdentifier</i>	Debe estar configurado
VPN	<i>AuthenticationMethod</i>	Debe fijarse en 'Certificate'.
VPN	<i>PayloadCertificateUUID</i>	Debe configurarse. Especifica el identificador único universal (UUID) del certificado de identidad utilizado como credencial de la cuenta.
VPN	<i>CertificateType</i>	Debe fijarse en RSA (default).
VPN	<i>ServerCertificateIssuerCommonName</i>	Debe estar configurado. Especifica el nombre común del emisor del certificado del servidor. Esta clave hará que IKE envíe una solicitud de certificado al servidor basada en el emisor de certificados especificado.
VPN	<i>EnableCertificateRevocationCheck</i>	Debe fijarse en '1'. Activa una comprobación de revocación de certificados para conexiones IKEv2.
IKESecurityAssociationParameters and ChildSecurityAssociationParameters Dictionary Keys		
VPN	<i>EncryptionAlgorithm</i>	'AES-256' (Default)
VPN	<i>Integrity Algorithm</i>	'SHA-256' (Default)
VPN	<i>DiffieHellmanGroup</i>	14
AlwaysOn Dictionary Keys		
VPN	<i>UIToggleEnabled</i>	Debe fijarse en '0'. Si se establece en «1», permite al usuario móvil desactivar esta configuración de VPN. El valor predeterminado es '0'.
VPN	<i>TunnelConfigurations - ProtocolType</i>	Debe fijarse en 'IKEv2'
OnDemandRules Dictionary Keys		

VPN	SSIDMatch	Debe estar configurado. Debe indicarse una serie de SSID permitidos a los que el dispositivo iOS puede conectarse.
-----	-----------	---

Tabla 4. 4VPN.

5.3 WLAN

46. Para el Extensible Authentication Protocol (EAP)-TLS, iOS implementa TLS 1.0, TLS 1.1, TLS 1.2 y TLS 1.3, soportando las ciphersuites listadas en la **¡Error! No se encuentra el origen de la referencia.¡Error! No se encuentra el origen de la referencia.**
47. En la configuración evaluada, los dispositivos móviles deben utilizar únicamente las ciphersuites EAP-TLS.

Cipher suite Yam
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256

Tabla 5WLAN Ciphersuites

5.4 PROTECCIÓN DE DATOS

48. Para garantizar la protección de datos en reposo, se debe configurar un código de acceso en el dispositivo móvil. Los usuarios pueden verificar que la protección de datos en reposo está habilitada en sus dispositivos de la siguiente manera:
49. Configuración → Configuración de Face ID y código de acceso
50. Esta pantalla permite al usuario habilitar la protección de datos en el dispositivo activando estas funciones de identificación. No se requiere configuración adicional para habilitar la protección de datos en el dispositivo. Más información sobre este tema se puede encontrar en los siguientes documentos y secciones.
- [iPhone_UG]: “Seguridad y privacidad” → “Proteger tu iPhone” → “Configurar un código de acceso en iPhone”
51. Los administradores de dispositivos móviles deben asegurarse de que los usuarios configuren un código de acceso utilizando la clave forcePIN en la carga útil del código de acceso. Otras claves disponibles en esta carga útil permiten a los administradores configurar los requisitos del código de acceso según la política organizacional.
52. Consulta la sección 5.4.1 Código de acceso para más información sobre cómo configurar tu código de acceso.
53. Los administradores de dispositivos móviles pueden restringir el acceso a unidades USB en la app archivos si lo desean, configurando la clave allowFilesUSBDriveAccess a 'false' en la sección de Restricciones del Perfil de Configuración.

54. Los administradores deben asegurarse, mediante políticas organizacionales, de que los usuarios de dispositivos móviles solo utilicen dispositivos de almacenamiento externo formateados con APFS y volúmenes cifrados. Los volúmenes sin cifrar y otros formatos no están permitidos en la configuración evaluada.

5.4.1 CÓDIGO DE ACCESO

55. Para más información, consultar: <https://support.apple.com/en-gb/guide/deployment/depeadc2af0b/1/web/1.0>

Payload	Key (Clave)	Descripción
Passcode	<i>allowSimple</i>	Debe fijarse en 'false'.
Passcode	<i>requireAlphanumeric</i>	Debe fijarse en 'true'
Passcode	<i>forcePIN</i>	Debe fijarse en 'true'.
Passcode	<i>maxFailedAttempts</i>	Debe establecerse en un valor definido por la política de la organización de despliegue. En este caso se establece en 10. Valor mínimo: 2 Valor máximo: 11
Passcode	<i>maxInactivity</i>	Debe establecerse en un valor definido por la política de la organización de despliegue. En este caso, se establece en 2. Valor mínimo: 0 Valor máximo: 15
Passcode	<i>maxPINAgeInDays</i>	Debe establecerse en un valor definido por la política de la organización de despliegue. En este caso, se establece en 360. Valor mínimo: 0 Valor máximo: 730
Passcode	<i>minComplexChars</i>	Debe establecerse en un valor definido por la política de la organización de despliegue. En este caso, se establece en 1. Valor mínimo: 0 Valor máximo: 4
Passcode	<i>minLength</i>	Debe establecerse en un valor definido por la política de la organización. En esta clave se establece en 6. Valor mínimo: 0 Valor máximo: 16

Tabla 6 Payloads para contraseñas

5.4.2 ELIMINACIÓN DE LA PROTECCIÓN DE DATOS

56. Una operación de borrado se realiza cuando el usuario del dispositivo móvil excede el límite de intentos fallidos de autenticación o al recibir una solicitud de un administrador autorizado. El administrador puede configurar el número de intentos fallidos utilizando la siguiente clave en el Perfil de Configuración dentro del Payload del código de acceso: `maxFailedAttempts`. Esta clave acepta un valor entero entre '2' y '11'.
57. Es obligatorio que el administrador del dispositivo móvil pueda emitir un comando de borrado remoto desde el servidor MDM utilizando el protocolo MDM, tal como se describe en `[DeployRef]` y `[DEV_MAN]`.
58. Se requiere la siguiente clave para realizar un borrado remoto del dispositivo: `RequestType` con un valor de 'EraseDevice' al enviar el comando `EraseDeviceCommand.Command`. Al recibir este comando, el dispositivo se borra inmediatamente, sin previo aviso al usuario, y se ejecuta incluso si el dispositivo está bloqueado.

`[DEV_MAN]: "Comandos y Consultas" → "Borrar un dispositivo" → "EraseDeviceCommand" → "EraseDeviceCommand.Command"`
59. Para ejecutar con éxito este comando, deben configurarse los derechos de acceso para borrar el dispositivo. Para habilitar este acceso, debe utilizarse la siguiente clave relacionada con la carga útil de MDM: `AccessRights`. El valor de esta clave se determina mediante un "OR" lógico que involucra el valor '8', donde 8 representa la autorización para borrar el dispositivo.
60. Para más información, consultar: <https://support.apple.com/en-gb/guide/deployment/dep0a819891e/1/web/1.0>

6. REFERENCIAS

Referencia	Ubicación
AGD_CC	Apple iOS 17: iPhones y Apple iPadOS 17: iPads Common Criteria Configuration Guide, versión xx, por determinar https://www.niap-ccevs.org/products/11349 --> Para actualizar
DeployRef	Apple Platform Deployment https://support.apple.com/guide/deployment/welcome/web
DEV_MAN	Device Management (online) https://developer.apple.com/documentation/devicemanagement
iPhone_UG	iPhone User Guide https://support.apple.com/guide/iphone/welcome/ios
APS	https://support.apple.com/es-es/guide/security/welcome/web

7. ABREVIATURAS

ENS	National Security Scheme.
BAF	Biometric Authentication Factor Type
BT	Bluetooth (version) (2400 MHz TO 2483.5 MHz)
Core	Wi-Fi/Bluetooth chip core
ISA	Instruction Set Architecture
NFC	Near Field Communication (13.56 MHz)
SAT	Satellite (Emergency SOS via satellite (Globalstar's L and S bands)
SoC	System on a Chip
UWB	Ultra-Wideband
MDM	Mobile Device Management
VPN	Virtual private network
IPSEC	Internet Protocol Security (Internet Protocol Security)
PKI	Public Key Infrastructure
CA	Certification Authority
OSCP	Online Certificate Status Protocol
ABM	Apple Business Manager

8. ANEXO I. PERFILES DE CONFIGURACIÓN.

61. Este apéndice muestra la política de restricciones que tienen los dispositivos iPhone bajo calificación en la configuración evaluada.

8.1 PERFIL DE CONFIGURACIÓN 1: "PERFIL DE CONFIGURACIÓN MDF PP PARA AIRPRINT"

```
<? xml version = "1.0" codificación = "UTF-8" ?>
<! DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd" >
< versión de plist = "1.0" >
  < dict >
    < clave > AccessRights </ clave >
    < entero > 8 </ > enteros
    < clave > ConsentText </ clave >
    < dict >
      < clave > </ clave predeterminada >
      < cadena > perfil de configuración logrando el cumplimiento de la
configuración de seguridad definida por
la evaluación CPSTIC. </ cuerda >
    </dict>
    < clave > HasRemovalPasscode </ clave >
    < falso />
    < clave > PayloadContent </ clave >
    < > de matriz
      < dict >
        < clave > AirPrint </ > de teclas
        < > de matriz
          < dict >
            < clave > ForceTLS </> de teclas
            < cierto />
          </dict>
        </ matriz >
        < clave > PayloadDescription </ clave >
        < cadena > AirPrint Configuración </ cadena >
        < clave > PayloadDisplayName </ > clave
        < cadena > AirPrint </ cadena >
        < clave > PayloadIdentifier </ > de clave
        < cadena > com.apple.airprint.F0AC096F-52CD-4FAB-83A3-675259987CD7 </
cadena >
        < clave > PayloadType </ > de clave
        < cadena > com.apple.airprint </ cadena >
        < clave > PayloadUUID </ clave >
        < cuerda > F0AC096F-52CD-4FAB-83A3-675259987CD7 </ cuerda >
        < clave > PayloadVersion </ clave >
```

```

        < entero > 1 </ > entero
    </dict>
</ matriz >
< clave > PayloadDescription </ clave >
< cadena > El perfil de configuración que define las restricciones de
AirPrint proporciona la información general
configuración compatible con la configuración evaluada por CPSTIC siguiendo el
dispositivo móvil
Perfil de protección fundamental. </ cuerda >
< clave > PayloadDisplayName </ > clave
< cadena > MDF PP Perfil de configuración AirPrint </ cadena >
< clave > PayloadIdentifier </ > de clave
< cuerda > MDFPP2020.7F5C2634-0C2B-4610-9FCB-65B6298D8734 </ cadena >
< clave > PayloadRemovalDisallowed </ clave >
< cierto />
< clave > PayloadType </ > de clave
< cadena > Configuración </ cadena >
< clave > PayloadUUID </ clave >
< cuerda > 42FA88A0-76CF-4D15-90C3-EED747194B32 </ cuerda >
< clave > PayloadVersion </ clave >
< entero > 1 </ > entero
</dict>
</plist>

```

8.2 PERFIL DE CONFIGURACIÓN 2: "PERFIL DE CONFIGURACIÓN DE MDF PP PARA RESTRICCIONES GENERALES"

```

<? xml version = "1.0" codificación = "UTF-8" ?>
<! DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd" >
< versión de plist = "1.0" >
    < dict >
        < clave > AccessRights </ clave >
        < entero > 8 </ > enteros
        < clave > ConsentText </ clave >
        < dict >
            < clave > </ clave predeterminada >
            < cadena > perfil de configuración logrando el cumplimiento
de la configuración de seguridad definida por
la evaluación CPSTIC. </ cuerda >
        </dict>
        < clave > HasRemovalPasscode </ clave >
        < falso />
        < clave > PayloadContent </ clave >
        < > de matriz
            < dict >

```

```

        < clave > PayloadDescription </ clave >
        < cadena > Configuración de restricción </ cadena >
        < clave > PayloadDisplayName </ > clave
        < cadena > Restricciones </ cadena >
        < clave > PayloadIdentifier </ > de clave
        < cadena > com.apple.applicationaccess.16FBE9FC-1D94-
49F8-91EA-806F0CE6B3EC </ cadena >
        < clave > PayloadType </ > de clave
        < cadena > com.apple.applicationaccess </ cadena >
        < clave > PayloadUUID </ clave >
        < cadena > 16FBE9FC-1D94-49F8-91EA-806F0CE6B3EC </ cuerda
>

        < clave > PayloadVersion </ clave >
        < entero > 1 </ > entero
        < tecla > allowAssistant </ > de teclas
        < falso />
        < clave > allowAssistantUserGeneratedContent </ > clave
        < falso />
        < clave > allowAssistantWhileLocked </ clave >
        < falso />
        < clave > allowLockScreenControlCenter </ > de teclas
        < falso />
        < clave > allowEnablingRestrictions </ clave >
        < falso />
        < clave > allowUSBRestrictedMode </ clave >
        < cierto />
        < clave > allowUntrustedTLSPrompt </ clave >
        < falso />
        < clave > forceAirPrintTrustedTLSRequirement </ key >
        < cierto />
        < clave > allowWallpaperModification </ clave >
        < cierto />
        < clave > forceAutomaticDateAndTime </ clave >
        < falso />
        <!-- Configuración opcional para restringir aún más los
permisos
<key>allowEraseContentAndSettings</key>
<falso/>
<key>allowCamera</key>
<falso/>
-->
        </dict>
    </ matriz >
    < clave > PayloadDescription </ clave >
    < cadena > El perfil de configuración que define las
restricciones generales de bloqueo varios mecanismos para

```

la configuración segura que cumple con la configuración evaluada de la CPSTIC siguiendo el

Perfil de protección de los aspectos básicos del dispositivo. </ cuerda >

```

    < clave > PayloadDisplayName </ > clave
    < cadena > MDF PP Perfil de configuración para restricciones
generales </ cadena >
    < clave > PayloadIdentifier </ > de clave
    < cadena > MDFPP2020.7F5C2634-0C2B-4610-9FCB-65B6298D8732 </
cadena >
    < clave > PayloadRemovalDisallowed </ clave >
    < cierto />
    < clave > PayloadType </ > de clave
    < cadena > Configuración </ cadena >
    < clave > PayloadUUID </ clave >
    < cadena > 1FAFA759-5DE3-4EEA-8F8E-8F742A2DADC2 </ cadena >
    < clave > PayloadVersion </ clave >
    < entero > 1 </ > entero
  </dict>
</plist>

```

8.3 PERFIL DE CONFIGURACIÓN 3: "PERFIL DE CONFIGURACIÓN MDF PP PARA RESTRICCIONES DE CONTRASEÑA"

```

<? xml version = "1.0" codificación = "UTF-8" ?>
<! DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd" >
< versión de plist = "1.0" >
  < dict >
    < clave > AccessRights </ clave >
    < entero > 8 </ > enteros
    < clave > ConsentText </ clave >
    < dict >
      < clave > </ clave predeterminada >
      < cadena > perfil de configuración logrando el cumplimiento
de la configuración de seguridad definida por
la evaluación CPSTIC. </ cuerda >
    </dict>
    < clave > HasRemovalPasscode </ clave >
    < falso />
    < clave > PayloadContent </ clave >
    < > de matriz
      < dict >
        < clave > PayloadDescription </ clave >
        < cadena > Restricciones de código de acceso </ cadena >
        < clave > PayloadDisplayName </ > clave

```

```

        < cadena > Código </ cadena >
        < clave > PayloadIdentifier </ > de clave
        < cadena >
com.apple.mobiledevice.passwordpolicy.41664EF5-450A-48C0-A19B-
970C5E522638 </ cadena >
        < clave > PayloadType </ > de clave
        < cadena > com.apple.mobiledevice.passwordpolicy </
cadena >

        < clave > PayloadUUID </ clave >
        < cuerda > 41664EF5-450A-48C0-A19B-970C5E522638 </ cuerda
>

        < clave > PayloadVersion </ clave >
        < entero > 1 </ > entero
        < clave > allowSimple </ > de teclas
        < falso />
        < clave > forcePIN </ llave >
        < cierto />

        <!-- Cualquier valor entre 2 y 11 -->
        < clave > maxFailedAttempts </ > clave
        < entero > 10 </ > enteros
        <!-- Cualquier valor definido por la organización -->
        < clave > maxInactividad </ > de teclas
        < entero > 2 </ > enteros

        <!-- Cualquier valor definido por la organización -->
        < clave > maxPINAgeInDays </ clave >
        < entero > 360 </ > entero

        <!-- Cualquier valor definido por la organización -->
        < clave > minComplexChars </ clave >
        < entero > 1 </ > entero

        <!-- Cualquier valor definido por la organización -->
        < clave > minLength </ clave >
        < entero > 6 </ > enteros

        <!-- Cualquier valor definido por la organización -->
        < tecla > pinHistory </ key >
        < entero > 1 </ > entero

        <!-- Cualquier valor definido por la organización -->
        < clave > maxGracePeriod </ > de clave
        < entero > 0 </ > entero

        <!-- Cualquier valor definido por la organización -->
        < clave > allowFingerprintModification </ clave >

```

```

        < cierto />
    </dict>
</ matriz >
< clave > PayloadDescription </ clave >
    <string> La plantilla de perfil de configuración proporciona
restricciones de código de acceso que cumplen con el
La configuración evaluada por CPSTIC siguiendo la protección de los
fundamentos de los dispositivos móviles
Perfil . </cuerda>
    < clave > PayloadDisplayName </ > clave
    < cadena > Perfil de configuración de PP de MDF para
restricciones de código de acceso </ cadena >
    < clave > PayloadIdentifier </ > de clave
    < cadena > MDFPP2020.7F5C2634-0C2B-4610-9FCB-65B6298D8733 </
cadena >
    < clave > PayloadRemovalDisallowed </ clave >
    < cierto />
    < clave > PayloadType </ > de clave
    < cadena > Configuración </ cadena >
    < clave > PayloadUUID </ clave >
    < cuerda > 754A56E0-6E64-444E-9675-FBBE0DE5CAB0 </ cuerda >
    < clave > PayloadVersion </ clave >
    < entero > 1 </ > entero
</dict>
</plist>

```

8.4 PERFIL DE CONFIGURACIÓN 4: "PERFIL DE CONFIGURACIÓN MDF PP PARA VPN"

62. El siguiente perfil de configuración VPN se presenta como un esquema para que el administrador de dispositivos de la organización lo utilice y modifique para configurar los dispositivos dentro de la organización.

```

<? xml version = "1.0" codificación = "UTF-8" ?>
<! DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd" >
< versión de plist = "1.0" >
< dict >
< clave > ConsentText </ clave >
< dict >
    < clave > </ clave predeterminada >
    < cadena > perfil de configuración logrando el cumplimiento de la
configuración de seguridad definida por la evaluación CPSTIC. </ cuerda >
</dict>
< clave > HasRemovalPasscode </ clave >

```

```

< falso />
< clave > PayloadContent </ clave >
< > de matriz
< dict >
  <!-- Reemplazar certificado -->
  < clave > Contraseña </ clave >
  < cuerda > 1234 </ cuerda >
  < clave > PayloadCertificateFileName </ clave >
  < cadena > cliente-certificado.p12 </ cadena >
  < clave > PayloadContent </ clave >
  < datos > NO VÁLIDOS </> de datos
  < clave > PayloadDescription </ clave >
  < cadena > certificado con formato PKCS#12 que DEBE reemplazarse </
cadena >
  < clave > PayloadDisplayName </ > clave
  < cadena > certificado con formato PKCS#12 que DEBE reemplazarse </
cadena >
  < clave > PayloadIdentifier </ > de clave
  < cadena > com.apple.security.pkcs12.51F4CAA0-B295-4557-8D91-
C4BDFB4AE825 </ cadena >
  < clave > PayloadType </ > de clave
  < cadena > com.apple.security.pkcs12 </ cadena >
  < clave > PayloadUUID </ clave >
  < cuerda > 51F4CAA0-B295-4557-8D91-C4BDFB4AE825 </ cuerda >
  < clave > PayloadVersion </ clave >
  < entero > 1 </ > entero
</dict>
< dict >
  < clave > AlwaysOn </ > clave
  < dict >
    <!-- Se permite cualquier valor definido por la organización -->
    < clave > AllowedCaptiveNetworkPlugins </ clave >
  </dict>
</dict>

```

