

MINISTERIO DE DEFENSA



cpage.mpr.gob.es

Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

Edita:



Pº de la Castellana 109, 28046 Madrid

© Centro Criptológico Nacional, 2025

NIPO: 083-25-196-3

Fecha de Edición: febrero 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.

INDICE

INDICE.....	2
INDICE DE TABLAS	3
INDICE 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	10
4. FASE DE INSTALACIÓN.....	11
4.1 REQUISITOS	11
4.2 ENTREGA SEGURA DE LOS PRODUCTOS	11
4.2.1 ADQUISICIÓN DE DISPOSITIVOS MÓVILES.	11
4.3 VERIFICACIÓN DEL DISPOSITIVOS.	11
4.3.1 BÚSQUEDA EN EL DISPOSITIVO	12
4.4 REGISTRAR DISPOSITIVOS EN MDM	13
4.4.1 CONFIGURACIÓN DE MDM.	13
4.4.2 REGISTRAR DISPOSITIVOS MÓVILES EN LA CONFIGURACIÓN DE GESTIÓN.....	15
4.4.3 INSTALAR PERFIL DE CONFIGURACIÓN EN IOS.	15
4.4.4 CONFIGURAR EL AGENTE MDM Y LAS COMUNICACIONES MDM	16
4.4.5 PREVENCIÓN ANTES DE LA BAJA DE UN DISPOSITIVO	16
5. FASE DE CONFIGURACIÓN	17
5.1 RESTRICCIONES GENERALES.	17
5.2 VPN.....	17
5.3 WLAN.....	20
5.4 PROTECCIÓN DE DATOS	20
5.4.1 CÓDIGO DE ACCESO	21
5.4.2 ELIMINACIÓN DE LA PROTECCIÓN DE DATOS.....	21
6. REFERENCIAS	23
7. ABREVIATURAS	24
8. ANEXO I. PERFILES DE CONFIGURACIÓN	25
8.1 PERFIL DE CONFIGURACIÓN 1: “PERFIL DE CONFIGURACIÓN MDF PP PARA AIRPRINT”	25
8.2 PERFIL DE CONFIGURACIÓN 2: “PERFIL DE CONFIGURACIÓN MDF PP PARA RESTRICCIONES GENERALES”	26
8.3 PERFIL DE CONFIGURACIÓN 3: “PERFIL DE CONFIGURACIÓN MDF PP PARA RESTRICCIONES DE CONTRASEÑA”	28
8.4 PERFIL DE CONFIGURACIÓN 4: “PERFIL DE CONFIGURACIÓN MDF PP PARA VPN”	30

INDICE DE TABLAS

Tabla 1. Mapeo de SoC a ISA	5
Tabla 2. Modelos de iPhone cualificados	9
Tabla 3. Restricciones Generales.....	17
Tabla 4 Restricciones para VPN.	20
Tabla 5. WLAN Ciphersuites	20
Tabla 6. Restricciones para contraseñas	21

INDICE DE FIGURAS

Figura 1. Identificación del modelo.	12
Figura 2. Identificación del modelo en el dispositivo (bandeja SIM)	12
Figura 3. Identificación del modelo en el dispositivo (conector de carga)	13
Figura 4. Entorno de Operación del dispositivo	13

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 con iOS 17 que han sido cualificados por el CCN y están listados 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 con iOS 17 pueden ser empleados como una solución de comunicaciones que proporciona conectividad móvil para el personal de una organización.
3. El dispositivo objeto de esta guía está formado por una plataforma hardware (modelo iPhone 13, iPhone 14, iPhone 14 Plus, iPhone 14 Pro, iPhone 14 Pro Max, iPhone 15, iPhone 15 Plus) y el propio sistema operativo, que se identifica como el software por su número de versión (iOS 17).
4. El dispositivo proporciona conectividad inalámbrica e incluye soporte para agentes de gestión de dispositivos móviles (MDM), conexiones de red privada virtual (VPN), cliente WLAN, Bluetooth, factores de autenticación biométrica (BAF), acceso a la red protegida de la organización, datos y aplicaciones de la organización.
5. El sistema operativo (iOS 17) gestiona el hardware del dispositivo y proporciona las tecnologías necesarias para desplegar aplicaciones nativas (también conocidas como apps). Una app nativa es una aplicación compilada para ejecutarse en una plataforma móvil específica. El dispositivo también proporciona una interfaz de programador de aplicaciones (API) denominada marco MDM, que ofrece funciones de gestión que pueden ser utilizadas por soluciones MDM de terceros, lo que permite a las organizaciones utilizar perfiles para controlar algunos de los ajustes del dispositivo.
6. El producto debe utilizarse como dispositivo móvil dentro del entorno de la organización 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 este procedimiento de empleo. Se proporcionan las características técnicas de cada dispositivo, incluida la arquitectura del conjunto de instrucciones, también conocida como microarquitectura.

SoC	ISA
A15 Bionic	ARMv8.6-A
A16 Bionic	

Tabla 1. Mapeo de SoC a ISA

Información del Dispositivo	Nº Modelo.	Cellular
iPhone 13 BAF: Face ID (GEN.2) BT: 5.0 NFC: Forks SAT: No SoC: A15 Bionic UWB: 6GHz – 8.5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) with 2.2 MIMO Core: 4387	A2482	5G (sub-6 GHz and mmWave) with 4x4 MIMO Gigabit LTE with 4x4 MIMO and LAA 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) 5G NR mmWave (Bands n258, n260, n261) FDD LTE (Bands 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 (Bands 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 and mmWave) with 4x4 MIMO Gigabit LTE with 4x4 MIMO and LAA 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) FDD LTE (Bands 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 (Bands 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 and mmWave) with 4x4 MIMO Gigabit LTE with 4x4 MIMO and LAA 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n38, n40, n41, n66, n71, n77, n78, n79) FDD-LTE (Bands 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 (Bands 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 and mmWave) with 4x4 MIMO Gigabit LTE with 4x4 MIMO and LAA 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n30, n38, n40, n41, n48, n66, n77, n78, n79) FDD LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD LTE (Bands 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 and mmWave) with 4x4 MIMO Gigabit LTE with 4x4 MIMO and LAA 5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n30, n38, n40, n41, n48, n66, n77, n78, n79) FDD LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66)

Información del Dispositivo	Nº Modelo.	Cellular
		TD LTE (Bands 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: Forks SAT: Forks SoC: A15 Bionic UWB: 6GHz – 8.5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) with 2.2 MIMO Core: 4387	A2649	5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) 5G NR mmWave (Bands n258, n260, n261) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bands 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 and mmWave) with 4x4 MIMO 5G, Gigabit-class LTE with 4x4 MIMO and LAA
	A2881	5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bands 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 and mmWave) with 4x4 MIMO 5G, Gigabit-class LTE with 4x4 MIMO and LAA
	A2882	5G NR (Bands 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 (Bands 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 (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bands 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: Forks SAT: Forks SoC: A15 Bionic UWB: 6GHz – 8.5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) with 2.2 MIMO Core: 4387	A2632	5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) 5G NR mmWave (Bands n258, n260, n261) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bands 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 and mmWave) with 4x4 MIMO 5G, Gigabit-class LTE with 4x4 MIMO and LAA
	A2885	5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bands 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 and mmWave) with 4x4 MIMO 5G, Gigabit-class LTE with 4x4 MIMO and LAA

Información del Dispositivo	Nº Modelo.	Cellular
	A2886	5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bands 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: Forks SAT: Forks SoC: A16 Bionic UWB: 6GHz – 8.5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) with 2.2 MIMO Core: 4387	A2650	5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) 5G NR mmWave (Bands n258, n260, n261) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bands 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 and mmWave) with 4x4 MIMO 5G, Gigabit-class LTE with 4x4 MIMO and LAA
	A2889	5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bands 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 and mmWave) with 4x4 MIMO 5G, Gigabit-class LTE with 4x4 MIMO and LAA
	A2890	5G NR (Bands 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 (Bands 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 (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bands 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 NFC: Forks SAT: Forks	A2651	5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) 5G NR mmWave (Bands n258, n260, n261) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71)

Información del Dispositivo	Nº Modelo.	Cellular
SoC: A16 Bionic UWB: 6GHz – 8.5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) with Fi: 2.2 MIMO Core: 4387		TD-LTE (Bands 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 and mmWave) with 4x4 MIMO 5G, Gigabit-class LTE with 4x4 MIMO and LAA
	A2893	5G NR (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n29, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD-LTE (Bands 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 and mmWave) with 4x4 MIMO 5G, Gigabit-class LTE with 4x4 MIMO and LAA
	A2894	5G NR (Bands 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 (Bands 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 (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bands 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: Forks SAT: Forks SoC: A16 Bionic UWB: 6GHz – 8.5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) with Fi: 2.2 MIMO Core: 4387	A2846	5G NR (Bands 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 (Bands n258, n260, n261) FDD LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bands 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 (Bands 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 (Bands 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 (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n53, n66, n70, n77, n78, n79)

Información del Dispositivo	Nº Modelo.	Cellular
		FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD LTE (Bands 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: Forks SAT: Forks SoC: A16 Bionic UWB: 6GHz – 8.5 GHz Wi-Fi: Wi-Fi 6 (802.11ax) with Fi: 2.2 MIMO Core: 4387	A2847	5G NR (Bands 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 (Bands n258, n260, n261) FDD LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bands 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 (Bands 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 (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 66, 71) TD LTE (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n53, n66, n70, n77, n78, n79) FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD-LTE (Bands 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 (Bands n1, n2, n3, n5, n7, n8, n12, n20, n25, n26, n28, n30, n38, n40, n41, n48, n66, n70, n77, n78, n79) FDD LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 28, 30, 32, 66) TD LTE (Bands 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)

Tabla 2. Modelos de iPhone cualificados

3. ORGANIZACIÓN DEL DOCUMENTO

9. 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. PERFILES DE CONFIGURACIÓN** 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

10. Antes de integrar los dispositivos móviles a la red corporativa, se debe 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 debe implementar una VPN siguiendo la sección “Descripción general de VPN para la implementación de dispositivos Apple” de [APD], para asegurar la comunicación de los dispositivos.
11. 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 LOS PRODUCTOS

12. Los dispositivos móviles objeto de esta guía están destinados fundamentalmente a ser empleados en organizaciones empresariales y organismos gubernamentales.
13. El administrador de dispositivos móviles es responsable de realizar la configuración necesaria para garantizar que los dispositivos estén configurados de acuerdo con este procedimiento de empleo.

4.2.1 ADQUISICIÓN DE DISPOSITIVOS MÓVILES.

14. 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. Asegúrese de que su proveedor tenga la capacidad de inscribir automáticamente dispositivos en Apple Business Manager.

4.3 VERIFICACIÓN DEL DISPOSITIVOS.

15. 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 .
16. 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 muestran en esta página <https://support.apple.com/es-es/106343>.

4.3.1 BÚSQUEDA EN EL DISPOSITIVO

17. 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 13 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)

- Los modelos de iPhone que solo son compatibles con eSIM no tienen bandeja SIM. Para encontrar el número de modelo, búscalo en el conector Lightning o USB-C. Asegúrese de estar en un lugar bien iluminado para

poder verlo. El número de modelo se encuentra 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.

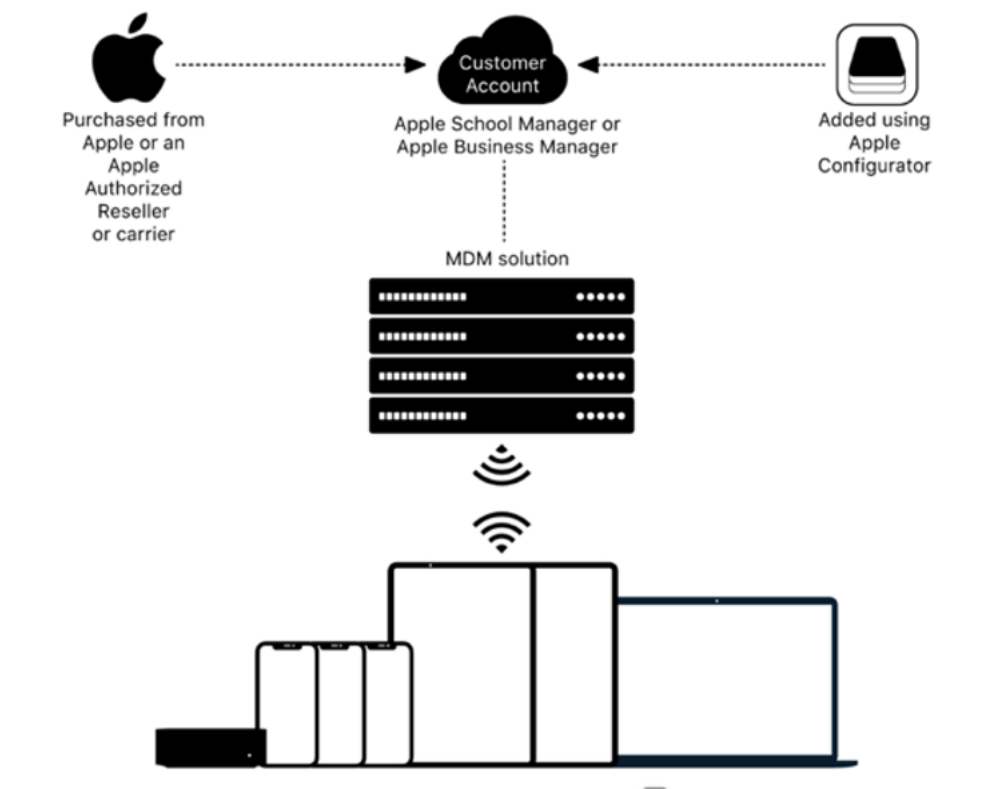


Figura 4. Entorno de Operación del dispositivo

18. El entorno operativo básico para el dispositivo consiste en el dispositivo móvil iPhone y una solución MDM para que el dispositivo funcione correctamente. Esto se puede ver en la Figura 4. . Entorno de Operación del .

19. La solución MDM proporciona una forma para aplicar 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 dispositivo para que opere de acuerdo con los requisitos definidos en este documento. La configuración cualificada 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 de 8 caracteres.
 - Se define un número máximo de intentos fallidos consecutivos para ingresar el código de acceso de 10.
 - Se define una política de bloqueo de sesión de 5 minutos.
 - Especificaciones para los dispositivos permitidos de recopilación de audio y video.
 - Especificación de conexiones VPN.
 - Se define una política para el almacenamiento externo a través de un conector de dispositivo.
21. Para cumplir con los requisitos de esta cualificación, los dispositivos deben configurarse en modo supervisado.
22. En términos generales, la supervisión indica que el dispositivo es propiedad de la organización, lo cual proporciona un control adicional sobre la configuración y sus restricciones. Las organizaciones pueden supervisar los dispositivos de distintas maneras.
23. Los dispositivos objeto de este PES se supervisarán automáticamente si sus números de serie aparecen en Apple Business Manager y están inscritos en una solución MDM mediante la inscripción automatizada de dispositivos.
24. Para identificar si un dispositivo está supervisado, ir a “Ajustes”, el texto aparece debajo del campo búsqueda, y encima del área de la cuenta de Apple: “Este [iPhone] [iPad] está supervisado. [Nombre de la organización] puede supervisar tu tráfico de Internet y localizar este dispositivo”.
25. Consulte: <https://support.apple.com/en-us/guide/deployment/dep1d89f0bff/web> para mas información al respecto.

4.4.2 REGISTRAR DISPOSITIVOS MÓVILES EN LA CONFIGURACIÓN DE GESTIÓN

26. Los dispositivos móviles se deben gestionar 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.
27. Apple proporciona una guía y más detalles sobre la implementación de las plataformas de Apple y la inscripción automatizada de dispositivo y MDM en los siguientes enlaces:
<https://support.apple.com/es-es/guide/deployment/depc0aadd3fe/web>
<https://support.apple.com/es-es/guide/deployment/dep73069dd57/web>
28. Se recomienda utilizar Apple Business Manager (ABM) para el registro en MDM. Apple Business Manager es un portal web para administradores de TI. Se integra con soluciones de gestión de dispositivos móviles (MDM) de terceros, lo que permite obtener contenido de manera masiva con facilidad.
29. Con Apple Business Manager, se puede 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. Puede registrar automáticamente los dispositivos en su solución MDM, siempre que el dispositivo haya sido agregado a su 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, consulte: <https://support.apple.com/es-es/guide/apple-business-manager/axm7909096bf/web>.
30. La Inscripción Automatizada de Dispositivos está diseñada para todos los dispositivos Apple propiedad de la organización. La Inscripción Automatizada de Dispositivos permite a las organizaciones configurar y gestionar los dispositivos directamente desde la caja. También puede usar todas las cargas útiles y restricciones disponibles definidas por Apple, y tiene la opción de evitar que el usuario elimine el perfil de registro en la solución de gestión de dispositivos móviles (MDM). Para más información, consulte: <https://support.apple.com/es-es/guide/deployment/dep73069dd57/web>

4.4.3 INSTALAR PERFIL DE CONFIGURACIÓN EN IOS.

31. 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.

32. La planificación de perfiles de configuración y cargas ayuda a reducir la complejidad. Para optimizar la gestión del cargas, 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

33. Al instalar y configurar su solución MDM, considere cómo configurar la red, Transport Layer Security (TLS), los servicios de infraestructura, los servicios de Apple y las copias de seguridad.
34. Cuando instale una solución MDM alojada localmente, debe configurar los siguientes elementos:
 - Usar un nombre de dominio completo (FQDN).
 - Tener una dirección IP estática.
 - Configurar el MDM con Transport Layer Security 1.2 o superior.
 - Mantener ciertos puertos del firewall abiertos.
35. Configure y pruebe cada uno de estos elementos desde el principio del proceso para garantizar un despliegue sin problemas. No es recomendable que su solución MDM sea gestionada externamente o esté alojada en la nube. Para más información, consulte: <https://support.apple.com/es-es/guide/deployment/dep2bcde692e/web>

4.4.5 PREVENCIÓN ANTES DE LA BAJA DE UN DISPOSITIVO

36. 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.
37. 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.
38. Para más información sobre "Volver a inscribir dispositivos en MDM", consulte: <https://support.apple.com/en-us/guide/deployment/dep26505df5d/1/web/1.0>

5. FASE DE CONFIGURACIÓN

39. Esta sección ofrece una guía más detallada sobre cómo configurar dispositivos móviles gestionados para cumplir con los requisitos de la cualificación CPSTIC.
40. Esta sección detalla los valores que deben usarse o los que no están permitidos.
41. Para los valores no mencionadas en este documento, consulte las políticas de seguridad de la organización que realiza el despliegue.

5.1 RESTRICCIONES GENERALES.

42. A continuación, se presentan los valores a configurar para Restricciones Generales

Payload	Clave	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 'true'
TLS/HTTPS Configuration		
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 3. Restricciones Generales.

5.2 VPN

43. 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** para el nivel de seguridad establecido.

44. 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.
45. 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'.
46. IKEv2 debe configurarse utilizando los siguientes parámetros 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.
47. 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, que permiten definir con mayor detalle un EncryptionAlgorithm, un IntegrityAlgorithm y un DiffieHellmanGroup, tal como se describe en la [Tabla 4 4: Restricciones](#) para VPN Para más información, consultar: <https://support.apple.com/es-es/guide/deployment/depae3d361d0/web>

Payload	Parámetros	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		

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

Tabla 4 Restricciones para VPN.

5.3 WLAN

48. Para el Extensible Authentication Protocol (EAP)-TLS, iOS debe implementar TLS 1.2 y TLS 1.3, soportando las ciphersuites listadas en la Tabla 5. . WLAN Ciphersuites
49. En la configuración cualificada, 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 5. WLAN Ciphersuites

5.4 PROTECCIÓN DE DATOS

50. 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:
 - Configuración → configuración de Face ID y código de acceso.
51. 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.
 - []: “Seguridad y privacidad” → “Proteger tu iPhone” → “Configurar un código de acceso en iPhone”
52. 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.
53. Consulta la sección [5.4.1 CÓDIGO DE ACCESO](#) para más información sobre cómo configurar tu código de acceso.
54. 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.

55. 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 para el nivel de seguridad establecido.

5.4.1 CÓDIGO DE ACCESO

56. 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 8. Valor mínimo: 0 Valor máximo: 16

Tabla 6. Restricciones para contraseñas

5.4.2 ELIMINACIÓN DE LA PROTECCIÓN DE DATOS

57. 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'.

58. 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].
59. La siguiente clave es necesaria 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 advertencia al usuario, y se ejecuta incluso si el dispositivo está bloqueado.

[DEV_MAN]: "Comandos y Consultas" → "Borrar un dispositivo" → "EraseDeviceCommand" → "EraseDeviceCommand.Command"
60. 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.
61. Para más información, consultar: <https://support.apple.com/es-es/guide/deployment/dep0a819891e/1/web/1.0>

6. REFERENCIAS

Referencia	Localización
AGD_CC	Apple iOS 16: iPhones and Apple iPadOS 16: iPads Common Criteria Configuration Guide, version 1.0, 2023-09-08 https://www.niap-ccevs.org/products/11349
APD	Apple Platform Deployment https://support.apple.com/en-gb/guide/deployment
APS	https://support.apple.com/es-es/guide/security/welcome/web
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

7. ABREVIATURAS

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

8. ANEXO I. PERFILES DE CONFIGURACIÓN

62. Este apéndice muestra la política de restricciones que tienen los dispositivos iPhone en la configuración cualificada.

8.1 PERFIL DE CONFIGURACIÓN 1: “PERFIL DE CONFIGURACIÓN MDF PP PARA AIRPRINT”

```
<? xml version = "1.0" encoding = "UTF-8" ?>
<! DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd" >
< plist version = "1.0" >
  < dict >
    < key > AccessRights </ key >
    < integer > 8 </ integer >
    < key > ConsentText </ key >
    < dict >
      < key > default </ key >
      < string > Configuration profile achieving compliance with the security
settings defined by
the CPSTIC evaluation. </ string >
    </dict>
    < key > HasRemovalPasscode </ key >
    < false />
    < key > PayloadContent </ key >
    < array >
      < dict >
        < key > AirPrint </ key >
        < array >
          < dict >
            < key > ForceTLS </ key >
            < true />
          </dict>
        </ array >
        < key > PayloadDescription </ key >
        < string > AirPrint Configuration </ string >
        < key > PayloadDisplayName </ key >
        < string > AirPrint </ string >
        < key > PayloadIdentifier </ key >
        < string > com.apple.airprint.F0AC096F-52CD-4FAB-83A3-675259987CD7 </
string >
        < key > PayloadType </ key >
        < string > com.apple.airprint </ string >
        < key > PayloadUUID </ key >
        < string > F0AC096F-52CD-4FAB-83A3-675259987CD7 </ string >
        < key > PayloadVersion </ key >
```

```

        < integer > 1 </ integer >
    </dict>
</ array >
< key > PayloadDescription </ key >
< string > The configuration profile defining the AirPrint restrictions
provides the general
settings compliant to the CPSTIC evaluated configuration following the Mobile Device
Fundamentals Protection Profile. </ string >
< key > PayloadDisplayName </ key >
< string > MDF PP Configuration Profile AirPrint </ string >
< key > PayloadIdentifier </ key >
< string > MDFPP2020.7F5C2634-0C2B-4610-9FCB-65B6298D8734 </ string >
< key > PayloadRemovalDisallowed </ key >
< true />
< key > PayloadType </ key >
< string > Configuration </ string >
< key > PayloadUUID </ key >
< string > 42FA88A0-76CF-4D15-90C3-EED747194B32 </ string >
< key > PayloadVersion </ key >
< integer > 1 </ integer >
</dict>
</plist>

```

8.2 PERFIL DE CONFIGURACIÓN 2: “PERFIL DE CONFIGURACIÓN MDF PP PARA RESTRICCIONES GENERALES”

```

<? xml version = "1.0" encoding = "UTF-8" ?>
<! DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd" >
< plist version = "1.0" >
    < dict >
        < key > AccessRights </ key >
        < integer > 8 </ integer >
        < key > ConsentText </ key >
        < dict >
            < key > default </ key >
            < string > Configuration profile achieving compliance with
the security settings defined by
the CPSTIC evaluation. </ string >
        </dict>
        < key > HasRemovalPasscode </ key >
        < false />
        < key > PayloadContent </ key >
        < array >
            < dict >
                < key > PayloadDescription </ key >

```

```

    < string > Restriction Configuration </ string >
    < key > PayloadDisplayName </ key >
    < string > Restrictions </ string >
    < key > PayloadIdentifier </ key >
    < string > com.apple.applicationaccess.16FBE9FC-1D94-
49F8-91EA-806F0CE6B3EC </ string >
    < key > PayloadType </ key >
    < string > com.apple.applicationaccess </ string >
    < key > PayloadUUID </ key >
    < string > 16FBE9FC-1D94-49F8-91EA-806F0CE6B3EC </ string
>

    < key > PayloadVersion </ key >
    < integer > 1 </ integer >
    < key > allowAssistant </ key >
    < false />
    < key > allowAssistantUserGeneratedContent </ key >
    < false />
    < key > allowAssistantWhileLocked </ key >
    < false />
    < key > allowLockScreenControlCenter </ key >
    < false />
    < key > allowEnablingRestrictions </ key >
    < false />
    < key > allowUSBRestrictedMode </ key >
    < true />
    < key > allowUntrustedTLSPrompt </ key >
    < false />
    < key > forceAirPrintTrustedTLSRequirement </ key >
    < true />
    < key > allowWallpaperModification </ key >
    < true />
    < key > forceAutomaticDateAndTime </ key >
    < false />
    <!-- Optional settings to further restrict permissions
<key>allowEraseContentAndSettings</key>
<false/>
<key>allowCamera</key>
<false/>
-->
    </dict>
  </ array >
  < key > PayloadDescription </ key >
  < string > The configuration profile defining general lock
restrictions various mechanisms to
the secure settings compliant to the CPSTIC evaluated configuration
following the Mobile
Device Fundamentals Protection Profile. </ string >

```

```

    < key > PayloadDisplayName </ key >
    < string > MDF PP Configuration Profile for General Restrictions
</ string >
    < key > PayloadIdentifier </ key >
    < string > MDFPP2020.7F5C2634-0C2B-4610-9FCB-65B6298D8732 </
string >
    < key > PayloadRemovalDisallowed </ key >
    < true />
    < key > PayloadType </ key >
    < string > Configuration </ string >
    < key > PayloadUUID </ key >
    < string > 1FAFA759-5DE3-4EEA-8F8E-8F742A2DADC2 </ string >
    < key > PayloadVersion </ key >
    < integer > 1 </ integer >
  </dict>
</plist>

```

8.3 PERFIL DE CONFIGURACIÓN 3: “PERFIL DE CONFIGURACIÓN MDF PP PARA RESTRICCIONES DE CONTRASEÑA”

```

<? xml version = "1.0" encoding = "UTF-8" ?>
<! DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd" >
< plist version = "1.0" >
  < dict >
    < key > AccessRights </ key >
    < integer > 8 </ integer >
    < key > ConsentText </ key >
    < dict >
      < key > default </ key >
      < string > Configuration profile achieving compliance with
the security settings defined by
the CPSTIC evaluation. </ string >
    </dict>
    < key > HasRemovalPasscode </ key >
    < false />
    < key > PayloadContent </ key >
    < array >
      < dict >
        < key > PayloadDescription </ key >
        < string > Passcode Restrictions </ string >
        < key > PayloadDisplayName </ key >
        < string > Code </ string >
        < key > PayloadIdentifier </ key >

```

```

        < string >
com.apple.mobiledevice.passwordpolicy.41664EF5-450A-48C0-A19B-
970C5E522638 </ string >
        < key > PayloadType </ key >
        < string > com.apple.mobiledevice.passwordpolicy </
string >
        < key > PayloadUUID </ key >
        < string > 41664EF5-450A-48C0-A19B-970C5E522638 </ string
>

        < key > PayloadVersion </ key >
        < integer > 1 </ integer >
        < key > allowSimple </ key >
        < false />
        < key > forcePIN </ key >
        < true />

        <!-- Any value between 2 and 11 -->
        < key > maxFailedAttempts </ key >
        < integer > 10 </ integer >
        <!-- Any value defined by organization -->
        < key > maxInactivity </ key >
        < integer > 2 </ integer >

        <!-- Any value defined by organization -->
        < key > maxPINAgeInDays </ key >
        < integer > 360 </ integer >

        <!-- Any value defined by organization -->
        < key > minComplexChars </ key >
        < integer > 1 </ integer >

        <!-- Any value defined by organization -->
        < key > minLength </ key >
        < integer > 8 </ integer >

        <!-- Any value defined by organization -->
        < key > pinHistory </ key >
        < integer > 1 </ integer >

        <!-- Any value defined by organization -->
        < key > maxGracePeriod </ key >
        < integer > 0 </ integer >

        <!-- Any value defined by organization -->
        < key > allowFingerprintModification </ key >
        < true />
</dict>

```

```

    </ array >
    < key > PayloadDescription </ key >
    <string> The configuration profile template provides passcode
restrictions compliant to the
CPSTIC evaluated configuration following the Mobile Device Fundamentals
Protection
Profile . </string>
    < key > PayloadDisplayName </ key >
    < string > MDF PP Configuration Profile for Passcode Restrictions
</ string >
    < key > PayloadIdentifier </ key >
    < string > MDFPP2020.7F5C2634-0C2B-4610-9FCB-65B6298D8733 </
string >
    < key > PayloadRemovalDisallowed </ key >
    < true />
    < key > PayloadType </ key >
    < string > Configuration </ string >
    < key > PayloadUUID </ key >
    < string > 754A56E0-6E64-444E-9675-FBBE0DE5CAB0 </ string >
    < key > PayloadVersion </ key >
    < integer > 1 </ integer >
  </dict>
</plist>

```

8.4 PERFIL DE CONFIGURACIÓN 4: “PERFIL DE CONFIGURACIÓN MDF PP PARA VPN”

63. 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" encoding = "UTF-8" ?>
<! DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd" >
< plist version = "1.0" >
< dict >
< key > ConsentText </ key >
< dict >
    < key > default </ key >
    < string > Configuration profile achieving compliance with the
security settings defined by the CPSTIC evaluation. </ string >
</dict>
< key > HasRemovalPasscode </ key >
< false />
< key > PayloadContent </ key >

```

```
< array >
< dict >
  <!-- Replace certificate -->
  < key > Password </ key >
  < string > 1234 </ string >
  < key > PayloadCertificateFileName </ key >
  < string > client-certificate.p12 </ string >
  < key > PayloadContent </ key >
  < data > INVALID </ data >
  < key > PayloadDescription </ key >
  < string > PKCS#12-formatted certificate that MUST be replaced </
string >
  < key > PayloadDisplayName </ key >
  < string > PKCS#12-formatted certificate that MUST be replaced </
string >
  < key > PayloadIdentifier </ key >
  < string > com.apple.security.pkcs12.51F4CAA0-B295-4557-8D91-
C4BDFB4AE825 </ string >
  < key > PayloadType </ key >
  < string > com.apple.security.pkcs12 </ string >
  < key > PayloadUUID </ key >
  < string > 51F4CAA0-B295-4557-8D91-C4BDFB4AE825 </ string >
  < key > PayloadVersion </ key >
  < integer > 1 </ integer >
</dict>
< dict >
  < key > AlwaysOn </ key >
  < dict >
    <!-- Any value defined by organization is allowed -->
    < key > AllowedCaptiveNetworkPlugins </ key >
  </dict>
</dict>
```

