centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1621

Procedimiento de empleo seguro
Lenovo Tab M8 4th Gen



Abril de 2023

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.05.03 12:25:48 +02'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2023

NIPO: 083-23-128-2.

Fecha de Edición: abril 2023.

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**
1. INTRODUCCIÓN **3**
2. OBJETO Y ALCANCE **4**
3. ORGANIZACIÓN DEL DOCUMENTO **5**
4. FASE PREVIA A LA INSTALACIÓN **6**
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.2 CONSIDERACIONES PREVIAS 7
4.3 COMPONENTES DEL ENTORNO DE OPERACIÓN 7
5. FASE DE INSTALACIÓN **8**
6. FASE DE CONFIGURACIÓN **16**
6.1 MODO DE OPERACIÓN SEGURO 16
6.2 AUTENTICACIÓN 17
6.3 ADMINISTRACIÓN DEL PRODUCTO 17
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 17
6.4 CONFIGURACIÓN DE IPSEC 17
6.5 CONFIGURACIÓN WI-FI RECOMENDADA 18
6.6 USO DE TLS SDK ANDROID 18
6.7 ACTUALIZACIONES 18
6.8 AUTO-CHEQUEOS 19
6.9 AUDITORÍA 19
6.9.1 REGISTRO DE EVENTOS 19
7. FASE DE OPERACIÓN **21**
8. REFERENCIAS **22**
9. ABREVIATURAS **23**

1. INTRODUCCIÓN

Lenovo Tab M8 4th Gen es una Tablet que se encuentra dentro de la familia de productos “Dispositivos Móviles”. La Tablet proporciona una API con la que pueden interaccionar las diferentes aplicaciones móviles (APPs); esta API permite a los usuarios conceder permisos de instalación a las APPs que requieran uso de la misma, o incluso conceder diferentes permisos a las APPs en tiempo de ejecución.

Además, el producto proporciona a los usuarios la capacidad de proteger la información en reposo (*data at rest*), incluyendo los datos del usuario y de las aplicaciones móviles almacenados en la partición de datos del usuario. El producto utiliza una jerarquía de claves que combina una clave de cifrado con la contraseña del usuario para proporcionar protección a todas las claves criptográficas de usuario y de aplicaciones almacenadas en el producto.

El producto puede interactuar con un sistema de gestión de dispositivos móviles (MDM) para permitir el control empresarial de la configuración y el funcionamiento del dispositivo con el fin de garantizar el cumplimiento de las políticas de toda la empresa (por ejemplo, la configuración de los intentos máximos de inicio de sesión, la obtención de registros de auditoría del producto, etc.). Un MDM se compone de dos partes: el agente MDM y el servidor MDM. El agente MDM se instala en el teléfono como administrador con permisos elevados (lo que permite cambiar la configuración relevante del dispositivo), mientras que el servidor MDM se utiliza para ejecutar los comandos en el agente MDM.

El dispositivo incluye varios niveles diferentes de ejecución que incluyen (de menor a mayor): hardware, un TEE (*Trusted Execution Environment*), el *bootloader* de Android y el espacio de usuario de Android, que proporciona APIs que permiten a las aplicaciones aprovechar la funcionalidad criptográfica del dispositivo.

Por último, el producto solicita al servidor que se actualice desde un canal seguro. Estas actualizaciones se firman utilizando una clave privada, que el producto verifica antes de instalarlas con su clave pública. Además, el dispositivo proporciona seguridad contra la manipulación del hardware mediante el uso de mecanismos *anti-tampering*.

2. OBJETO Y ALCANCE

Esta guía es compatible con el siguiente dispositivo y versión:

- Modelo *hardware*: **Lenovo Tab M8 4th Gen (TB300XU)**
- Versión del *firmware*: **TB300XU_S000111_230408_ROW (Android 12)**

3. ORGANIZACIÓN DEL DOCUMENTO

Este documento se compone de los siguientes apartados:

a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Para verificar que el producto ha sido recibido de manera segura y que su integridad no ha sido alterada, se deberán seguir los siguientes pasos:

1. Comprobar que la tablet presenta dos (2) pegatinas *anti-tamper,* una en el margen inferior y otra en el margen superior. Ambas pegatinas deben encontrarse en un en perfecto estado, de manera que garanticen que la tablet no ha sido abierta ni modificada internamente durante el proceso de envío.



2. Encender el producto y comprobar que no aparece ningún mensaje de fallo de integridad, garantizando de esta manera que el firmware es auténtico.
3. Una vez terminado el proceso de instalación, ir a Ajustes > Información del Tablet y comprobar que el modelo y firmware (número de compilación) corresponden con el declarado en la sección *2 OBJETO Y ALCANCE*.

4.2 CONSIDERACIONES PREVIAS

El dispositivo es compatible con diferentes elementos que pueden ser incluidos en el entorno operacional. Para hacer uso de estas funcionalidades extra (no son obligatorias, hará uso de ellas el usuario en función de sus necesidades), es necesario contar con elementos específicos y que cumplan con una serie de requisitos en el entorno operacional. Ver *4.3. COMPONENTES DEL ENTORNO DE OPERACIÓN* para más información.

4.3 COMPONENTES DEL ENTORNO DE OPERACIÓN

El dispositivo puede interactuar con un servidor MDM para ser gestionado de manera remota. Durante el desarrollo de esta guía se ha hecho uso de TestDPC, aunque a la hora de documentar se ha intentado dar indicaciones generales que pueden seguirse con cualquier MDM.

Test DPC es una aplicación diseñada para ayudar a los MDM, ISV *(Independent Software Vendor*) y OEM (*Original Equipment Manufacturer*) a probar sus aplicaciones y plataformas en un perfil administrado por la empresa de Android (es decir, el perfil de trabajo / *Workspace* / Contenedor). Sirve como un controlador de políticas de dispositivo y una aplicación de prueba para ejecutar las API disponibles Android Enterprise.

En un entorno real, la organización deberá elegir el MDM compatible con Android 12 que mejor cumpla con sus requisitos de seguridad, así como con sus requisitos operativos. En ningún caso deberá usarse *TestDPC* en producción, pero sí que se recomienda su uso para comprobar el efecto que tienen diferentes políticas en el dispositivo.

El dispositivo también implementa el protocolo EAP-TLS para establecer comunicación con un servidor RADIUS y autenticarse en una red WLAN. Es importante tener en cuenta que, si se quiere hacer uso de esta funcionalidad, deberá desplegarse en el entorno operacional un punto de acceso compatible con el estándar IEEE 802.1X para un PAE (*Port Access Entity*) en el rol de “Autenticador” y que se comunique de la manera esperada con un servidor de autenticación RADIUS (por ejemplo, *FreeRADIUS*).

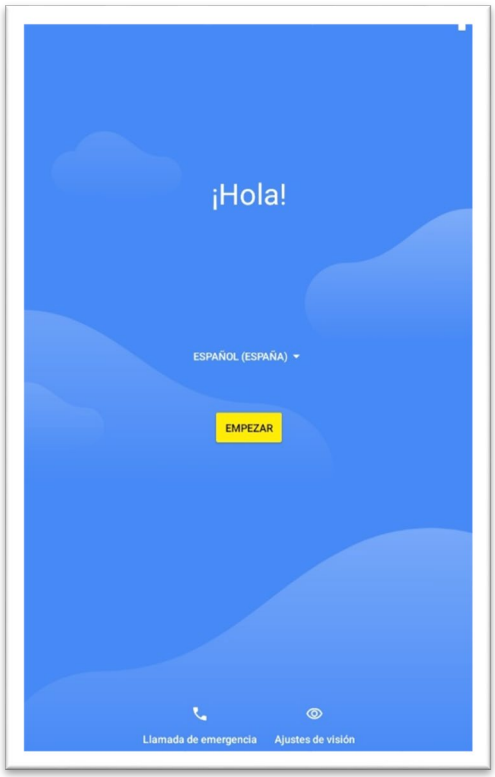
Por último, el producto ofrece una API para que una aplicación de terceros pueda establecer un canal seguro mediante un canal IPSEC. Para hacer uso de esta funcionalidad, es necesario que la organización cuente con un servidor IPSEC (por ejemplo, *strongSwan*).

5. FASE DE INSTALACIÓN

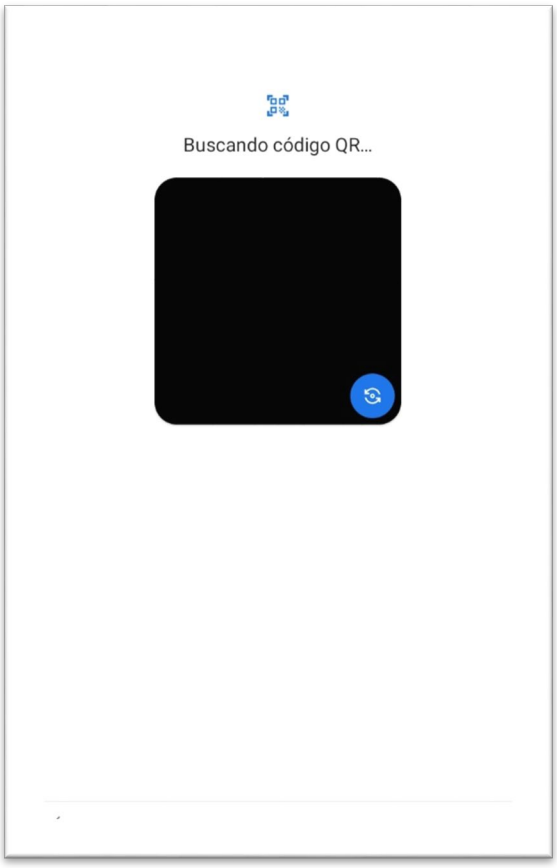
Encender la Tablet y seguir los pasos descritos en la sección *4.1 ENTREGA SEGURA DEL PRODUCTO*.

Una vez encendida, y pendiente de comprobar la versión del dispositivo, llevar a cabo los siguientes pasos para realizar la instalación:

1. Elegir un idioma y país (por ejemplo, ESPAÑOL (ESPAÑA)).
2. Hacer *click* en "¡Hola!" de manera repetitiva hasta que aparezca un lector de QR.



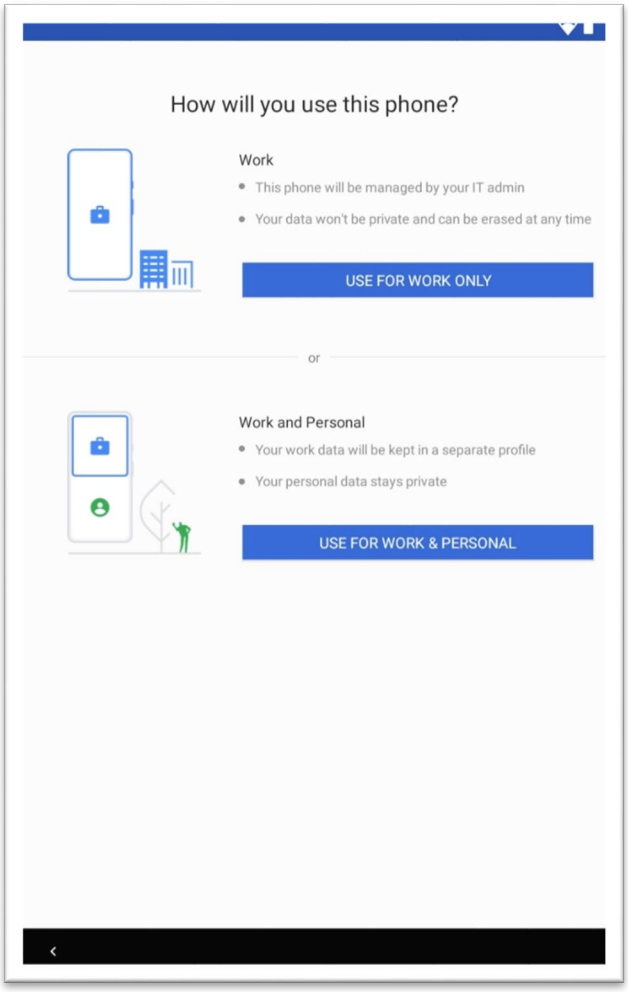
3. Escanear el código QR generado por el servidor MDM elegido.



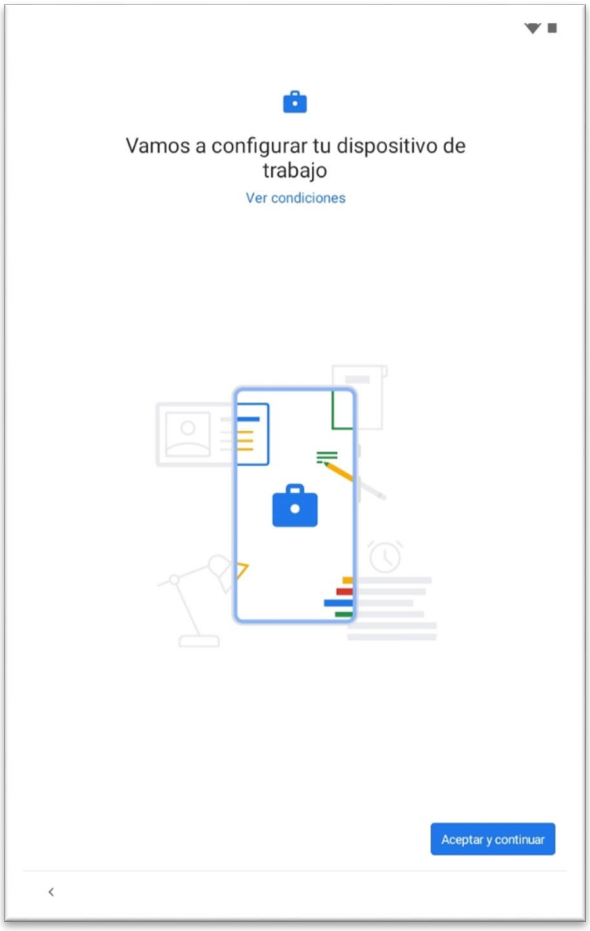
4. Conectar el dispositivo a una red Wi-Fi. Para más información sobre la seguridad recomendada para redes Wi-Fi, ver *6.5 CONFIGURACIÓN* .
5. Hacer *click* en "*Siguiente*".



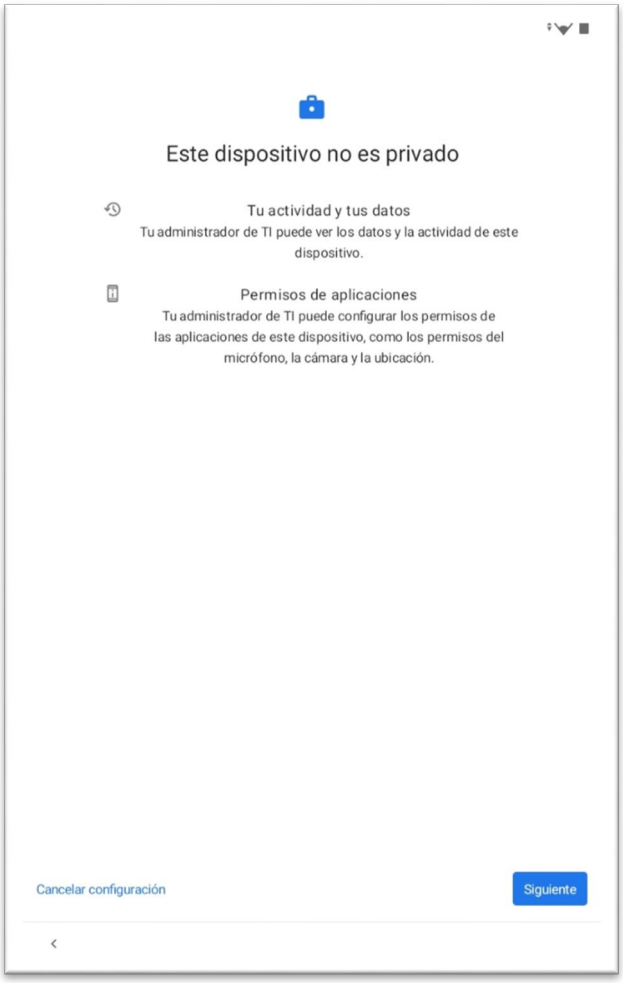
6. Seleccionar "*USE FOR WORK ONLY*".



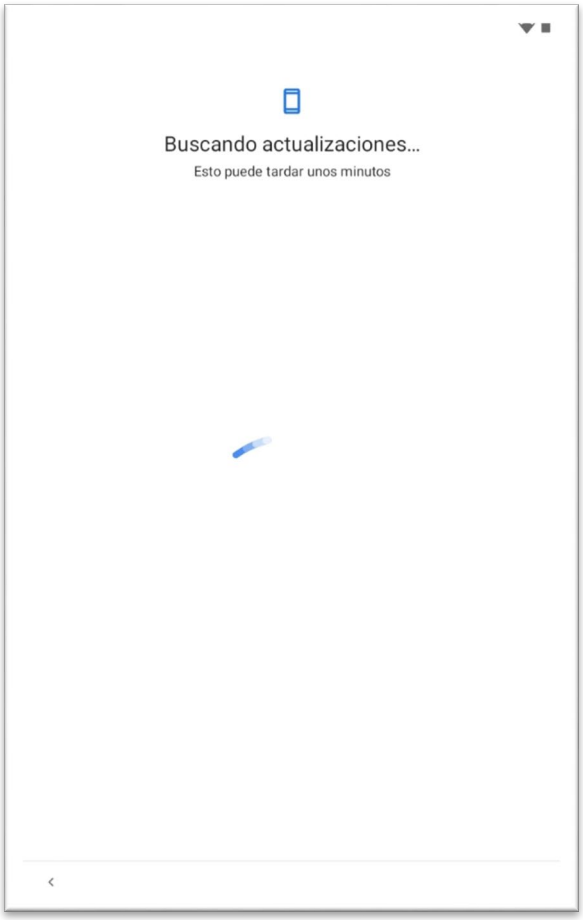
7. Hacer *click* en "*Aceptar y continuar*".



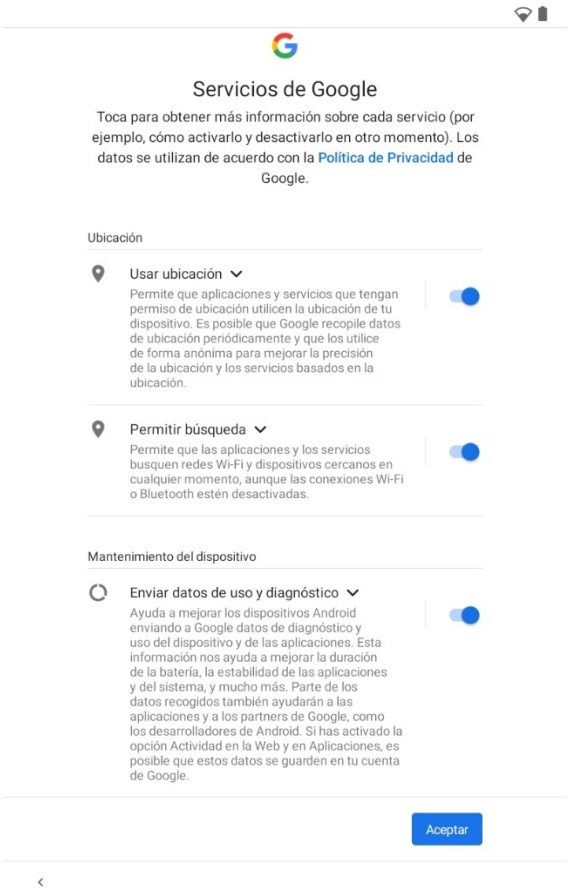
8. Hacer *click* en "*Siguiente*".



9. El dispositivo buscará actualizaciones. En caso de existir actualizaciones de *firmware*, rechazar.



10. Configurar los permisos de los servicios de Google en función de las necesidades y políticas de la empresa.



11. Hacer *click* en “Aceptar”.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

A continuación, se describen los pasos necesarios para activar la configuración específica para que el dispositivo opere en modo seguro. Los siguientes pasos deberán realizarse como administrador desde el MDM:

- **Deshabilitar la funcionalidad de *debug*** *(addUserRestriction -> DISALLOW_DEBUGGING_FEATURES).*
- Establecer la **calidad mínima de la contraseña a ALTA** (*setRequiredPasswordComplexity*).
- Habilitar la **política *Common Criteria*** *(setCommonCriteriaModeEnabled).*
- **Deshabilitar la instalación de aplicaciones desde fuentes no conocidas** *(addUserRestrictions –> DISALLOW_INSTALL_UNKNOWN_SOURCES y DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY).*
- Habilitar **auditoría de seguridad** (*setSecurityLoggingEnabled*).
- Establecer un número razonable (por ejemplo 5) de intent**os fallidos de inicio de sesión** tras los cuales el dispositivo realizará un borrado de datos de usuario (*setMaximumFailedPasswordsForWipe*).

En la aplicación *Ajustes* del dispositivo, ir a *Privacidad* y deseleccionar *"Mostrar contraseñas".*

A continuación, **deshabilitar el modo *Fastboot*** siguiendo los siguientes pasos:

1. Apagar la Tablet.
2. Encender la Tablet manteniendo pulsado el botón de subir volumen hasta que aparezca un menú.
3. Pulsar el botón de bajar volumen para entrar en modo *Fastboot*.
4. Conectar a un ordenador con las herramientas de la plataforma del SDK de Android.
5. Ejecutar el comando "*fastboot oem factory-mode 0*" para deshabilitar el modo *Fastboot*.
6. Ejecutar el comando "*fastboot reboot*" para reiniciar al sistema operativo Android, o simplemente apagar siguiendo las instrucciones en pantalla (en español: "Mantener pulsado los botones "*Volumen abajo*" y "*Encendido*" a la vez para forzar el apagado del dispositivo). La siguiente vez que se inicie el dispositivo, arrancará el sistema operativo Android.

Por último, **es recomendable deshabilitar las actualizaciones automáticas de manera que el operador sea consciente de las actualizaciones**, de manera que se mantenga en la versión del producto objeto de este documento. Para ello, desde la aplicación Ajustes ir a *Sistema > Actualización del sistema* y arriba a la izquierda hacer *click* en el botón con

3 puntos. En la nueva pantalla, deseleccionar la opción *"Descargar e instalar automáticamente cuando esté conectado a WLAN".*

6.2 AUTENTICACIÓN

Un usuario puede autenticarse en el dispositivo haciendo uso de dos mecanismos de autenticación: PIN o contraseña.

Las restricciones aplicadas en la sección anterior aplican a ambas y se consideran equivalentes, por lo que la organización es libre de decidir el mecanismo en función de las garantías que necesiten.

En cualquier caso, los datos del usuario solo son accesibles únicamente cuando se desbloquea (autentica) por primera vez tras el encendido de la Tablet. Hasta entonces, permanecen cifrados con una clave interna que se deriva de la entrada del usuario.

Además de esto, un usuario debe autenticarse antes de ejercer la mayor parte de la funcionalidad disponible en el dispositivo. Mientras que el usuario no se autentique, la funcionalidad que puede realizarse en la Tablet es muy limitada. Únicamente se permite:

- Reiniciar.
- Hacer llamada de emergencias.
- Habilitar funcionalidad no restringida por el administrador (MDM).

Además de otras opciones que no afectan a la seguridad del producto.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

El dispositivo puede administrarse únicamente mediante dos (2) interfaces:

- Interfaz local. El usuario se autentica en la Tablet y puede acceder a las diferentes aplicaciones y ajustes permitidos por el MDM (administrador).
- MDM. El dispositivo es gestionado por un servidor MDM, del cual recibe configuración y políticas a aplicar.

6.4 CONFIGURACIÓN DE IPSEC

El producto ofrece una API a las aplicaciones de terceros para que un usuario pueda instalar una aplicación que redirija todo el tráfico que se produzca en el producto a través de un túnel IPSEC.

Si un usuario desea hacer uso de esta funcionalidad, lo primero que deberá hacer será elegir un cliente IPSEC (por ejemplo, *strongSwan VPN client*).

Durante la configuración, se recomienda que se establezca el canal haciendo uso de algoritmos seguros tales como IKEv2 EAP y que, además, en cuanto a certificados, se

hagan uso de tamaños de claves permitidos por la categoría ALTA de ENS (por ejemplo, mayor que 3072 bits en RSA).

6.5 CONFIGURACIÓN WI-FI RECOMENDADA

El producto es capaz de conectarse a un punto de acceso haciendo uso de protocolos domésticos tales como WEP, WPA o WPA2 Personal. No obstante, se recomienda el uso de protocolos más seguros como WPA2 Enterprise. Concretamente, el producto es compatible con el protocolo de autenticación EAP-TLS, el cual puede ser configurado por el usuario de la siguiente manera:

1. Importar en el producto la CA y el par clave-certificado (p12) del usuario instalándolos.
2. Abrir la aplicación de Ajustes y desde el menú "*Redes e Internet*", hacer *click* en Internet.
3. Hacer *click* en el punto de acceso WPA/WPA2-Enterprise.
4. En Método EAP, seleccionar TLS.
5. En Certificado AC, seleccionar la CA importada.
6. En Dominio, establecer el *Common Name* del certificado del servidor.
7. En Certificado de usuario, seleccionar el certificado del usuario importado.
8. En Identidad, establecer el nombre de usuario que se ha definido en el servidor RADIUS.
9. Finalmente, hacer *click* en "*Conectar*"

6.6 USO DE TLS SDK ANDROID

El producto ofrece una API para que las aplicaciones de terceros puedan establecer comunicaciones con entidades externas. Se recomienda que las aplicaciones que hagan uso de TLS cumplan con los requisitos criptográficos descritos en la guía [CCN-STIC-807] (versión de TLS v1.2 o superior y uso exclusivamente de suites de cifrado recomendadas).

La API del producto permite realizar esta restricción de la siguiente manera:

- Para versión TLS: función *setEnabledProtocols* de la clase *SSLSocket*.
- Para suites de cifrado: función *setEnabledCipherSuites* de la clase *SSLSocket*.

6.7 ACTUALIZACIONES

Para recibir actualizaciones, el producto se conecta a los servidores de Lenovo. Esta comunicación se hace mediante el uso de TLSv1.2. Existen dos (2) opciones para recibir actualizaciones:

- Actualizaciones manuales. El usuario, desde la aplicación de Ajustes, puede ir a Sistema > Actualización del sistema y hacer click en "Buscar actualizaciones" para comprobar si hay actualizaciones disponibles. De existir, el usuario puede decidir si actualizar o no el firmware del dispositivo.
- Actualizaciones automáticas. El usuario puede configurar si quiere que el dispositivo consulte de manera periódica si existen actualizaciones disponibles y que se instalen de manera desatendida. Para ello, desde el mismo menú descrito en el punto anterior, hacer click en los 3 puntos arriba a la izquierda y habilitar "*Descargar e instalar automáticamente cuando esté conectado a WLAN*".

6.8 AUTO-CHEQUEOS

El producto incluye funciones para realizar auto-chequeos y comprobaciones de integridad del software/firmware, de forma que pueda detectar cuándo está fallando o puede estar corrupta. Si falla algún auto-chequeo (los cuales se ejecutan al inicio), el producto no entrará en modo operativo. También incluye mecanismos (es decir, verificación de la firma digital de cada nueva imagen) para que el propio dispositivo pueda actualizarse garantizando al mismo tiempo que las actualizaciones no introducirán cambios maliciosos o inesperados en el producto. La comprobación de la firma digital también se extiende a la verificación de las aplicaciones antes de su instalación, ya que todas las aplicaciones deben estar firmadas (incluso si están autofirmadas).

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

El producto usa diferentes tipos de registros de auditoria para recopilar todos los eventos necesarios:

1. Auditoría de seguridad. Una lista completa de los eventos auditables puede encontrarse aquí:

   https://developer.android.com/reference/android/app/admin/SecurityLog#constants_1.

   Los valores que se encuentran en la lista representan las palabras clave del registro de seguridad utilizadas en esta función de registro junto con una descripción de lo que significa el registro y cualquier información/variable adicional presente en el registro de auditoría. Además, el siguiente enlace proporciona la información adicional que se puede obtener cuando un MDM solicita una copia de estos registros:

   https://developer.android.com/reference/android/app/admin/SecurityLog.SecurityEvent.

Cada registro contiene una palabra clave o frase que describe el suceso, la fecha y la hora del suceso, así como otros valores específicos que proporcionan información sobre el éxito, el fracaso y otros datos relevantes.

2. Logcat. Al igual que la auditoría de seguridad, los registros Logcat contienen la fecha, la hora y otros valores específicos. Además, los registros Logcat proporcionan un valor que se asigna a un ID de usuario para identificar qué usuario causó el evento que generó el registro. Por último, los registros Logcat son descriptivos y no requieren que el administrador conozca la plantilla del registro para comprender sus valores. Los registros Logcat no se pueden exportar, pero pueden ser visualizados por un administrador a través de un agente MDM.

7. FASE DE OPERACIÓN

Los procedimientos operativos mínimos que deben llevarse a cabo durante la fase de operación y mantenimiento del producto son los siguientes:

- Comprobaciones periódicas del *hardware* y *software* para garantizar que no se ha introducido hardware o software no autorizado. Para ello, repetir los pasos descritos en *4.1 ENTREGA SEGURA DEL PRODUCTO*.
- Aplicación regular de los parches de seguridad, con objeto de mantener una configuración segura.
- Mantenimiento de los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.
- Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

8. REFERENCIAS

CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad, Mayo 2022.

9. ABREVIATURAS

API	Application Programming Interface
CA	Certificate authority
CPSTIC	Catálogo de Productos STIC.
EAP	Extensible Authentication Protocol
ENS	Esquema Nacional de Seguridad.
IPSEC	IP Security
MDM	Mobile Device Management
PIN	Personal Identification Number
QR	Quick Response code
RSA	Rivest-Shamir-Adleman algorithm
SDK	Software Development Kit
TEE	Trusted Execution Environment
TLS	Transport Layer Security
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL