Universitat Oberta de Catalunya

uoc.edu

Sistema de Comunicaciones Móviles Seguras en un entorno empresarial

Daniel Brande Hernández
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones.
Seguridad Empresarial

Amadeu Albós Raya

31 de diciembre de 2019


Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Copyright © 2019 Daniel Brande Hernández.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU Free Documentation License".

C) Copyright

© Daniel Brande Hernández
Reservados todos los derechos. Está prohibido la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la impresión, la reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler y préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Comunicaciones Móviles Seguras en un entorno empresarial*
Nombre del autor:	*Daniel Brande Hernández*
Nombre del consultor/a:	*Amadeu Albós Raya*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	12/2019
Titulación:	Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Área del Trabajo Final:	*Seguridad empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*Seguridad empresarial, comunicaciones seguras, movilidad.*

Resumen del Trabajo

Este proyecto pretende ser un documento técnico que sirva como arquitectura de referencia para la implementación de un sistema de comunicaciones móviles seguras corporativas para una gran entidad bancaria en la que se gestiona información con distintos niveles de protección en función de su clasificación.

Para ello:

- Se partirá de un análisis de la tecnología y de los principales riesgos y amenazas a los que puede estar sometida una organización por el uso de un sistema de estas características.
- Se revisará y analizará el estado del arte de las soluciones de gestión de la movilidad empresarial existentes actualmente en el mercado.
- Se revisará y analizará el estado del arte de las soluciones de comunicaciones móviles seguras existentes actualmente en el mercado.
- Se propondrán las directrices, pautas y guías del modelo a implementar, teniendo en cuenta las diferentes amenazas y contramedidas para mitigarlas, y el estado del arte del mercado.
- Se llevará una validación de los requisitos de seguridad del diseño, revisando si efectivamente se están mitigando las amenazas.

En cualquier caso, el proyecto no estará condicionado a una única solución de mercado, sino que podrá implementarse combinando una o varias soluciones de las ya existentes, siempre y cuando la combinación de las mismas respete los principios que en este documento se indican.

Abstract

This Project aims to be a reference architecture for the implementation of a corporate secure mobile communications system for a large banking company. Information with different levels of protection is managed by the organization based on its classification.

To achieve this, it will be necessary:

- To perform an analysis of technology and main risk and threats to which the organization may be exposed.
- To analyze the state of the art of business mobility management solutions.
- To analyze the state of the art of secure mobile communications solutions.
- To propose the guidelines and requirements to be implemented, considering the different threats and countermeasures to mitigate them, and the state of the art previously analyzed.
- To carry out a validation of the different security requirements of the design.

The project will never be conditioned to a single market solution and may be implemented by combining one or several solutions, as long as the combination of them respects the principles and requirements indicated within the document.

Agradecimientos

En primer lugar, quisiera agradecer a mi tutor, Amadeu Albós, toda su ayuda y sus consejos para poder llevar a cabo mi TFM. Agradecer también tanto a Amadeu como a Víctor García la posibilidad que me han dado de poder hacer mi propia propuesta en lo que respecta a la temática de este trabajo.

Quisiera también agradecer la ayuda y la predisposición de todos los profesores consultores del máster, que, a pesar de la distancia, han sido capaces de transmitir sus conocimientos y la motivación suficiente a los alumnos para conseguir que saquemos tiempo de nuestro día a día tras el trabajo para seguir aprendiendo y en contacto constante con la universidad.

No puedo no mencionar aquí a mis compañeros del CESTIC que empezaron siendo compañeros de trabajo y que se convirtieron en amigos casi de un día para otro. Gracias por haber hecho que haya vivido una de las mejores etapas de mi vida a vuestro lado y por la cantidad de buenos momentos y anécdotas que me llevo conmigo (de esas que te pasarías el día contando a tus nietos).

Gracias también a mis nuevos compañeros de trabajo por ser tan buena gente y por darme la seguridad de que esta nueva etapa promete a vuestro lado.

Gracias a mis amigos (presentes, pasados y futuros) por los buenos momentos compartidos, por vuestro apoyo y por aguantarme a pesar de ser tan cansino.

Y, por último, pero no menos importante: gracias a mi familia. A mis abuelos, mis padres, mi hermana, mis tíos y primos, Rober, Gonzalo, Vicky y Manolo. Gracias por vuestra paciencia, por cuidarme, por vuestro apoyo, por todos los buenos momentos que pasamos juntos y por quererme tal y como soy.

Y gracias a todo aquél que habiendo leído todo esto, no haya encontrado su nombre. Probablemente, se me haya pasado.

Daniel Brande Hernández
Diciembre de 2019

"Un gran obstáculo para alcanzar la felicidad es el prometerse una felicidad demasiado grande". BERNARD LE BOVIER DE FONTENELLE.

ÍNDICE

1. Introducción

1.1 Contexto y justificación del Trabajo

En plena era de la digitalización, la proliferación de dispositivos móviles y la mejora del ancho de banda de las conexiones inalámbricas a internet han impactado de manera muy significativa en la forma de trabajar y de relacionarse entre las empresas y los empleados.

Hoy en día es cada vez más frecuente que las empresas pongan a disposición de sus empleados los medios tecnológicos necesarios para que éstos puedan trabajar prácticamente desde cualquier lugar y en cualquier momento. Para ello, cada vez son más los departamentos de TI que se apoyan en este tipo de tecnologías que facilitan y promueven el acceso a la información y a los recursos corporativos en múltiples situaciones:

- Empleados que acceden desde casa o cuando están de viaje a los recursos corporativos haciendo uso de los dispositivos móviles: portátiles, smartphones, etc.
- Personal ajeno a la organización, que hace uso de este tipo de tecnologías para acceder a ciertos recursos que la organización pone a su disposición para llevar a cabo ciertas gestiones.
- Empleados que están teletrabajando y que necesitan hacer uso de los recursos corporativos como si estuviesen físicamente en la oficina.

No cabe duda de que este tipo de tecnologías proporcionan una serie de ventajas tanto para la empresa como para los empleados:

- Reducción de costes en desplazamientos.
- Aumento en la productividad y en el rendimiento de trabajo de los empleados.
- Mayor satisfacción y flexibilidad de los empleados, lo que conlleva el aumento del compromiso con la empresa.
- Eficiencia en el servicio al gestionarlo en tiempo real.

Si embargo, el hecho de trabajar con dispositivos móviles que acceden a recursos corporativos conlleva una serie de riesgos importantes de seguridad para las empresas, a los que habrá que prestar especial atención:

- Pérdida o robo de información.
- Mal uso de los dispositivos móviles.
- Robo de credenciales.
- Robo de los dispositivos.
- Utilización de sistemas de conexión no seguros, etc.

Por ejemplo, imaginemos que una organización permite el acceso desde cualquier dispositivo móvil (bien sea proporcionado por la propia organización, o propiedad del usuario) al correo electrónico, el calendario y la gestión de los

contactos. Si hay datos sensibles que se almacenan en un dispositivo móvil sobre el que no se han implementado unas medidas mínimas de seguridad, un atacante puede fácilmente obtener acceso no autorizado a todos esos datos. Además, y si se permite también el acceso remoto a otros datos de la organización, el atacante podría obtener acceso no autorizado no sólo a los datos que persisten en el dispositivo, sino también a cualquier otro potencialmente accesible por el dispositivo, dentro de la organización.

¿Qué problema se pretende resolver con este trabajo?

Hasta ahora se ha hecho referencia a un problema común al que se enfrentan la mayor parte de las organizaciones: cómo gestionar el acceso a los recursos corporativos desde los dispositivos móviles. En este trabajo, abordaremos esta problemática desde el punto de vista de una gran organización bancaria, en la que además de enfrentarse al problema de cómo gestionar los dispositivos móviles y el acceso a los recursos corporativos, es necesario tener en consideración los siguientes aspectos:

- Como parte de la gestión de riesgos de seguridad de la información, la organización ha diseñado una **taxonomía de referencia para clasificar la información**. El propietario de cada activo de información es el encargado de realizar la clasificación de la información, y ello determina las medidas de seguridad que se aplican a la información en todo su ciclo de vida. Actualmente la organización dispone de los siguientes niveles de clasificación de la información, y los dispositivos móviles han de ser capaces de gestionarlo:
    - Confidencial.
    - Restringido.
    - Uso interno.
    - Uso público.

- Además de la información y el acceso a los recursos corporativos, la organización ha mostrado una gran preocupación por las **comunicaciones de voz y el envío de mensajería desde el teléfono móvil**. Si bien es cierto que no les preocupa que la mayoría de sus empleados lleven a cabo las llamadas a través de la red móvil habitual, la organización precisa de un sistema de mensajería que sea seguro desde el móvil y necesitan que se asegure que para ciertos departamentos existe un nivel de seguridad adicional en las llamadas que garantice que están protegidas frente al acceso de un tercero a las mismas:
    - Comunicaciones estratégicas de personal de alta dirección.
    - Comunicaciones en áreas o entornos especialmente sensibles y regulados, tratando aspectos confidenciales.

1.2 Objetivos del Trabajo

El objetivo del proyecto consiste en elaborar un documento técnico que permita a una organización con las características descritas en el apartado anterior establecer un modelo o **arquitectura de referencia** para la **implementación de**

un sistema de comunicaciones móviles seguro corporativo, con la flexibilidad suficiente para que sea posible:

- Gestionar **información categorizada con distintos niveles de seguridad** (y, por lo tanto, con distintas medidas de protección de la información).
- Permitir el **envío seguro de mensajes entre los dispositivos** de todos los empleados.
- Permitir la activación de un **sistema de llamadas seguras** entre ciertos empleados o departamentos, según las necesidades definidas por la organización.

En definitiva, el trabajo tendrá que diseñar un sistema de estas características, estableciendo un conjunto de directrices, pautas y guías para implementar un nuevo despliegue corporativo. Para ello, considerará la combinación de:

- Soluciones de **gestión de la movilidad empresarial** (EMM) ya existentes en el mercado, centradas en la protección y gestión de los dispositivos, sus aplicaciones, el contenido al que acceden y los servicios de identificación, autorización y monitorización de éstos de cara al acceso a los recursos corporativos.

- Soluciones de **comunicaciones móviles seguras** existentes en el mercado, que protejan las comunicaciones por voz y el envío de mensajes entre empleados de la organización de las redes de terceros (no confiables) por las que pueda pasar la información en tránsito.

1.3 Enfoque y método seguido

La metodología a seguir va muy en línea con los objetivos detallados en el apartado anterior, y con la planificación temporal propuesta por la Universidad para las diferentes entregas que deben realizarse en este trabajo. Los diferentes pasos a llevar a cabo son los que se detallan a continuación:

a) Se partirá de un **análisis de la tecnología y de los principales riesgos y amenazas** a los que puede estar sometida una organización. Para ello, profundizaremos en la revisión de estándares y guías (NIST, CCN-STIC, ISO 2700X, etc.) relacionados con el análisis de riesgos y llevaremos a cabo una aplicación práctica de los mismos que nos permita definir los controles de seguridad que implementaremos en nuestro diseño.

En cualquier caso y como requisito inicial de diseño, se partirá de la base de que se utilizarán dispositivos móviles de mercado, a cuyo proceso de diseño y fabricación no ha tenido acceso la organización. Además, estos dispositivos harán uso de las redes de acceso de telefonía móvil de operadores comerciales. Estas hipótesis de partida imponen ciertas limitaciones y requieren de la realización de ciertas matizaciones y esfuerzos sobre el modelado de la solución final, pero aportan enormes ventajas en cuanto al coste, el tiempo de despliegue y la flexibilidad en la reposición de los terminales.

b) Se revisará y analizará el **estado del arte de las soluciones de gestión de la movilidad empresarial** existentes actualmente en el mercado (EMM). De esta forma conseguiremos entender cómo abordan los problemas de seguridad empresarial en este ámbito las soluciones ya existentes en el mercado con el objetivo de adquirir el aprendizaje suficiente para el diseño de la gestión de la seguridad en los dispositivos.

c) Se revisará y analizará el **estado del arte sobre las soluciones de comunicaciones móviles seguras** existentes actualmente en el mercado. En este punto nos referimos a soluciones utilizadas para proteger las comunicaciones móviles (voz y mensajería) efectuadas desde los dispositivos móviles. Al igual que el punto anterior, este punto nos permitirá entender cómo abordan las comunicaciones de voz y de mensajería alguna de las soluciones de Voz IP existentes en el mercado, con el objetivo de aplicarlas al diseño de la parte de comunicaciones.

d) Con la información recopilada de los puntos anteriores, se llevará a cabo el **diseño de una arquitectura de referencia para la implantación en la organización propuesta de un sistema de comunicaciones móviles corporativos**, describiendo los bloques funcionales involucrados, los componentes necesarios y los requisitos de seguridad a implementar para mitigar los riesgos previamente identificados. Este punto permitirá profundizar en los conceptos de diseño de red, aplicación de controles de seguridad, así como en aspectos más relacionados con el análisis y la estructuración de cara a presentar un diseño y a mantener la trazabilidad con el conjunto de requisitos definidos y los riesgos analizados.

e) Por último, **se llevará a cabo una validación de los requisitos de seguridad del diseño**, en la que se revisará si efectivamente se están cubriendo los riesgos que se han identificado con las medidas de seguridad implementadas en el diseño, extraeremos las conclusiones del trabajo realizado y propondremos mejoras o aspectos a desarrollar en el futuro.

Para conseguir llevar a cabo esta metodología, planteamos el desarrollo del trabajo en las siguientes fases:

1. **Fase de planificación (2 semanas).** Esta primera fase se centra en la elaboración del plan de trabajo. Se describe el problema a resolver, los objetivos y la metodología a emplear con la realización del TFM, las tareas a llevar a cabo para alcanzar los objetivos descritos y la planificación temporal detallada de cada tarea (con sus posibles dependencias).

2. **Fase de búsqueda de información y documentación (2 semanas)**. En esta fase se revisarán todos los aspectos relativos al estado del arte de las soluciones de gestión de la movilidad empresarial y de comunicaciones móviles seguras existentes actualmente en el mercado, así como las guías y estándares de aplicación vigentes en los que se puede encontrar información sobre requisitos de seguridad relativos a las

comunicaciones móviles. Los resultados de esta fase se plasmarán en un capítulo de introducción en el TFM.

3. **Fase de análisis de riesgos (2 semanas)**. En esta fase se llevará a cabo el análisis de los principales riesgos a los que están sometidos las organizaciones y sus usuarios por el hecho de utilizar los dispositivos móviles en un entorno corporativo.

4. **Fase de diseño de la solución (7,5 semanas)**. Una vez se han estudiado las diferentes soluciones existentes en el mercado, y se han analizado los riesgos del uso de la tecnología, se llevará a cabo la propuesta de diseño de la arquitectura o modelo de referencia, detallando los bloques funcionales y componentes utilizados y los requisitos correspondientes. Adicionalmente, se desarrollará el modelo con la solución técnica. La idea es tener una primera versión para la Entrega 3 que se irá completando con los aspectos que se vayan viendo hasta cerrarla en la Entrega 4.

5. **Fase de validación de requisitos (3 semanas)**. El objetivo de esta fase consiste en verificar que efectivamente se están mitigando los riesgos detectados en la fase de análisis de riesgos con el diseño realizado.

6. **Fase de presentación de resultados, conclusiones y trabajo futuro (1 semana)**. En esta fase sintetizarán las conclusiones del trabajo realizado, y se presentarán futuras líneas de trabajo.

1.4 Planificación del Trabajo

En este apartado se presentan las distintas tareas que se llevarán a cabo en cada una de las fases anteriormente descritas para alcanzar los objetivos del presente Trabajo Fin de Máster. Se describen también los entregables de la memoria que serán efectivos para cada una de las entregas parciales.

Tal y como se observa en la tabla de la página siguiente, el trabajo constará de 5 entregas, que coinciden con las Pruebas de Evaluación Continua (PEC) marcadas por la Universidad para la entrega de este TFM.

En las próximas páginas se relacionan las fases descritas anteriormente con las entregas propuestas en la tabla anterior. Además, se hace una breve descripción del contenido a plasmar en cada uno de los capítulos y se relacionan con la entrega que corresponde.

ID	TÍTULO	INICIO	FIN	DURACIÓN
1	ENTREGA 1: PLAN DE TRABAJO	18/09/2019	01/10/2019	13
1.1	Contexto y justificación del trabajo	23/09/2019	25/09/2019	2
1.2	Objetivos del trabajo	25/09/2019	27/09/2019	2
1.3	Enfoque y método seguido	27/09/2019	28/09/2019	1
1.4	Planificación del trabajo	28/09/2019	30/09/2019	2
2	ENTREGA 2: INTRODUCCIÓN y ANÁLISIS DE AMENAZAS	02/10/2019	29/10/2019	27
2.1	Revisión estado del arte Movilidad Empresarial	02/10/2019	06/10/2019	4
2.2	Revisión estado del arte Comunicaciones móviles seguras	07/10/2019	13/10/2019	6
2.3	Introducción	02/10/2019	13/10/2019	11
2.4	Análisis de amenazas y principales contramedidas	14/10/2019	29/10/2019	15
3	ENTREGA 3: DISEÑO DE LA SOLUCIÓN (PARCIAL)	30/10/2019	26/11/2019	27
3.1	Búsqueda de información	30/10/2019	06/11/2019	7
3.2	Descripción de la empresa y su infraestructura	07/11/2019	13/11/2019	6
3.3	Elaboración del modelo de referencia	13/11/2019	26/11/2019	13
3.3.1	Bloques funcionales: Dispositivo	13/11/2019	16/11/2019	3
3.3.2	Bloques funcionales: Red móvil	18/11/2019	20/11/2019	2
3.3.3	Bloques funcionales: Infraestructura organización	21/11/2019	26/11/2019	5
3.4	Solución técnica. Implementación del modelo de referencia.	13/11/2019	20/12/2019	37
4	ENTREGA 4: MEMORIA FINAL	27/11/2019	31/12/2019	34
4.2	Validación de requisitos	20/12/2019	30/12/2019	10
4.3	Conclusiones	20/12/2019	25/12/2019	5
4.4	Bibliografía	25/12/2019	30/12/2019	5
4.5	Glosario	25/12/2019	30/12/2019	5
5	ENTREGA 5: PRESENTACIÓN	01/01/2020	07/01/2020	6
5.1	Elaboración de la presentación	01/01/2020	07/01/2020	6

Tabla 1 Planificación temporal TFM

PLANIFICACIÓN TEMPORAL PARA TFM SEGURIDAD EMPRESARIAL

TÍTULO	SISTEMA COMUNICACIONES MÓVILES SEGURAS EN UN ENTORNO EMPRESARIAL
AUTOR	DANIEL BRANDE HERNÁNDEZ
PROFESOR	AMADEU ALBÓS RAYA
FECHA	domingo, 29 de septiembre de 2019

					FASE 1		FASE 2		FASE 3		FASE 4							FASE 5		FASE 6
ID	**TÍTULO**	**INICIO**	**FIN**	**DURACIÓN**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**S9**	**S10**	**S11**	**S12**	**S13**	**S14**	**S15**	**S16**
1	ENTREGA 1: PLAN DE TRABAJO	18/09/2019	01/10/2019	13																
1.1	Contexto y justificación del trabajo	23/09/2019	25/09/2019	2																
1.2	Objetivos del trabajo	25/09/2019	27/09/2019	2																
1.3	Enfoque y método seguido	27/09/2019	28/09/2019	1																
1.4	Planificación del trabajo	28/09/2019	30/09/2019	2																
2	ENTREGA 2: INTRODUCCIÓN y ANÁLISIS DE RIESGOS	02/10/2019	29/10/2019	27																
2.1	Revisión estado del arte Movilidad Empresarial	02/10/2019	06/10/2019	4																
2.2	Revisión estado del arte Comunicaciones móviles seguras	07/10/2019	13/10/2019	6																
2.3	Introducción	02/10/2019	13/10/2019	11																
2.4	Análisis de amenazas y principales contramedidas	14/10/2019	29/10/2019	15																
3	ENTREGA 3: DISEÑO DE LA SOLUCIÓN (PARCIAL)	30/10/2019	26/11/2019	27																
3.1	Búsqueda de información	30/10/2019	06/11/2019	7																
3.2	Descripción de la empresa y su infraestructura	07/11/2019	13/11/2019	6																
3.3	Elaboración del modelo de referencia	13/11/2019	26/11/2019	13																
3.3.1	Bloques funcionales: Dispositivo	13/11/2019	16/11/2019	3																
3.3.2	Bloques funcionales: Red móvil	18/11/2019	20/11/2019	2																
3.3.3	Bloques funcionales: Infraestructura organización	21/11/2019	26/11/2019	5																
3.4	Solución técnica. Implementación del modelo de referencia.	13/11/2019	20/12/2019	37																
4	ENTREGA 4: MEMORIA FINAL	27/11/2019	31/12/2019	34																
4.2	Validación de requisitos	20/12/2019	30/12/2019	10																
4.3	Conclusiones	20/12/2019	25/12/2019	5																
4.4	Bibliografía	25/12/2019	30/12/2019	5																
4.5	Glosario	25/12/2019	30/12/2019	5																
5	ENTREGA 5: PRESENTACIÓN	01/01/2020	07/01/2020	6																
5.1	Elaboración de la presentación	01/01/2020	07/01/2020	6																

Figura 1 Diagrama temporal desarrollo TFM

1.5 Breve sumario de productos obtenidos

Como se ha detallado en apartados anteriores, el principal producto a obtener en este TFM es una guía o arquitectura de referencia que permita ayudar una organización de cualquier sector empresarial a desarrollar una implementación de un sistema de comunicaciones móviles que sea seguro, flexible y orientado a riesgos. En la medida de lo posible, se intentará facilitar el diseño para que la implementación de los mecanismos de seguridad se pueda incorporar prácticamente desde el comienzo del proyecto.

1.6 Breve descripción de los otros capítulos de la memoria

En este apartado describimos a grandes rasgos el contenido de la memoria de este Trabajo Fin de Máster:

1. **Sobre este trabajo de fin de máster (Entrega 1).** Se trata del capítulo en el que estamos actualmente, donde se introduce el contexto y justificación del trabajo explicando el detalle del problema a resolver, se enumeran los objetivos que se quieren alcanzar con la realización del TFM, se describe la metodología a seguir durante el desarrollo y se presenta una planificación orientativa de las tareas a llevar a cabo para alcanzar los objetivos propuestos.

2. **Introducción (Entrega 2).** El objetivo de este capítulo consiste en poner al lector en situación sobre lo que es un Sistema de Comunicaciones Móviles Seguros. Se hará referencia al estado del arte de las soluciones de gestión de la movilidad empresarial y comunicaciones móviles seguras existentes actualmente en el mercado, así como a las principales guías y estándares de aplicación vigentes que recogen normativa al respecto.

3. **Análisis de amenazas (Entrega 2).** En este capítulo se hará mención a los principales riesgos y amenazas que pueden afectar a las organizaciones y usuarios por el hecho de utilizar los dispositivos móviles en un entorno corporativo, y algunas de las principales contramedidas para mitigar dichos riesgos.

4. **Modelo de referencia (Entrega 3).** En este capítulo se presentará un modelo de referencia para el diseño de un Sistema de Comunicaciones móviles seguras, en base al análisis de riesgos propuesto en el capítulo 3.

5. **Diseño de la solución (Entregas 3 y 4).** En este capítulo se presentará una implementación real del modelo de referencia, describiendo el detalle de los componentes y los requisitos de seguridad que aplican.

6. **Validación de requisitos (Entrega 4).** En este capítulo se presentará el diseño realizado, y una matriz de trazabilidad en la que se relacionarán los riesgos o problemas de seguridad detectados con los controles implantados en el modelo diseñado. De esta manera será posible verificar en qué medida se están mitigando esos riesgos detectados.

7. **Conclusiones y trabajo futuro (Entrega 4).** En este capítulo se presentarán las principales conclusiones de este TFM y futuras líneas de trabajo.

8. **Glosario, bibliografía y anexos (Entrega 4).** Como parte final de este TFM, se propondrán las referencias, los términos y los anexos para complementar los aspectos explicados en el mismo.

2. Introducción a los Sistemas de Comunicaciones Móviles Seguros

2.1 Introducción

Los dispositivos móviles que existen actualmente en el mercado son complejos y ofrecen una gran variedad de funcionalidades y capacidad computacional. Desde el punto de vista de estas capacidades que tienen son equiparables a cualquier ordenador portátil o de escritorio. Es más, disponen de capacidades adicionales a las de un ordenador cualquiera, lo que significa que no sólo comparten las amenazas de seguridad típicas que pueden afectar a un ordenador, sino que además existen algunas específicas para los dispositivos móviles. El conjunto de todas estas amenazas se presenta en el Informe de Evaluación de amenazas a dispositivos móviles e infraestructura del NIST, (NISTIR 8144, Assessing Threats to Mobile Devices & Infrastructure: the Mobile Threat Catalogue, 2016).

No obstante, y antes de introducir este tipo de amenazas en el próximo capítulo, es fundamental comprender que en un Sistema de Comunicaciones Móviles seguras interviene un ecosistema de elementos que se relacionan también con el dispositivo móvil, y sobre los que también existe una gran variedad de amenazas.

En este capítulo pondremos al lector en situación definiendo este conjunto de elementos que deben tenerse en cuenta. Se hará referencia también a las soluciones de movilidad empresarial y comunicaciones móviles seguras existentes actualmente, así como a los principales guías y estándares que recogen aspectos de seguridad relativos al entorno de la movilidad empresarial.

2.2 Elementos que conforman el sistema

El primer aspecto a tener en cuenta a la hora de pensar en un Sistema de Comunicaciones Móviles seguras para nuestra organización es que existe un ecosistema de elementos con los que el teléfono móvil va a interactuar y que debemos tener en cuenta a la hora de evaluar la seguridad móvil en un entorno empresarial. En la Figura 2 Elementos del Sistema (*Study on Mobile Device Security, 2017*) se presenta el conjunto de estos elementos, que pasamos a describir a continuación:

1. El **dispositivo móvil**, dividido en varias capas: aplicaciones, sistema operativo, firmware y hardware.
2. Las **redes** que utiliza el dispositivo (Wi-Fi, Bluetooth, NFC, etc.) y los distintos servicios proporcionados por los operadores de red.
3. Los **servicios y la infraestructura proporcionados por fabricantes**, relacionados fundamentalmente con actualizaciones de los dispositivos, copias de seguridad y mercados de aplicaciones específicos.
4. Los **servicios proporcionados por terceros.** Bajo esta casuística se encuentran una infinidad de servicios proporcionados por terceros (copias de seguridad, pagos, almacenamiento en la nube, etc.). No obstante, a

efectos de este trabajo nos referiremos en este punto a los grandes distribuidores digitales de aplicaciones (Google Play, Apple Store).

5. Los **servicios y la propia infraestructura de la organización**, incluyendo todos los aspectos relativos a la gestión de dispositivos móviles (MDM), mercados de aplicaciones internos y gestión de aplicaciones y contenido (MAM, MCM).

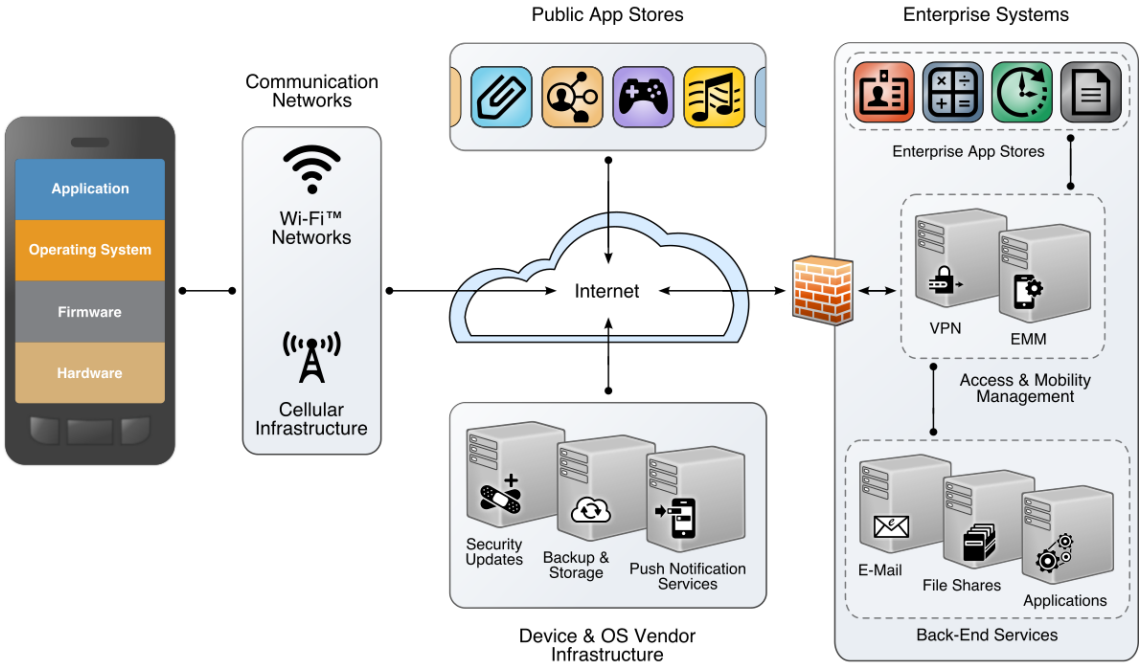

Figura 2 Elementos del Sistema

Adicionalmente, y de cara a valorar las amenazas en el próximo capítulo, es necesario tener en consideración la gran cantidad de interfaces que presenta un dispositivo móvil (múltiples interfaces radio, gran variedad de sensores, etc.).

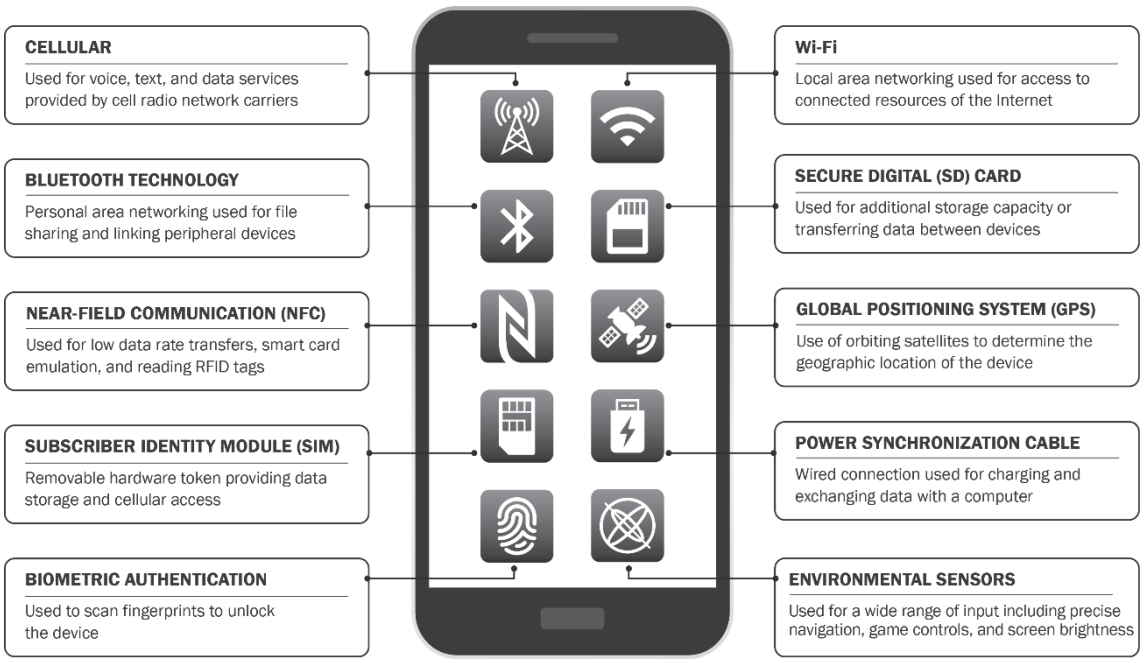

Figura 3 Interfaces de un dispositivo móvil

2.3 Gestión de la movilidad empresarial

Para asegurar que el conjunto de todos estos elementos se comporta de manera segura, es necesario recurrir a la Gestión de la Movilidad Empresarial (Enterprise Mobility Management). Podríamos definirlo como un conjunto de tecnologías, procesos y políticas para garantizar y administrar el uso de los dispositivos móviles corporativos (INCIBE, Dispositivos móviles personales para uso profesional (BYOD). Una guía de aproximación para el empresario.).

Las tecnologías de Gestión de la Movilidad Empresarial proporcionan servicios de gestión de dispositivos, aplicaciones y contenido para los usuarios, ayudando así a reforzar la política de ciberseguridad de la organización a través de la gestión centralizada del dispositivo y de la aplicación de una serie de medidas y configuraciones de seguridad.

Además de abordar los problemas de seguridad, este tipo de tecnologías contribuyen a mejorar la productividad de los empleados, ya que los departamentos de TI pueden proporcionar las aplicaciones y los datos que necesitan para realizar las tareas relacionadas con el trabajo en los propios dispositivos móviles.

Este tipo de soluciones surgieron a partir de la administración de dispositivos móviles o MDM (Mobile Device Management). La gestión de dispositivos móviles se ocupa de implementar, proteger, monitorizar, integrar y administrar los dispositivos móviles en una organización con el objetivo de optimizar la funcionalidad y seguridad de los dispositivos móviles dentro de la empresa y proteger la red corporativa.

A continuación describiremos algunos de los servicios más habituales (NIST, Guidelines for Managing the Security of Mobile Devices in the Enterprise) que son necesarios para la gestión de los dispositivos móviles. Estos servicios deben ser proporcionados bien por el sistema operativo, por el software MDM o bien con controles suplementarios.

La mayoría de las organizaciones no necesitarán todos los servicios de seguridad detallados en esta sección. Cada organización determina los que necesita en base a su contexto y después diseña y adquiere una o más soluciones que provean los servicios necesarios.

1. **Aspectos generales** de la **política de seguridad** de la organización. La utilización de mecanismos de centralización (como el MDM) permiten aplicar las políticas de seguridad de la empresa a los dispositivos móviles. Algunos de los aspectos son los siguientes:
    a. Restringir al usuario y las aplicaciones del dispositivo el acceso a la cámara, al GPS, al interfaz bluetooth, al interfaz USB y al almacenamiento extraíble.
    b. Restringir al usuario y las aplicaciones el acceso a los servicios nativos del sistema operativo, como el navegador nativo, el cliente de e-mail, el calendario, los contactos, etc.
    c. Gestionar las interfaces inalámbricas (Wi-Fi, Bluetooth, etc.).

d. Automáticamente monitorizar, detectar y reportar cuando se produzcan incumplimientos de la política o cambios sobre la configuración de seguridad aplicada.
e. Limitar o prevenir el acceso en función de la versión del sistema operativo (incluyendo si el sistema ha sido rooteado o se ha hecho el jailbreak).

2. **Comunicaciones y almacenamiento**.
    a. Cifrado de las comunicaciones entre el dispositivo y la organización. Lo más frecuente es que se lleve a cabo a través de una VPN, aunque se pueden utilizar otros protocolos distintos.
    b. Cifrado de los datos almacenados, tanto en el propio almacenamiento del dispositivo como en la tarjeta de memoria. En algunos casos puede incluso asociarse una tarjeta a un dispositivo, de tal manera que la información de la misma sólo puede descifrarse cuando ésta está insertada en el dispositivo asociado.
    c. Borrado del dispositivo antes de asociarlo a otro usuario, tras el tiempo de vida útil del dispositivo, etc.
    d. Borrado remoto del dispositivo si se tiene la sospecha de que se ha perdido o ha sido robado, o bien que ha caído en manos de un tercero no confiable.
    e. Borrado tras un cierto número de intentos fallidos en la autenticación.

3. **Autenticación del usuario y el dispositivo**
    a. Requerir una contraseña, acompañada de otro mecanismo de autenticación (token, autenticación basada en el dispositivo, autenticación a nivel de dominio, etc.) antes de acceder a los recursos de la organización. Esto incluye los parámetros básicos de longitud de contraseñas y número de intentos permitidos antes de que se produzca un bloqueo de la cuenta, un borrado del dispositivo, etc.
    b. Si se ha producido un bloqueo, o se ha olvidado la contraseña, un administrador ha de poder restablecer el dispositivo de forma remota para restaurar el acceso del usuario al dispositivo siguiendo el protocolo que la organización determine.
    c. El dispositivo ha de bloquearse automáticamente después de un tiempo de inactividad.
    d. El dispositivo debe poder bloquearse de forma remota a través de un administrador en los casos que la organización considere necesarios.

4. **Aplicaciones**
    a. Restringir qué aplicaciones pueden ser utilizadas.
    b. Restringir qué aplicaciones pueden ser instaladas.
    c. Restringir los permisos (acceso a la cámara, acceso a la localización) asignados a cada aplicación.
    d. Regular la instalación, actualización y eliminación de aplicaciones. Salvaguardar los mecanismos utilizados para llevar a cabo estas

acciones, y mantener un inventario de las aplicaciones instaladas en cada dispositivo.

e. Restringir el uso de sincronización del sistema operativo o ciertas aplicaciones.
f. Verificar la firma digital de las aplicaciones para asegurar que sólo las aplicaciones de entidades confiables son instaladas en el dispositivo, y que el código no ha sido modificado.
g. Distribuir las aplicaciones de la organización desde un repositorio de aplicaciones.

2.4 Evolución de las tecnologías de Gestión de la Movilidad Empresarial

Normalmente, EMM implica una combinación de gestión de dispositivos (MDM), con gestión de aplicaciones móviles (MAM), gestión de contenido móvil (MCM) y gestión de identidades y accesos. Estas cuatro tecnologías comenzaron siendo productos individuales, pero cada vez más la tendencia es la de ir hacia paquetes de software EMM que las integran para ofrecer una solución más global.

A continuación describiremos brevemente cada una de las tecnologías (Department of Homeland Security, Mobile Security Reference Architecture, 2013):

2.4.1 Gestión de dispositivos (MDM)

Podemos definir el MDM (Mobile Device Managment) como cualquier herramienta o proceso destinada a gestionar aplicaciones, datos y aspectos de configuración en dispositivos móviles. La intención de un MDM consiste en centralizar y optimizar la funcionalidad y la gestión de la seguridad de las comunicaciones móviles. Es el primer mecanismo para implementar técnicamente las políticas de seguridad de la organización. Como comentábamos en el apartado anterior, MDM es la base de cualquier suite de movilidad empresarial. Normalmente se basa en la combinación de un agente instalado en el dispositivo (cliente), y un software en la parte servidora del centro corporativo (o en la nube). Los administradores utilizan la consola de administración para establecer las políticas y configurar el acceso de los dispositivos a la red corporativa.

Entre las características que suelen soportar se encuentran: alcance de los dispositivos, las plataformas y las aplicaciones gestionadas; el registro y la cancelación de dispositivos, la seguridad de los mecanismos utilizados para la autenticación, registro de logs, etc.

2.4.2 Gestión de aplicaciones móviles (MAM)

Los sistemas MAM proporcionan una gestión más granular. Permite a los administradores establecer políticas que controlen la distribución, configuración, el control de los datos y el ciclo de vida de la gestión de aplicaciones específicas instaladas en el dispositivo. Al igual que en el MDM, algunas de las características típicas de este tipo de herramientas incluyen el tipo de dispositivos, plataformas y aplicaciones soportadas; la seguridad de los

mecanismos usados para la autenticación y control del dispositivo, etc. Además, pueden incluir características relativas al diagnóstico de intentos de inicio de sesión, logs, solución de problemas… Una aplicación muy útil de los MAMs consiste en la aplicación de las políticas a una serie de contenedores de aplicaciones ("sandboxes"), lo que lo hace de gran utilidad en entornos empresariales, en los que se pueden aplicar políticas generales con un MDM y además ejercer un control más granular sobre ciertos contenedores de aplicaciones empresariales.

2.4.3 Gestión de contenido móvil (MCM)

También conocido como Mobile Information Management (MIM) o gestión de la información, se centra en el acceso a los datos corporativos. Normalmente está más enfocado en asegurar que únicamente las aplicaciones autorizadas pueden acceder, transmitir o almacenar los datos de la organización.

2.4.4 Gestión de identidades y accesos (IAM)

No todos los usuarios de los dispositivos móviles tienen necesidad de acceder a los mismos datos, tienen los mismos requisitos de seguridad en el dispositivo o usan las mismas aplicaciones. Los sistemas de gestión de identidades y accesos se utilizan para integrar los servicios de autenticación y autorización en la solución móvil para proporcionar un perfilado acorde a cada tipo de usuario. En definitiva, permite una aplicación consistente de la política de seguridad en todos los dispositivos móviles de la organización, así como la integración con los mecanismos de autenticación y autorización ya existentes en la organización. Como ejemplo, el uso de un sistema de IAM en conjunto con un sistema MDM permite a cada usuario tener múltiples dispositivos (por ejemplo, una Tablet y un smartphone) configurados con el mismo nivel de acceso y el mismo perfil de seguridad. Puede incluso utilizarse para facilitar la sincronización de datos entre múltiples dispositivos y usuarios.

2.5 Comunicaciones a través de voz y mensajería instantánea

Si nuestra organización tiene la necesidad de cifrar las llamadas o los mensajes enviados desde los dispositivos móviles, es necesario recurrir a sistemas VoIP, es decir, a las llamadas de voz por internet.

Aunque entraremos en detalles técnicos más adelante, lo que sí es realmente importante es que las aplicaciones dispongan de cifrado extremo a extremo. Con este tipo de cifrado lo que se consigue es que sólo los dos dispositivos que se están comunicando sean capaces de descifrar el contenido, y por lo tanto, evitar así que terceras personas que intercepten las comunicaciones puedan acceder al contenido en claro de las mismas.

Existen en el mercado múltiples aplicaciones para el público general que permiten este tipo de comunicaciones cifradas extremo a extremo (Whatsapp, Signal…). No obstante, y en un entorno empresarial, es muy recomendable recurrir a soluciones certificadas por organismos oficiales, como el Centro Criptológico Nacional. A modo de guía, es posible recurrir a catálogos de

productos certificados a nivel Nacional, como es el caso de la Guía STIC 105 (Catálogo de Productos de Seguridad de las Tecnologías de la Información). En este documento se recogen distintos productos que se han certificado para el uso divididos por distintas taxonomías. Es posible encontrar soluciones de este tipo en la familia de herramientas para comunicaciones móviles seguras.

2.6 Mejores prácticas y estándares de aplicación

En el *Anexo I. Guías de buenas prácticas en seguridad móvil empresarial* de este documento se presentan algunos de los documentos de estándares y guías de mejores prácticas por cada uno de los componentes mencionados en el apartado *2.2 Elementos que conforman el sistema*. La adopción de estas guías de buenas prácticas permite a las organizaciones disponer de los pilares de defensa necesarios para resistir a los ciberataques y al compromiso de la información. Si bien las guías de buenas prácticas son recomendaciones, es posible aplicar también una serie de estándares para algunos de los componentes del ecosistema con el objetivo de garantizar unas medidas básicas de seguridad.

3. Principales amenazas y contramedidas relativas a los Sistemas de Comunicaciones Móviles Seguros

3.1 Introducción

La funcionalidad proporcionada por los dispositivos móviles ha evolucionado mucho en las últimas décadas, y continúa avanzando. Cuando aparecieron por primera vez, los dispositivos móviles eran teléfonos diseñados para hacer llamadas telefónicas y enviar mensajes de texto. En estas circunstancias, el fraude criminal no se centró mucho en los usuarios finales.

Sin embargo, la aparición de los smartphones y la introducción de los sistemas operativos en los dispositivos móviles hizo que el panorama de amenazas cambiase de una forma drástica, a medida que los usuarios comenzaron a utilizarlos y a gestionar grandes cantidades de información personal confidencial en los dispositivos.

En líneas generales, un dispositivo móvil que sea seguro debe conseguir al menos los siguientes objetivos:

- **Confidencialidad**. Asegurar que los datos almacenados y transmitidos no pueden ser accedidos por personas no autorizadas.
- **Integridad**. Asegurar que las personas no autorizadas no pueden alterar la información.
- **Disponibilidad**. Asegurar que los usuarios pueden acceder a los recursos puestos a su disposición cuando sea necesario.
- **Autenticación**. Garantizar que un usuario o dispositivo es realmente quien dice ser.
- **Autorización**. Asegurar que un usuario o dispositivo tiene acceso únicamente a los recursos a los que la organización le ha permitido acceder.
- **Trazabilidad**. Garantizar que se puede relacionar cualquier acción llevada a cabo por un usuario o dispositivo sobre un recurso, y el momento en el que ésta tuvo lugar.
- **No repudio**. Garantizar que las partes involucradas en un intercambio de información no puedan negar ilegítimamente que un determinado evento o acción haya tenido lugar.

Para conseguir que los dispositivos móviles sean seguros, es necesario entender qué amenazas pueden afectar a los mismos para implementar ciertos controles que mitiguen los riesgos. Para entender las amenazas que afectan a un sistema de comunicaciones móviles seguras, es necesario retomar la *Figura 2 Elementos del Sistema* del capítulo anterior. Estos elementos pueden considerarse como las diferentes superficies de ataque, y nos servirán para definir la taxonomía que utilizaremos de cara a definir las amenazas: tecnologías utilizadas en el dispositivo móvil, los protocolos de red utilizados, el acceso físico al dispositivo y la infraestructura móvil de la organización.

No obstante, es raro que una amenaza impacte solamente en un elemento del sistema de comunicaciones. Por ello, es necesario tener en cuenta que los requisitos de seguridad que se implementen (o las defensas) deben cubrir siempre toda la superficie de la amenaza, y no limitarse únicamente a la categoría en la que se encuadre.

3.2 Amenazas generales

Independientemente de las superficies de ataque, podemos hablar de la siguiente tipología de amenazas sobre los dispositivos móviles y su infraestructura:

1. **Denegación de servicio** (DoS). Degradación o denegación de los servicios de los usuarios legítimos. Entre los objetivos de esta tipología de ataques, se encuentran:
    - Sobrecarga de las redes con tráfico.
    - Robo de servicios.
    - Reinicio de los dispositivos.

2. **Seguimiento del usuario** (User tracking). Persigue hacer seguimiento remoto de la actividad y el comportamiento del usuario sin su consentimiento, mediante la adquisición de datos de:
    - Geolocalización
    - Audio
    - Fotografías
    - Vídeos
    - Llamadas
    - Contactos
    - Mensajes

3. **Robo de información personal** del usuario (Information Disclosure). Persigue el acceso no autorizado a los datos personales y los servicios del usuario, con el fin de utilizarlos para actividades ilícitas. Entre los datos que pueden conseguirse estarían:
    - Imágenes, vídeos, audio, documentos, conversaciones con información personal o de la organización.
    - Datos del usuario en aplicaciones.
    - Lista de contactos.
    - Registros de llamadas.
    - Número de teléfono.
    - Historial de navegación del usuario.
    - Datos de configuración del dispositivo, red, etc.

4. **Suplantación** (Spoofing). Persigue conseguir el robo de credenciales del usuario en aplicaciones sensibles. Algunos ejemplos de intentos de suplantación son:
    - Redirección de SMS’s.
    - Envío de mensajes de correo electrónico llevando a cabo ataques de ingeniería social.

- Suplantación de una página o aplicación legítima con el objetivo de obtener información de la víctima.
- Publicaciones en redes sociales…

5. **Modificación de datos, software, firmware o hardware sin autorización** (Tampering):
   - Modificación de datos en tránsito.
   - Modificación de datos en reposo.
   - Reempaquetado de aplicaciones legítimas para incluir código malicioso.
   - Modificación de parámetros de red, o del dispositivo para causar un comportamiento anómalo del dispositivo (agotamiento de batería, consumo de recursos, memoria, etc.).

6. **Control remoto del dispositivo**. Permite a un usuario malicioso acceder y tomar el control del dispositivo. Algunos de los objetivos de este tipo de ataques son los que se detallan a continuación:
   - Lanzamiento de ataques de Denegación de Servicio (DoS).
   - Envío de spam.
   - Provocar un daño económico: envío de SMS a servicios de tarificación especial, subscripción a servicios de pago, robo contraseñas de autenticación de transacciones, llamadas a servicios premium, antivirus falsos, etc.
   - Bloquear el dispositivo del usuario cifrando la información a cambio de un rescate económico (ransomware).

7. **Acceso a las comunicaciones del usuario** (Eavesdropping).

3.3 Amenazas por superficie de ataque

En este apartado comprenderemos cuáles son las diferentes superficies de ataque, y las amenazas que pueden producirse por cada una de ellas. El objetivo es entender cada una de las superficies de ataque y la infraestructura asociada, enumerar las principales amenazas y proponer algunos de las contramedidas que se pueden aplicar para mitigar los riesgos.

Para el desarrollo de este apartado nos basaremos en el documento *(NIST, Assessing Threats to Mobile Devices & Infrastructure, 2016)*, y en el Catálogo de Amenazas desarrollado también por NIST *(NIST, Mobile Threat Catalogue, s.f.)*.

Comenzaremos en primer lugar por el acceso físico al dispositivo. Continuaremos con el acceso a través de las diferentes tecnologías utilizadas en dispositivos móviles (firmware y sistema operativo) y las aplicaciones. Seguiremos con las superficies de ataque relacionadas con las distintas redes que utilizan los dispositivos móviles (redes de operador y locales de área personal) y finalizaremos con el objetivo fundamental del ataque: la gestión empresarial de las comunicaciones.

3.3.1 Acceso físico al dispositivo y evasión de mecanismos de autenticación

La naturaleza portable de los dispositivos móviles los hace más susceptibles a las amenazas basadas en el acceso físico al dispositivo.

Entre las principales **amenazas** de este tipo, podríamos destacar las siguientes:

- A.AF.1. Robo o pérdida del dispositivo
- A.AF.2. Ataque a través de la conexión de un dispositivo no confiable o comprometido.
- A.AF.3. Gestión incorrecta del ciclo de vida de los dispositivos (por ejemplo, no borrando los datos antes de ceder el teléfono a otro usuario).
- A.AF.4. Robo de datos provocados por el acceso temporal de un tercero a un dispositivo no bloqueado.
- A.AF.5. Acceso a las claves privadas almacenadas en el dispositivo.
- A.AF.6. Evasión del mecanismo de bloqueo de pantalla.
- A.AF.7. Fuerza bruta en PIN o contraseñas de usuario.
- A.AF.8. Suplantación de token NFC o Bluetooth que desbloquea el dispositivo.
- A.AF.9. Suplantación biométrica.

Las principales **contramedidas** para mitigar los riesgos derivados de este tipo de amenazas serían las siguientes:

- C.AF.1. Asegurar que los dispositivos son gestionados por la organización a través de un sistema de gestión centralizado (EMM, MDM). Esto permite activar las políticas de seguridad, monitorizar el estado del dispositivo, llevar a cabo un seguimiento de los dispositivos y borrar los datos de aquéllos que se han perdido, robado o se han podido ver comprometidos. Además:
    a) Cifrar los datos almacenados en el dispositivo.
    b) Activar los mecanismos de bloqueo de pantalla.
    c) Activar las capacidades de bloqueo remoto, seguimiento de dispositivos y borrado remoto.
    d) Deshabilitar las capacidades de USB debugging en Android.
- C.AF.2. Enseñar y concienciar a los usuarios a utilizar los dispositivos, incidiendo en los principales riesgos derivados del uso de los mismos.
- C.AF.3. Evitar, en la medida de lo posible, la conexión de los dispositivos móviles a ordenadores.
- C.AF.4. Requerir la autenticación del usuario en cualquier acceso a datos de la organización.
- C.AF.5. Incorporar los dispositivos móviles a los mecanismos de detección de acciones sospechosas de la organización (autenticación desde dominios nuevos, acceso a servicios poco frecuentes, etc.) y requerir pasos adicionales en la autenticación de este tipo de accesos.
- C.AF.6. Emplear mecanismos fuertes de autenticación (multifactor).

C.AF.7. Llevar a cabo una gestión centralizada de usuarios y credenciales, de tal forma que se permita revocar los accesos de forma instantánea cuando unas credenciales hayan sido comprometidas (y las sesiones activas asociadas a dichas credenciales).
C.AF.8. Regular en las políticas de la organización todos los aspectos relativos a las contraseñas, caducidad, política de contraseñas, longitud y algoritmo de generación de las mismas, etc.
C.AF.9. Incorporar en todas las políticas el principio del mínimo privilegio.
C.AF.10. Emplear mecanismos de autenticación que garanticen el uso de OTPs o tokens generados para el acceso desde localizaciones no confiables.
C.AF.11. Asegurar que las actualizaciones de seguridad se llevan a cabo en tiempo y forma en todos los elementos de la infraestructura.
C.AF.12. Mecanismos de protección frente a ataques de fuerza bruta: complejidad de contraseñas y PIN de usuario, borrado tras un número de intentos de desbloqueo, etc.

3.3.2 Componentes de bajo nivel

En la siguiente figura se presentan las distintas capas de tecnología utilizadas en un dispositivo móvil: desde el hardware, pasando por el firmware hasta llegar a las aplicaciones móviles y los datos.

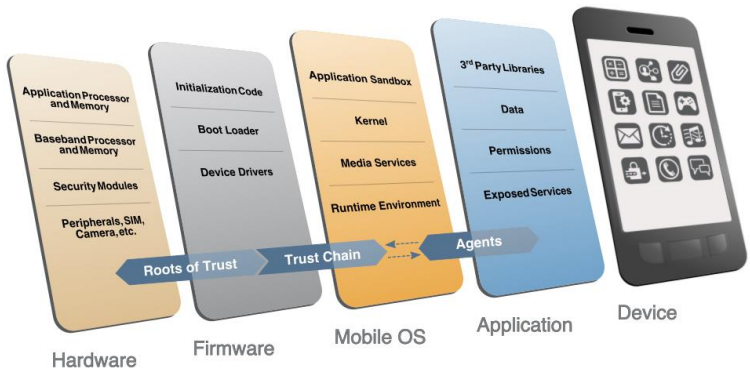

Figura 4 Pila de tecnologías utilizadas en un dispositivo móvil

La seguridad del sistema operativo del dispositivo móvil normalmente depende de componentes de más bajo nivel para su funcionamiento seguro. Como ejemplo, al iniciarse, el dispositivo móvil enciende un componente llamado gestor de arranque que carga el código del sistema operativo. Si el gestor de arranque contiene vulnerabilidades, o no está configurado de forma segura, un atacante podría alterar el funcionamiento del código del sistema y cargar una versión alternativa con un comportamiento malicioso.

Es conveniente resaltar en este apartado que los dispositivos móviles generalmente usan un entorno de ejecución aislado conocido como TEE en Android (Trusted Execution Environment) y Secure Enclave (en Apple iOS). Este tipo de entornos proveen capacidades de seguridad fundamentales como es el almacenamiento de claves criptográficas, incluyendo las claves de cifrado para cifrar datos sensibles en el dispositivo. Mover las capacidades críticas a un

entorno de ejecución aislado permite tener más resiliencia frente a ataques que explotan el sistema operativo.

Las principales **amenazas** relacionadas con este tipo de componentes son:

A.RM.1. La explotación de vulnerabilidades relacionadas con el gestor de arranque, el chip de banda base, el entorno de ejecución aislado y la cadena de suministro de los distintos componentes.

Como principales **contramedidas** para este tipo de amenazas, podríamos destacar:

C.CB.1. Instalar parches de seguridad, asegurando que los dispositivos disponen de la última versión de los parches de seguridad.
C.CB.2. Retirar los dispositivos que no soportan actualizaciones de seguridad del fabricante o del operador.
C.CB.3. Cuando sea posible, activar capacidades de comprobación de la integridad en los dispositivos, que puedan ser utilizadas para detectar y responder como indicadores de compromiso.
C.CB.4. Adquirir sólo dispositivos que reúnan los criterios de seguridad definidos por la organización. Es importante conseguir que operadores y fabricantes proporcionen las actualizaciones de seguridad en tiempo y forma, y que se aseguren las actualizaciones durante un período de tiempo concreto.

3.3.3 Sistema operativo

La arquitectura de seguridad del sistema operativo representa un rol importante en la protección del dispositivo móvil. La aplicación de las capacidades de aislamiento de los sistemas operativos dota al dispositivo de protección frente a posibles comportamientos maliciosos, controlando las interacciones permitidas entre las propias aplicaciones y con los diferentes componentes del dispositivo.

En ciertos sistemas operativos las aplicaciones no pueden acceder a los datos almacenados por otras aplicaciones, y existen restricciones en cuanto a la interacción con otras aplicaciones. Adicionalmente, las aplicaciones deben obtener el permiso del usuario para acceder a ciertos componentes del dispositivo, como la cámara, el GPS, el micrófono, la agenda de contactos, etc.

Algunas de las principales **amenazas** relacionadas con el compromiso del sistema operativo del dispositivo serían las siguientes:

A.SO.1. Explotación de vulnerabilidades existentes en el sistema operativo para ganar privilegios.
A.SO.2. Jailbreak o root del dispositivo, lo que puede provocar que los controles de seguridad no sean efectivos.
A.SO.3. Uso de servicios ilegítimos que fuerzan al usuario a instalar una configuración insegura en el dispositivo.
A.SO.4. Instalación de aplicaciones potencialmente maliciosas, o uso de librerías inseguras.

Como **contramedidas** para las amenazas anteriormente descritas, podríamos detallar las siguientes:

C.SO.1. Monitorizar el estado de parcheado de los dispositivos, y bloquear la conectividad de los dispositivos con vulnerabilidades conocidas.
C.SO.2. Adquirir dispositivos de operadores y fabricantes que se hayan comprometido a proporcionar las actualizaciones del sistema operativo en un tiempo razonable, o que son conocidos por disponer de actualizaciones frecuentes de los dispositivos.
C.SO.3. Retirar los dispositivos que no soportan actualizaciones de seguridad del fabricante o del operador.
C.SO.4. Utilizar herramientas o APIs para detectar y bloquear la conectividad empresarial desde los dispositivos comprometidos.
C.SO.5. Usar mecanismos para detectar dispositivos rooteados o con jailbreak, notificar al usuario y bloquear la conectividad de los mismos.
C.SO.6. Concienciar a los usuarios del riesgo asociado al rooteo / jailbreak del dispositivo.
C.SO.7. Restringir la instalación de apps de markets no oficiales, en los que no se someten las aplicaciones a la validación de certificados correspondiente.
C.SO.8. Actualizar los dispositivos tan pronto como las actualizaciones estén disponibles.
C.SO.9. Mantener el modo debug USB deshabilitado en los dispositivos Android, salvo en los casos en los que sea necesario habilitarlo.
C.SO.10. Para defenderse de posibles amenazas relacionadas con servicios en la nube proporcionados por el fabricante del dispositivo, o para el sistema operativo, se debería educar a los usuarios para que usen mecanismos de autenticación fuertes (como el doble factor de autenticación). Además, en las organizaciones se puede forzar el uso de cuentas gestionadas por la empresa en lugar de las gestionadas por los propios usuarios (cuando sea posible).

3.3.4 Aplicaciones móviles

La mayor parte de las aplicaciones son provisionadas a través de markets públicos, como Google Play o Apple Store. Sin embargo, las organizaciones también distribuyen aplicaciones a través de markets privados, que normalmente son para el uso de los empleados de la organización (y no para uso público).

Normalmente, las vulnerabilidades en aplicaciones móviles desarrolladas por la organización son el resultado de cometer errores a la hora de seguir las recomendaciones de desarrollo seguro. Algunos ejemplos de vulnerabilidades de este tipo serían las siguientes:

- Conexiones inseguras a la red.
- Almacenamiento de ficheros inseguro.
- Almacenamiento de información sensible en logs.
- Vulnerabilidades en navegador.

- Vulnerabilidades en librerías de terceros.
- Vulnerabilidades criptográficas.

No obstante, existen casos en los que se desarrollan aplicaciones móviles maliciosas que han sido especialmente diseñadas para recopilar o comprometer datos sensibles de los usuarios. En la mayoría de los casos, el acceso a estos datos se lleva a cabo sin el consentimiento del usuario. En otros, la aplicación instalada requiere el acceso a datos o servicios adicionales a los que ésta necesita para su funcionamiento normal, sin que el usuario sea realmente consciente de lo que esto implica en su seguridad y en la de sus datos.

En el informe del Departamento de Seguridad Nacional de los Estados Unidos de 2017 (Study on Mobile Device Security, 2017) se examinan las principales vulnerabilidades y riesgos que afectan a un ecosistema móvil, y prestan especial atención a las aplicaciones. Tal y como se presenta en la figura, existen múltiples formas en las que una aplicación maliciosa puede afectar a los dispositivos móviles.

Las principales **amenazas** relacionadas con el uso de aplicaciones en una organización que se detallan en dicho informe serían las siguientes:

A.AP.1. El escalado de privilegios en el dispositivo.
A.AP.2. El acceso a la grabación del micrófono o la cámara del dispositivo, sin el consentimiento del usuario.
A.AP.3. El cifrado de los datos del usuario a cambio de una cantidad de dinero para que pueda recuperar la información.
A.AP.4. La distribución de aplicaciones maliciosas a través de markets no oficiales.
A.AP.5. La ejecución de código dinámico tras la instalación de una aplicación para evadir los controles llevados a cabo durante la verificación de aplicaciones.

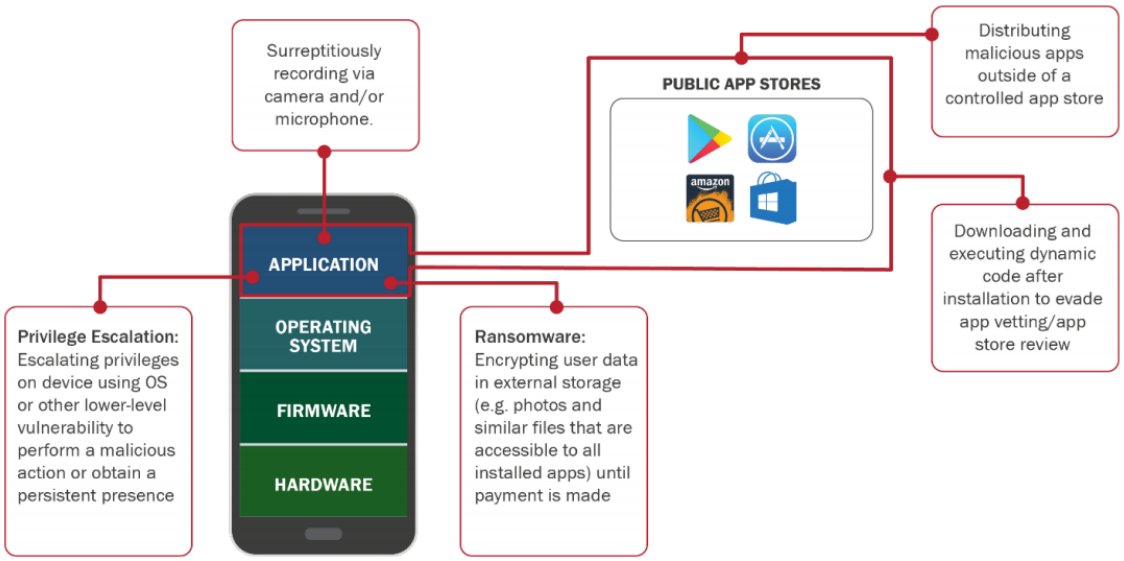

Figura 5 Amenazas a través de aplicaciones móviles

Aunque se han presentado las principales amenazas, consideramos necesario también tener en consideración algunas de las que se citan en el documento (NIST, Mobile Threat Catalogue, s.f.):

A.AP.6. Recopilación de información del dispositivo o del usuario.
A.AP.7. Acceso a información del dispositivo: ubicación GPS, ficheros, fotografías, etc.
A.AP.8. Exfiltración de información de la organización a través de aplicaciones maliciosas.

Las principales **contramedidas** que deberían tenerse en consideración son las siguientes:

C.AP.1. Disponer de servicios de hacking ético o herramientas que sean capaces de detectar vulnerabilidades en aplicaciones. Se debe asegurar que existe un procedimiento claro para determinar en qué casos se llevan a cabo análisis estáticos, y en qué casos se complementan con un análisis dinámico.
C.AP.2. Asegurar el cifrado adecuado de todos los datos en tránsito de la organización.
C.AP.3. Monitorización de los dispositivos de la organización en busca de aplicaciones que ya no están soportadas por la organización o que tienen vulnerabilidades conocidas, y solicitar a los usuarios que eliminen dichas aplicaciones.
C.AP.4. Evitar aprobar aplicaciones que solicitan permisos que pueden poner en riesgo la privacidad de los usuarios (acceso a GPS, contactos, etc.).
C.AP.5. Utilizar proxy y VPN para todo el tráfico con la organización, e identificar y bloquear conexiones a sitios webs maliciosos.
C.AP.6. Asegurar que existe un programa de concienciación para los usuarios en el uso de aplicaciones móviles.
C.AP.7. Asegurar que los procesos de revisión de aplicaciones internas son rigurosos, y que existen mecanismos (por ejemplo, ciber inteligencia) que permitan detectar el uso de librerías con vulnerabilidades ya conocidas.
C.AP.8. Utilizar características que permitan separar las aplicaciones personales de las corporativas, de tal forma que vulnerabilidades que afectan al área de la organización no afecten a la personal y viceversa.
C.AP.9. Prohibir la instalación de aplicaciones fuera de los repositorios autorizados.
C.AP.10. Incorporar a los procesos de ciberinteligencia de la organización todos los aspectos relacionados con los potenciales riesgos asociados a las aplicaciones instaladas en los dispositivos.
C.AP.11. Eliminar las aplicaciones preinstaladas en los dispositivos que no se necesitan, o evitar que puedan ejecutarse.
C.AP.12. Usar mecanismos de autenticación fuertes que aseguren que una aplicación maliciosa no puede acceder a los datos de la organización.

C.AP.13. Monitorizar los intentos de acceso de aplicaciones a recursos corporativos.
C.AP.14. Disponer de mecanismos MDM/EMM con políticas de seguridad. Como ejemplos (aunque deben ser particularizados a un análisis de riesgos de la organización) tendríamos la siguiente tipología de políticas:
    a) Restringir el uso de aplicaciones haciendo uso de listas blancas / negras.
    b) Responder a aplicaciones que incumplan los requisitos de seguridad con acciones automáticas: notificaciones, borrado de información, etc.
    c) Requerir a los usuarios que actualicen el dispositivo.
    d) Restringir el uso de ciertas características del dispositivo: cámara, almacenamiento externo, Bluetooth, tethering, etc.
    e) Deshabilitar el acceso a los markets oficiales, si se va a usar únicamente el interno para la distribución de aplicaciones.
    f) Controlar las conexiones Wi-Fi.
    g) Deshabilitar el contenido compartido (portapapeles, impresión, etc.).
    h) Configurar los requisitos de seguridad de las aplicaciones.

Adicionalmente, y como aspectos a tener en cuenta por parte de organizaciones que desarrollan sus propias aplicaciones:

C.AP.15. Llevar a cabo revisiones periódicas de los logs de las aplicaciones desarrolladas internamente para asegurar que no se están almacenando datos sensibles.
C.AP.16. Si se desarrollan aplicaciones internas, asegurar que se siguen las mejores prácticas para el desarrollo seguro (OWASP).
C.AP.17. Seguir las mejores prácticas para la implementación de la criptografía en aplicaciones móviles.

3.3.5 Redes móviles

Las redes móviles generalmente operan en tres planos distintos: voz, datos y control. Actualmente tanto la voz como los datos van juntos como tráfico IP, aunque en el pasado iban separados. El plano de control siempre está fuera de banda: el dispositivo normalmente no tiene acceso al mismo y va en distintos canales.

Independientemente de la generación, todas las redes móviles de hoy en día están formadas por los elementos que se detallan a continuación:

1. Red de Acceso Móvil (RAN, Radio Access Network). Es la parte de la red que conecta a los usuarios al proveedor de servicio usando señalización radio (RF). Normalmente esta parte de la arquitectura incluye antenas, RF transceivers y RF controllers. Para proteger la privacidad de las llamadas, esta parte del tráfico va cifrada, aunque normalmente el nivel de cifrado depende del tipo de red y de la operadora que lo implementa. Una vez

que la señal se convierte de RF a cable, la señal ya no va cifrada en la red. Este cambio implica que cualquier atacante que tenga acceso a este punto puede fácilmente hacerse con el tráfico que ya no está protegido por ninguna capa de cifrado adicional. Este tipo de protección al que hacemos mención se llama cifrado end-to-end y previene precisamente este tipo de ataques.

2. Núcleo de la red. Mantiene toda la lógica de red y es responsable de crear y mantener la conexión entre los dispositivos móviles y los servicios externos (internet, teléfonos fijos, otras operadoras y empresas privadas…) así como rastrear todo el equipamiento de usuario para enrutar las llamadas y los flujos de datos a medida que los usuarios se desplazan. El núcleo transfiere los datos de usuario y de control, autentica los dispositivos, gestiona la facturación y hace cumplir la calidad de servicio.

3. Servicios que serán proporcionados por el operador. Las redes de servicios externos contienen servicios adicionales para los usuarios, y pueden incluir conexiones a la red de telefonía fija (PSTN) o redes voz ip, internet, interconexión a otros proveedores u organizaciones y otros proveedores como Google, Facebook, Apple, etc.

Las principales **amenazas** relacionadas con la red móvil y la infraestructura relacionada son las siguientes:

A.RM.1. Robo o clonado de la tarjeta SIM.
A.RM.2. Denegación de servicio o “jamming”. Las redes inalámbricas son susceptibles de sufrir interferencias en los canales de subida y bajada.
A.RM.3. Ataques físicos a la infraestructura de las estaciones base.
A.RM.4. Ataques de denegación de servicio (DoS) de la red.
A.RM.5. Backhaul eavestropping o compromiso de las comunicaciones.
A.RM.6. Acceso a buzón de voz de un usuario usando el PIN por defecto.
A.RM.7. Acceso físico a la infraestructura de la red.
A.RM.8. Ingeniería social contra el operador para asociar el número de teléfono a una SIM distinta.
A.RM.9. Robo de información de dispositivos (IMEI…).
A.RM.10. Seguimiento de la ubicación del usuario.
A.RM.11. Explotar vulnerabilidades del sistema de señalización SS7 para conseguir monitorizar o redirigir llamadas o mensajes de texto.
A.RM.12. Acceso a las comunicaciones (escucha de llamadas).

La principal **contramedida** de cara a mitigar los posibles riesgos asociados a la confidencialidad y la integridad de las comunicaciones a través de redes móviles es asegurar que los dispositivos utilizan un cifrado extremo a extremo en todas las comunicaciones (voz y datos).

3.3.6 Redes locales y de área personal

Los dispositivos móviles hacen uso de redes locales y de área personal como es el caso de Wi-Fi y Bluetooth. Algunas de las principales **amenazas** derivadas del uso de redes Wi-Fi son las que se detallan a continuación:

A.RL.1. Seguimiento de SSID de las redes Wi-Fi a las que se ha conectado el teléfono.
A.RL.2. Conexión a redes Wi-Fi no cifradas o cifradas con algoritmos débiles (por ejemplo, WEP).
A.RL.3. Seguimiento de la MAC del dispositivo.

Como principales **contramedidas**, citaremos las siguientes:

C.RL.1. Concienciar a los usuarios y prohibir el uso de redes públicas o no cifradas sin mecanismos de protección adicionales.
C.RL.2. Sólo permitir a los dispositivos móviles la conectividad a las redes Wi-Fi autorizadas que usen mecanismos de cifrado WPA2.
C.RL.3. Modificar los SSID de forma frecuente y con valores no relacionados entre sí.
C.RL.4. Deshabilitar las interfaces cuando no se estén utilizando (NFC, Bluetooth, etc.).

3.3.7 Sistemas de gestión de la movilidad empresarial

Como hemos visto, las organizaciones confían en las tecnologías EMM para controlar y administrar los datos móviles, los dispositivos y sus conexiones con los recursos de la organización.

Este tipo de soluciones constan de un agente en el dispositivo móvil que recibe e implementa comandos administrativos enviados por un servidor que reside en la infraestructura de la organización o en la nube. Vimos que permiten asegurar las conexiones entre el dispositivo y los recursos empresariales, y que además pueden constar de la siguiente tipología de servicios:

- MDM, o gestión del dispositivo (cumplimiento de políticas de seguridad, borrado y bloqueo remoto, bloqueo de instalación de aplicaciones no autorizadas, etc.).
- MAM, para controlar las aplicaciones empresariales, instalar y desinstalar las de la organización de forma remota, gestionar el inventario de aplicaciones, asegurar que las aplicaciones están actualizadas y gestionan los datos de éstas de forma correcta.

Por tanto, la seguridad en los sistemas EMM es fundamental de cara a proteger los recursos de la organización. A continuación, detallamos las principales **amenazas** a considerar en este tipo de sistemas:

A.GM.1. Fallo en la validación del certificado digital de la aplicación del EMM.
A.GM.2. Un usuario de una instancia de la organización tiene acceso a información a otra instancia del EMM de la organización.

A.GM.3. Acceso no autorizado a la consola administrativa del sistema de gestión del EMM/MDM, por ejemplo, explotando vulnerabilidades.
A.GM.4. Suplantar el servidor EMM / MDM en un dispositivo registrado para ejecutar acciones no autorizadas, como activar un borrado del dispositivo o instalar un perfil MDM malicioso.
A.GM.5. Gestión insegura de los datos sensibles de usuario por parte de la solución EMM/MDM (por ejemplo, las credenciales de autenticación en el dominio).
A.GM.6. Un dispositivo comprometido y rooteado pasa por alto los requisitos de seguridad.
A.GM.7. Un atacante inscribe un dispositivo móvil en el EMM/MDM sin el consentimiento del propietario del dispositivo, lo que facilita los ataques contra el dispositivo o seguimiento del comportamiento del usuario.
A.GM.8. Ataque a la privacidad de un usuario por parte de un administrador un atacante con acceso administrativo a la consola del EMM/MDM (por ejemplo: seguimiento de la ubicación del dispositivo, registros de llamadas, mensajes de texto, contactos, etc.).
A.GM.9. Borrado de datos personales del usuario en el dispositivo sin autorización del usuario.
A.GM.10. Sincronización de datos de la organización con servicios cloud de terceros no gestionados por la organización.
A.GM.11. Aplicaciones inseguras instaladas en los dispositivos de la organización a través de las políticas MAM.

Las principales contramedidas contra este tipo de amenazas son las siguientes:

C.GM.1. Asegurar que el sistema EMM valida los certificados.
C.GM.2. Auditorías de seguridad sobre las actividades de administración, los registros de dispositivos, las actividades llevadas a cabo en la red, etc.
C.GM.3. Auditorías de seguridad sobre la actividad de los dispositivos, instalando aplicaciones o agentes en los dispositivos que puedan monitorizar el sistema operativo, las aplicaciones y las conexiones de red para identificar un comportamiento malicioso. Incluye la monitorización del agente EMM/MDM.
C.GM.4. Inteligencia para amenazas. Consolidar y correlacionar toda la información de los registros de seguridad para identificar actividad sospechosa.
C.GM.5. Servicios de autorización granulares. Permitir múltiples niveles de permisos, y la gestión de roles a los portales administrativos, así como asegurar el principio del mínimo privilegio.
C.GM.6. Soportar mecanismos de autenticación fuertes (doble factor) para accesos administrativos.
C.GM.7. Soportar la integración de los mecanismos de autenticación con la infraestructura corporativa (Single-Sign-On / Oauth).
C.GM.8. Establecimiento de canales seguros de comunicación entre todos los componentes que interactúan con el EMM/MDM.

4. Modelo de Referencia y Solución técnica

4.1 Introducción

El objetivo de este capítulo consiste en proporcionar una solución para el diseño del Sistema de Comunicaciones Móviles corporativos de la organización propuesta en este proyecto. Para la implementación, tendremos en cuenta el modelo que se ha visto en el Capítulo 2 de este trabajo, así como los distintos aspectos relativos a riesgos, amenazas y posibles contramedidas descritos en el Capítulo 3. Para favorecer una mejor comprensión del diseño, y de cómo éste se adapta a nuestra organización, presentaremos los contenidos en el siguiente orden:

- Comenzaremos llevando a cabo un breve análisis de la situación actual de la organización, describiendo las principales necesidades y los puntos de conflicto con respecto al proyecto.
- A continuación, se proporcionará una definición del proyecto a diseñar, basado en las necesidades descritas previamente.
- Por último, bajaremos al detalle técnico. Describiremos el esquema de la solución, los servicios y/o funciones de seguridad que la organización ha de implementar y adaptar y la descripción funcional de cada componente de la infraestructura.

4.2 Análisis de la situación actual

Como ya se comentó en el Capítulo 1, la organización en la que es necesario llevar a cabo la instalación del Sistema de Comunicaciones Móviles Seguras es una gran entidad bancaria, con sede en Madrid y con presencia en varios países. Desde comienzos de 2018 la organización ha establecido un plan a tres años para mejorar todos sus procesos y mecanismos de defensa en lo relativo a la seguridad de la información y la transformación digital.

Actualmente, y en materia de movilidad, la organización cuenta con teléfonos fijos para la mayor parte de los empleados, y móviles para una parte de ellos. Los móviles existentes actualmente no están gestionados de forma centralizada, ni se les aplican políticas de seguridad específicas. Únicamente se adquirieron al operador de telefonía móvil y se gestiona un inventario con todos los teléfonos existentes, las tarjetas SIM activas y los empleados a los que han sido asignados.

Aprovechando la contratación de un nuevo operador para los servicios de telefonía móvil y la renovación del parque de teléfonos móviles, la compañía quiere cumplir con algunos de los hitos establecidos en el plan de transformación digital y garantizar que todos los empleados pueden trabajar de forma remota y acceder a los sistemas de la organización de forma segura. Para ello, se pretende que todos los dispositivos móviles que se entreguen a los empleados del Centro Corporativo en Madrid estén gestionados de forma centralizada, y se adapten a los mecanismos de seguridad que se requieren actualmente para acceder a cualquier sistema de la organización, intercambiar y almacenar información de ésta.

Por otro lado, durante los últimos dos años la organización ha estado redefiniendo las políticas de seguridad de la información, y migrando sus sistemas a una nueva arquitectura en la que se definen distintos dominios en función de la información que éstos gestionan. En este sentido, los sistemas que gestionan información confidencial tienen una serie de medidas de seguridad adicionales que se justifican con el análisis de riesgos que la organización ha llevado a cabo. Para cumplir con el plan, la organización necesita también prestar un servicio de llamadas móviles de carácter confidencial para algunos de sus empleados, en el que se garantice un cifrado extremo a extremo de las conversaciones que se mantienen.

En este sentido, se detectan los siguientes puntos de conflicto o aspectos a considerar en el contexto de la situación actual de la organización.

- Actualmente no se dispone de una infraestructura para centralizar y gestionar los dispositivos móviles, por lo que será necesario instalar los elementos que sean necesarios desde cero.
- La organización actualmente no presta el servicio de llamadas confidenciales, por lo que también será necesario instalar todos los elementos que sean necesarios desde cero.
- La organización debe definir los requisitos que necesita para ambos servicios desde el comienzo, para poder adquirir los terminales móviles que en ambos casos serán terminales comerciales.
- La organización se encuentra en un proceso de migración de sus sistemas a la nueva arquitectura puesta en producción, por lo que se debe tomar como punto de partida para el diseño el esquema de dicha arquitectura y definir las necesidades sobre dicho esquema.
- Se deben integrar los todos los procesos y/o funciones que se requieran para la prestación de estos servicios en los ya existentes en la organización.

A continuación, se proporciona un diagrama de red a alto nivel de la nueva arquitectura implantada en la organización (Figura 6, página 32). Como se puede observar, la organización dispone de una DMZ donde tiene los servicios de navegación, las conexiones VPN de terceros a la organización, y los servicios DMZ (frontal de correo, servicios DNS externos y servicios SFTP).

Por otro lado, y dentro de la red interna disponemos de:

- Servicios corporativos de dominio interno. En este segmento de red se encuentran la mayoría de los servicios corporativos: servicios de red, servicios de bases de datos y servicios corporativos que manejan información interna. A todos estos servicios se añaden los servicios de gestión y de seguridad de dicho dominio.
- Servicios corporativos de dominio confidencial. En este dominio se encuentran los servicios corporativos que manejan información confidencial. Además, existen también servicios de seguridad y gestión específicos.
- Red corporativa. En este segmento de la red se encuentran todos los equipos de usuario e impresoras.

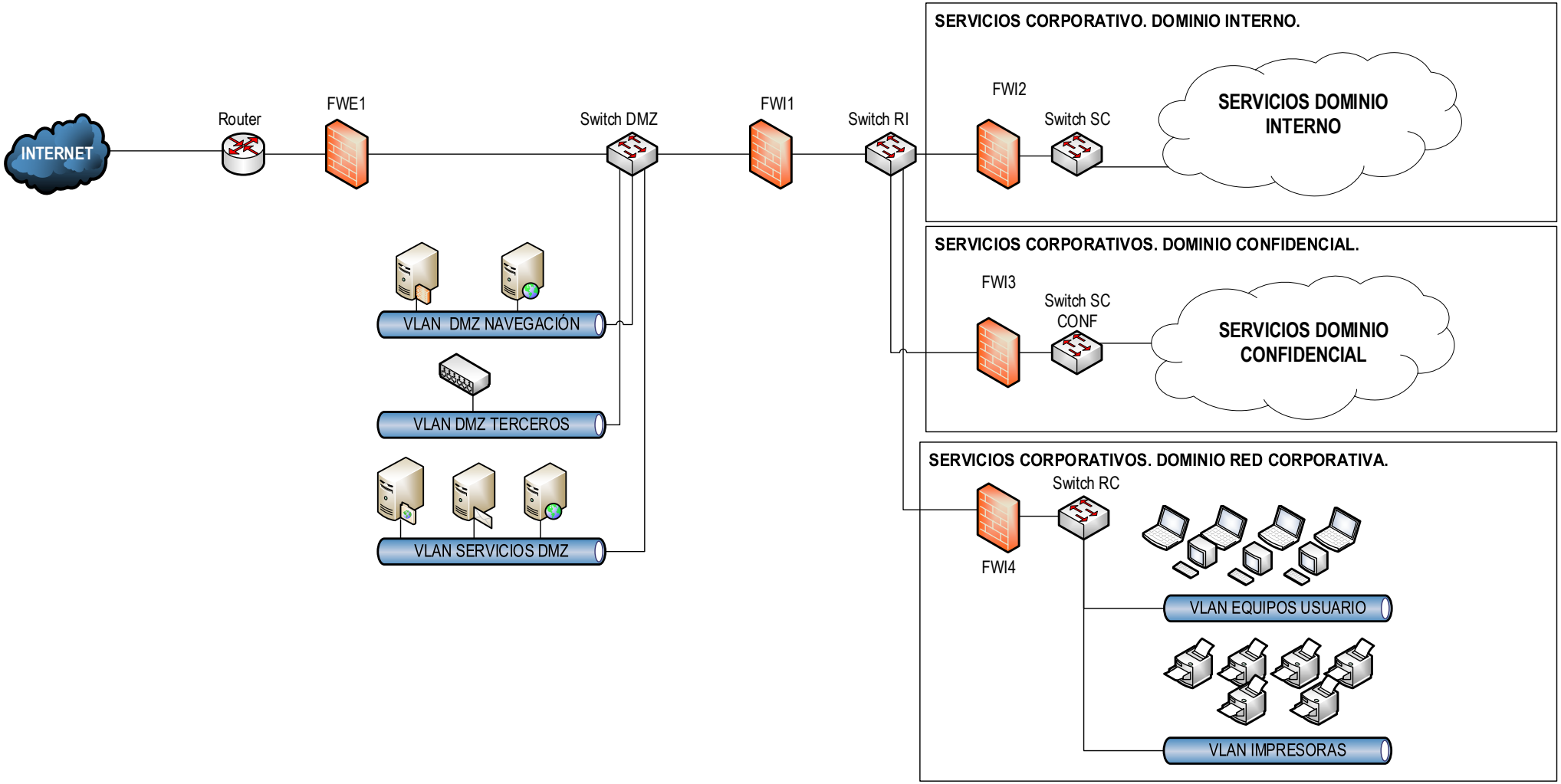

Figura 6 Diagrama de red a alto nivel de la organización

4.3 Definición del proyecto

4.3.1 Objetivos

En este apartado se describen los principales objetivos que la organización descrita en el apartado anterior pretende conseguir para la sede corporativa de Madrid con este proyecto. Son los que se detallan a continuación:

1. Distribuir un dispositivo móvil comercial a cada uno de los 6.000 empleados que forman parte de la sede corporativa de Madrid.
2. Asegurar que todos los dispositivos móviles distribuidos son gestionados de forma centralizada.
3. Asegurar la aplicación de las políticas de seguridad de la información definidas por la organización en el acceso, el procesamiento y el almacenamiento de la información y los sistemas que son de su propiedad.
4. Asegurar la monitorización de la actividad de los diferentes dispositivos, y del cumplimiento de las políticas mencionadas en el apartado anterior.
5. Conseguir que la organización disponga de un servicio de llamadas y mensajes cifrados extremo a extremo para los empleados que la organización determine.
6. Permitir que los empleados puedan acceder a los recursos corporativos, gestionar información con diferentes medidas de protección en función de las categorías que la organización ha definido y facilitar el uso personal que el empleado necesite hacer del dispositivo.

No obstante, resaltar que este documento es sólo un proyecto que pretende describir las funcionalidades, los requisitos y un diseño a alto nivel de la solución sobre la arquitectura que la organización tiene actualmente. El proyecto debe poder implementarse con una o varias soluciones comerciales que cumplan los requisitos descritos, y adaptando e incorporando a la organización los procesos y/o funciones que aquí se describirán en los próximos apartados.

4.3.2 Requisitos del sistema desplegar

Definidos los objetivos, y partiendo de la situación actual descrita en los apartados anteriores, la organización ha definido los siguientes requisitos para el diseño de la solución:

Requisitos funcionales

RQ-1. La solución debe gestionar todos los teléfonos móviles de los 6.000 empleados de los que consta la organización en la sede corporativa de Madrid.

RQ-2. Se considera que en torno a un 10% de los empleados gestionan diariamente llamadas de carácter confidencial, por lo que será necesario garantizar al menos en estos casos que las comunicaciones por voz y mensajería presentan un cifrado extremo a extremo.

RQ-3. Los empleados deben poder acceder a los recursos corporativos con las medidas de seguridad definidas por la organización, pero también podrán hacer un uso personal del dispositivo.

Requisitos técnicos

RQ-4. La gestión debe ser centralizada. Todos los elementos necesarios serán instalados en el CPD que la organización tiene en Madrid.

RQ-5. El despliegue de todos los elementos que se instalen ha de ser on-premise.

RQ-6. La plataforma a instalar debe ser escalable, de cara a plantear futuras integraciones con el resto de sedes.

RQ-7. Se debe garantizar la alta disponibilidad de los sistemas clave de la plataforma que se instale.

RQ-8. La organización dispone actualmente de una taxonomía de referencia para clasificar la información. Las categorías definidas actualmente son: confidencial, restringido, uso interno y uso público. Los sistemas que gestionan información confidencial están separados del resto, y disponen de medidas de seguridad más restrictivas (como se ha visto en la Figura 6).

RQ-9. La solución debe poder integrarse con los siguientes sistemas corporativos:

- Sistema de gestión de identidades.
- Infraestructura PKI de la organización para la generación de los certificados.
- Servios de gestión de identidades de la organización.
- Servicio DNS, para la gestión de las IPs de los terminales y la navegación por internet.
- Servicio NTP, para la sincronización de las fechas en todos los servidores corporativos.
- Servicio de correo corporativo. Los usuarios podrán consultar su cuenta profesional desde los teléfonos móviles.
- Servicio de internet corporativo. Los terminales navegarán en internet a través de la red de la organización.
- Servicio de telefonía fija y móvil corporativa, para la gestión de las llamadas confidenciales entre los terminales.

RQ-10. Se deben garantizar los siguientes principios de seguridad de la información de la organización: confidencialidad, integridad, disponibilidad, autenticación, autorización, trazabilidad y no repudio.

RQ-11. La solución debe garantizar que se establecen túneles cifrados de datos desde los terminales hasta un concentrador de túneles instalado en el CPD.

RQ-12. Al menos para el grupo de empleados que gestionan las llamadas confidenciales se debe usar una aplicación que gestione Voz IP, que

garantice un cifrado extremo a extremo tanto de la señalización como de los datos.

RQ-13. Deben existir mecanismos de control de acceso que garanticen la seguridad de los sistemas y los propios terminales.

RQ-14. El contenido de los terminales debe estar cifrado. Todas las comunicaciones con la organización también estarán cifradas.

RQ-15. Se debe garantizar que además de la gestión de los terminales, existe un contenedor de aplicaciones corporativas que son gestionadas por la organización y que no pueden compartir datos con el resto de las aplicaciones.

4.4 Diseño técnico del proyecto

4.4.1 Catálogo de servicios de usuario

En este apartado se detalla el conjunto de los diferentes servicios que el Sistema de Telefonía Móvil Segura proporcionará:

Servicios no seguros

Definimos como servicios no seguros aquellos que se realizan a través de la red de operador tradicional. Son los que se detallan a continuación:

S1. Llamada telefónica a numeración pública (a través de la SIM). Servicio de llamadas a la numeración móvil y fija externa.

S2. Llamadas a red privada virtual de la organización. Servicio de llamadas a la numeración móvil y fija interna de la organización.

S3. Envío de mensajes SMS. Servicio de envío de SMS a numeración móvil interna y externa.

Servicios seguros

Definimos como servicios seguros aquellos que son controlados por la organización. Son los que se detallan a continuación.

S4. Llamadas cifradas extremo a extremo haciendo uso de la aplicación para Voz IP (sólo usuarios VIP). Servicio para establecer una llamada a través de VoIP, haciendo uso de la infraestructura y la aplicación móvil.

S5. Mensajería instantánea (sólo usuarios VIP). Servicio de envío de mensajes y ficheros a través de la aplicación de Voz IP.

S6. Navegación a internet a través de la red corporativa. Servicio de navegación a través de la red corporativa de la organización.

S7. Acceso al correo corporativo. Servicio de acceso al correo corporativo de la organización (independientemente del mecanismo de acceso: internet, app, etc.).

S8. Acceso a los servicios de dominio interno de la organización. Conjunto de servicios de dominio interno de la organización: intranet, gestión de vacaciones, etc.

S9. Acceso a los servicios de dominio confidencial de la organización. Conjunto de servicios de dominio confidencial de la organización.

S10. Acceso al repositorio corporativo de aplicaciones. Acceso a la descarga de las aplicaciones autorizadas.

4.4.2 Funciones de seguridad

Este apartado presenta una breve descripción de las funciones de seguridad que se deben implementar en la organización. Parte de estas funciones son de nueva implementación, pero en la gran mayoría de casos se trata de adaptar y/o complementar los procesos, las prácticas y la tecnología ya existente en la organización para proporcionar los nuevos servicios requeridos. Puede entenderse como un modelo de referencia que se aterrizará desde el punto de vista tecnológico en los apartados posteriores.

Gestión de la información

La función de seguridad de gestión incluye los procesos para evaluar y gestionar el procesamiento de la información y los riesgos asociados con este sistema. Entre las principales características, se encuentran las que se detallan a continuación:

1. La organización ha de desarrollar, documentar e implementar las políticas de seguridad que identifican qué usuarios están autorizados para conectarse al sistema, y el tipo de información que puede ser transmitido a través de éste.
2. La organización ha de llevar a cabo una evaluación de los riesgos para entender las amenazas que pueden afectar al ecosistema del sistema, la probabilidad de que se materialicen las amenazas y el potencial impacto sobre el valor de los activos de información.
3. La organización ha de disponer del personal adecuado y entrenado para gestionar la infraestructura móvil.
4. La organización debe establecer los requisitos básicos que han de cumplirse (en línea con la política) para garantizar que el hardware, el firmware, el software, el hardware de la infraestructura móvil y la documentación existente son adecuados para proteger toda la infraestructura de la organización.
5. La organización debe asegurarse que se incluye la infraestructura y los dispositivos en los ciclos de detección y gestión de vulnerabilidades, para garantizar la seguridad continua de la infraestructura móvil.
6. La organización debe asegurar que existen procesos rigurosos para la aprobación de aplicaciones. Para ello, puede basarse en la guía NIST SP 800-163 del NIST (Anexo I), en la que se propone tanto las pruebas para detectar vulnerabilidades en aplicaciones como los análisis de riesgos y cumplimientos de políticas corporativas.

Formación

Los procesos de formación abordan las necesidades de la organización para disponer de personal con formación suficiente para llevar a cabo la administración de los sistemas de la infraestructura móvil, y la concienciación a los usuarios de los dispositivos sobre los riesgos de utilizarlos. Algunos de los aspectos formativos que debe contemplar la organización son los siguientes:

1. Capacitación en seguridad para el personal técnico que administra la infraestructura móvil y el resto de personal técnico:

    a. Riesgos de seguridad asociados con los diferentes métodos de autenticación o cifrado.
    b. Requisitos de seguridad para la infraestructura móvil, incluyendo las medidas para datos en reposo, en tránsito, privacidad…
2. Concienciación a usuarios, incluyendo conocimientos sobre seguridad móvil, descripción general de las políticas y mejores prácticas en lo relativo a:
    a. Control físico del dispositivo móvil.
    b. Protección de datos confidenciales en los dispositivos utilizando cifrado.
    c. Deshabilitar interfaces inalámbricas de los dispositivos cuando no se están utilizando.
    d. Reportar el robo o la pérdida del dispositivo tan pronto como sea posible.
    e. Utilización del dispositivo en redes de la organización, y con redes externas.
    f. Gestión de las contraseñas.
    g. Uso de redes sociales.
    h. Riesgos de root/jailbreak.

Controles de seguridad física

La función de controles de seguridad especifica los estándares necesarios para asegurar la seguridad física y resiliencia operacional de la infraestructura. Entre los aspectos fundamentales a tener en cuenta detallaremos el plan de seguridad física que asegura que los componentes son instalados de forma segura y que sólo el personal autorizado tiene acceso a los mismos.

Gestión de identidades y accesos

La función de Gestión de identidades y accesos se divide, a su vez, en las siguientes funciones o procesos:

1. **Autenticación**. Es el proceso de verificar la identidad de un usuario, proceso o dispositivo. En una infraestructura móvil existen muchas capas de autenticación, y la mayor parte se gestionan gracias tanto al IAM como al MDM/MAM. En cada apartado de los bloques funcionales se han explicado los mecanismos a implementar para la autenticación que aplica en cada caso.
2. **Autorización**. Todos los usuarios no tienen acceso a las mismas funcionalidades, y los procesos de autorización deben regular lo que el usuario puede hacer con el dispositivo (ejemplo: instalaciones, configuraciones…), así como a qué activos de información puede acceder en la organización.
3. **Control de acceso a la red**. Define el proceso a través del cual el dispositivo se autentica con la red antes de poder utilizar sus servicios.

Protección de los datos

La función de protección de los datos es uno de los mecanismos de mayor relevancia en la infraestructura de gestión de dispositivos. Podemos hablar de dos grandes puntos:

1. Protección de los activos:
    a. Acceso a los activos de información y las aplicaciones que los rodean.

b. Datos en reposo (Data at Rest): gestión de todo el ciclo de vida de los datos que residen en distintas partes de la infraestructura, así como en los diferentes dispositivos.
c. Datos en tránsito (Data in Transit): gestión de los datos que viajan desde los dispositivos hasta la infraestructura y viceversa.
d. Requisitos a tener en cuenta a la hora de destruir los distintos componentes.

2. Gestión de los datos de diagnóstico. En este grupo se encuentran todos los procesos que ayudan a la gestión de la infraestructura de diagnóstico, al análisis forense y a la identificación de comportamientos anómalos en la infraestructura.

Esta función y los procesos correspondientes se apoyarán en los siguientes elementos de infraestructura:

1. MDM, que gestiona la configuración y monitoriza los dispositivos de usuario.
2. VPN, que asegura el cifrado de los datos en tránsito y la identificación del usuario y del dispositivo.
3. Proxies, que analizan el tráfico de datos.
4. IDS/IPS que proporcionan alertas y mecanismos de defensa ante posibles intrusiones.
5. SIEM, que proporciona capacidad de monitorización de distintos eventos, y la aplicación de entornos para el análisis de seguridad.
6. IAM, que proporciona las funciones de autenticación y autorización.
7. Entornos aislados en los dispositivos (contenedores), que aseguran que los datos en reposo son aislados entre las distintas aplicaciones.
8. Cifrado de datos, que asegura que los datos almacenados en el dispositivo se guardan cifrados, protegiéndolos ante la pérdida, el robo o el compromiso del dispositivo.
9. Almacenamiento de datos de auditoría y política de retención de logs, con el objetivo de investigar posibles incidentes.

Gestión de los dispositivos y configuración de la infraestructura

Probablemente el proceso más crítico del dispositivo de usuario es su gestión. Dentro de la gestión, encontramos los siguientes procesos:

1. Seguridad del dispositivo:
    a. Parches para sistema operativo y aplicaciones.
    b. Gestión de la configuración: sistema operativo, aplicaciones (funcional y datos a los que tienen acceso), segmentación de datos, acceso a la red e interfaces.
    c. Aplicación de antivirus (protección de endpoint), firewall y políticas de auditoría y monitorización.
2. Configuración. Esta función hace referencia a la configuración física y lógica que es necesario desplegar para mantener una infraestructura móvil segura, incluyendo los dispositivos de usuario. En este punto, será necesario:
    a. Desarrollar las guías de configuración, con los requisitos mínimos hardware, firmware, software y de documentación.
    b. Elementos criptográficos necesarios para la infraestructura.

c. Gestión de las contraseñas y las cuentas por defecto.
d. Acceso administrativo para configurar la infraestructura.
e. Reglas de filtrado a aplicar en la navegación.

3. Validación de software y gestión de parches. Al igual que con los dispositivos tradicionales, la validación del software y la gestión de parches es parte fundamental en la gestión de los dispositivos. El MDM es tradicionalmente el primer mecanismo para llevar a cabo estas funciones.

Comunicaciones seguras

La función de comunicaciones móviles seguras asegura las comunicaciones desde el punto de vista de accesos no autorizados, divulgación y modificación no autorizada de la información. Para ello, se requiere de un protocolo de comunicación seguro para proteger adecuadamente la confidencialidad, la integridad, la disponibilidad de la información y garantizar la autenticación, autorización, trazabilidad y no repudio. Normalmente se utilizan mecanismos de cifrado mediante red VPN (basada en hardware o software) en la capa de datos o en la de red, o bien cifrado a través de la propia aplicación.

Algunas de las características a implementar en la infraestructura de comunicaciones móviles son las siguientes (se detallarán en el apartado 4.4.3 Bloques Funcionales):

1. La administración y la gestión de los equipos utilizan cifrado y mecanismos de autenticación fuerte para todas las comunicaciones.
2. Todos los elementos criptográficos deben cumplir las políticas de seguridad de la organización. El MDM debe hacer cumplir, administrar y monitorizar estas políticas.
3. Se deben implementar mecanismos de protección frente a posibles ataques de denegación de servicio contra la infraestructura de la organización.
4. Cifrar el canal de comunicaciones de la red para proteger los datos en tránsito, utilizando además aplicaciones que cifran los datos tanto en tránsito como en reposo.

Monitorización continua y procesos de auditoría

La monitorización y los procesos de auditoría son procesos esenciales para mantener un conocimiento de la situación de los dominios críticos de la infraestructura de dispositivos móviles (por ejemplo: red, sistemas, aplicaciones, entornos de autenticación y autorización…).

Es esencial monitorizar y auditar no sólo el servicio y los planos de datos en el dispositivo móvil y la infraestructura, sino también el plano de control. Si el plano de control se ve comprometido, la organización podría volverse altamente vulnerable a la explotación con poca o ninguna detección al evadir el atacante los procesos de monitorización haciendo reconfiguraciones sobre la infraestructura. Algunas de las principales características en este sentido son las que se detallan a continuación:

1. Se desarrollan procesos y procedimientos de auditoría de seguridad de la infraestructura móvil. Es necesario asegurar que se llevan a cabo

evaluaciones de seguridad de la infraestructura de forma regular para asegurar que se cumplen los requisitos de seguridad de la infraestructura.
2. Los dispositivos móviles se auditan periódicamente para garantizar que cumplen los requisitos de seguridad de la organización, incluidos los mecanismos de autenticación, cifrado de datos y acceso administrativo.
3. Los registros de auditoría se revisan con frecuencia indicada en las políticas de seguridad.
4. Se define una política de retención para los datos de auditoría.
5. Existe una estrecha integración de los elementos dentro de la infraestructura móvil, incluyendo la gestión de aplicaciones, la gestión de la configuración y la gestión de los dispositivos.

Toda esta información se utiliza con el objetivo de mejorar la seguridad de la infraestructura móvil a través de:

- La detección de dispositivos no autorizados.
- La detección del uso de aplicaciones no autorizadas.
- La identificación de anomalías o comportamientos de un dispositivo o un conjunto de ellos que se desvían del comportamiento estándar.
- La verificación de que los dispositivos que se están utilizando son los autorizados por la organización.
- La monitorización de la configuración y el comportamiento del dispositivo, así como el uso del mismo.

Respuesta a incidentes

La función de respuesta a incidentes abarca todas las facetas de la respuesta a incidentes. Para ello es necesario implementar procesos y procedimientos efectivos para cada una de las seis fases de la respuesta a incidentes: preparación, identificación, contención, erradicación, recuperación y seguimiento en lo relativo al nuevo sistema.

4.4.3 Bloques funcionales

En este apartado se propone una implementación del modelo desde el punto de vista técnico. No obstante, no es una solución cerrada, ya que se puede implementar de muchas formas y utilizando distintas soluciones o productos existentes en el mercado. El proceso de diseño, despliegue, así como la tipología y los componentes utilizados en un sistema de estas características dependerá de una serie de factores que la organización debe analizar, entre los que se incluyen:

- El perfil de riesgo de la organización.
- Aspectos financieros.
- Legislación aplicable.
- Capacidad técnica de la organización.
- Arquitectura admitida e integración de las diferentes soluciones EMM disponibles en el mercado en la infraestructura de la organización.

Cada organización es responsable de conocer y evaluar los factores que le son de aplicación previamente al diseño del sistema, la reserva de recursos y la selección de los componentes a incluir.

A alto nivel, la solución constará de los siguientes elementos fundamentales:

1. Los dispositivos móviles de los usuarios.
2. Las aplicaciones que la organización considere necesarias para dar los servicios especificados en los requisitos.
3. La infraestructura necesaria para gestionar los dispositivos, las aplicaciones y el contenido de los dispositivos móviles, e integrarlos en la infraestructura de la organización.
4. La infraestructura necesaria para dotar a la organización del servicio de llamadas a través de Voz IP para los usuarios móviles VIP.

A continuación se presenta un esquema o modelo de referencia de los diferentes bloques que forman parte del diseño a alto nivel para esta organización:

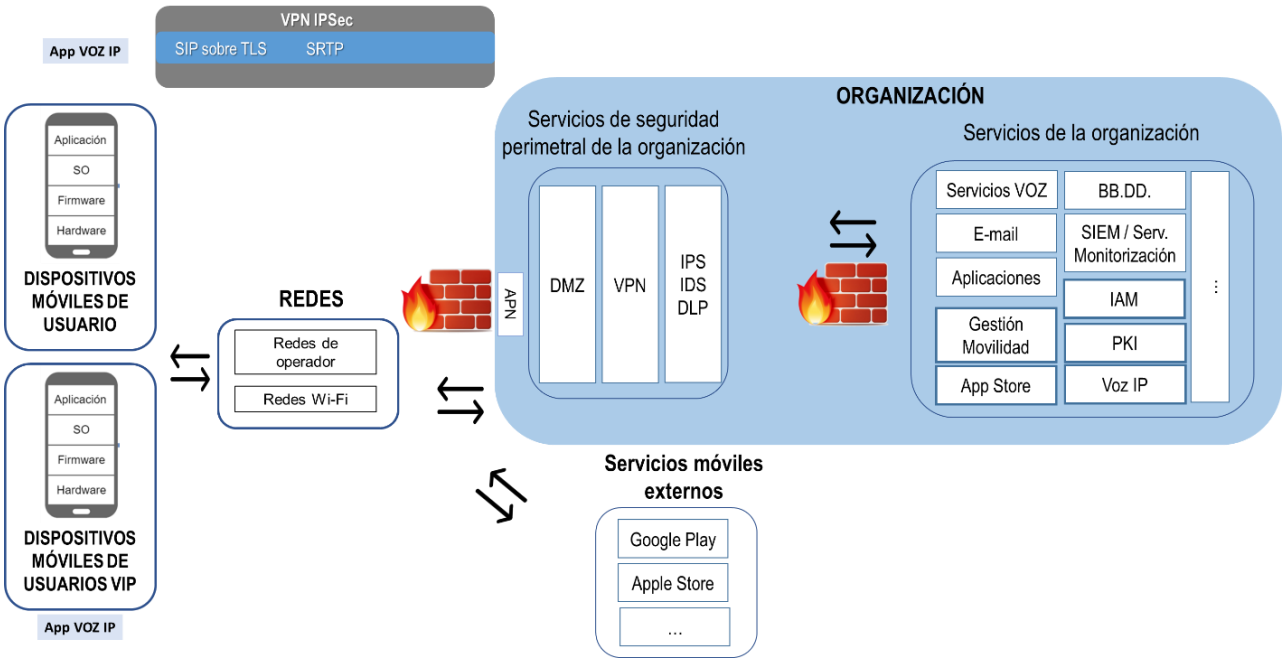

Figura 7 Arquitectura de referencia de alto nivel.

DISPOSITIVO MÓVIL DE USUARIO

El dispositivo móvil representa uno de los puntos más críticos de la seguridad de la red de comunicaciones, debido en gran parte al bajo nivel de protección física que se deriva de los principales casos de uso (utilización en el domicilio, en lugares públicos…), que lo hacen muy vulnerable a pérdidas o sustracciones.

Existirán dos maquetas o tipos de dispositivos: por un lado, los dispositivos móviles de usuario, y por el otro los dispositivos móviles de usuarios VIP. Esta clasificación no hace referencia al tipo o modelo de dispositivo, sino al grado de clasificación de la información que éstos podrán manejar. Los primeros podrán consumir los servicios de uso interno y público, mientras que los segundos podrán también acceder a los servicios de carácter confidencial y restringido.

Almacenamiento de información y uso de aplicaciones

Se dispondrá de un contenedor aislado para los datos y las aplicaciones de la organización. La solución debe además permitir a la organización seleccionar

qué datos estarán cifrados cuando el teléfono esté apagado y/o bloqueado. Aplicarán políticas de seguridad distintas en función de la clasificación de los datos por parte de la organización. Además, las aplicaciones y los datos almacenados dentro de un contenedor no deben poder utilizar métodos de uso compartido de datos ni comunicarse con procesos o aplicaciones instaladas fuera de éste (ni con medios de almacenamiento externo, como tarjeta SD y USB).

En líneas generales, la solución dispondrá de los siguientes entornos:

1. Entorno de uso personal, donde el usuario podrá instalar aplicaciones permitidas por la organización de los markets públicos (habrá listas negras de aplicaciones que el usuario no podrá instalar). En ningún caso se permitirá la instalación de aplicaciones "de orígenes desconocidos", es decir, las que están fuera de estos markets oficiales.
2. Entorno de uso profesional para servicios de uso interno, donde se podrán instalar las aplicaciones del repositorio interno de la organización.
3. Entorno de uso profesional para servicios confidenciales, donde se podrán instalar las aplicaciones restringidas del repositorio interno de la organización. Este último entorno sólo estará disponible para la maqueta de usuarios VIP.

Autenticación del usuario en el dispositivo

La solución debe permitir, al menos: un código PIN numérico para acceder al dispositivo, y una contraseña más segura para acceder a los contenedores de datos profesionales.

Autenticación del usuario en los servicios de la organización

La solución se integrará con los servicios de autenticación únicos (SSO) y Active Directory de la organización. La autenticación en las aplicaciones corporativas se hará siempre dentro del contenedor correspondiente, y se requerirá tanto la contraseña del usuario en el dominio de la organización, como el correspondiente certificado instalado en el dispositivo para consumir los servicios.

Para ello será necesario aprovisionar los siguientes certificados de cliente a través de la solución de gestión de la movilidad empresarial:

1. Certificado de autoridad de certificación (CA) de la organización, utilizado para validar los certificados de servidor de la organización.
2. Un certificado de cliente para el uso de los servicios corporativos (Wi-Fi, aplicaciones, correo, etc.).
3. Un certificado de cliente VPN para cada túnel VPN que se establezca con la organización.
4. Un certificado de cliente SSL para la autenticación en los servicios de la intranet de la organización.

Aplicación de políticas de seguridad de la organización

La solución debe ser compatible con los aspectos indicados en la política de seguridad de la organización en relación con:

1. Listas blancas o negras para la descarga de las tiendas de aplicaciones oficiales (entorno personal).
2. Impedir los ajustes de modo de desarrollador, incluyendo la depuración de USB y el modo de almacenamiento USB.
3. Características de los algoritmos de cifrado de la información en el dispositivo (para cada contenedor).
4. Deshabilitar o no el acceso a la tarjeta SD.
5. Políticas de contraseña (longitud, número máximo de intentos erróneos, historial de contraseñas y caducidad).
6. Tiempo de inactividad para bloqueo.
7. Establecimiento de VPN (se detalla en el apartado de Redes de Comunicaciones).
8. Validación e instalación de los certificados de la organización.
9. Deshabilitar las interfaces innecesarias (USB, Bluetooth, NFC).
10. Políticas de borrado remoto y respuesta a eventos (como intentos de login erróneos).

Recopilación de eventos para su análisis por parte de la organización

Es necesario que la solución permita registrar datos de auditoría y recuperar los registros de los dispositivos, con el fin de poder monitorizar eventos fallidos de desbloqueo, instalación o desinstalación de aplicaciones, etc. Se trata de eventos independientes de la navegación, que será supervisada al pasar el tráfico a través de la organización.

Respuesta a incidentes

La solución debe permitir el bloqueo y el borrado remoto del dispositivo y las aplicaciones, y activar mecanismos de actuación ante introducciones incorrectas del PIN de acceso al dispositivo o al contenedor correspondiente.

Requisitos en relación con los dispositivos móviles de usuario

La solución debe considerar los siguientes requisitos, en relación con los dispositivos móviles de usuario y su autenticación en la infraestructura de la organización:

DM-1. Los usuarios de los dispositivos móviles deben autenticarse correctamente en los servicios a los que acceden haciendo uso de un mecanismo de autenticación aprobado por la organización.

DM-2. Los usuarios de la organización deben firmar un documento de aceptación de condiciones antes de ser autorizados a utilizar los dispositivos móviles de la organización. Al menos, en el documento se deben cubrir los siguientes aspectos:

- Consentimiento de monitorización de la actividad de los dispositivos.
- Requisitos para operar los dispositivos.
- Requisitos físicos de protección del dispositivo cuando se está utilizando y cuando éste se almacene.
- Especificación del cuándo, dónde y bajo qué condiciones se utilizarán los dispositivos.
- Responsabilidad del usuario, de cara a reportar posibles incidentes de seguridad.
- Verificación de que ha llevado a cabo la formación necesaria para su uso.
- Verificación de las autorizaciones necesarias para el uso del dispositivo.
- Justificación de uso del dispositivo.
- Información del usuario.
- Fecha de caducidad de la cuenta.
- Responsabilidades del usuario.

DM-3. Los usuarios deben recibir formación para utilizar los dispositivos móviles antes de que éstos sean utilizados.

DM-4. Será necesario disponer de mecanismos fuertes de autenticación del dispositivo en la infraestructura de la organización.

DM-5. El dispositivo debe poder ser gestionado de forma remota y centralizada desde la infraestructura corporativa, para lo que será necesario prever la instalación de un agente en el mismo que permita la actualización y configuración de las políticas de seguridad vigentes en cada momento.

DM-6. Se deben deshabilitar todos los datos GPS y servicios de localización de los dispositivos, dejando únicamente activos los autorizados por la organización.

DM-7. Se deben deshabilitar las actualizaciones llevadas a cabo por los operadores.

DM-8. Se deben deshabilitar todas las interfaces inalámbricas no autorizadas por la organización.

DM-9. La descarga, instalación y ejecución de aplicaciones en el dispositivo debe llevarse a cabo a través de listas blancas gestionadas por la organización a través de un repositorio de aplicaciones corporativo.

DM-10. No estará permitida la descarga de aplicaciones de tiendas no oficiales en los entornos de trabajo de la organización. La descarga de markets oficiales debe estar regulada por la propia organización (y detallada en la política de seguridad de dispositivos móviles).

DM-11. La información almacenada en el dispositivo debe ser supervisada por la organización, y aplicar los mecanismos de cifrado que la organización determine.

DM-12. Las llamadas y el envío de mensajes confidenciales en la organización se realizarán haciendo uno de una aplicación de Voz IP que implemente un cifrado extremo a extremo de las comunicaciones. El uso de otros servicios de operador (como buzón de voz) debe ser deshabilitado, salvo autorización expresa por parte de la organización.

DM-13. Los dispositivos deben ser monitorizados. En caso de sospecha de compromiso, se revocarán los accesos y serán remitidos a la organización para llevar a cabo un análisis forense que determine si se ha visto comprometido.

DM-14. Los dispositivos deben disponer de certificados revocados antes de que se entreguen. Se activarán una vez que se asignen a usuarios.

DM-15. Todas las contraseñas de acceso a recursos corporativos deben cumplir la política corporativa de la organización.

DM-16. Debe existir un ciclo de vida de todas las contraseñas que se utilicen en el dispositivo.

DM-17. La pantalla del dispositivo se debe bloquear al menos después de tres minutos de inactividad.

DM-18. Se debe implementar un borrado de los datos después de un número de intentos fallidos determinado por la organización.

DM-19. El dispositivo móvil se conectará a través de una VPN a cualquier recurso de la organización.

DM-20. El dispositivo será configurado con la política de seguridad definida en la organización a través del MDM.

DM-21. Se deben deshabilitar las notificaciones mientras el dispositivo está bloqueado.

DM-22. Se debe deshabilitar la funcionalidad de almacenamiento USB del dispositivo.

DM-23. De debe deshabilitar la transferencia de información a través del puerto USB.

DM-24. El usuario sólo debe estar autorizado a acceder a las aplicaciones que deba utilizar para el desempeño de sus funciones, dentro del contenedor corporativo de aplicaciones.

DM-25. Los dispositivos deben ser actualizados regularmente.

DM-26. Se debe deshabilitar el modo debug USB de los dispositivos móviles.

REDES DE COMUNICACIONES

Desde el punto de vista de las comunicaciones, los dispositivos podrán usar las siguientes redes:

- Redes móviles de datos de operador.
- Redes WiFi, tanto corporativas como de terceros.

El criterio general en cuanto a la red de acceso será considerarla potencialmente comprometida o no confiable, y ser conscientes de los riesgos que implica su utilización:

a) Riesgo de acceso a la información que se transmite a través de esta red por parte de terceros.
b) Posible falta de transparencia del proveedor de servicios en cuanto a sus infraestructuras (subcontratación).
c) Fragilidad del medio en cuanto a disponibilidad (denegación de servicio).
d) Dificultad para conseguir protección por anonimato.

Uso de la red de datos móviles

Es recomendable la contratación con el proveedor de comunicaciones de un APN privado para la organización. El APN es el punto donde se conectan los dispositivos móviles cuando acceden a los servicios de datos del operador (MMS, internet, etc.).

De esta forma, sólo se pueden conectar al mismo los identificadores de tarjetas SIM definidos por la organización. Esto permite establecer una primera capa de protección para la subred móvil de la organización (delegada en el proveedor de comunicaciones).

El proveedor de comunicaciones entregará de esta forma (y recogerá) todo el tráfico de datos generado por (y destinado a) los dispositivos de la organización en este punto, que será la frontera exterior de la infraestructura corporativa dedicada a la movilidad.

Protección de las comunicaciones

Independientemente de la red utilizada, se requiere el uso de soluciones que permitan establecer una VPN basada en IPSec con autenticación mutua para acceder a la red y a los servicios de la organización basados en certificados PKI protegidos en el dispositivo.

Existen distintas soluciones en el mercado integradas en los mecanismos de gestión empresarial. En el caso de la plataforma Samsung Knox, a modo de ejemplo, las APIs de gestión permiten que las configuraciones VPN se puedan aplicar a todo el dispositivo, por contenedor o por aplicación.

El modo “por aplicación” permite que la solución MDM seleccione aplicaciones (dentro y fuera del contenedor) para conectarse a la red con un perfil de VPN específico. El uso de esta VPN garantiza que el tráfico procedente de todas las aplicaciones seleccionadas se transmitirá a través de la VPN, por lo que las aplicaciones no tendrán acceso a la conectividad hasta que se establezca la VPN.

Para nuestra organización en concreto se requerirá el establecimiento de un túnel VPN tanto para las aplicaciones dentro del contenedor de la organización como para las que no, garantizando que todo el tráfico se transmite mediante la VPN hasta la organización, y sale a internet a través de ésta. Estableceremos dos túneles:

- Uno para el tráfico de las aplicaciones que tienen acceso a los servicios del dominio interno de la organización, incluyendo las de uso personal del usuario.
- Uno para el tráfico de las aplicaciones que tienen acceso a los servicios del dominio confidencial de la organización.

Además, será preciso que la solución de MDM aprovisione los perfiles VPN de forma automática, sin que el usuario pueda deshabilitarlos o modificarlos, de tal forma que el tráfico se tunelice de forma automática sin interacción por parte de éste.

Comunicaciones a través de Voz IP

Adicionalmente a la capa de protección de la VPN para todos los datos transmitidos hacia la organización, es necesario considerar en este apartado los aspectos a tener en cuanto a las comunicaciones a través del sistema de Voz IP para los usuarios VIP (aplicación en el dispositivo móvil, e infraestructura asociada en la organización).

Para garantizar la confidencialidad de las comunicaciones, se requerirá una solución que utilice SIP sobre TLS para la señalización, y ZRTP y SRTP para el contenido multimedia (o nivel de seguridad equivalente).

[1] Seguridad en la **señalización**:

- SIP es el protocolo de señalización: acciones como sonar el dispositivo, responder a la llamada y colgar. No interactúa con la secuencia de audio y vídeo.
- TLS es el protocolo de seguridad entre los puntos extremos de señalización de la sesión. Es la misma tecnología que se utiliza para sitios web SSL.

[2] Seguridad en el **contenido multimedia** (secuencia de audio/vídeo):

- ZRTP es el protocolo que se lleva a cabo para realizar el intercambio de claves entre los extremos de la comunicación. En Voz IP todos los dispositivos son cliente y servidor a la vez, así que tenemos sólo “extremos” en lugar de “clientes” o “servidores”.
- Una vez que los extremos están de acuerdo en el secreto compartido, la sesión ZRTP termina y comienza la sesión SRTP, en la que se cifra el tráfico multimedia en tiempo real.

Requisitos en relación con la protección de las comunicaciones

La solución debe considerar los siguientes requisitos, en relación con la protección de las comunicaciones:

PC-1. Los componentes TLS deben utilizar TLS 1.2 o posterior.

PC-2. Los componentes TLS de la infraestructura deben utilizar certificados X.509 para la autenticación mutua con los dispositivos de usuario.

PC-3. Los certificados por defecto, autofirmados que normalmente vienen preinstalados en los dispositivos deben ser deshabilitados y eliminados.

PC-4. El terminador de túneles debe usar el modo IPSec.

PC-5. El terminador cifrará todo el tráfico, con la única excepción del tráfico necesario para que el dispositivo se conecte físicamente a la red (por ejemplo, tráfico DHCP).

COMPONENTES DE INFRAESTRUCTURA

Como hemos comentado en apartados anteriores, todas las comunicaciones del dispositivo con la organización han de estar protegidas por al menos dos capas de cifrado, usando VPN sobre IPSec sobre TLS/SRTP.

Además es necesario considerar aspectos como los equipos para administrar la infraestructura, el equipamiento a instalar y la integración con los elementos ya existentes en la organización: IDS/IPS, SIEM, firewalls, CAs para gestión de certificados con infraestructura PKI, proxies de navegación, etc.

A continuación, se presenta una propuesta de diagrama de diseño, en el que se han introducido los diferentes elementos (tanto los nuevos como los que interactúan con el sistema).

En el apartado *4.4.4 Flujos de información* se relaciona la información con los distintos componentes de la infraestructura.

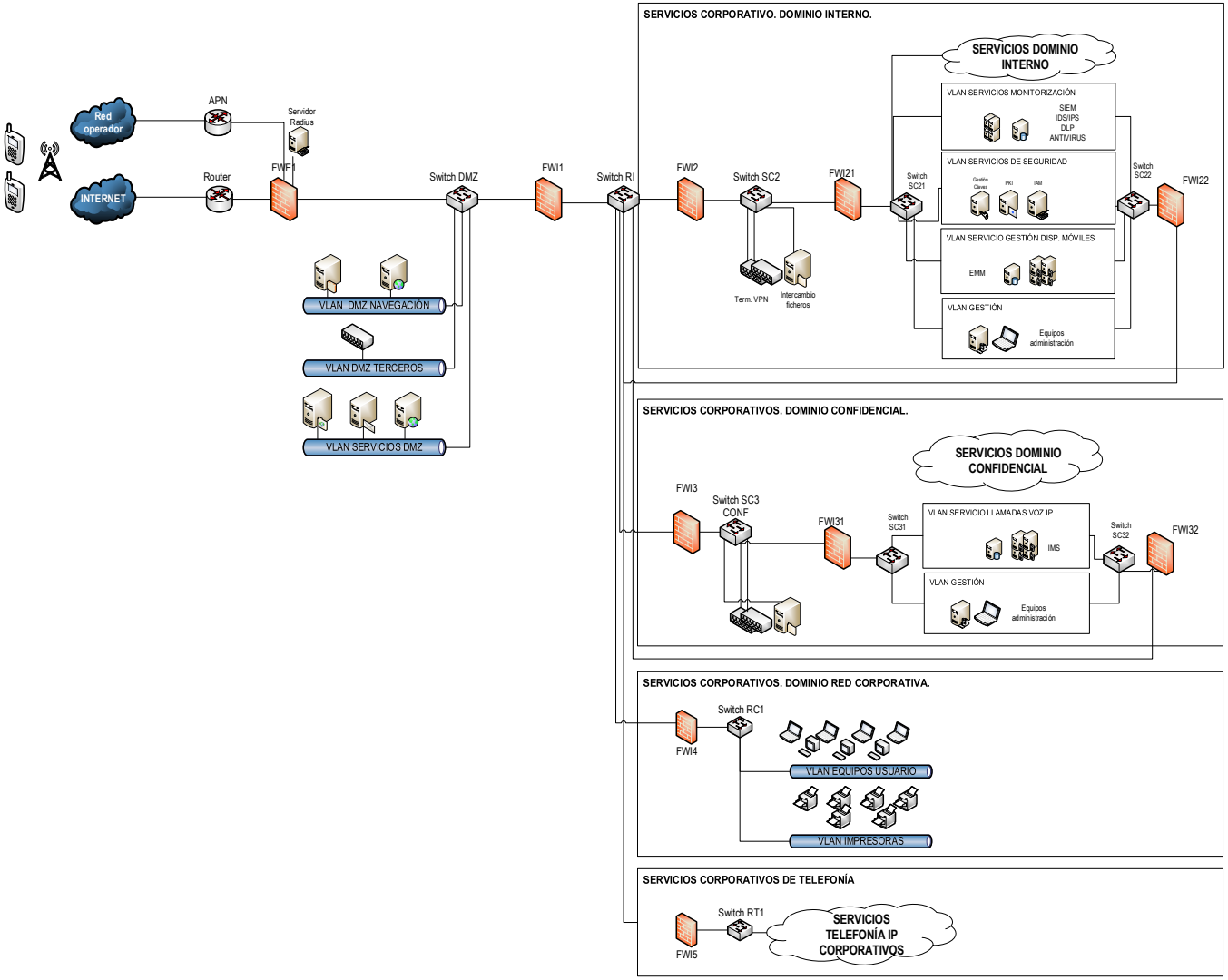

Figura 8 Diseño del sistema en la red corporativa.

Router externo

Router de tráfico entrante y saliente de internet de la organización. Se utiliza para el tráfico entrante y saliente desde y hacia los dispositivos móviles que establecen el túnel VPN con la organización. Además, se utiliza para las salidas de tráfico de internet desde la organización.

APN operador

Punto de interconexión con la red de operador, donde se reciben y se envían los datos procedentes o hacia los diferentes dispositivos conectados. El servidor Radius autentica las distintas tarjetas SIM que están autorizadas a consumir estos servicios.

Firewall Externo, FWE1

Es el punto de entrada y salida de tráfico en la organización. Controla el tráfico recibido y enviado a los dispositivos móviles a través de internet y de la red móvil del operador (APN). Regula también los flujos de tráfico con las DMZs de la organización.

Firewall Interno Primer Nivel, FWE1

Punto de entrada de tráfico desde el exterior a través de las DMZs a la red interna. Recibe el túnel VPN de los dispositivos móviles y ha de permitir su paso hasta que pueda alcanzar el terminador de túneles correspondiente. Por otro lado, regula el tráfico saliente de la organización hacia la DMZ de navegación.

Firewall Interno Dominio Interno, FWI2

Punto de entrada a los servicios de la organización que gestionan información restringida, de uso interno y de uso público. Permitirá el tráfico desde los dispositivos hasta el terminador de túneles, donde finaliza el flujo de la VPN.

Terminador de túneles Dominio Interno

Extremo de la VPN entre los terminales y los servicios de Dominio Interno de la organización. Permite autenticar los componentes VPN y ofrece protección criptográfica de los datos en tránsito y la aplicación de las reglas de manejo de los paquetes de la red para el consumo de los servicios internos.

Firewall Interno Dominio Interno, FWI21

Segundo nivel dentro de los servicios de dominio interno. Este firewall permitirá el paso del tráfico desde el terminador de túneles hasta los diferentes servicios:

- Servicios de seguridad, para la autenticación de los dispositivos, los usuarios y la comprobación de los certificados.
- Servicios de movilidad: gestión de los dispositivos y repositorio interno de aplicaciones.

- Servicios de dominio interno de la organización: correo corporativo, navegación, DNS, etc.

Firewall Interno Dominio Interno, FWI22

Firewall de tráfico saliente hacia internet del dominio interno. Permitirá que los dispositivos móviles naveguen a internet haciendo uso de la DMZ de navegación de la organización. También filtrará el tráfico entre las distintas VLANs del dominio (consultas a servidor de correo, DNS corporativo, servicios de seguridad, etc.).

Firewall Interno Dominio Confidencial, FWI3

Punto de entrada a los servicios de la organización que gestionan información confidencial. Permitirá el tráfico desde los dispositivos hasta el terminador de túneles, donde finaliza el flujo de la VPN.

Terminador de túneles Dominio Confidencial

Extremo de la VPN entre los terminales y los servicios de Dominio Confidencial de la organización. Permite autenticar los componentes VPN y ofrece protección criptográfica de los datos en tránsito y la aplicación de las reglas de manejo de los paquetes de la red para el consumo de los servicios confidenciales de la organización.

Firewall Interno Dominio Confidencial, FWI31

Segundo nivel dentro de los servicios de dominio confidencial. Este firewall permitirá el paso del tráfico desde el terminador de túneles hasta los diferentes servicios:

- Servicios de carácter confidencial de la organización.
- Servicio de llamadas seguras a través de Voz IP.

Firewall Interno Dominio Confidencial, FWI32

Firewall de interconexión del dominio con otros dominios. Se utilizará para filtrar el tráfico hacia la pasarela de telefonía (Servicios Corporativos de Telefonía).

Servidor IMS

Servidor centralizado de comunicaciones. Está formado por un servidor de aplicaciones, donde se encontrará el módulo principal que gestiona la conectividad y la lógica de aplicación y por otro lado un servidor de base de datos, en el que se almacenan los datos que la aplicación necesita.

Servidores de Gestión de dispositivos móviles (EMM)
Conjunto de servidores de aplicaciones y de bases de datos para llevar a cabo la gestión centralizada de los dispositivos. Incluye la gestión de los markets de aplicaciones de la organización.

Requisitos en relación con la configuración y los componentes de la infraestructura

La solución debe considerar los siguientes requisitos, en relación con la configuración de los distintos componentes de la infraestructura:

CI-1. Los servicios de red proporcionados por los protocolos del plano de control (como DNS o NTP) deben ubicarse en la red interna.

CI-2. El tiempo de todos los elementos de la infraestructura se sincronizará con la misma fuente, que estará ubicada en el dominio interno de los servicios corporativos.

CI-3. Las cuentas por defecto, así como las contraseñas y otros mecanismos de acceso por defecto deben ser modificadas o eliminadas.

CI-4. Todos los componentes de infraestructura recibirán firmas de virus actualizadas.

CI-5. Todos los componentes de infraestructura deben ser configurados únicamente a través de una interfaz dedicada para la gestión.

CI-6. Los servidores DNS en dispositivos de infraestructura deben ser especificados o deshabilitados.

CI-7. Los servicios de configuración remotos en tiempo de arranque deben estar deshabilitados (por ejemplo, la configuración automática a través de TFTP en el arranque).

CI-8. Todos los componentes dentro de la infraestructura deben tener las interfaces restringidas al menor número de rangos IP, puertos y protocolos posible.

CI-9. Se deben deshabilitar todas las interfaces de red no utilizadas en los componentes de infraestructura.

CI-10. Se debe disponer de un estándar de configuración para todos los componentes, que será mantenido por el administrador de seguridad.

CI-11. Deben existir procesos automáticos que garanticen que los cambios de configuración son registrados.

CI-12. Todos los componentes deben ser configurados con un servicio de monitorización que detecten cambios en la configuración.

CI-13. Los dispositivos de usuario deben generar logs que serán enviados al SIEM de la organización.

CI-14. Existirán estaciones de administración en cada uno de los dominios.

CI-15. El envío de logs al SIEM se hará haciendo uso de protocolos de cifrado.

CI-16. El tráfico de cada uno de los dominios, y en especial el situado en las DMZs debe ser monitorizado por el IDS/IPS corporativo.

CI-17. Se deben establecer patrones para el flujo de datos habitual, y revisar diariamente: sistemas generando cantidades excesivas de tráfico; sistemas intentando conectarse a IPs no habituales; sistemas intentando conectarse a puertos cerrados o servidores internos.

CI-18. Los terminadores de túneles deben registrar todos los eventos relacionados con el establecimiento y la finalización de túneles.

CI-19. Los servidores protegidos con TLS deben almacenar los eventos de establecimiento y finalización de conexiones.

CI-20. Los componentes de la infraestructura den registrar todas las acciones llevadas a cabo en el log de administración (borrados, descargas, etc.).

CI-21. Los componentes de infraestructura deben registrar los intentos de acciones no autorizadas (lectura, escritura, ejecución, borrado…) de objetos.

CI-22. Los componentes de infraestructura deben registrar todas las acciones llevadas a cabo desde un usuario con privilegios administrativos.

CI-23. Los componentes de infraestructura deben registrar todos los eventos de escalado de privilegios.

CI-24. Los componentes de infraestructura deben registrar todas las cargas y revocaciones de certificados.

CI-25. Los componentes de infraestructura deben registrar todos los eventos de cambio de hora.

CI-26. Cada entrada de log debe registrar la fecha y la hora del evento, así como el tipo de evento.

CI-27. Cada entrada del log debe registrar si el evento se llevó a cabo con éxito o falló, y el código de fallo cuando sea posible.

CI-28. Todos los sistemas de la solución se integrarán con los servicios corporativos de PKI, IAM y gestión de claves, con el fin de asegurar que se cumplen las políticas corporativas relativas a cuentas, contraseñas, ciclo de vida de certificados y gestión de perfilado.

CI-29. Todos los sistemas de la solución se integrarán con los servicios corporativos de prevención de ataques de denegación de servicio, y fuerza bruta.

CI-30. Los sistemas de la solución se integrarán con los proxies corporativos para llevar a cabo el análisis de tráfico y las reglas de filtrado oportunas (VLAN DMZ NAVEGACIÓN).

4.4.4 Flujos de información

En este apartado se describirán brevemente los flujos de información, con el objetivo de contextualizar los distintos componentes por los que pasará la información para el consumo de los diferentes servicios que el sistema prestará.

Establecimiento de túneles VPN

Como se indicó en el apartado anterior, los terminales móviles establecerán dos túneles VPN con la organización: uno con los servicios de dominio interno, y otro con los servicios del dominio confidencial. Todo el tráfico intercambiado con la organización pasará a través de estos túneles.

Si la entrada se produce a través del APN del operador (datos móviles), el flujo del tráfico será el que se detalla a continuación (marcado en naranja). El tráfico de vuelta sigue exactamente el camino inverso al indicado en el dibujo.

1. Entrada de datos a través del APN desde la red móvil.
2. Identificación de la tarjeta SIM en el servidor Radius.
3. Paso de tráfico a través de FWE1 hasta terminadores VPN de cada dominio (un túnel distinto para cada terminador).

Para proveer este servicio, será necesario que el proveedor incluya en sus DNS la IP del servicio.

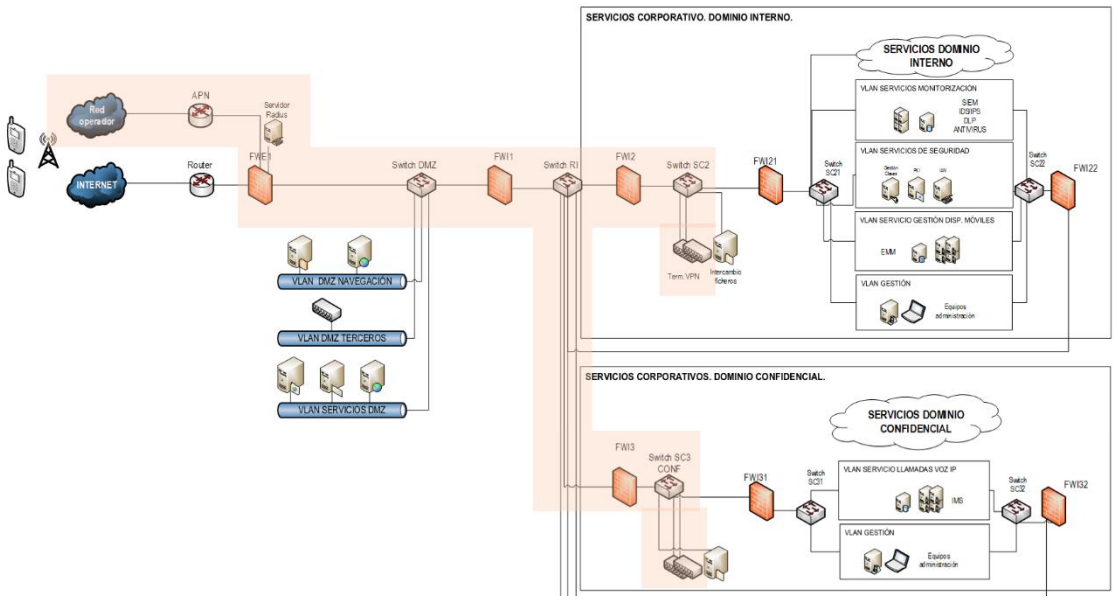

Figura 9 Flujo establecimiento de túnel con APN.

Si la entrada no se produce a través del APN de operador, el flujo del tráfico será muy similar (marcado también en naranja en la Figura 10). El tráfico de vuelta, como en el caso anterior, seguirá exactamente el camino inverso al indicado en el dibujo.

1. Entrada de datos a través del router de la organización.
2. Identificación en FWE1 y paso de tráfico hasta terminadores VPN de cada uno de los dominios.

Para proveer este servicio, será necesario que en la VLAN de servicios DMZ, el servidor DNS de servicios expuestos de la organización publique este servicio hacia el exterior.

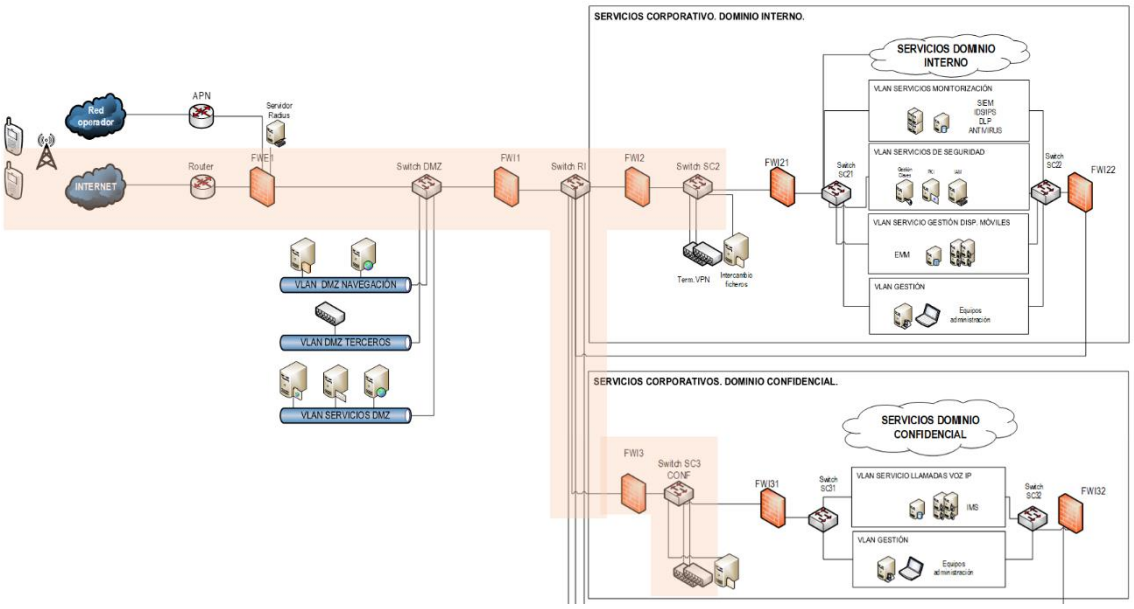

Figura 10 Flujo establecimiento de túnel sin APN.

Llamadas cifradas extremo a extremo

Para establecer las llamadas cifradas extremo a extremo, cada terminal móvil hará uso del túnel VPN que habrá establecido con los servicios corporativos del dominio confidencial para llegar hasta el servidor IMS. Como detallamos en el apartado anterior, el servidor IMS se encarga de todos los aspectos relativos a la señalización, sabe qué terminales están disponibles y cuáles son sus direcciones IP. El servidor IMS permitirá que ambos terminales tengan visibilidad entre sí y lleven a cabo el intercambio de credenciales que tiene que ocurrir para que se establezca la comunicación directa entre ambos. En la siguiente figura se representa un esquema de lo que podrían ser los dos flujos de información involucrados:

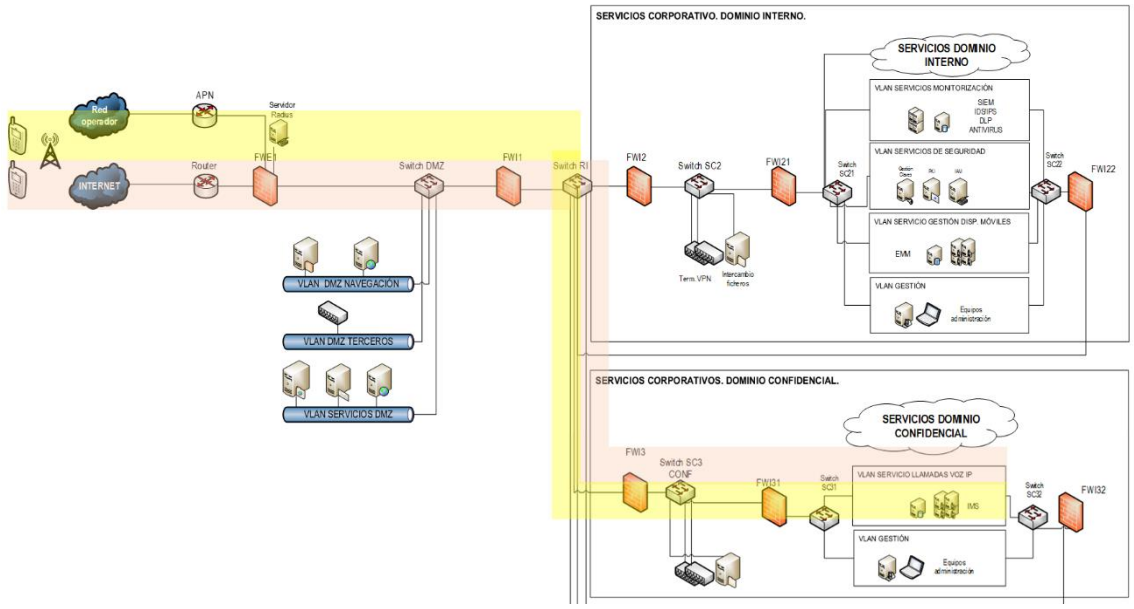

Figura 11 Flujo llamadas cifradas extremo a extremo.

Consumo del servicio de navegación corporativa

Para consumir los servicios corporativos del dominio interno, el terminal hará uso del túnel VPN que tiene establecido con el terminador de túneles conectado a dicho dominio (switch SC2), independientemente de si se conecta por APN o red WiFi.

Por dicho túnel, intercambiará todo el tráfico cifrado con la organización. A partir de aquí, saldrá a navegar haciendo uso de los servicios de navegación internos, para lo que tendrá que alcanzar la DMZ de navegación siguiendo el camino marcado en azul. Esta es la forma de asegurar que todo el tráfico interno pasa por el mismo sitio, que se le aplican las reglas del proxy situado en la DMZ de navegación, y que además el tráfico pasa por los procesos de monitorización que la organización tiene habilitados.

El tráfico de vuelta de la navegación (por ejemplo, la web que el usuario está visitando), hará el camino inverso (desde la DMZ de navegación) y será devuelto al móvil a través del túnel VPN.

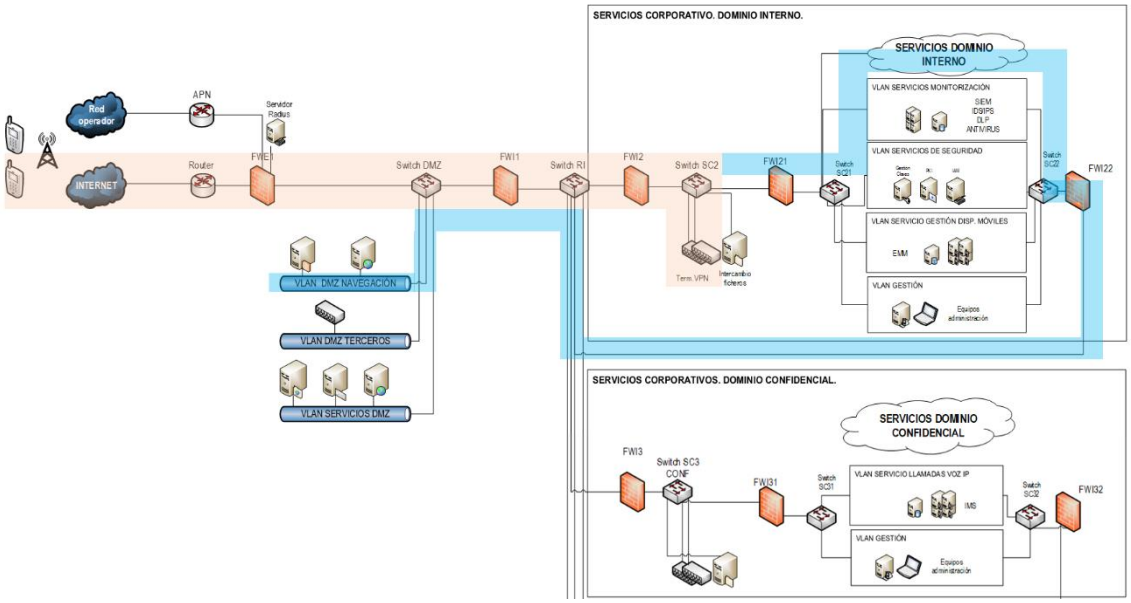

Figura 12 Flujo de información para la navegación corporativa.

Consumo de otros servicios del dominio interno

El ejemplo sería exactamente igual que el visto en el caso anterior, pero llegando al servidor front del servicio en cuestión (pasarela de correo, front de aplicación, etc.).

Consumo de servicios del dominio confidencial

Para consumir los servicios corporativos del dominio confidencial, el terminal hará uso del túnel VPN que tiene establecido con el terminador de túneles conectado a dicho dominio (switch SC3), independientemente de si se conecta por APN o red WiFi.

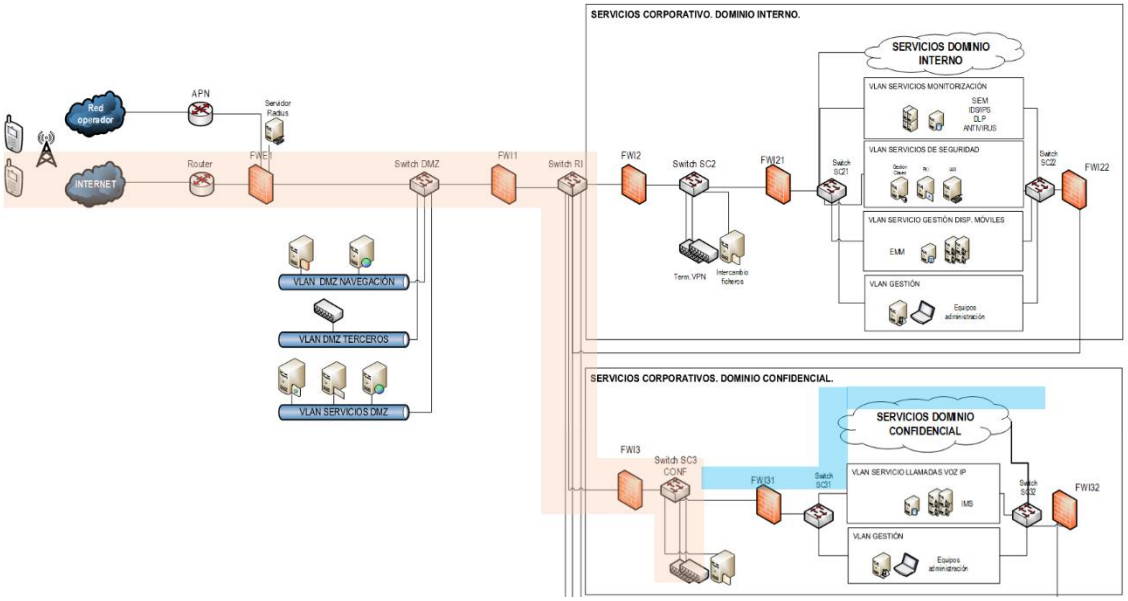

Figura 13 Flujo de información para los servicios del dominio confidencial.

De manera similar a como ocurría con los servicios de dominio interno, alcanzará el front del servicio que corresponda, devolviendo siempre el tráfico resultante al dispositivo móvil a través del terminador de túneles.

4.5 Validación de requisitos

En el Anexo II de este documento se recoge la matriz de trazabilidad que relaciona las distintas contramedidas para las amenazas presentadas en el Capítulo 3 con los distintos elementos de diseño presentados en este Capítulo 4. Esta validación de requisitos nos permite asegurar que no se han quedado amenazas relevantes sin cubrir con controles mitigantes, así como justificar aquellas contramedidas que no son necesarias en el contexto de este proyecto.

Resumiremos aquí las principales medidas de seguridad a alto nivel que se han incluido en la solución, haciendo mención a los objetivos que se citaron en el Capítulo 3 para garantizar la seguridad del sistema:

- **Confidencialidad**. Asegurar que los datos almacenados y transmitidos no pueden ser accedidos por personas no autorizadas.
    - Se han previsto dos capas de cifrado sobre las comunicaciones: un túnel VPN que asegura el cifrado de los datos en tránsito y la identificación del usuario y del dispositivo y el cifrado a nivel de aplicación de voz IP (SIP sobre TLS y SRTP).
    - Cifrado de datos en reposo, que asegura que los datos almacenados en el dispositivo se guardan cifrados, protegiéndolos ante la pérdida, el robo o el compromiso del dispositivo.
    - Tres entornos aislados en los dispositivos (contenedores), que aseguran que los datos en reposo son aislados entre las distintas aplicaciones (y para cada tipo de información que el usuario gestiona).

    - Se menciona la necesidad de que la organización adopte procesos para destruir los componentes de forma segura.

- **Integridad**. Asegurar que las personas no autorizadas no pueden alterar la información.
    - Integración con IDS/IPS de la organización que proporcionan alertas y mecanismos de defensa ante posibles intrusiones.
    - Integración con proxy y SIEM de la organización, analizando el tráfico y proporcionando capacidad de monitorización.
    - Navegación y servicio de correo supervisado por la organización.
    - Almacenamiento de datos de auditoría, con el objetivo de poder investigar posibles incidentes.
    - Políticas de borrado remoto y respuesta a eventos (por ejemplo, intentos de login erróneos).
    - Aplicación de políticas de seguridad sobre los dispositivos y las aplicaciones a las que éstos pueden acceder con MDM.
    - Inclusión de la infraestructura en los ciclos de detección y gestión de vulnerabilidades.
    - Actualizaciones de seguridad para los terminales, y firmas de virus actualizadas para toda la infraestructura.
    - Uso de cortafuegos y VLANs para segregar el tráfico de la red en función de la información que ésta gestiona dentro de la organización.

- **Disponibilidad**. Asegurar que los usuarios pueden acceder a los recursos puestos a su disposición cuando sea necesario.
    - Mecanismos de protección frente a posibles ataques de denegación de servicio contra la infraestructura de la organización.
    - Inclusión de la infraestructura en los ciclos de detección y gestión de vulnerabilidades.
    - Aplican también las medidas indicadas para el apartado “Integridad”.

- **Autenticación**. Garantizar que un usuario o dispositivo es realmente quien dice ser.
    - Forzar la autenticación del usuario en el dispositivo con, al menos: código PIN numérico para acceso al dispositivo y contraseña de acceso al contenedor de aplicaciones profesionales.
    - Autenticación del usuario en los servicios de la organización, haciendo uso de los servicios SSO de los que la organización ya dispone. Mecanismo fuerte de autenticación: contraseña y certificados instalados en dispositivo (al menos uno para autenticarse en los servicios corporativos, y otro para cada túnel VPN).

- **Autorización**. Asegurar que un usuario o dispositivo tiene acceso únicamente a los recursos a los que la organización le ha permitido acceder.
    - Servicios de autorización granulares y principio del mínimo privilegio.

    - Integración con servicios corporativos de PKI, IAM y gestión de claves, con el fin de asegurar que se cumplen las políticas corporativas relativas a cuentas, contraseñas, ciclo de vida de certificados y gestión de perfilado.

- **Trazabilidad**. Garantizar que se puede relacionar cualquier acción llevada a cabo por un usuario o dispositivo sobre un recurso, y el momento en el que ésta tuvo lugar.
    - Almacenamiento de datos de auditoría, con el objetivo de poder investigar posibles incidentes.
    - Revisión de los registros de auditoría con la frecuencia indicada en las políticas de seguridad.
    - Definición de políticas de retención para los datos de auditoría.

- **No repudio**. Garantizar que las partes involucradas en un intercambio de información no puedan negar ilegítimamente que un determinado evento o acción haya tenido lugar.
    - Mecanismos de autenticación fuertes, combinando el uso de contraseñas con certificados digitales que garantizan la identidad de los empleados.

5. Conclusiones y trabajo futuro

5.1 Conclusiones

En este trabajo se ha abordado la problemática de cómo diseñar un Sistema de Comunicaciones móviles seguras, garantizando la confidencialidad, integridad, disponibilidad, autenticación, autorización, trazabilidad y no repudio tanto en las comunicaciones corporativas como en el acceso y el tratamiento de la información relativa a los recursos corporativos de una gran organización.

Si bien es cierto que hoy en día se trata de una problemática que ya está resuelta con multitud de tecnologías y soluciones existentes en el mercado, se ha pretendido dar un enfoque algo distinto y proponer un modelo flexible que pueda ser implementado en su totalidad o de manera parcial por una organización en función de sus necesidades y considerando los siguientes aspectos:

- **No sólo se aborda el acceso y el tratamiento de la información corporativa**, sino que **se integran también las comunicaciones por voz y mensajería instantánea** entre los usuarios de la organización para proponer así un modelo de comunicaciones móviles seguras corporativas que contemple la información corporativa como un todo (incluidas las comunicaciones).
- **Se dota al modelo de la posibilidad de que la organización pueda gestionar taxonomías de referencia para clasificar la información**. Si bien esto es muy frecuente en organismos gubernamentales, donde se trabaja con información clasificada, cada vez son más las organizaciones que clasifican su información y disponen de medidas de seguridad diferentes en función de la criticidad de ésta.
- **No sólo se han tenido en cuenta los aspectos puramente técnicos de los sistemas a implementar**, sino que se han propuesto las funciones o los procesos que la organización debe integrar en los que ya dispone para poder disponer de este servicio.

Para la elaboración del modelo, se ha partido de una revisión del estado del arte de las soluciones existentes tanto de gestión de movilidad empresarial como de comunicaciones móviles seguras, así como de diferentes artículos, documentos y guías de buenas prácticas que abordan esta problemática desde distintos puntos de vista (Anexo I).

Adicionalmente y por contextualizar dicho modelo en una organización en concreto, se ha presentado el análisis de la situación actual de la organización, los requisitos y una breve definición de proyecto y el diagrama de red con la arquitectura actual a alto nivel de la organización.

Por último, el proyecto recoge una descripción a alto nivel de los servicios que incluirá el diseño, las funciones que deben tenerse en consideración y los bloques funcionales con sus funciones y requisitos.

5.2 Desarrollo del TFM

En líneas generales, podemos decir que se ha cumplido la planificación definida inicialmente en el Apartado *1.4 Planificación del Trabajo*. Como principal dificultad a la hora de llevar a cabo el proyecto podríamos destacar la gran cantidad de información generalista existente al respecto y la poca información de aplicaciones reales a organizaciones.

Esto motivó también un cambio con respecto a la planificación que inicialmente se definió. En un primer momento se pensó en dividir el diseño en dos partes: una primera de definición de un modelo de referencia alto nivel, y una segunda en la que se detallase la arquitectura de una organización para aplicar ese modelo. Sin embargo, durante la redacción del proyecto se entendió que tenía más sentido partir de un análisis de la situación actual de la organización, para definir el proyecto a implementar y pasar al diseño técnico del mismo, integrando directamente el modelo de referencia en el propio diseño, simplificando así la exposición.

Otra de las dificultades es quizás el nivel de detalle al que presentar la información: la intención de este documento es presentar un modelo y ver una posible aplicación a una organización grande, pero está claro que se podría dar mucho más nivel de detalle a nivel de diseño. Se ha intentado hacer mención a las principales funciones que la organización ha de implementar y ver la aplicación con un diagrama de red más o menos real. Sin embargo, todavía quedan muchos aspectos que deben ser definidos en un diseño real: equipos a utilizar, definición de rangos de IPs, VLANs, espacios, racks necesarios, conexión de equipos, requisitos de alimentación, integraciones con red corporativa, etc. En este trabajo no se ha dado relevancia estos aspectos, ya que se consideran que vendrían en una fase posterior al modelado que aquí se está intentando presentar.

5.3 Trabajo futuro

Este trabajo presenta, como hemos indicado, lo que podría considerarse como un modelo de diseño inicial de un Sistema de Comunicaciones Móviles seguras en un entorno corporativo. Para facilitar la comprensión, se ha contextualizado en una organización grande, pero se han omitido muchos detalles de la organización con el objetivo de presentar más un modelo flexible adaptable a distintas organizaciones, que un modelo para una organización específica.

En próximos trabajos se podría relatar la experiencia de cómo implementar este modelo en una organización real, exponiendo los distintos pasos llevados a cabo y las conclusiones y lecciones aprendidas en el proceso. No obstante, se trata de un proceso en el que entran en juego múltiples aspectos, por lo que se podría considerar centrase en algún tema en concreto del proceso si la organización es muy grande:

- Procesos de RFIs o RFPs para buscar una solución de mercado acorde con las necesidades de la organización.
- Adaptar las soluciones escogidas a la arquitectura de red ya existente en la organización.

- Llevar a cabo un levantamiento de la situación actual, el objetivo final con la solución o soluciones elegidas y el faseado para llevar a cabo la implementación del proyecto.
- La modificación de las políticas de la organización, y la creación o modificación de procesos y procedimientos organizativos para contemplar las nuevas funciones asociadas a los servicios que la organización quiere prestar a sus empleados.
- Los protocolos de pruebas para verificar el correcto funcionamiento del sistema antes de su puesta en producción.
- El ciclo de vida de todo el material criptográfico.
- La gestión de los terminales y los procesos de distribución a los empleados.

Anexo I. Guías de buenas prácticas en seguridad móvil empresarial

[1] **NIST SP 1800-4 Practice Guide: Mobile Device Security**. (*NIST, NCCoE*). El documento propone un diseño de referencia sobre cómo proteger el acceso a los recursos corporativos. Las soluciones de ejemplo presentadas pueden ser utilizadas por cualquier organización que implemente una solución EMM on premise o en la nube.

[2] **NIST SP 800124r1: Guidelines for Managing the Security of Mobile Devices in the Enterprise**. (*NIST*). Esta publicación ayuda a las organizaciones entender los problemas de seguridad de los dispositivos móviles y a gestionar su seguridad. Proporciona recomendaciones para seleccionar, implementar, y utilizar soluciones de gestión centralizada, además de proteger los dispositivos en todo su ciclo de vida.

[3] **Commercial Solutions for Classified Mobile Access Capability Package**. (*NSA*). Describe un marco de referencia a nivel de sistemas para implementar soluciones móviles con datos en tránsito, utilizando productos comerciales en las distintas capas para proteger la información clasificada.

[4] **Guía de Seguridad de las TIC CCN-STIC 407: Seguridad en telefonía móvil**. (*CCN*). Recomendaciones de seguridad para sistemas de telefonía móvil basados en los estándares GSM, GPRS y UMTS.

[5] **Guía de Seguridad de las TIC CCN-STIC 450: Seguridad en dispositivos móviles.** (*CCN*). Proporciona información necesaria para la evaluación y el análisis de riesgos, amenazas y vulnerabilidades de seguridad a la que están expuestos los dispositivos móviles en la actualidad.

[6] **Guía de Seguridad de las TIC CCN STIC 457: Gestión de dispositivos móviles MDM (Mobile Device Management)**. (*CCN*). Establece una lista de características, capacidades y recomendaciones de seguridad para permitir la adecuada gestión de los dispositivos móviles en entornos empresariales a través de las soluciones MDM.

[7] **Guía de Seguridad de las TIC CCN-STIC 496: Sistemas de Comunicaciones Móviles Seguras.** (*CCN*). Establece un conjunto de directrices para el diseño de sistemas de comunicaciones móviles corporativos, así como para la revisión y adaptación de despliegues ya existentes. El objetivo en ambos casos es dotar a dichos sistemas de mayor seguridad, tanto para las comunicaciones establecidas con los dispositivos como para la información almacenada en los mismos.

[8] **Guía Esquema Nacional de Seguridad 827: Gestión y uso de dispositivos móviles.** (*CCN*). Guía que establece unas pautas de carácter general que puedan resultar de aplicación a entidades de distinta

naturaleza. Analiza la problemática derivada del uso de los dispositivos móviles y propone un modelo de gestión y uso para el cumplimiento del Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.

Guías para el desarrollo de programa de movilidad en una organización

[1] **Mobile Computing Decision Framework (MCDF)**. (*MTTT*). El documento proporciona un marco para la toma de decisiones de forma holística en cuanto a la decisión de la solución móvil a utilizar para dar soporte a la actividad de la organización.

[2] **Federal Mobile Computing Security Baseline**. (*DHS, DoD, NIST*). Casos de uso y algunos de los controles a aplicar para la gestión de los dispositivos móviles, las aplicaciones y la gestión de identidades.

[3] **Mobile Security Reference Architecture**. (*DHS, DoD*). Arquitectura flexible que permite adaptarse a las necesidades de la organización.

[4] **NISTIR 8144: Assessing Threats to Mobile Devices & Infrastructure**.

[5] **Draft NIST Catálogo de amenazas en dispositivos móviles y en la infraestructura asociada**. Soporte al desarrollo y la implementación de las capacidades de seguridad empresariales.

Guías relacionadas con las aplicaciones móviles

[1] **NIST SP 800-163. (NIST)**. Documento que establece el proceso para la aprobación de aplicaciones en una organización. Comprende dos actividades: por un lado la prueba de las aplicaciones para detectar posibles vulnerabilidades. Por el otro, las actividades relativas a la aprobación de las aplicaciones en base a análisis de riesgos y cumplimientos de la política corporativa.

[2] **Open Web Application Security Project (OWASP) – Mobile Security Project**. (*OWASP*). Proyecto que ofrece una serie de recursos para desarrolladores y equipos de seguridad para desarrollar y mantener las aplicaciones móviles seguras. El proyecto tiene como objetivo clasificar los riesgos de seguridad de los dispositivos móviles para reducir el impacto o la probabilidad de explotarlos.

[3] **Cloud Security Alliance (CSA) Mobile Application Security Testing Initiative**. (*Cloud Security Alliance*). Esta iniciativa busca crear un ecosistema más seguro en la nube, focalizado fundamentalmente en la seguridad de los dispositivos de usuario y aplicaciones móviles.

Seguridad en sistemas operativos móviles

[1] **Guía CCN - STIC 453D**. (CCN). Seguridad en dispositivos móviles Android 6.x.

[2] **Guía CCN - STIC 453E**. (CCN). Seguridad en dispositivos móviles Android 7.x.
[3] **Guía CCN - STIC 453F**. (CCN). Seguridad en dispositivos móviles Android 8.x.
[4] **Guía CCN - STIC 453G**. (CCN). Seguridad en dispositivos móviles Android 9.x.
[5] **Guía CCN - STIC 455C**. (CCN). Seguridad en dispositivos móviles: iPhone (iOS 12.x).
[6] **Guía CCN - STIC 455D**. (CCN). Seguridad en dispositivos móviles: iPhone (iOS 12.x).

Catálogo de seguridad en productos

[1] **Guía CCN – STIC 105**. (CCN). Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación recomendados.

Anexo II. Matriz de trazabilidad para la validación de requisitos.

CATEGORÍA	CONTRAMEDIDAS (CAPÍTULO 3)		DISEÑO (CAPÍTULO 4)
	CÓDIGO	BREVE DESCRIPCIÓN	MAPEO DISEÑO
Acceso físico al dispositivo y evasión de mecanismos de autenticación	C.AF.1.	Gestión centralizada dispositivos	4.4.2 Funciones de seguridad: Gestión de los dispositivos y configuración de la infraestructura 4.4.3 Bloques funcionales. Componentes de infraestructura.
	C.AF.2.	Concienciación de usuarios	4.4.2 Funciones de seguridad: Formación
	C.AF.3.	Evitar la conexión de los dispositivos a ordenadores	4.4.3 Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-23.
	C.AF.4.	Requerir la autenticación del usuario en cualquier acceso a datos de la organización	4.4.3 Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-1.
	C.AF.5.	Mecanismos de detección de acciones sospechosas	4.4.3 Bloques funcionales. Componentes de infraestructura. Requisito CI-13.
	C.AF.6.	Mecanismos fuertes de autenticación (multifactor)	4.4.3 Bloques funcionales. Dispositivo móvil de usuario: Autenticación del usuario en el dispositivo. Autenticación del usuario en los servicios de la organización. Requisitos DM-1, DM-4, DM-14. 4.4.3 Bloques funcionales. Redes de comunicaciones. Protección de las comunicaciones. Requisito PC-2.
	C.AF.7.	Gestión centralizada de usuarios y credenciales	4.4.2 Funciones de seguridad. Gestión de identidades y accesos. 4.4.3 Bloques funcionales. Componentes de infraestructura. Requisito CI-28.
	C.AF.8.	Requisitos de contraseñas en políticas de la organización	4.4.3 Bloques funcionales. Dispositivo móvil de usuario. Aplicación de políticas de seguridad de la organización. Requisitos: DM-15, DM-16. 4.4.3 Bloques funcionales. Componentes de infraestructura. Requisitos CI-3, CI-28.

	C.AF.9.	Principio del mínimo privilegio	4.4.2 Funciones de seguridad. Gestión de identidades y accesos. 4.4.3 Bloques funcionales. Dispositivos móviles de usuario. Requisito DM-24. 4.4.3 Bloques funcionales. Componentes de infraestructura. Requisito CI-28.
	C.AF.10.	Mecanismos de autenticación que garanticen el uso de OTPs o tokens generados desde ubicaciones no confiables	4.4.3 Bloques funcionales. Dispositivo móvil de usuario: Autenticación del usuario en el dispositivo. Autenticación del usuario en los servicios de la organización. Requisitos DM-1, DM-4, DM-14. 4.4.3 Bloques funcionales. Redes de comunicaciones. Protección de las comunicaciones. Requisito PC-2.
	C.AF.11.	Actualizaciones de seguridad	4.4.2. Funciones de seguridad. Gestión de los dispositivos y configuración de la infraestructura.
	C.AF.12.	Mecanismos de protección frente a ataques de fuerza bruta.	4.4.2. Funciones de seguridad. Comunicaciones seguras. 4.4.3. Bloques funcionales. Componentes de infraestructura. Requisito CI-29.
Componentes de bajo nivel	C.CB.1.	Instalación de parches de seguridad	4.4.2. Funciones de seguridad. Gestión de los dispositivos y configuración de la infraestructura.
	C.CB.2.	Retirar los dispositivos que no soportan actualizaciones	4.4.2. Funciones de seguridad. Monitorización continua y procesos de auditoría. 4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-13.
	C.CB.3.	Capacidades de comprobación de la integridad en los dispositivos	4.4.2. Funciones de seguridad. Protección de los datos. Monitorización continua y proceso de auditoría. 4.4.3. Bloques funcionales. Almacenamiento de información y uso de aplicaciones. Recopilación de eventos para su análisis por parte de la organización.
	C.CB.4.	Asegurar que los dispositivos reúnan los criterios de seguridad definidos por la organización	4.4.2. Funciones de seguridad. Monitorización continua y procesos de auditoría. 4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-11.

Sistema operativo	C.SO.1.	Monitorizar el estado del parcheado de los dispositivos, y bloquear la conectividad de los dispositivos con vulnerabilidades conocidas.	4.4.2. Funciones de seguridad. Monitorización continua y procesos de auditoría. 4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-13.
	C.SO.2.	Adquirir dispositivos de operadores y fabricantes que se hayan comprometido a proporcionar las actualizaciones del sistema operativo en un tiempo razonable.	Se considera parte del diseño y de la elección de la solución.
	C.SO.3.	Retirar los dispositivos que no soportan actualizaciones de seguridad.	4.4.2. Funciones de seguridad. Monitorización continua y procesos de auditoría. 4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-13.
	C.SO.4.	Bloquear la conectividad desde los dispositivos comprometidos	.4.2. Funciones de seguridad. Monitorización continua y procesos de auditoría. 4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-13.
	C.SO.5.	Detección de root / jailbreak	.4.2. Funciones de seguridad. Monitorización continua y procesos de auditoría. 4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-13
	C.SO.6.	Concienciación de usuarios en relación con root / jailbreak	4.4.2 Funciones de seguridad: Formación
	C.SO.7.	Restringir las apps de markets no oficiales	4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Almacenamiento de información y uso de aplicaciones. Requisitos DM-9, DM-10, DM-24.
	C.SO.8.	Actualizar los dispositivos de forma regular	4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-25.
	C.SO.9.	Deshabilitar modo debug USB	4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-26.

	C.SO.10.	Concienciación uso de mecanismos de autenticación fuerte en cuentas de terceros / cuentas en la nube gestionadas por la organización.	4.4.2 Funciones de seguridad: Formación
Aplicaciones móviles	C.AP.1.	Detección de vulnerabilidades en aplicaciones / servicios de hacking ético	4.4.2 Funciones de seguridad: Gestión de la información.
	C.AP.2.	Cifrado de datos en tránsito	4.4.2. Funciones de seguridad: Protección de los datos. Comunicaciones seguras. 4.4.3. Bloques funcionales. Redes de comunicaciones.
	C.AP.3.	Monitorización de aplicaciones no soportadas por la organización	4.4.2. Funciones de seguridad. Monitorización continua y procesos de auditoría. 4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-11.
	C.AP.4.	No aprobación de aplicaciones que solicitan permisos que pueden poner en riesgo la privacidad de los usuarios	4.4.2. Funciones de seguridad: Gestión de información.
	C.AP.5.	Uso de proxy y VPN para todo el tráfico con la organización	4.4.2. Funciones de seguridad: Protección de los datos. 4.4.3. Bloques funcionales. Componentes de infraestructura. Requisito CI-30.
	C.AP.6.	Concienciación de usuarios en el uso de apps móviles	4.4.2 Funciones de seguridad: Formación
	C.AP.7.	Procesos de revisión de apps internas rigurosos	4.4.2. Funciones de seguridad: Gestión de información.
	C.AP.8.	Separación de aplicaciones personales de corporativas	4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Almacenamiento de información y uso de aplicaciones.
	C.AP.9.	Prohibir la instalación de las aplicaciones fuera de los repositorios autorizados	4.4.2. Funciones de seguridad: Gestión de información. 4.4.2. Funciones de seguridad. Monitorización continua y procesos de auditoría. 4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-11.
	C.AP.10.	Incorporar a los procesos de ciber inteligencia los riesgos de aplicaciones instaladas en dispositivos	No tenido en cuenta en el diseño.

	C.AP.11.	Eliminar aplicaciones preinstaladas	4.4.2. Funciones de seguridad. Monitorización continua y procesos de auditoría. 4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-11.
	C.AP.12.	Usar mecanismos de autenticación fuertes para acceder a datos de la organización	4.4.3 Bloques funcionales. Dispositivo móvil de usuario: Autenticación del usuario en el dispositivo. Autenticación del usuario en los servicios de la organización. Requisitos DM-1, DM-4, DM-14. 4.4.3 Bloques funcionales. Redes de comunicaciones. Protección de las comunicaciones. Requisito PC-2.
	C.AP.13.	Monitorizar los intentos de acceso de aplicaciones a recursos corporativos	4.4.2. Funciones de seguridad. Monitorización continua y procesos de auditoría. 4.4.3. Recopilación de eventos para su análisis por parte de la organización.
	C.AP.14.	Mecanismos MDM / EMM	4.4.2 Funciones de seguridad: Gestión de los dispositivos y configuración de la infraestructura 4.4.3 Bloques funcionales. Componentes de infraestructura.
	C.AP.15.	Llevar a cabo revisiones periódicas de los logs para evitar que se dejen datos sensibles	No se ha contemplado
	C.AP.16.	Hay que asegurar que se siguen las mejores prácticas de OWASP para el desarrollo seguro de apps móviles	No se ha contemplado.
	C.AP.17.	Seguir las mejores prácticas para la implementación de la criptografía en apps móviles.	No se ha contemplado
Redes móviles	C.RM.1.	Asegurar que los dispositivos utilizan un cifrado extremo a extremo en todas las comunicaciones (voz y datos).	4.4.2. Funciones de seguridad: Protección de los datos. Comunicaciones seguras. 4.4.3. Bloques funcionales. Redes de comunicaciones.
Redes locales y de área personal	C.RL.1.	Concienciar a los usuarios y prohibir el uso de redes públicas sin mecanismos de protección adicionales	4.4.2 Funciones de seguridad: Formación
	C.RL.2.	Limitar la conectividad a las redes Wi-Fi, autorizando sólo las que usen mecanismos de cifrado WPA2.	No se ha contemplado.

	C.RL.3.	Modificar los SSID de forma frecuente y con valores no relacionados entre sí.	No se ha contemplado
	C.RL.4.	Deshabilitar las interfaces cuando no se estén utilizando.	4.4.3. Bloques funcionales. Dispositivo móvil de usuario. Requisito DM-8.
Gestión de la movilidad empresarial	C.GM.1.	Asegurar que el sistema MDM/EMM valida los certificados.	4.4.3. Bloques funcionales. Autenticación del usuario en los servicios de la organización.
	C.GM.2.	Asegurar que se llevan a cabo auditorías de seguridad sobre las actividades de administración, los registros de los dispositivos, las actividades llevadas a cabo en la red, etc.	4.4.2. Funciones de seguridad: Gestión de información.
	C.GM.3.	Auditorías de seguridad sobre la actividad de los dispositivos.	4.4.2. Funciones de seguridad: Gestión de información.
	C.GM.4.	Consolidar y correlacionar toda la información de los registros de seguridad para identificar actividad sospechosa.	4.4.3 Bloques funcionales. Componentes de infraestructura. Requisito CI-13.
	C.GM.5.	Servicios de autorización granulares y principio del mínimo privilegio.	4.4.2 Funciones de seguridad. Gestión de identidades y accesos. 4.4.3 Bloques funcionales. Dispositivos móviles de usuario. Requisito DM-24. 4.4.3 Bloques funcionales. Componentes de infraestructura. Requisito CI-28.
	C.GM.6.	Mecanismos de autenticación fuertes.	4.4.3 Bloques funcionales. Dispositivo móvil de usuario: Autenticación del usuario en el dispositivo. Autenticación del usuario en los servicios de la organización. Requisitos DM-1, DM-4, DM-14. 4.4.3 Bloques funcionales. Redes de comunicaciones. Protección de las comunicaciones. Requisito PC-2.
	C.GM.7.	Soportar la integración con mecanismos de autenticación con la infraestructura corporativa.	4.4.2 Funciones de seguridad. Gestión de identidades y accesos. 4.4.3 Bloques funcionales. Componentes de infraestructura. Requisito CI-28.
	C.GM.8.	Establecimiento de canales seguro de comunicación entre todos los componentes.	4.4.2. Funciones de seguridad. Comunicaciones seguras. 4.4.3. Bloques funcionales. Redes de comunicaciones. 4.4.3. Bloques funcionales. Componentes de infraestructura.

Bibliografía

[1] Centro Criptológico Nacional. (s.f.). *Catálogo de Productos de Seguridad de las Tecnologías de la Información*. Obtenido de Guía de Seguridad de las TIC CCN-STIC 105: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html

[2] *Department of Homeland Security, Mobile Security Reference Architecture.* (23 de 05 de 2013). Obtenido de https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/Mobile-Security-Reference-Architecture.pdf

[3] *INCIBE, Dispositivos móviles personales para uso profesional (BYOD). Una guía de aproximación para el empresario.* (s.f.). Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

[4] NIST. (s.f.). Obtenido de Guidelines for Managing the Security of Mobile Devices in the Enterprise: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

[5] NIST. (Septiembre de 2016). *Assessing Threats to Mobile Devices & Infrastructure*. Obtenido de https://csrc.nist.gov/CSRC/media/Publications/nistir/8144/draft/documents/nistir8144_draft.pdf

[6] NIST. (s.f.). *Guidelines for Managing the Security of Mobile Devices in the Enterprise.* Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

[7] NIST. (s.f.). *Mobile Threat Catalogue*. Obtenido de https://pages.nist.gov/mobile-threat-catalogue/

[8] *NISTIR 8144, Assessing Threats to Mobile Devices & Infrastructure: the Mobile Threat Catalogue*. (Septiembre de 2016). Obtenido de https://csrc.nist.gov/csrc/media/publications/nistir/8144/draft/documents/nistir8144_draft.pdf

[9] *Study on Mobile Device Security*. (2017). Obtenido de https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf