Sistema de Comunicaciones Móviles Seguras en un entorno empresarial

Daniel Brande Hernández

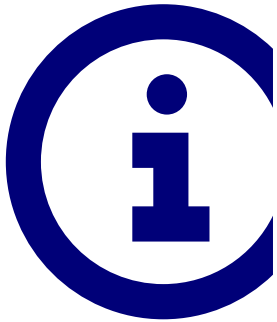
Diciembre de 2019

Tutor: Amadeu Albós Raya

Profesor: Víctor García Font

Universitat Oberta
de Catalunya

Índice



01

¿En qué consiste el trabajo?

Objetivos, enfoque y planificación

Objetivos

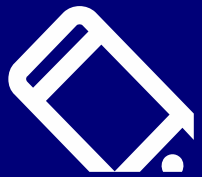
« Proponer un **modelo** o **arquitectura de referencia** para la implementación de un Sistema de Comunicaciones Móviles Seguras corporativo. »

GESTIÓN DE LA MOVILIDAD EMPRESARIAL

Protección y gestión de los dispositivos e información

COMUNICACIONES SEGURAS

Voz y envío de mensajes



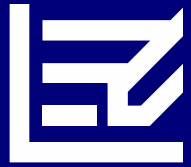
Enfoque y faseado

01 PLANIFICACIÓN

02 BÚSQUEDA DE INFORMACIÓN

03 ANÁLISIS DE RIESGOS

04 DISEÑO



05 VALIDACIÓN DE REQUISITOS

06 PRESENTACIÓN DE RESULTADOS

Enfoque y faseado

01 PLANIFICACIÓN

02 BÚSQUEDA DE INFORMACIÓN

03 ANÁLISIS DE RIESGOS

04 DISEÑO

05 VALIDACIÓN DE REQUISITOS

06 PRESENTACIÓN DE RESULTADOS

					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																

02

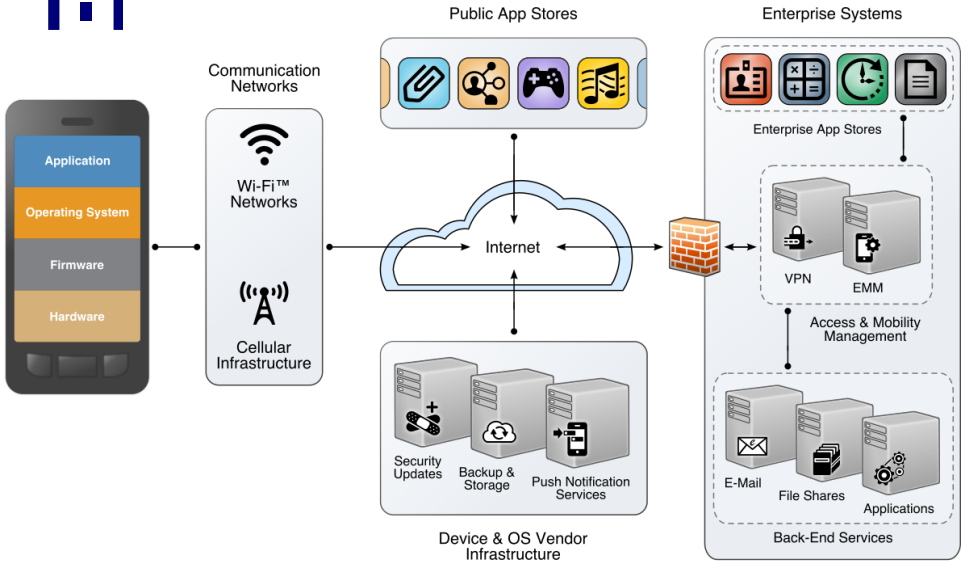
Sistemas de Comunicaciones Móviles Seguras

Descripción del sistema y soluciones existentes

Descripción del “ecosistema”

1. El **dispositivo móvil**
2. Las distintas **redes** que utiliza el dispositivo.
3. Los **servicios y la infraestructura** proporcionados por los **fabricantes**.
4. Los **servicios proporcionados por terceros**.
5. Los **servicios y la propia infraestructura de la organización**.

Elementos del “ecosistema”



Fuente: *Study on Mobile Device Security, 2017, Departamento Seguridad Nacional Estados Unidos.*

GESTIÓN DE LA MOVILIDAD EMPRESARIAL

Protección y gestión de los dispositivos e información

COMUNICACIONES SEGURAS

Voz y envío de mensajes

Evaluar las necesidades de la organización

«Cada organización debe determinar qué **servicios de seguridad necesita** y después diseñar y adquirir una o más soluciones»

Políticas de seguridad

Interfaces del dispositivo

Servicios nativos del sistema operativo

Interfaces inalámbricas

Incumplimientos de políticas

Gestión de las aplicaciones

Distribución de aplicaciones

Restricción en el uso de aplicaciones

Restricción de los permisos de las aplicaciones

Comunicaciones y almacenamiento

Datos en tránsito y en reposo

Comunicaciones por voz y mensajería

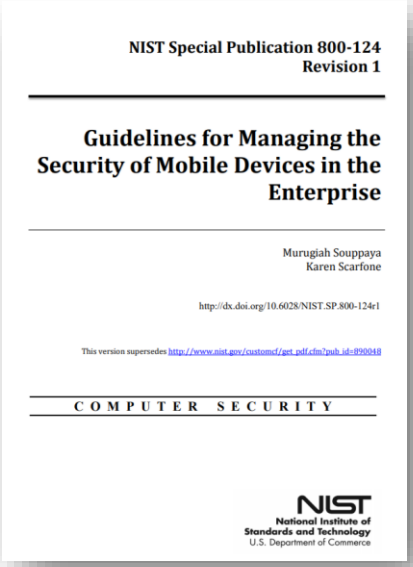
Políticas de borrado remoto

Borrado de dispositivos

Autenticación del usuario y del dispositivo

Mecanismos de autenticación

Bloqueos automáticos y en remoto


NIST Special Publication 800-124
Revision 1

Guidelines for Managing the Security of Mobile Devices in the Enterprise

Murugiah Souppaya
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-124r1

This version supersedes http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890048

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

GESTIÓN DE LA MOVILIDAD EMPRESARIAL

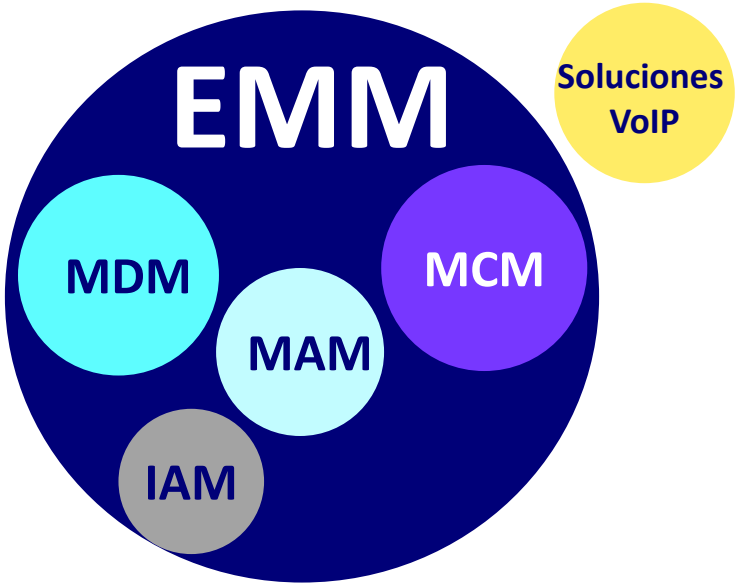
Protección y gestión de los dispositivos e información

COMUNICACIONES SEGURAS

Voz y envío de mensajes

Tecnologías existentes

Las soluciones EMM (Enterprise Mobility Management) combinan la gestión de dispositivos (MDM) con gestión de aplicaciones móviles (MAM), gestión de contenido móvil (MCM) y gestión de identidades y accesos (IAM).



Políticas de seguridad

- Interfaces del dispositivo
- Servicios nativos del sistema operativo
- Interfaces inalámbricas
- Incumplimientos de políticas

Gestión de las aplicaciones

- Distribución de aplicaciones
- Restricción en el uso de aplicaciones
- Restricción de los permisos de las aplicaciones

Comunicaciones y almacenamiento

- Datos en tránsito y en reposo
- Comunicaciones por voz y mensajería
- Políticas de borrado remoto
- Borrado de dispositivos

Autenticación del usuario y del dispositivo

- Mecanismos de autenticación
- Bloqueos automáticos y en remoto

GESTIÓN DE LA MOVILIDAD EMPRESARIAL

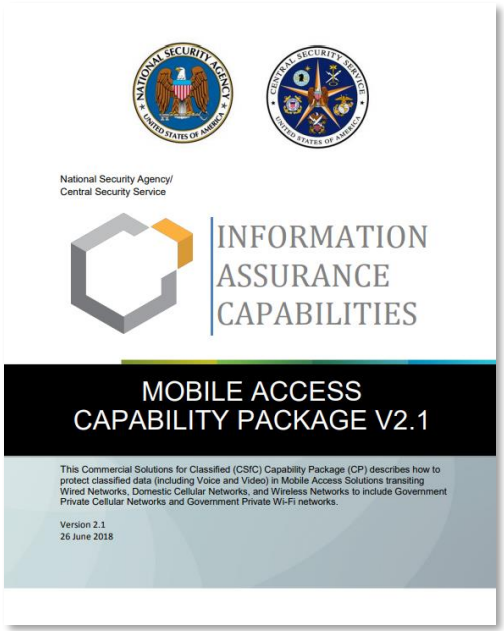
Protección y gestión de los dispositivos e información

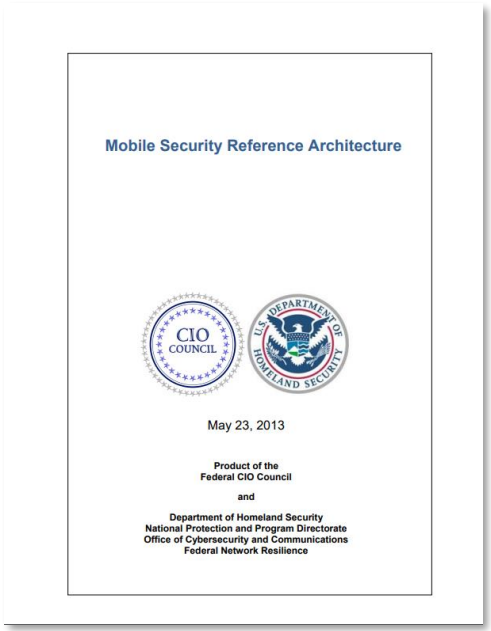
COMUNICACIONES SEGURAS

Voz y envío de mensajes

¿En qué nos apoyamos?

«Lo más difícil es analizar las necesidades de la organización. Para el resto, **existe documentación**.» (*Anexo I de la memoria*)





03

¿A qué amenazas nos enfrentamos?

Principales amenazas y contramedidas a implementar

Principales amenazas y objetivos para implementar la seguridad

Es necesario entender qué amenazas pueden afectar a cada uno de los elementos del "ecosistema" para poder implementar la seguridad.

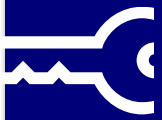
AMENAZAS GENERALES

- Denegación de servicio
- Seguimiento del usuario
- Robo de información
- Suplantación
- Modificación de datos
- Control remoto del dispositivo
- Acceso a comunicaciones del usuario

OBJETIVOS

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación
- Autorización
- Trazabilidad
- No repudio

AMENAZAS POR SUPERFICIE DE ATAQUE



CONTRAMEDIDAS

Amenazas por superficie de ataque

Acceso físico al dispositivo / Evasión mecanismos de autenticación

Aplicaciones

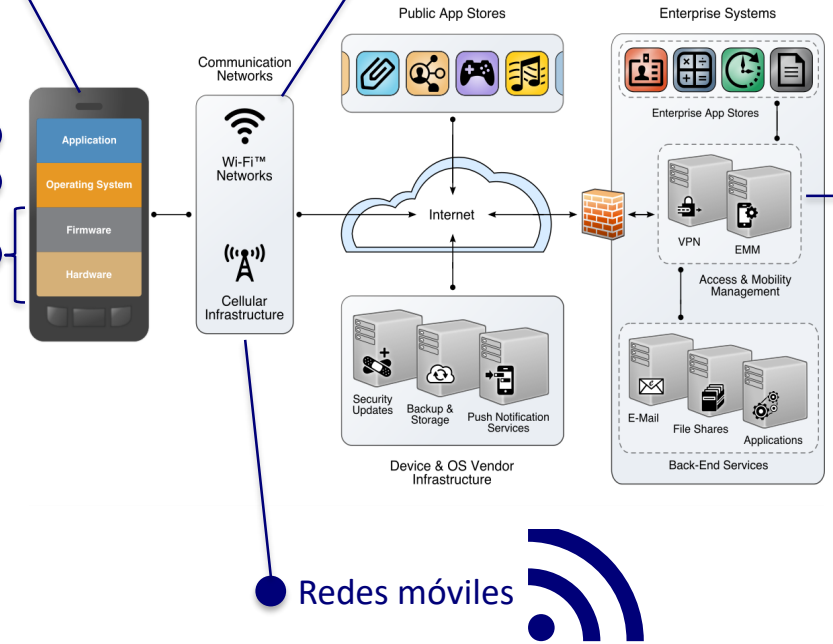
Sistema Operativo

Componentes de bajo nivel

Redes locales y de área personal

Redes móviles

Sistema de gestión de la movilidad



04

¿Qué solución proponemos?

Modelo de Referencia y Solución Técnica

¿Por dónde empezamos?

Por el principio: evaluemos cuál es la situación actual, y definamos los objetivos y los requisitos del proyecto que la organización va a implementar.

ANÁLISIS DE SITUACIÓN ACTUAL

Gran entidad bancaria.

Móviles no gestionados de forma centralizada

Migración a nueva arquitectura. Nuevo operador de telefonia.

DEFINICIÓN OBJETIVOS

DEFINICIÓN REQUISITOS

Arquitectura actual de la organización

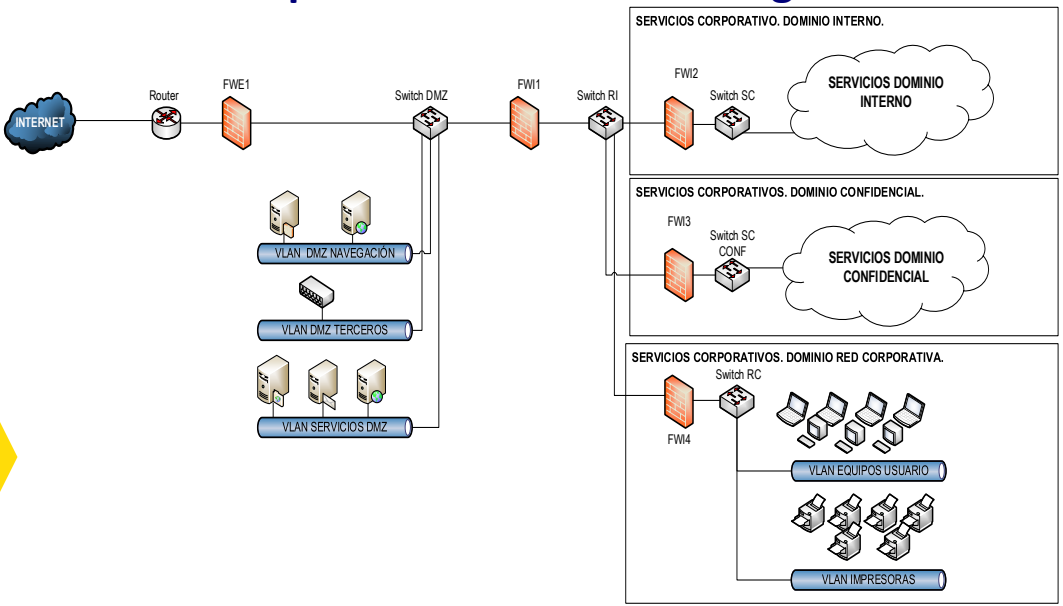
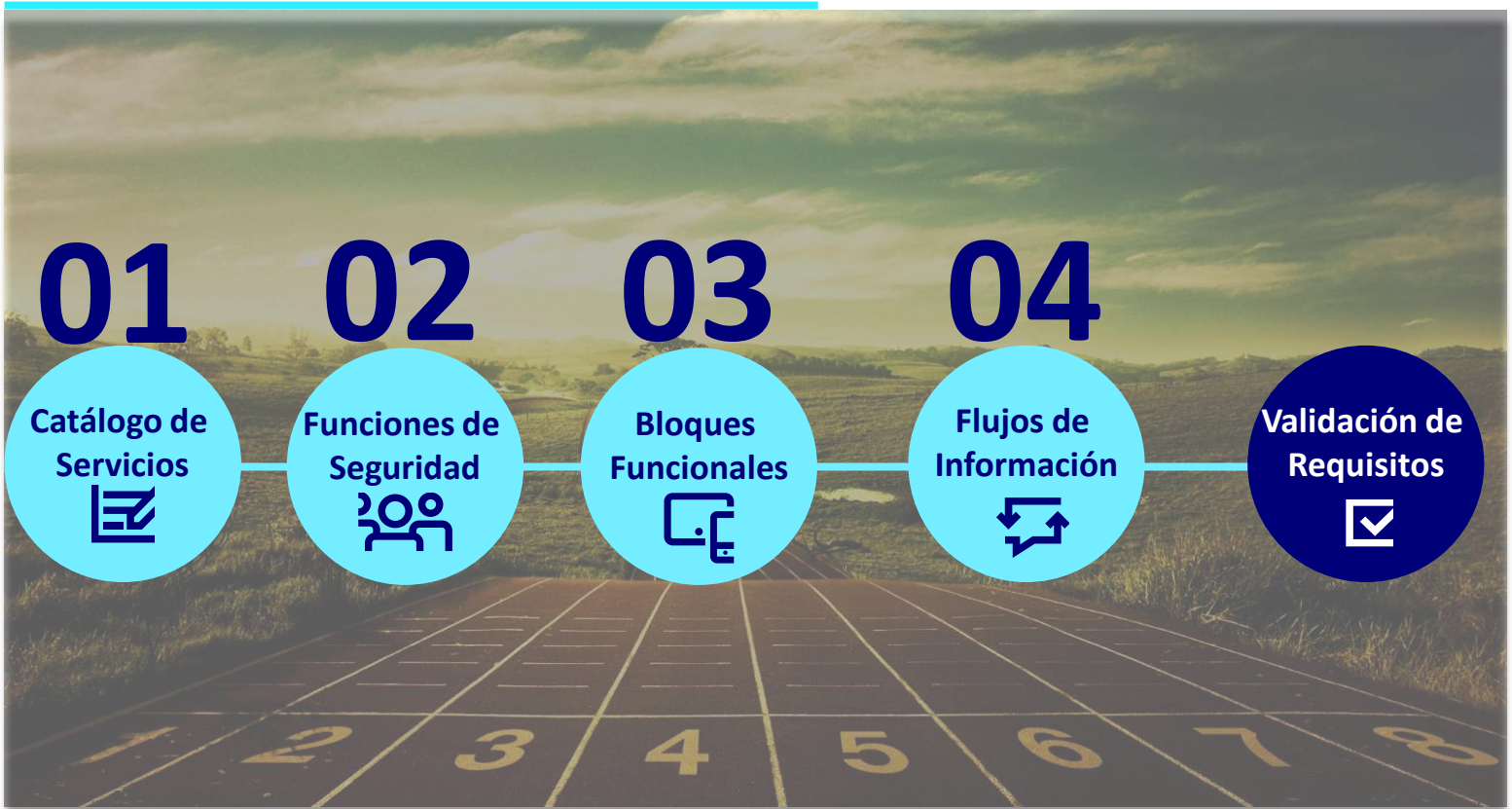
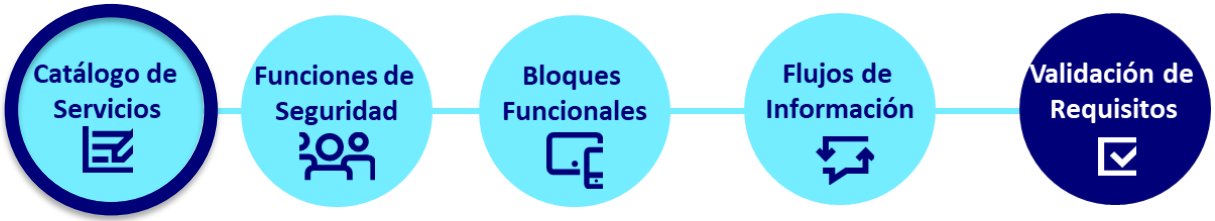


Diagrama de red a alto nivel de la organización.

Diseño técnico



Diseño técnico.
Catálogo servicios



De los objetivos y los requisitos que describe la organización, obtenemos una definición de la taxonomía de servicios que el sistema debe proporcionar a los usuarios de la organización.

SERVICIOS NO SEGUROS

- Llamada telefónica a numeración pública
- Llamada telefónica a red privada virtual de la organización
- Envío de mensajes SMS

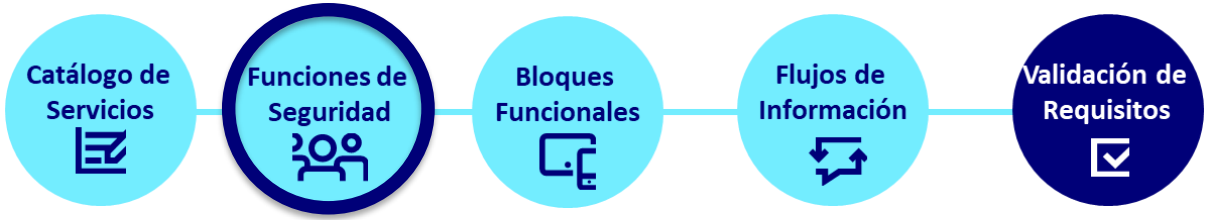
SERVICIOS "NO GESTIONADOS" POR LA ORGANIZACIÓN

SERVICIOS SEGUROS

- Llamadas cifradas
- Mensajería instantánea
- Navegación corporativa
- Correo corporativo
- Acceso a los servicios de la organización
- Repositorio corporativo de apps

SEGURIDAD "GESTIONADA" POR LA ORGANIZACIÓN

Diseño técnico. Funciones

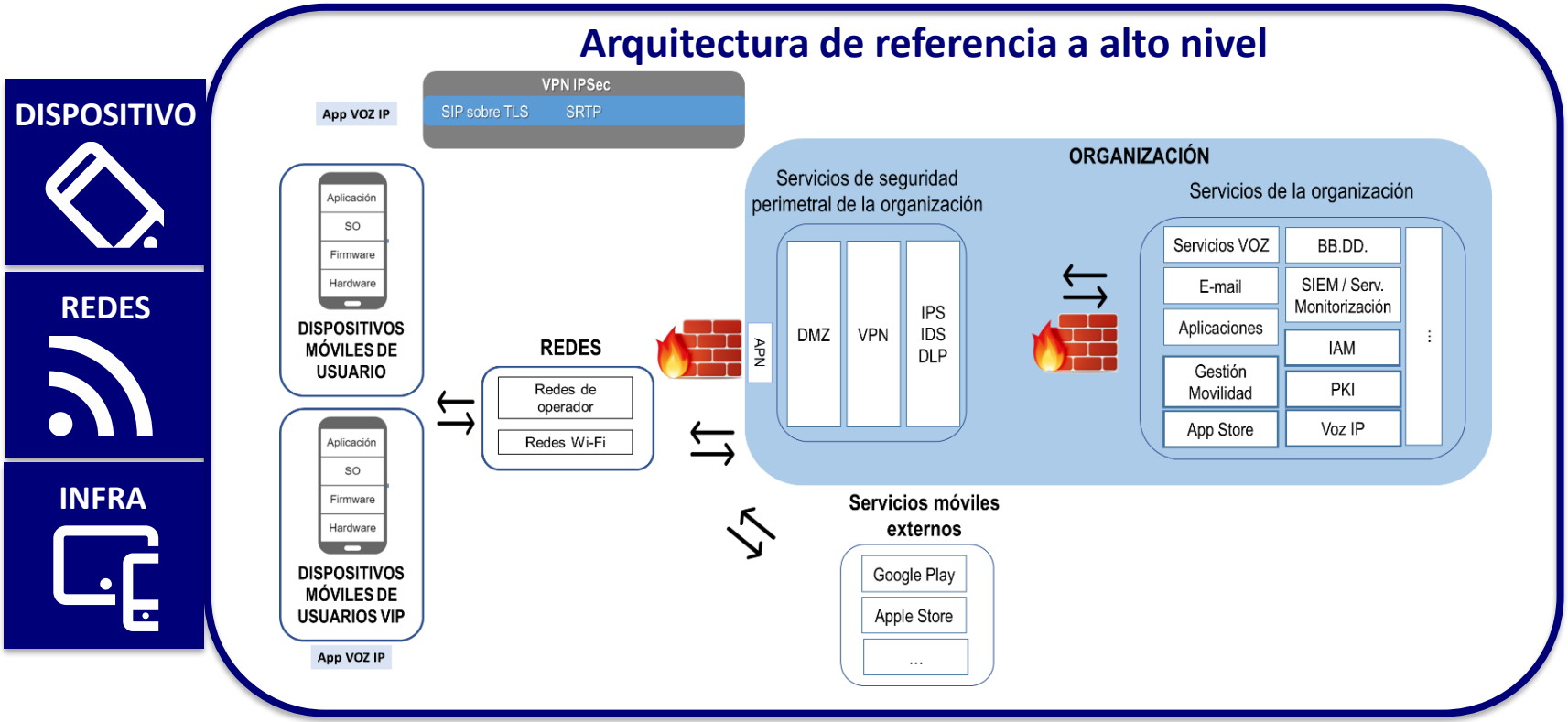


Las funciones representan las necesidades de la organización desde el punto de vista de procesos, prácticas y tecnología que necesitará implementar para proporcionar los servicios especificados.

Diseño técnico.
Bloques funcionales

Catálogo de Servicios → Funciones de Seguridad → **Bloques Funcionales** → Flujos de Información → Validación de Requisitos

Arquitectura de referencia a alto nivel



Diseño técnico.
Bloques funcionales

Catálogo de Servicios → Funciones de Seguridad → **Bloques Funcionales** → Flujos de Información → Validación de Requisitos

DISPOSITIVO

REDES

INFRA

DISPOSITIVO

- Almacenamiento de información
- Autenticación del usuario en dispositivo
- Autenticación del usuario en servicios
- Aplicación de políticas de seguridad
- Recopilación de eventos
- Respuesta a incidentes

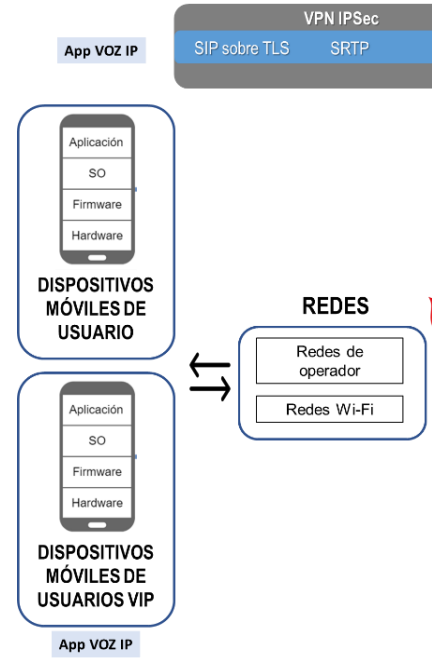
Diseño técnico.
Bloques funcionales

Catálogo de Servicios → Funciones de Seguridad → **Bloques Funcionales** → Flujos de Información → Validación de Requisitos

DISPOSITIVO

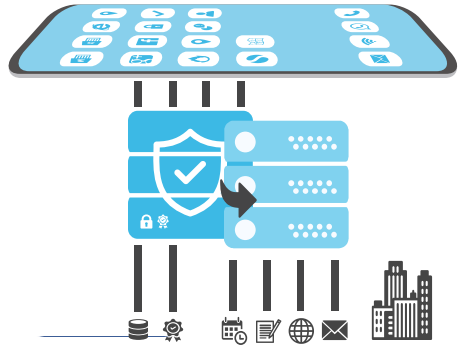
REDES

INFRA



REDES

- Conexión con la red del operador
- Protección de las comunicaciones
- Comunicaciones a través de Voz IP



Catálogo de Servicios

Funciones de Seguridad

Bloques Funcionales

Flujos de Información

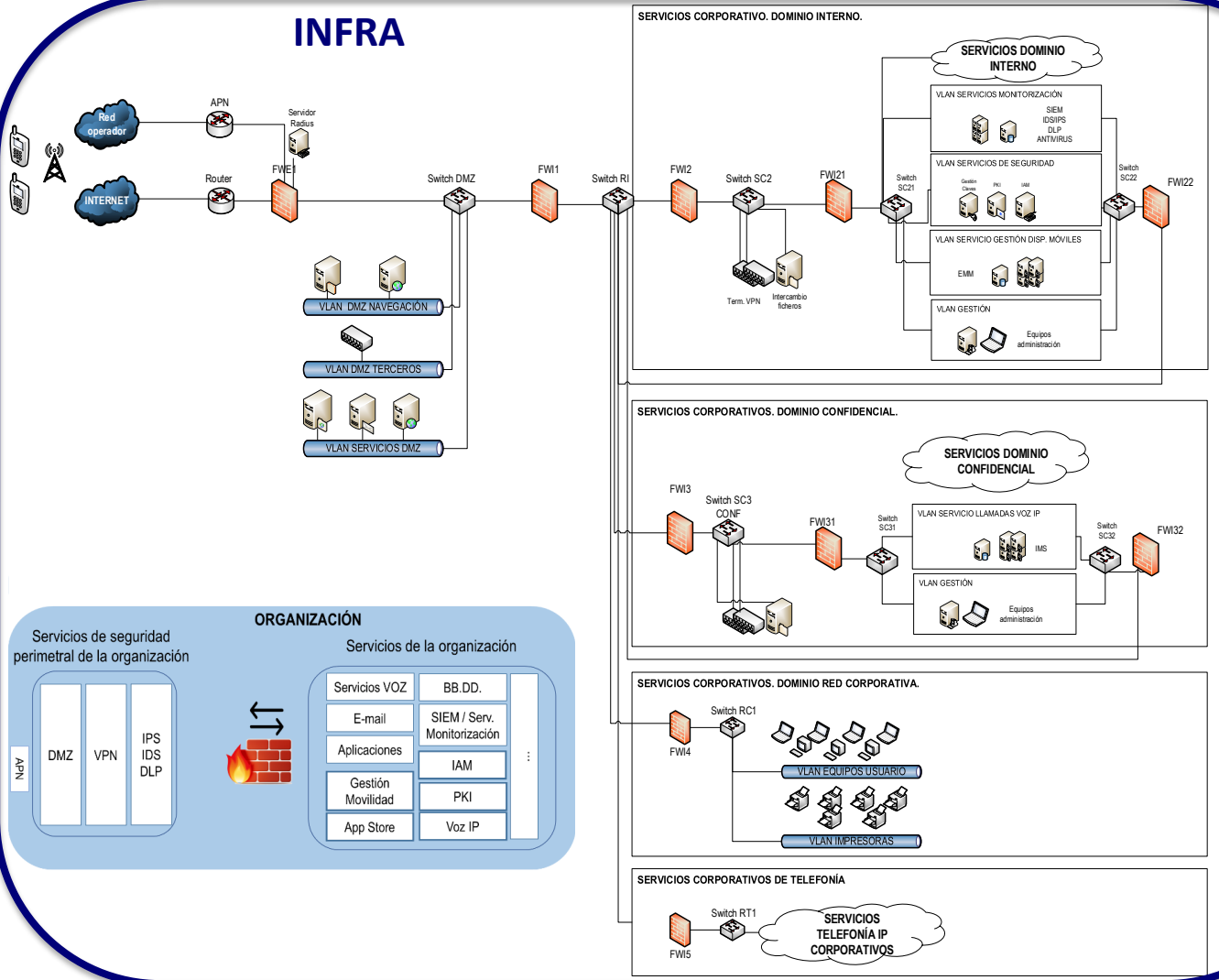
Validación de Requisitos

DISPOSITIVO

REDES

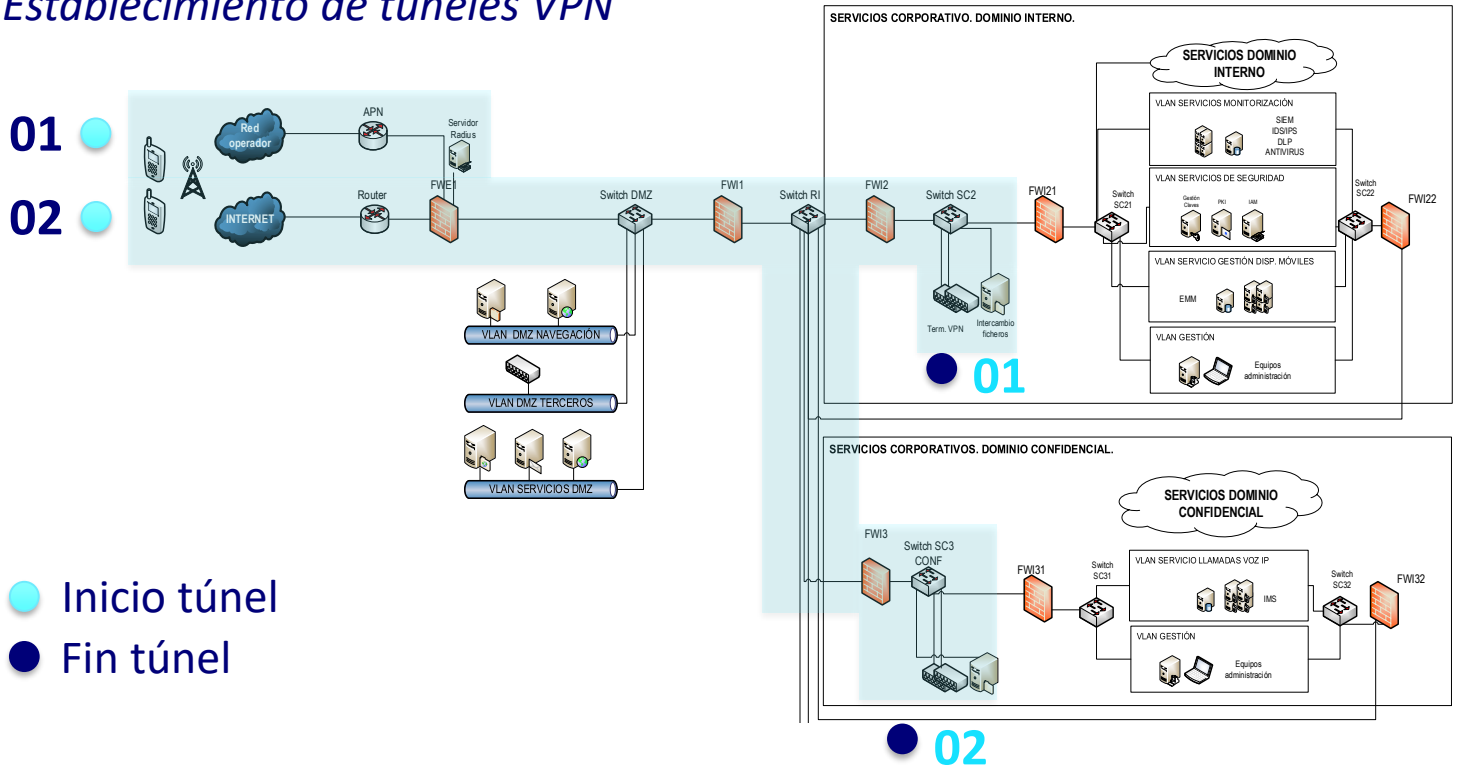
INFRA

INFRA



Diseño técnico.
Flujos de información

Establecimiento de túneles VPN



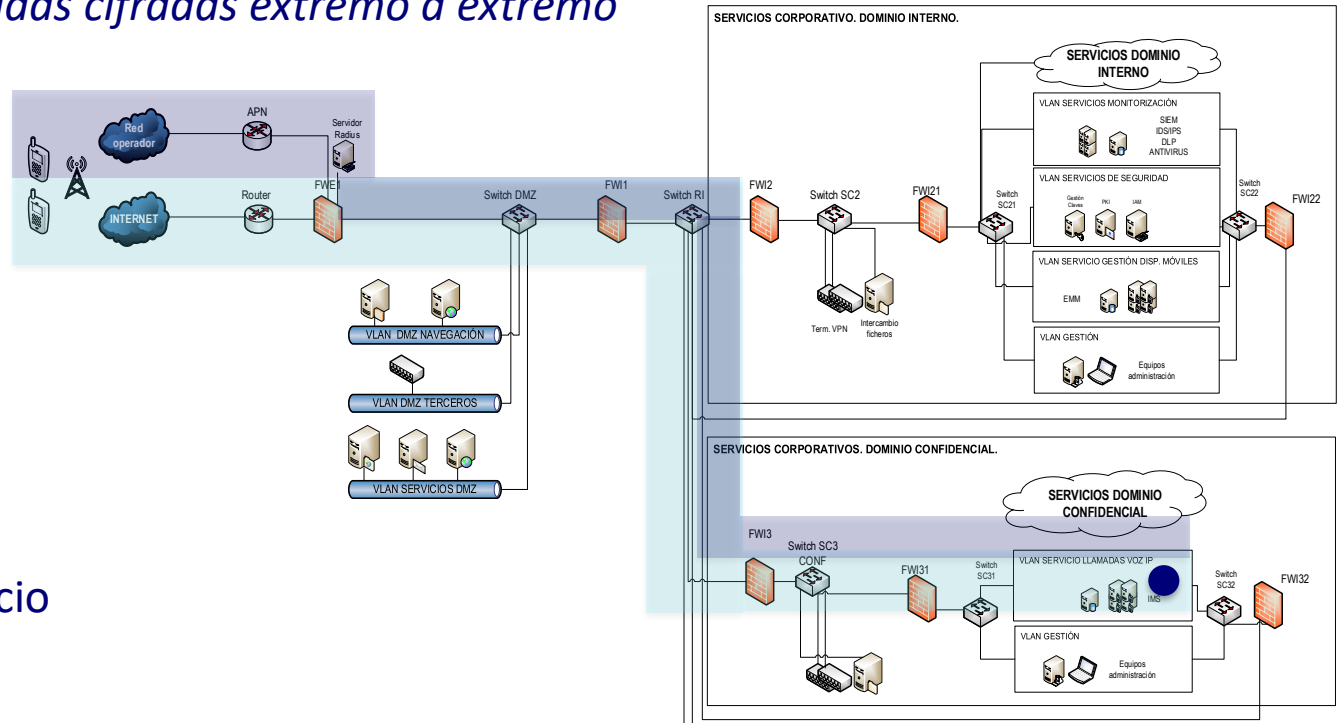
- Inicio túnel
- Fin túnel

Diseño técnico.
Flujos de información

Llamadas cifradas extremo a extremo

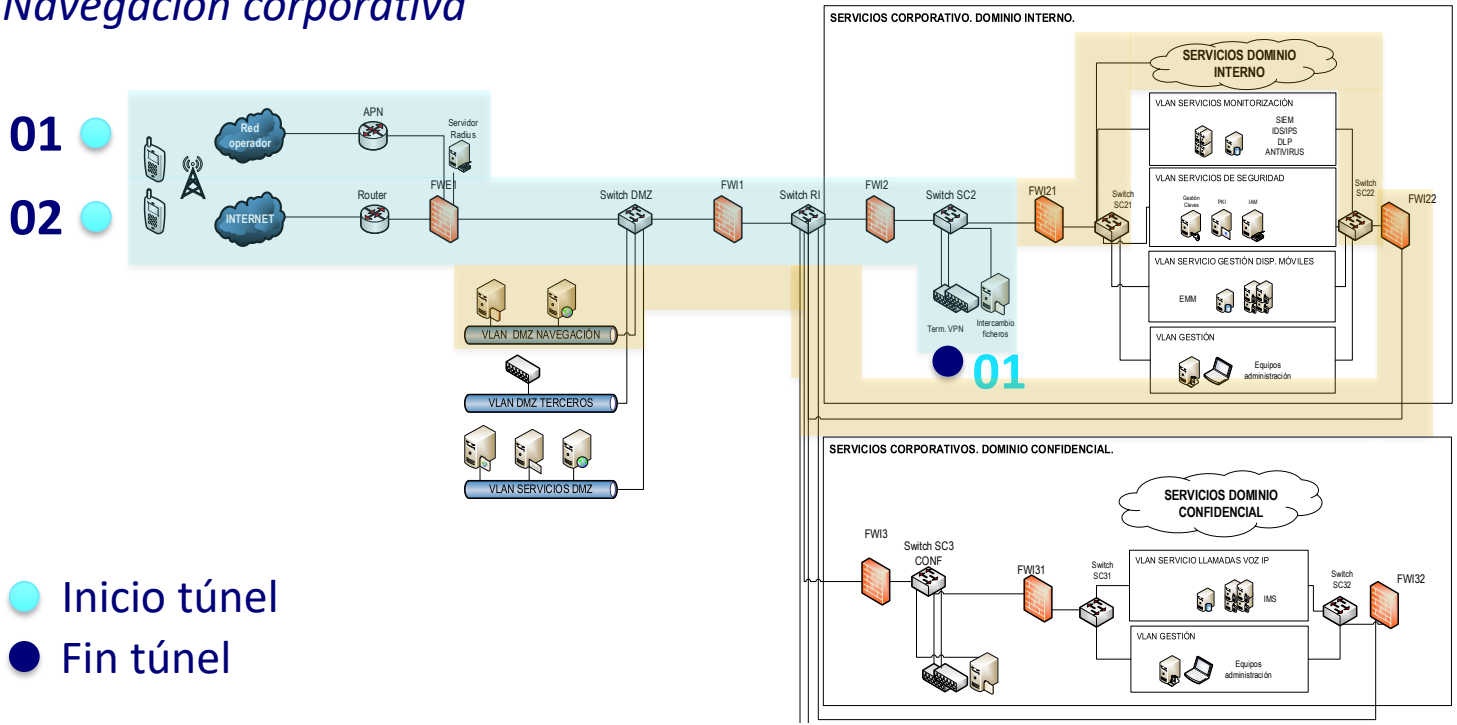
01 Inicio

02 Fin



Diseño técnico.
Flujos de información

Navegación corporativa



- Inicio túnel
- Fin túnel

Diseño técnico.
Validación requisitos

Catálogo de Servicios → Funciones de Seguridad → Bloques Funcionales → Flujos de Información → **Validación de Requisitos**

Con la validación de requisitos nos realimentamos para enriquecer el diseño, y aseguramos que el sistema cumple los principales objetivos de seguridad que nos habíamos propuesto.

Principales amenazas y objetivos para implementar la seguridad

Es necesario entender qué amenazas pueden afectar a cada uno de los elementos del "ecosistema" para poder implementar la seguridad.

AMENAZAS GENERALES
- Denegación de servicio
- Seguimiento del usuario
- Robo de información
- Suplantación
- Modificación de datos
- Control remoto del dispositivo
- Acceso a comunicaciones del usuario

AMENAZAS POR SUPERFICIE DE ATAQUE

OBJETIVOS
- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación
- Autorización
- Trazabilidad
- No repudio

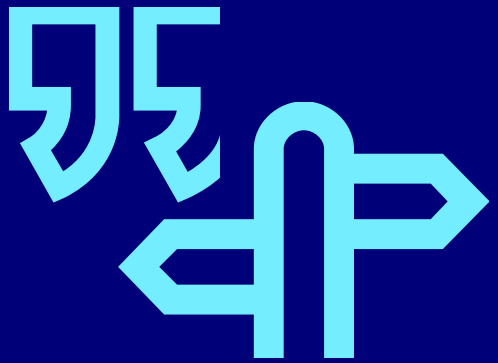
CONTRAMEDIDAS

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.

05

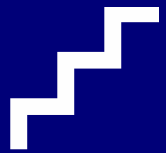
Conclusiones y Trabajo Futuro



Conclusiones y Trabajo Futuro

¿QUÉ HEMOS HECHO?

¿CÓMO LO HEMOS HECHO?



¿QUÉ HEMOS APORTADO?

¿QUÉ PODEMOS MEJORAR?

¿QUÉ QUEDA POR HACER?

Gracias
Thank you
Gràcies

UOC.universitat
@UOCuniversitat
@uocuniversitat

uoc.edu

Universitat Oberta
de Catalunya