VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
www.tecnimap.com
Ponencias

Implantación de los Servicios Básicos de la Intranet Administrativa

Isabel Fábregas Reigosa

Ingeniero de Telecomunicación y funcionaria del Cuerpo Superior de Sistemas y Tecnologías de la Información.

José María Vinagre Bachiller

Licenciado en Informática y funcionario del Cuerpo Superior de Sistemas y Tecnologías de la Información.

Miguel A. Amutio Gómez

Licenciado en Informática y funcionario del Cuerpo Superior de Sistemas y Tecnologías de la Información.

1. Objetivos

El objetivo del Proyecto "Intranet Administrativa" es dotar a la Administración General del Estado de una plataforma básica de comunicaciones que proporcione un conjunto integrado de servicios telemáticos para el intercambio electrónico de información entre los distintos Órganos de la Administración, superando así las actuales islas informáticas administrativas.

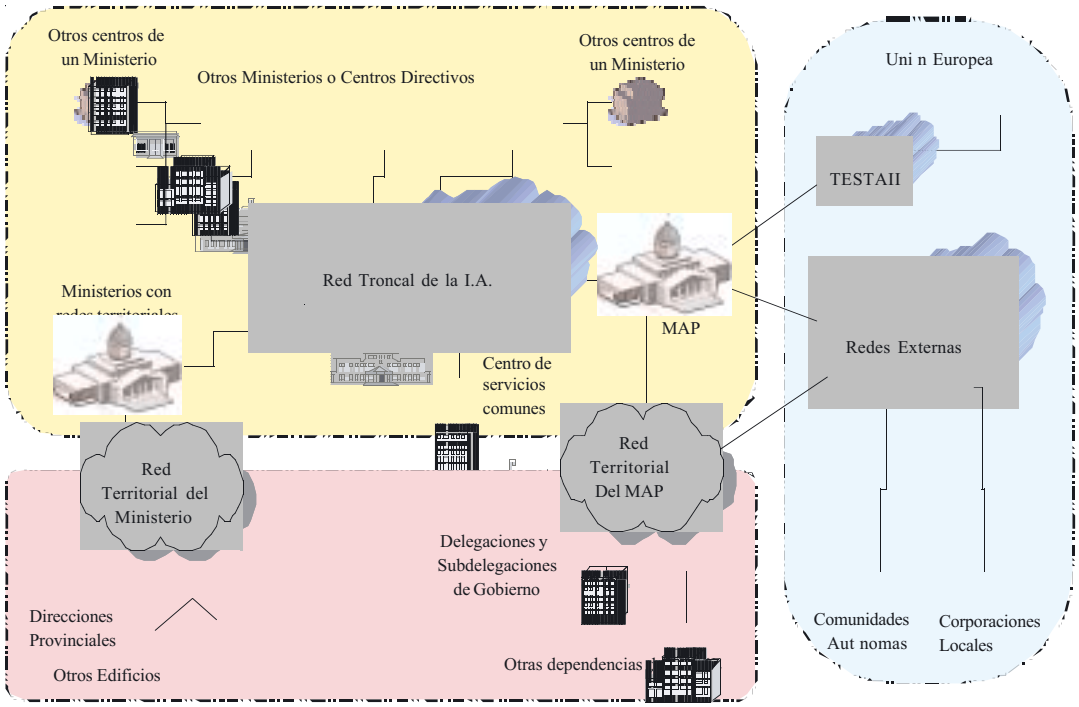
En esta fase del proyecto se van a desarrollar:

- Los servicios básicos de la Intranet Administrativa: DNS, Correo electrónico, directorio, web, y foros de discusión
- Centro de acceso único para las comunicaciones con Comunidades Autónomas, Corporaciones Locales y Unión Europea
- Establecimiento de una política de seguridad común

2. Arquitectura de la Intranet Administrativa.

En el Plan Director de la Intranet Administrativa (IA) se identificaron los siguientes participantes (usuarios y proveedores de sistemas de información):

- Departamentos Ministeriales, algunos de ellos disponen de grandes redes territoriales.
- El Ministerio de Administraciones Públicas, con una red que conecta las Delegaciones de Gobierno y Subdelegaciones
- Redes Externas de otras Administraciones, Comunidades Autónomas, Corporaciones Locales y Unión Europea



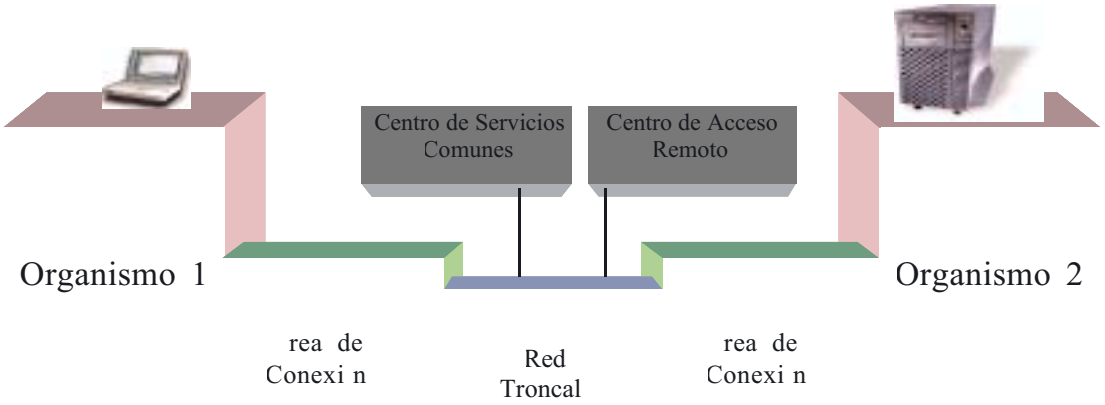
La arquitectura definida consta de los siguientes componentes:

- Red Troncal de la IA, proporciona la interconexión entre las diferentes infraestructuras.

- Área de Conexión, en la que se establecerán los sistemas que coordinan la interoperabilidad de cada entidad con el resto de organismos a nivel de servicios, aportando el nivel de seguridad que impida el conocimiento directo sobre su organización interna.

- Establecimiento de un Centro de Servicios Comunes (CSC) para toda la Intranet Administrativa, donde se situarán los servicios que permitan la coordinación entre todas las entidades y a su vez le aporten un mayor nivel de disponibilidad actuando como respaldo

- Centro de Acceso Remoto (CAR), para la conexión hacia otras Administraciones



En el diseño técnico de esta solución se ha tenido en cuenta:

- Estándares y software de libre distribución
- Elementos de seguridad existentes
- Funcionalidades de VPN en los elementos cortafuegos
- EL CAR se integra en el CSC y se eliminan los elementos de seguridad coincidentes para simplificar el proceso de instalación.

- Se ha optado por la propuesta de elementos hardware fácilmente escalable que permita un alto grado de crecimiento. Se ha preferido comenzar con una solución sencilla que soporte los servicios básicos y que pueda ampliarse de acuerdo al incremento de la demanda de servicios.

La Red Troncal estará formada por enlaces de alta velocidad, con capacidad suficiente para la prestación de los servicios de voz y datos requeridos. Se demanda una solución de alta disponibilidad y fiabilidad.

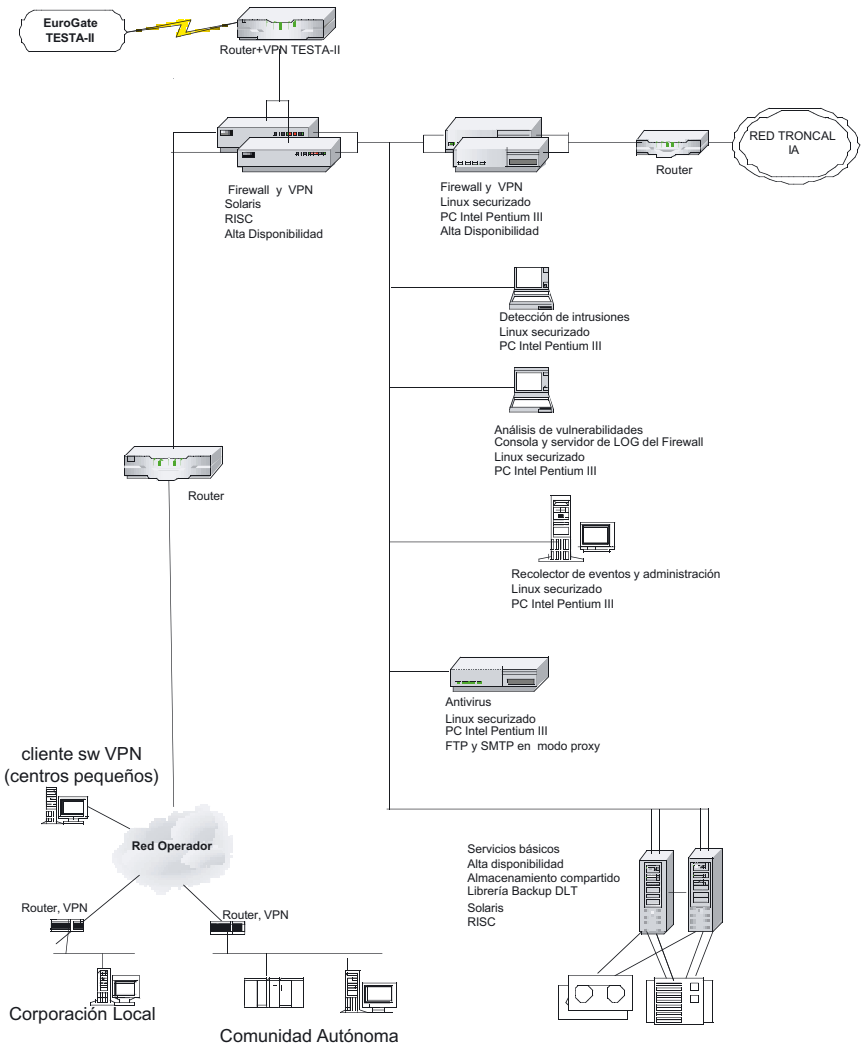
Se ha diseñado una solución para el CSC/CAR, en la que se puede destacar:

- Los sistemas Unix en alta disponibilidad que albergarán los servicios básicos
- Las consolas de administración centralizan las alertas de seguridad (análisis de vulnerabilidades y detección de intrusión) de todas las zonas
- Cortafuegos de acceso a la red troncal y acceso remoto en alta disponibilidad
- Antivirus para inspección de contenidos
- El Centro de Acceso Remoto (CAR) se conectará a una red privada virtual (proporcionada por un operador de servicios de telecomunicaciones), para la transmisión cifrada de datos. Esta infraestructura permitirá el acceso desde cada uno de los nodos de salida de las Administraciones de las Comunidades Autónomas y Corporaciones Locales, mediante enlaces dedicados (para las administraciones con mayor flujo de datos), o accesos conmutados (para el resto de nodos).
- La conexión con la Administración Europea se proporcionará por la red TESTAII que permite la interconexión entre los distintos países miembros de la Unión Europea. Tiene una infraestructura propia contratada con un operador global que en estos momentos es Equant. El proyecto de la Intranet Administrativa contempla la inclusión de una conexión segura desde todos los ministerios al resto de la Unión Europea utilizando la red TESTAII

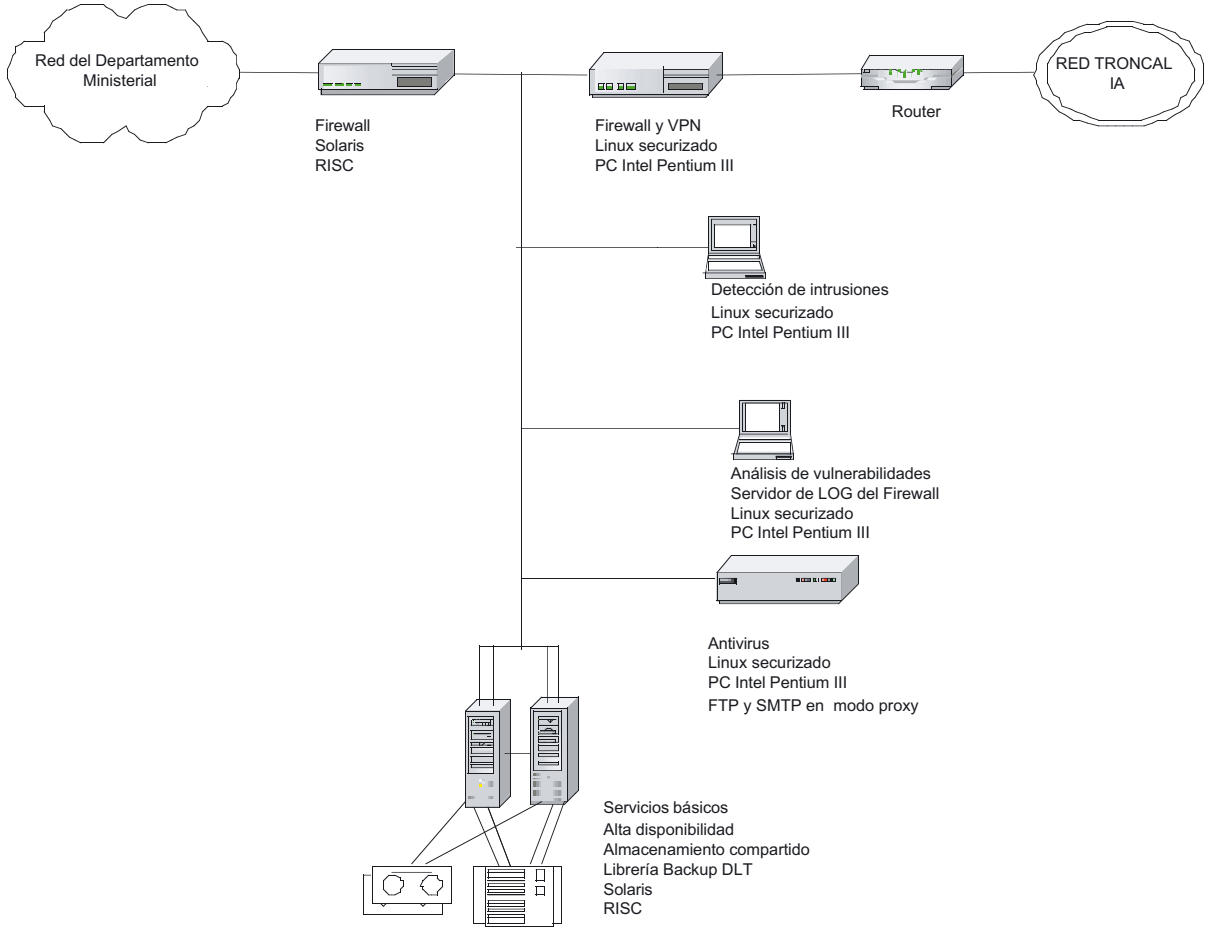
En la solución propuesta para las Áreas de Conexión que se instalarán en los Departamentos Ministeriales se puede señalar:

- Los sistemas Unix en alta disponibilidad que albergarán los servicios básicos
- Los equipos que realizan funciones de seguridad enviarán sus alertas al CSC.
- Los cortafuegos de acceso a la red troncal y de acceso a la red Departamental son de diferente tecnología

Centro de Servicios Comunes y Centro de Accesos Remotos (CSC/CAR)

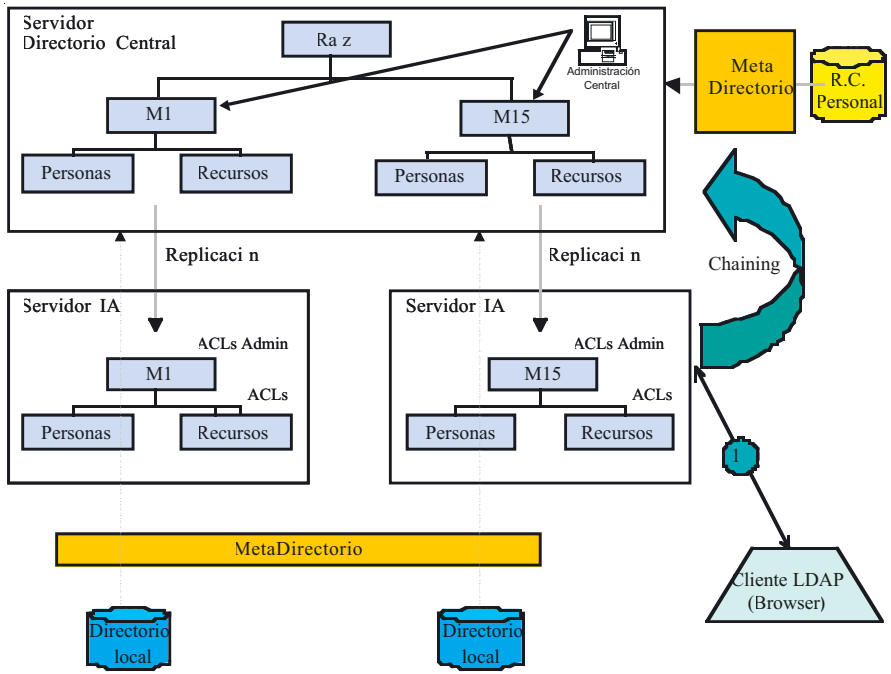


Área de Conexión (en cada Departamento Ministerial)



En cuanto a la configuración de los Servicios Básicos de la IA se puede señalar:

- DNS, se integrará con el servicio local que exista en las infraestructuras departamentales
- Correo electrónico, funcionará como relay de correo para las comunicaciones entre los departamentos ministeriales y para los intercambios con otras administraciones
- Foros de discusión, servicio proporcionado desde el CSC accesible con navegador
- Directorio, constituye la pieza fundamental del proyecto para el que se propone la arquitectura siguiente:



Se ha identificado al Registro Central de Personal (RCP) como fuente externa de datos para el Directorio del CSC. Se realizarán réplicas de las ramas de cada Departamento a los servidores alojados en las Áreas de Conexión.

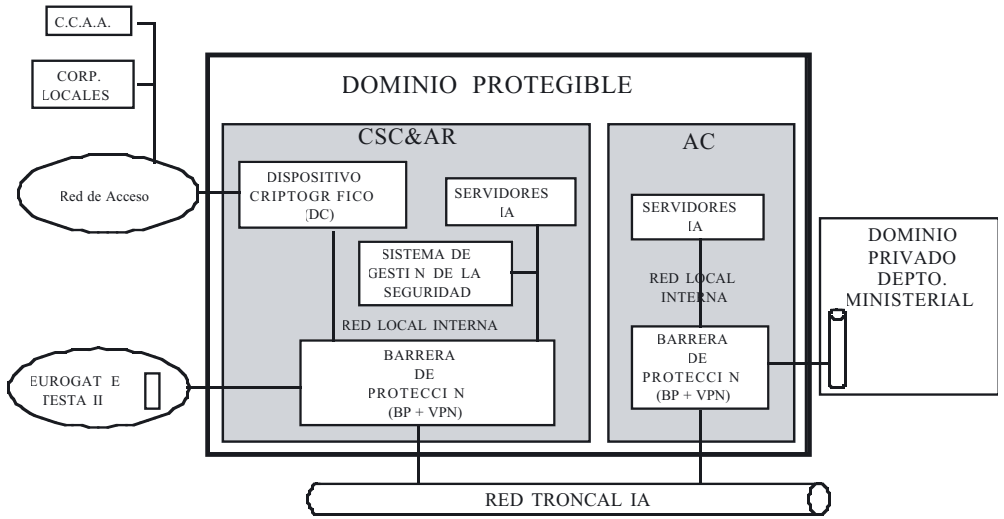
Se establecerán otras fuentes externas para los datos y los colectivos que no están dentro del ámbito del RCP.

Los usuarios consultan el directorio existente en su Área de Conexión, si el dato solicitado no se encuentra allí dicho servidor busca en el Directorio del CSC. Esta operación se realiza de forma transparente al usuario

Se establecerán medidas de seguridad para controlar el acceso a los datos del Directorio y distintos niveles de administración.

3. Política de seguridad común

El objetivo de la Política de Seguridad es definir un entorno homogéneo de seguridad donde se establezcan las normas, medidas y procedimientos de seguridad a adoptar para garantizar la autenticidad, confidencialidad, integridad y disponibilidad del sistema de información englobado en el Dominio de la Intranet Administrativa, que se muestra en el siguiente esquema:



La elaboración de la Política de Seguridad se ha basado en la aplicación de la Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT) [1] y de los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades [2]. Así mismo, se ha tenido como referente el trabajo que en el mismo sentido se viene realizando en la red transeuropea TESTA II financiada por el Programa IDA.

En la realización de la Política de Seguridad destacan los siguientes pasos:

1. Análisis y gestión de riesgos

- Definición del Dominio Protegible de la Intranet Administrativa, es decir, del sistema sobre el cual se va a llevar a cabo el análisis y gestión de riesgos y que es objeto de la Política de Seguridad
- Identificación y valoración de los activos del Dominio, en función de los cuatro subestados de seguridad: autenticación, confidencialidad, integridad y disponibilidad.
- Identificación de las amenazas, que pueden incidir sobre los activos de la Intranet Administrativa. Para ello, se ha partido de un conjunto amplio de amenazas pormenorizadas y en una primera selección, se han tenido en cuenta aquellas que pudieran afectar al Dominio Protegible.
- Valoración del impacto y vulnerabilidad de cada amenaza identificada sobre cada activo afectado; y, a continuación, cuantificación del riesgo de materialización de la amenaza sobre el activo.
- Identificación de escenarios de riesgo y selección de salvaguardas, agrupando las amenazas identificadas en escenarios de riesgo y realizando un estudio minucioso de las salvaguardas aplicables para cada escenario.

2. Redacción de la Política de Seguridad

- Articulación de las salvaguardas obtenidas como resultado del proceso previo de análisis y gestión de riesgos en la estructura de contenidos aportada por los Criterios de seguridad, basados en gran medida en Código de buenas prácticas para la gestión de la seguridad de la información, ISO/IEC 17799. Así, la política de seguridad contempla los siguientes capítulos.

- Organización de la seguridad: funciones y responsabilidades.
- Identificación y clasificación de activos
- Seguridad personal
- Seguridad física
- Identificación, autenticación y control de accesos
- Confidencialidad, integridad y disponibilidad
- Acceso a través de redes
- Utilización de técnicas criptográficas
- Gestión de soportes de información y copias de respaldo
- Explotación de sistemas
- Gestión y registro de incidencias
- Contingencias y continuidad de servicio
- Auditoría y control de la seguridad

- Identificación de las responsabilidades, dado que entre las salvaguardas que se incluyen, se encuentran algunas cuya responsabilidad de implantación recae sobre los distintos departamentos y entidades conectadas a la Intranet Administrativa (Departamentos Ministeriales, Comunidades Autónomas y Corporaciones Locales) y otras, cuya responsabilidad debe asumir el Dominio Protegible de la Intranet Administrativa (Centro de Servicios Comunes y Acceso Remoto y Áreas de Conexión).

4. Estado de situación del proyecto

En la fecha de redacción de esta comunicación (julio 2002) el proyecto se encuentra en fase de implantación y las actividades desarrolladas se resumen a continuación.

Implantación de los Servicios Básicos, Red troncal y Red de Acceso Remoto

- Se han realizado un Inventario de la situación actual de los servicios básicos en los Departamentos y un catálogo de los Servicios de interés común
- Adquisición del equipamiento hardware y software del CSC/CAR y de las Áreas de Conexión
- Preparación del Pliego para la licitación de los servicios de Telecomunicaciones (Red Troncal y Red de Acceso Remoto)

Conectividad con otras administraciones

- Se han establecido las líneas generales de conectividad e infraestructura necesaria para proporcionar la comunicación entre el Centro de Acceso Remoto (CAR) y Comunidades Autónomas, Corporaciones Locales y Administración Europea
- Los dos problemas más graves que se presentan son la heterogeneidad de los accesos y el volumen de clientes potenciales. Se han clasificado todos estos clientes potenciales en distintos grupos, dependiendo de sus características.

Directorio

- Se ha propuesto un modelo de datos para el Directorio
- Se está desarrollando una aplicación de consulta de los datos básicos del Directorio ("páginas blancas")

Infraestructura de clave pública

Se ha realizado un estudio sobre las necesidades de certificación de la IA, que incluye entre otros aspectos los siguientes:

- Especificación de requisitos más precisos de los servicios de certificación necesarios.
- Las normas y estándares aplicables.
- Los elementos a certificar.
- El uso de los certificados y su ámbito de aplicación.
- Estudio de alternativas.
- Recomendaciones.

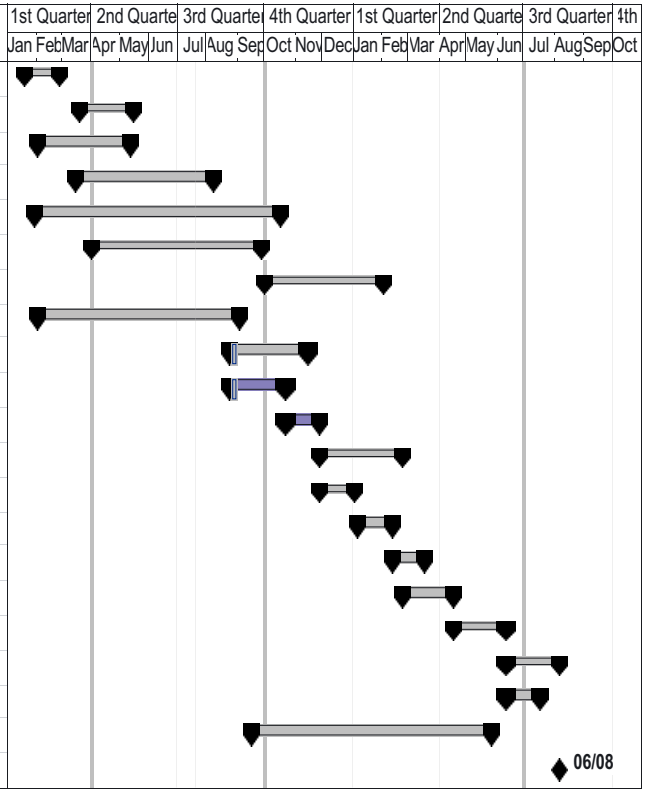
Política de seguridad

- Se han realizado el análisis y gestión de riesgos y la política de seguridad.
- Las siguientes tareas son la elaboración del perfil de protección de la Intranet Administrativa conforme a los Criterios comunes de evaluación de la seguridad de las tecnologías de la información (ISO/IEC 15408) y la Guía para producción de perfiles de protección (ISO/IEC 15446), así como la elaboración del plan de contingencias y del plan de continuidad de negocio.

5. Planificación

Se incluye a continuación la planificación de las actividades más importantes del proyecto y su duración estimada:

ID	Nombre de tarea	Duration
1	**Plan gestión inicial**	**26 days**
16	**Actualización Plan proyecto**	**36 days**
21	**Estudios de equipamiento**	**64 days**
73	**Procesos compra HW & SW**	**100 days**
84	**Definición Política de Seguridad**	**176 days**
111	**Diseño y desarrollo Directorio**	**127 days**
135	**Instalación directorio**	**85 days**
145	**Consultoría de dimensionamiento y conectividad**	**143 days**
189	**Instalación Infraestructura CSC/CAR**	**58 days**
242	**Instalación Infraestructura Mº1 y Mº 2**	**41 days**
255	**Instalación Mºs 3, 4 y 5**	**25 days**
260	**Formación CSC**	**58 days**
274	**Instalación Mºs 6, 7 y 8**	**25 days**
279	**Instalación Mºs 9,10 y 11**	**25 days**
284	**Instalación Mºs 12, 13, 14 y 15**	**25 days**
289	**Primera Formación 5 Áreas Conexión**	**38 days**
298	**Segunda Formación 5 Areas Conexión**	**38 days**
307	**Tercera Formación 5 Áreas Conexión**	**39 days**
316	**Formación adicional**	**24 days**
323	**Aseguramiento Calidad**	**174 days**
327	**Cierre proyecto**	5 days



Referencias

[1] MAGERIT, Metodología de análisis y gestión de riesgos de los sistemas de información http://www.map.es/csi/pg5m20.htm

[2] Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades http://www.map.es/csi/pg5c10.htm