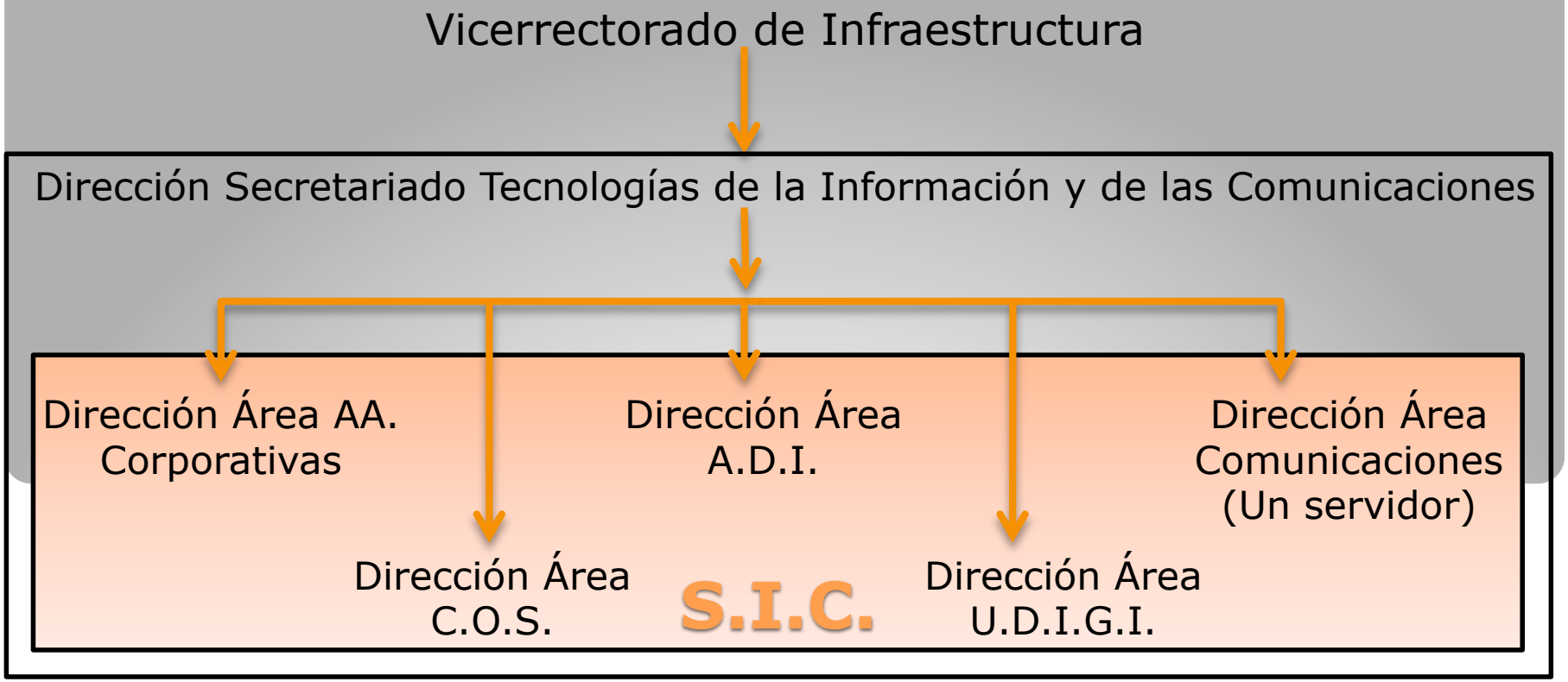
Experiencia en la implantación del E.N.S. en la Universidad de Sevilla

Servicio de Informática y Comunicaciones (S.I.C.)

Organigrama S.I.C.



La Dirección del Secretariado y las Direcciones de cada Área conforman el Comité de Dirección del S.I.C.

Se reúne semanalmente para tratar de lo asuntos específicos de cada Área y de los transversales del Servicio

Algunas fechas claves en el proceso:

01/02/2010
30/01/2011
06-07/03/2012
18/07/2013
30/01/2014
26/02/2014

Algunas fechas claves en el proceso: 01/02/2010

Primeras noticias sobre el E.N.S., me las envía el Sr. Vicesecretario de la Diputación de Sevilla (que casualmente es mi hermano) y...

a dormir el sueño de los justos.

Algunas fechas claves en el proceso: 30/01/2011

Ha pasado un año, ha llegado la ficha límite del primer plazo y no tenemos implantado el E.N.S.
¿Qué nos puede ocurrir?

Bueno, como estamos estudiando la posibilidad de diseñar y desarrollar un Plan de Adecuación lo mismo eso nos permite un plazo más amplio…¿O no?

Algunas fechas claves en el proceso: 22y23/02/2012

Se celebra II Congreso Nacional de Interoperabilidad y Seguridad (CNIS), al que asisto, y en el que el profesor Carlos Galán de la UCIII, entre otros ponentes, hace una exposición muy clara del marco jurídico en el que nos movemos o al menos deberíamos movernos.

Algunas fechas claves en el proceso:
05/03/2012

Me pongo en contacto con el profesor Carlos Galán al que le pregunto ¿Qué ocurriría si una institución no tuviera implantado el ENS en la fecha límite del 2014?.

A vuelta de correo 06/03/2012, muy amablemente, lo que agradecí en su momento y agradezco otra vez, ya que lo cito, me responde:

El cumplimiento del ENS deviene obligatorio para todos los organismos de todas las Administraciones Públicas y de sus organismos vinculados (como es el caso de las Universidades) o dependientes.

Por otro lado, la Disposición Transitoria del ENS señala un plazo máximo de 48 meses desde la entrada en vigor del ENS (30 de enero de 2010) para que todos los Sistemas de Información del organismo en cuestión que estén comprendidos en el ámbito del ENS sean conformes a lo allí dispuesto.

Los sistemas que se encuentran afectados por el ENS son:

- Sedes electrónicas.
- Registros electrónicos.
- Sistemas de Información (SI's) accesibles electrónicamente por los ciudadanos, profesionales y empresas.
- SI's para el ejercicio de derechos (por parte de ciudadanos, profesionales y empresas).
- SI's para el cumplimiento de deberes (de los ciudadanos, profesionales y empresas).
- SI's para recabar información y estado del procedimiento administrativo.
- SI's para el desarrollo del procedimiento administrativo.

Y todos ellos, sea cual fuere la forma de prestación o ejecución: propia, subcontratada, externa, modalidad Cloud Computing, etc.

No obstante lo anterior, si el organismo en cuestión, pasados doce meses desde la entrada en vigor del ENS (es decir, a 30 de enero de 2011) no tuviera sus sistemas conforme a lo dispuesto en el ENS, debería redactar y aprobar un Plan de Adecuación que contemple (en un escenario temporal que debe terminar el 30 de enero de 2014) toda la planificación que acciones que debe acometer para que, llegada tal fecha, sus sistemas sean conformes a lo exigido por el ENI.

Por lo tanto, lo primero que hay que hacer es redactar y aprobar por el órgano superior el antedicho Plan de Adecuación al ENS (y al ENI, también).

Si superada la fecha del 30 de enero de 2014 algunos sistemas no fueran todavía conformes con lo dispuesto en el ENS, se estaría incumpliendo la ley y, por tanto, se estaría sujeto a lo que se llama Responsabilidad Patrimonial de las Administraciones Públicas.

Es decir, estaría expuesto a que alguien que se pudiera ver perjudicado por tal incumplimiento interpusiera por la vía contencioso-administrativa una reclamación, que, caso de prosperar, obligaría al organismo a asumir su responsabilidad e, incluso, a satisfacer económicamente a los perjudicados por los daños y perjuicios ocasionados.

Llegado este caso, la existencia del antedicho Plan de Adecuación podría aligerar el peso de la responsabilidad, si se demostrara que el incumplimiento no se ha producido por una falta de interés del organismo, sino por casusas sobrevenidas de fuerza mayor que han imposibilitado su cumplimiento.

Algunas fechas claves en el proceso: 06-07/03/2012

(X Foro de Seguridad de RedIRIS.)

Estado del arte: Un 60% de las instituciones no tiene Plan de Adecuación (la US entre ellas).

¡Hay que ponerse las pilas, ya que mal de muchos...!

Algunas fechas claves en el proceso: 06-07/03/2012

(X Foro de Seguridad de RedIRIS.)

Estado del arte: Más de la mitad de las instituciones piensa contar con ayuda externa para el diseño del proceso de Adecuación

La US se apunta, si es posible

Algunas fechas claves en el proceso: 09/03/2012

Se empiezan los contactos para ver la posibilidad de esa colaboración externa.

Parece que la cosa empieza a marchar, o eso creía yo.

Algunas fechas claves en el proceso: 09/03/2012

Pero: ¿Cómo acometer un proyecto de adecuación en estos tiempos, con la crisis que hay?¿De dónde sacar dinero para ello?

¿De dónde sacar tiempo a pesar de la colaboración externa?

¿Cómo implicar a los responsables políticos?

Algunas fechas claves en el proceso: 29/05/2012

Tras más de dos meses y medio de conversaciones e intentos de ajustar agendas, por fin se realiza la primera presentación al Comité de Dirección del S.I.C. de cómo sería una posible colaboración externa y sus implicaciones tanto económicas y políticas, como de trabajo a realizar por nuestra parte.

Algunas fechas claves en el proceso:
29/05/2012

Dadas las circunstancias se acuerda el estudio de lo que implicaría, desde todos los puntos de vista, la posibilidad de realización de un Plan de Adecuación.

Será el Comité de Dirección del S.I.C. el que se implique directamente en ello por nuestra parte.

Algunas fechas claves en el proceso: del 01/06/2012 al 31/07/2013

Se contacta con 6 empresas para explicarles lo que queremos y recibir ofertas de la realización del Plan de Adecuación:

Abast, BDO, Isoluciones, Isotrol, Nextel y Sferia

Algunas fechas claves en el proceso: del 01/06/2012 al 31/07/2013

En paralelo, se contacta con distintas instituciones para conocer sus opinión sobre las citadas empresas, por las referencias dadas, y, por otro lado, se plantea la posibilidad de hacerlo junto con la UMA con la que se habían firmado los acuerdos de Andalucía Tech.

Algunas fechas claves en el proceso: del 01/06/2012 al 31/07/2013

Más en paralelo aún, se empieza a hacer encajes presupuestarios (encaje de bolillos) para ver como obtener los fondos (hablamos inicialmente de unos 15 K €).

En el ínterin nos recortan el presupuesto un 15%

Algunas fechas claves en el proceso: A partir del 01/08/2012

Está claro que obtener los fondos necesarios en 2012 (seguimos hablamos de unos 15 K €) va a ser difícil.

Se inicia una negociación económica (regateo puro y duro) con los ofertantes mejor situados.

En el ínterin, me hospitalizan ¿Es culpa del E.N.S.? No, es mala suerte ☺.

Algunas fechas claves en el proceso: 04/12/2012

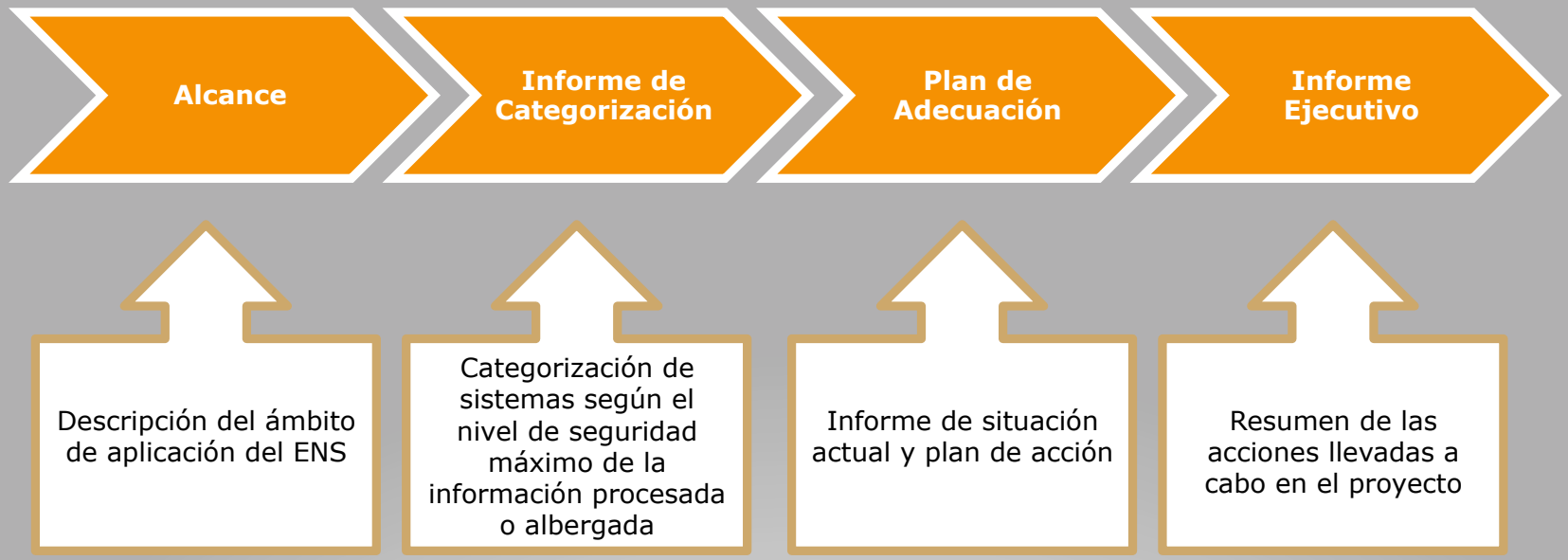
Tras la negociación mencionada antes y con el vºbº de Comité, después de despejadas y aclaradas toda clase de dudas, se inicia el expediente para la adjudicación de la elaboración del Plan de Adecuación al E.N.S. de la US a la empresa Nextel.

Se seguirán el siguiente esquema y etapas:

Etapas y Fases del proyecto (S.I.C.)

ETAPAS PROYECTO		
Etapa I – Diseño del Plan de Adecuación	Fase I - Lanzamiento	• Definición equipo de trabajo • Definición de roles y funciones • Definición de responsabilidades • Definición del Alcance • Definición del plan de trabajo
	Fase II – Análisis	• Diagnóstico del estado actual respecto a requisitos del E.N.S.

Productos de la Etapa I
Diseño del Plan de Adecuación al E.N.S. (S.I.C.)



Algunas fechas claves en el proceso:
A partir del 27/12/2012

Se inician los trabajos recopilando la información solicitada, recopilación previa a las primeras reuniones de lanzamiento del proyecto entre Nextel y el Comité de Dirección, las Direcciones de las distintas Áreas y el personal de éstas.

Dichas reuniones se fijan para los días 16 y 17/01/2013.

Algunas fechas claves en el proceso: a partir del 17/01/2013

Las reuniones se inician finalmente el 17/01/2013:

- La primera, previa a las demás, con el Comité de Dirección.
- Posteriores, indistinta o conjuntamente, con:
  - Dtor. STIC.
  - Cada Dtor. de Área.
  - Integrante de cada una de las Áreas y del equipo de Admin.

En ellas se trata de la:

- Gestión de compras
- Identificación y valoración de servicios.
- Identificación de la arquitectura tecnológica.
- Gestión de la seguridad:
  - Roles y responsabilidades.
  - Normativas aplicables.
  - Procesos implantados.
  - Etc.

Algunas fechas claves en el proceso: a partir del 17/01/2013

Más asuntos tratados en las reuniones:

- El análisis de aspectos técnicos y de seguridad en relación con:
  - Las aplicaciones.
  - La gestión de sistemas y el equipamiento.
  - La tecnología.
  - Gestión de identidades y el e-mail.
- Posibles avances ya realizados en materia de seguridad (ISO27001, LOPD, etc.)
- Revisión de valoración de servicios.
- Revisión de resultados preliminares.

¡Por fin parece que arrancamos!

Algunas fechas claves en el proceso: a partir del 17/01/2013

- Revisión por parte del Comité de Dirección de la primera propuesta de valoración de los servicios del S.I.C. presentada, hecha en base a las implicaciones de seguridad (integridad, confidencialidad, autenticidad, disponibilidad y trazabilidad).

  - Dicha propuesta se recibe el 29/01/2013
  - El 01/03/2013 aún sigue planteando dudas y generando intercambio de correos.
  - Tanto es así que se pierde el rastro de cuando se aprueba, aunque por fin se hace, y queda como se muestra a continuación:

¡Parece mentira pero cuesta un gran trabajo!

Valoración de Servicios

Servicios	Subservicios	D	I	C	A	T
SS.001	Red cableada RIUS (+ VSS)	4	4	3	1	1
SS.002	Red Inalámbrica REINUS	4	4	3	1	1
SS.003	Resolución de nombres (DNS)	4	2	2	2	2
SS.004	Servicio de VPN	2	4	4	3	3
SS.011	Directorio Corporativo (LDAP)	3	4	1	3	2
SS.012	Gestión de Identidades (IdM)	3	4	2	4	3
SS.013	Single Sign On (OpenSSO)	3	4	5	4	4
SS.014	Federación de Identidades	3	4	3	4	3
SS.015	Servicio de Ficheros e Impresión en Red	2	3	3	2	3
SS.021	Estafetas y seguimiento de correo electrónico	3	3	4	3	3
SS.022	Buzones de correo electrónico/Agenda Virtual	3	3	4	3	3
SS.023	Listas distribución	3	3	1	2	1
SS.031	SOS	3	2	2	2	2
SS.032	Puntos de información universitaria (PIU)	2	3	1	3	1
SS.033	Centro de Atención Multicanal (CAMUS)	3	2	2	2	2
SS.041	Aulas de informática de campus	3	2	1	1	1
SS.042	Reserva de aulas de informática	2	2	1	1	1
SS.043	Plataforma de Enseñanza Virtual	4	3	3	3	2
SS.044	Biblioteca	2	3	2	2	2
SS.045	RODAS -Repositorio de objectos de aprendizaje (materiales de docencia)	4	3	3	3	2
SS.046	Salas Virtuales	4	2	1	1	1
SS.111	Antivirus de red (Desktops US, PC's aulas)	3	3	2	3	2
SS.112	Servicio Firewall	4	4	3	4	4
SS.113	Servicio Backup	2	4	3	3	3

Servicios	Subservicios	D	I	C	A	T
SS.051	Gestión universitaria académica	4	4	5	4	3
SS.052	Gestión universitaria de RRHH	4	4	4	3	3
SS.053	Gestión universitaria económica	4	4	3	3	3
SS.054	Gestión universitaria del registro	4	4	3	4	4
SS.055	Administración electrónica (ESTELA + Reg. Telemático)	4	4	4	4	4
SS.056	Secretaría virtual (SEVIUS)	4	4	4	4	4
SS.057	Automatrícula	4	4	3	3	4
SS.058	Gestión de acceso empresas externas	2	3	2	2	2
SS.059	Servicio de información a Dirección	2	3	3	3	2
SS.05a	Impresión masiva	2	2	3	1	1
SS.05b	Gestión de PA y PD ALGIDUS	2	3	3	3	2
SS.05c	Portal de Gestión Enseñanza Virtual (EV)	3	3	2	2	2
SS.05d	Gestión del Archivo General	4	3	3	3	3
SS.061	Videoconferencia y Access Grid	2	1	2	1	1
SS.071	Portal de la Universidad de Sevilla	3	3	1	1	2
SS.072	Consigna de ficheros	3	3	3	2	2
SS.073	Descarga de Software	3	2	2	2	1
SS.074	Alojamiento de Páginas WEB	3	3	3	3	3
SS.075	Aplicaciones WEB	3	3	3	3	3
SS.076	Gestor Documental (Alfresco)	3	3	3	2	3
SS.077	Portal OpenCourseWare (OCW)	3	3	2	2	2
SS.101	Entorno de Hosting Virtual de Dominios de Correo Externo	3	3	3	3	2
SS.102	Servicio de Hosting Virtual Investigación	3	3	3	3	2
SS.103	Servicio de clonación (PC's y PIU's)	2	2	1	1	1
SS.104	Servicio de alojamiento de aplicaciones y/o bases de datos	3	3	3	3	2

Servicio de Informática y Comunicaciones (S.I.C.)

Algunas fechas claves en el proceso: a partir del 17/01/2013

- Para la categorización de los sistemas se ha tomado como Modelo de Activos el desarrollado con anterioridad por el S.I.C., dentro del marco de gestión de la continuidad de sus servicios.

- Al categorizar los sistemas de información se determina asociarles niveles BAJO y MEDIO, no considerándose necesarios niveles más altos.

- Se muestra a continuación la categorización resultante, ya en funcionamiento, y el modelo de activos en el que se basa:

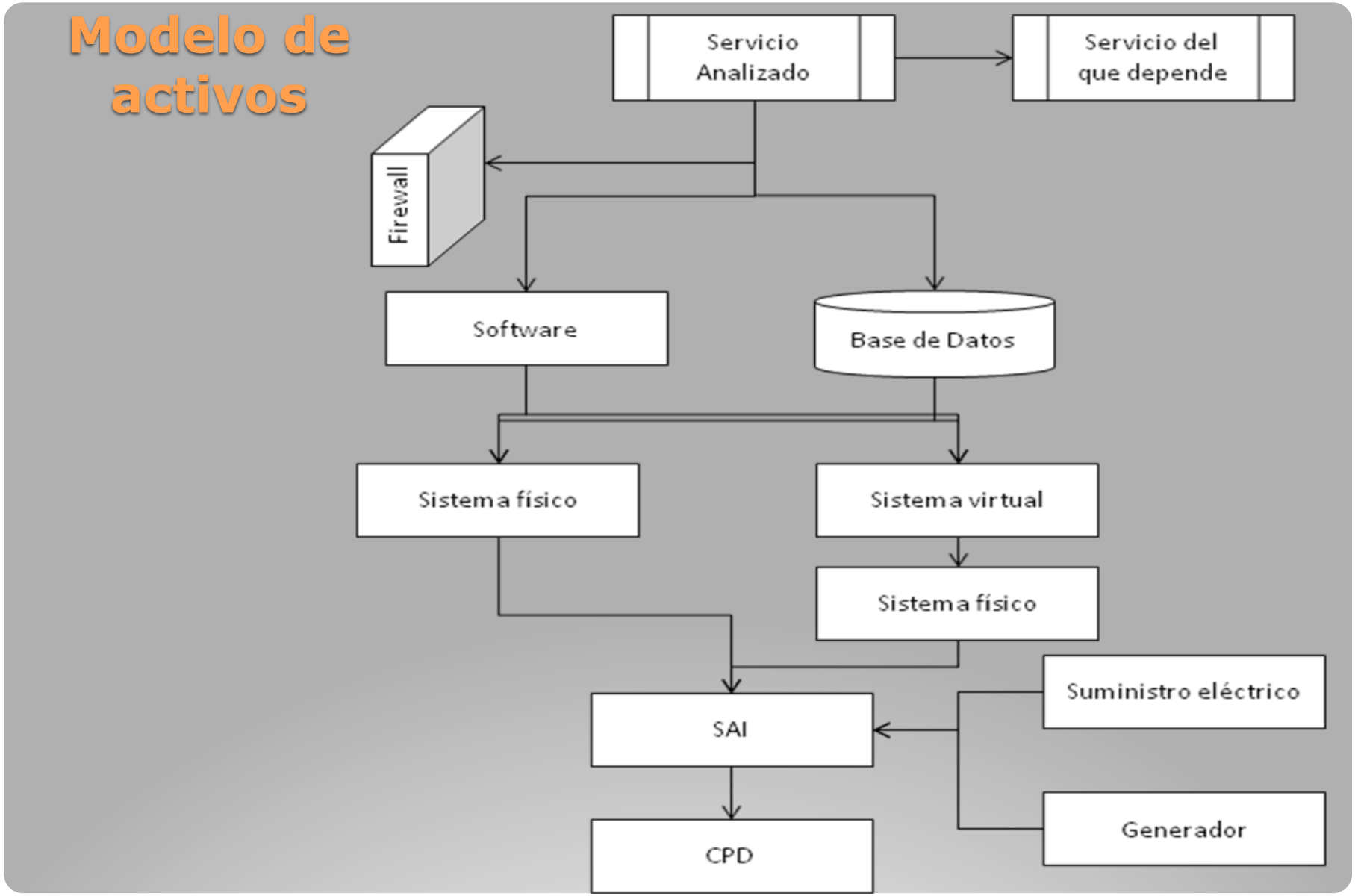
Categorización de Sistemas

Sistemas	D	I	C	A	T
Red cableada RIUS (+ VSS)	MEDIO	MEDIO	BAJO	BAJO	BAJO
Red Inalámbrica REINUS	BAJO	BAJO	BAJO	BAJO	BAJO
Resolución de nombres (DNS)	MEDIO	BAJO	BAJO	BAJO	BAJO
Servicio de VPN	BAJO	BAJO	BAJO	BAJO	BAJO
Directorio Corporativo (LDAP)	BAJO	MEDIO	BAJO	BAJO	BAJO
Gestión de Identidades (IdM)	BAJO	MEDIO	BAJO	MEDIO	BAJO
Single Sign On (OpenSSO)	BAJO	MEDIO	MEDIO	MEDIO	MEDIO
Federación de Identidades	BAJO	MEDIO	BAJO	MEDIO	BAJO
Servicio de Ficheros e Impresión en Red	BAJO	BAJO	BAJO	BAJO	BAJO
Estafetas y seguimiento de correo electrónico	BAJO	BAJO	BAJO	BAJO	BAJO
Buzones de correo electrónico/Agenda Virtual	BAJO	BAJO	BAJO	BAJO	BAJO
Listas distribución	BAJO	BAJO	BAJO	BAJO	BAJO
SOS	BAJO	BAJO	BAJO	BAJO	BAJO
Puntos de información universitaria (PIU)	BAJO	BAJO	BAJO	BAJO	BAJO
Centro de Atención Multicanal (CAMUS)	BAJO	BAJO	BAJO	BAJO	BAJO
Aulas de informática de campus	BAJO	BAJO	BAJO	BAJO	BAJO
Reserva de aulas de informática	BAJO	BAJO	BAJO	BAJO	BAJO
Plataforma de Enseñanza Virtual	BAJO	BAJO	BAJO	BAJO	BAJO
Biblioteca	BAJO	BAJO	BAJO	BAJO	BAJO
RODAS -Repositorio de objectos de aprendizaje (materiales de docencia)	BAJO	BAJO	BAJO	BAJO	BAJO
Salas Virtuales	BAJO	BAJO	BAJO	BAJO	BAJO
Antivirus de red (Desktops US, PC's aulas)	BAJO	BAJO	BAJO	BAJO	BAJO
Servicio Firewall	MEDIO	MEDIO	BAJO	MEDIO	MEDIO
Servicio Backup	BAJO	MEDIO	BAJO	BAJO	BAJO

Sistemas	D	I	C	A	T
Gestión universitaria académica	BAJO	BAJO	BAJO	BAJO	BAJO
Gestión universitaria de RRHH	BAJO	BAJO	BAJO	BAJO	BAJO
Gestión universitaria económica	BAJO	BAJO	BAJO	BAJO	BAJO
Gestión universitaria del registro	MEDIO	MEDIO	BAJO	MEDIO	MEDIO
Administración electrónica (ESTELA + Reg. Telemático)	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO
Secretaría virtual (SEVIUS)	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO
Automatrícula	BAJO	BAJO	BAJO	BAJO	BAJO
Gestión de acceso empresas externas	BAJO	BAJO	BAJO	BAJO	BAJO
Servicio de información a Dirección	BAJO	BAJO	BAJO	BAJO	BAJO
Impresión masiva	BAJO	BAJO	BAJO	BAJO	BAJO
Gestión de PA y PD ALGIDUS	BAJO	BAJO	BAJO	BAJO	BAJO
Portal de Gestión Enseñanza Virtual (EV)	BAJO	BAJO	BAJO	BAJO	BAJO
Gestión del Archivo General	BAJO	BAJO	BAJO	BAJO	BAJO
Videoconferencia y Access Grid	BAJO	BAJO	BAJO	BAJO	BAJO
Portal de la Universidad de Sevilla	BAJO	BAJO	BAJO	BAJO	BAJO
Consigna de ficheros	BAJO	BAJO	BAJO	BAJO	BAJO
Descarga de Software	BAJO	BAJO	BAJO	BAJO	BAJO
Alojamiento de Páginas WEB	BAJO	BAJO	BAJO	BAJO	BAJO
Aplicaciones WEB	BAJO	BAJO	BAJO	BAJO	BAJO
Gestor Documental (Alfresco)	BAJO	BAJO	BAJO	BAJO	BAJO
Portal OpenCourseWare (OCW)	BAJO	BAJO	BAJO	BAJO	BAJO
Entorno de Hosting Virtual de Dominios de Correo Externo	BAJO	BAJO	BAJO	BAJO	BAJO
Servicio de Hosting Virtual Investigación	BAJO	BAJO	BAJO	BAJO	BAJO
Servicio de clonación (PC's y PIU's)	BAJO	BAJO	BAJO	BAJO	BAJO
Servicio de alojamiento de aplicaciones y/o bases de datos	BAJO	BAJO	BAJO	BAJO	BAJO

Servicio de Informática y Comunicaciones (S.I.C.)

Modelo de activos



Algunas fechas claves en el proceso: a partir del 17/01/2013

- Se inicia el proceso de elaboración del informe de estado en relación al cumplimiento del E.N.S., enviándose a Nextel información sobre cifrado de cintas de backup, software antivirus disponible para los equipos de PAS y PDI, gestión de incidencias de LOPD, etc.

- Se hace la valoración de las medidas de seguridad, detectándose las principales carencias y presentándose de forma cuantitativa, de acuerdo a los criterios básicos de valoración propuestos por la metodología Mageri.

- Primer borrador del Informe de Estado (primer "entregable" de los que consta el proyecto) 07/03/2013, que como en el caso de la valoración de los servicios da lugar a múltiples comentarios y modificaciones hasta que por fin se obtiene el documento final, cuyo resumen se adjunta:

Informe de estado

Código	Medida de seguridad	Valor actual	Valor objetivo	Nivel cumplimiento
C:org	Marco organizativo	30%	90%	34%
C:op	Marco operacional	62%	69%	68%
op.pl	Planificación	66%	76%	68%
op.acc	Control de acceso	67%	83%	81%
op.exp	Explotación	65%	84%	77%
op.ext	Servicios externos	76%	90%	84%
op.cont	Continuidad del servicio	100%	33%	100%
op.mon	Monitorización del sistema	NA%	NA%	NA
C:mp	Medidas de protección	55%	80%	69%
mp.if	Protección de las instalaciones e infraestructuras	93%	86%	100%
mp.per	Gestión del personal	50%	74%	68%
mp.eq	Protección de los equipos	10%	68%	12%
mp.com	Protección de las comunicaciones	95%	86%	100%
mp.si	Protección de los soportes de información	50%	81%	62%
mp.sw	Protección de las aplicaciones informáticas (SW)	30%	90%	34%
mp.info	Protección de la información	32%	75%	43%
mp.s	Protección de los servicios	81%	82%	98%

NIVEL	EXPLICACIÓN
L0 (Nivel 0)	Inexistente. No hay ningún tipo de evidencia suficientemente significativa del aspecto evaluado, o esta es anecdótica.
L1 (Nivel 1)	Inicial / Ad-Hoc. Los aspectos evaluados se llevan a cabo de forma muy puntual, dependiendo de quién y cuándo lo ejecuta.
L2 (Nivel 2)	Repetible. Se han identificado medidas que se llevan a cabo, en general, de manera sistemática, aunque no existe una regulación formal al respecto. La sistematización se debe a la repetición.
L3 (Nivel 3)	Definido. Las medidas identificadas se llevan a cabo de acuerdo a una regulación específica que determina cómo deben ser, de modo que todo el mundo lo cumpla. Pueden existir aspectos puntuales no completamente cubiertos.
L4 (Nivel 4)	Gestionado y medible. Las medidas identificadas se aplican de forma sistemática y controlada, existiendo indicadores que determinan la bondad de los mismos.
L5 (Nivel 5)	Optimizado. Se lleva a cabo una gestión completa de las medidas identificadas, que han sido mejoradas a partir de los resultados de las mediciones efectuadas.

Algunas fechas claves en el proceso: a partir del 17/01/2013

-Aunque siempre se podrá ver la botella medio vacía, es claro que los resultados, en general, no son muy desalentadores.

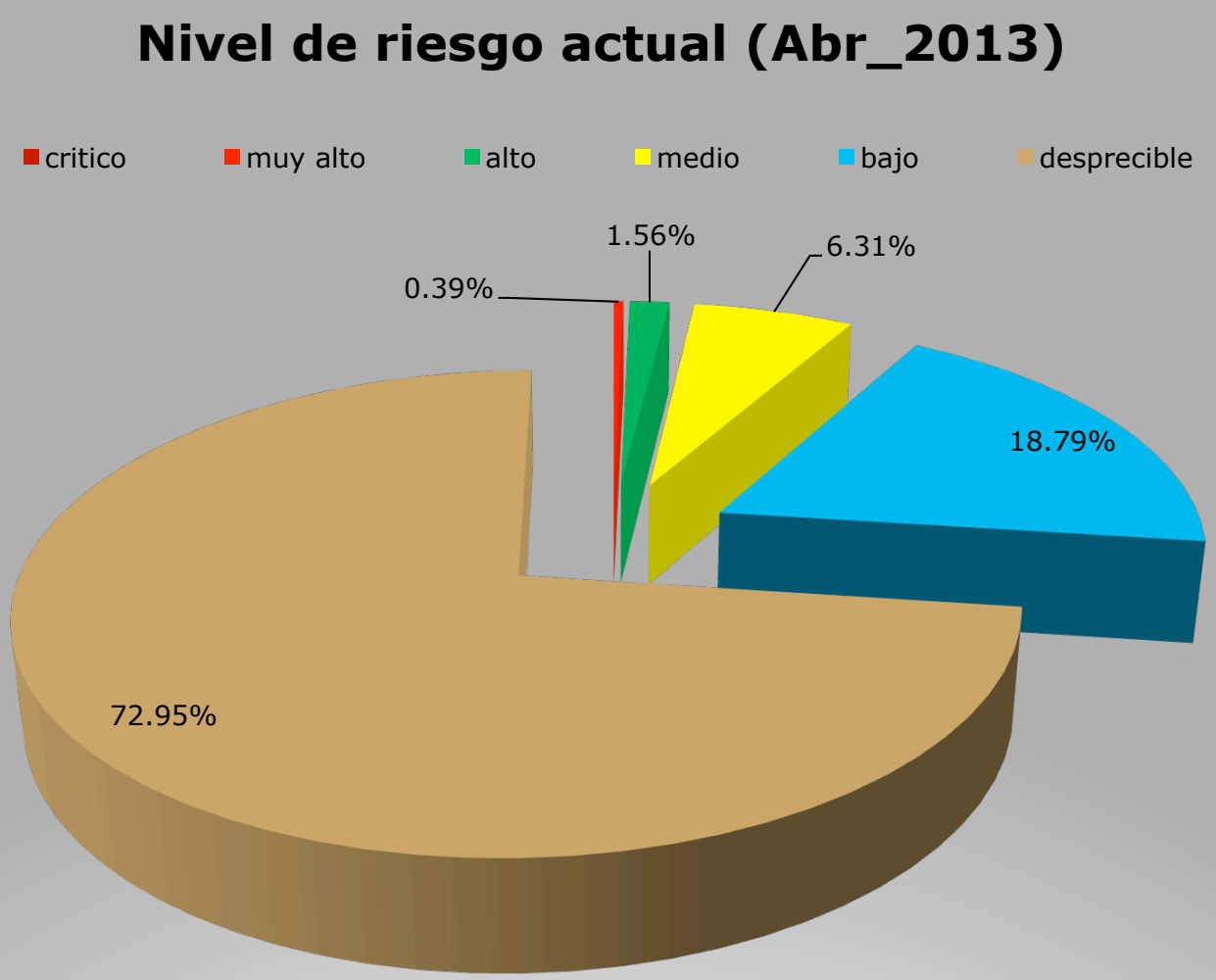
-Nextel ofrece realizar en esta fase una tarea, que aunque prevista para la fase 2, puede ser de utilidad para comparar resultados: el análisis de riesgo

-Esto último no comportará coste adicional alguno.

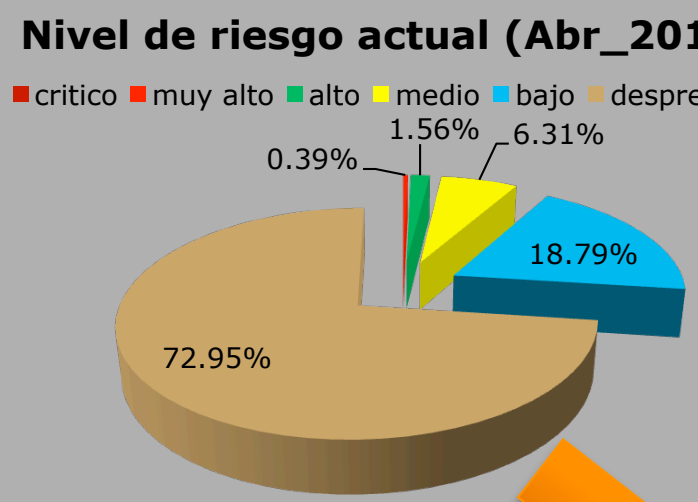
-Para ello se partirá del análisis de riesgo existente, resultado del Plan de Contingencia del S.I.C. y del fichero PILAR, que ya teníamos.

-Tras otra tanda de correciones al borrador por parte del Comité de Dirección del S.I.C., se recibe el documento definitivo, el 22/04/2013, cuyo resumen es el que aparece a continuación:

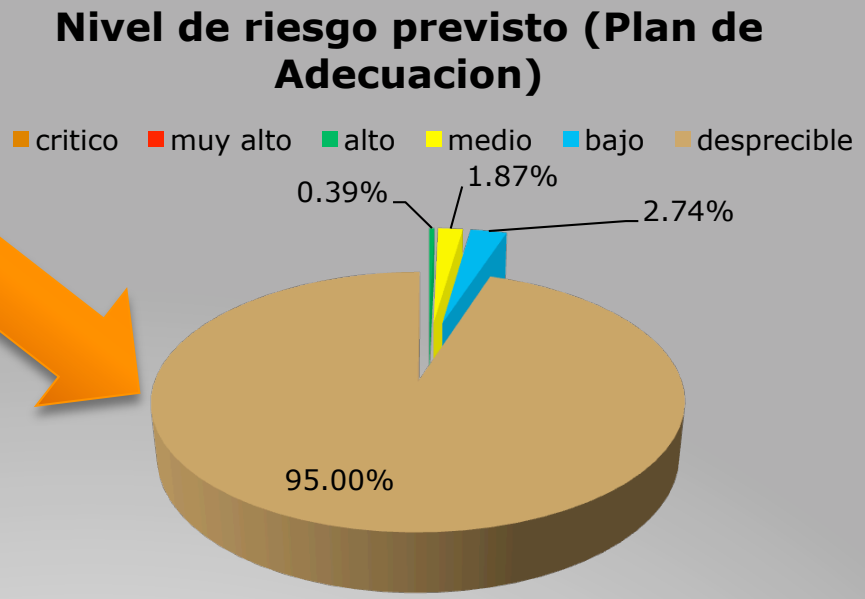
Análisis de riesgo



Previsiones en el Análisis de riesgos



Implantación del Plan de Adecuación



Algunas fechas claves en el proceso: a partir del 17/01/2013

- El 27/03/2013 se recibe el primer borrador del Plan de Adecuación, que como todos los demás borradores es analizado a fondo por el Comité.

-En él, aunque se hace una estimación temporal de 310 jornadas, no se contempla aún planificación reflejada en un diagrama de Gantt, entre otras razones porque:

- Hay que definir una posible fecha de inicio para la fase de Implantación.
- Hay que decidir si se pretende un Plan de Adecuación "realista" o "cumplidor de los plazos oficiales". Nos quedan unos 8 meses, pero lo más objetivo es pensar en un año.
- ¿Definimos nosotros el criterio de priorización de tareas o estudiamos uno propuesto?.

Algunas fechas claves en el proceso: a partir del 17/01/2013

- Nextel, que ha desarrollado un trabajo magnífico, envía informe auxiliar sobre cómo desarrollar algunas de las medidas del plan de adecuación. Este informe había sido solicitado por el Director del STIC.

- En el se analizan implicaciones de toda índole derivadas de la aplicación de las medidas de seguridad resultantes de la implantación del Plan de Adecuación, entre las que cabe destacar:
    - Medidas organizativas.
    - Medidas de seguridad de los usuarios.
    - Medidas técnicas de seguridad:
        - Limpieza de metadatos.
        - Cifrado de medios de usuario.
        - Reconfiguración de los sistemas.
        - Gestión de accesos y claves.
        - Red de comunicaciones.

18/07/2013

Finaliza el proyecto de diseño del Plan de Adecuación.

¿Pero está aprobado?
¿Quién lo va a aprobar?
¿Cómo se va a implantar?
¿Implica su no aprobación inicial que no pueda ir desarrollándose?

¿Pero está aprobado?

Es evidente que no, pero no obstante pueden empezarse a dar los pasos para conseguir su aprobación, a ser posible por las más altas instancias:

Rector o Consejo de Gobierno.

El Director del S.T.I.C, asume la tarea de informar y conseguir su aprobación.

¿Cómo se va a implantar?

La experiencia del proceso anterior nos índica claramente las dificultades que ha habido tanto económicas, que se agudizarán, como de recursos humanos dedicados, prácticamente ha sido el Comité de Dirección el que ha realizado la mayor parte de las tareas en nuestra institución, por lo que seguirá siendo necesaria una colaboración externa.

¿Implica el que no esté aprobado que no se pueda ir desarrollando?

Rotundamente, NO.

Es evidente que más tarde o más temprano se aprobará y que hay aspectos de la implantación que se pueden ir definiendo y desarrollando, entre otras razones porque mientras más claros y simplificado estén, será más fácil transmitirlos a los responsables de su aprobación.

Algunas fechas claves en el proceso:

entre el 18/07/2013 y el 26/02/2014

A partir del 18/07/2013

Por lo tanto, definido el Plan de Adecuación lo más lógico es continuar desarrollando el proceso con la definición clara de una Política de Seguridad, en la que se establezca claramente:

-Alcance de la misma, en cuanto al ámbito de aplicación y de inclusión o exclusión en o de ella.

-Marco normativo aplicable, que será de ámbito estatal, autonómico e interno.

-Organización de la seguridad, con la definición de los comités y roles específicos, en especial la Comisión de Seguridad y los Responsables de la Información, del Servicio, de la Seguridad y de los Sistemas

A partir del 18/07/2013

Se elabora un borrador en el que se detallan los tres puntos antes enumerados y se definen todos los aspectos de la Política de Seguridad según exige el E.N.S.

Este borrador se presenta y aprueba como tal, para su posterior presentación y aprobación formal, en una reunión presidida por el Vicerrector de Infraestructuras y en la que participan entre otros el Gerente y la Secretaría General.

Por la importancia que tienen en el proceso, se detallan los puntos más significativos, en especial la definición de roles y la asignación de responsabilidades, bajo el epígrafe de la organización de la seguridad.

Organización de la Seguridad (I)

- Que garantice que todas la etapas del ciclo de protección de la información, se lleven a cabo de forma apropiada, a la vez que se asegure una asignación adecuada de las responsabilidades, para lo que se definen:

- **Comisión de la Seguridad de la Información.**
- **Responsable de la Información.**
- **Responsable del Servicio.**
- **Responsable de la Seguridad.**
- **Responsables del Sistemas.**

Organización de la Seguridad (II)

- **Comisión de la Seguridad de la Información**, es el órgano de gestión interna al que compete la Seguridad de la Información en la US, compuesta por:

- **- Vicerrector o Vicerrectora de Infraestructura**, como presidente.
- **- Gerente**.
- **- Secretaria o Secretario General**.
- **- Máximo responsable de los Servicios Jurídicos**.
- **- Responsable de la Seguridad**.
- **- Responsables de los Sistemas**.
- Todas las funciones de esta Comisión se recogen en el documento.

Organización de la Seguridad (III)

- **Responsable de la Información**, su figura recaerá en la Comisión de Seguridad de la Información, desarrolla las funciones y responsabilidades siguientes:

- - Establecer los **requisitos de seguridad** que se han de garantizar.
- - Valorar las diferentes **implicaciones de seguridad** (autenticidad, confidencialidad, disponibilidad, integridad y trazabilidad) derivadas de **cada información** que se contemple en el análisis de riesgos.
- - En colaboración con los Responsables de Seguridad y de los Sistemas **mantener los sistemas** catalogados en el Anexo I del E.N.S..
- - **Asegurar la inclusión** de cláusulas sobre seguridad en la contratación con terceros y **velar por su cumplimiento**.

Organización de la Seguridad (IV)

- **Responsable del Servicio**, su figura recaerá en la Comisión de Seguridad de la Información, desarrolla las funciones y responsabilidades siguientes:

- - Establecer los **requisitos** de los servicios en **materia de seguridad** que se han de garantizar.
- -Valorar las diferentes **implicaciones de seguridad** (autenticidad, confidencialidad, disponibilidad, integridad y trazabilidad) derivadas de **cada servicio** que se contemple en el análisis de riesgos.
- - En colaboración con el Responsable de Seguridad **mantener los sistemas** catalogados en el Anexo I del E.N.S.

Organización de la Seguridad (V)

- **Responsable de la Seguridad**, su figura recaerá en el Dtor. del Secretariado de Tecnologías de la Información y las Comunicaciones, desarrolla las **funciones y responsabilidades derivadas de la aplicación técnica del E.N.S. a la información manejada y los servicios prestados por los sistemas TIC**.
- - Como secretario de la Comisión, **elabora los informes** periódicos:
  - * Resumen consolidado del **estado de desarrollo** del Plan de Adecuación.
  - * Resumen consolidado de **incidentes de seguridad registrados** desde la última reunión de la Comisión.
  - * Valoración del **estado de seguridad de los sistemas** afectados por el E.N.S. y **evolución de los niveles de riesgo** a los que se exponen.
  - * Resumen consolidado de los **procedimientos de seguridad aprobados** por el Responsable de Seguridad desde la última reunión de la Comisión.
- - Actuará como secretarios del Comité de Seguridad de la Información.

Organización de la Seguridad (y VI)

- **Responsables de los Sistemas**, serán los Directores de Área del S.I.C., desarrollarán dentro de su ámbito de competencias las funciones y responsabilidades derivadas de la aplicación técnica del E.N.S. a la información manejada y los servicios prestados **en el desarrollo diario de la actividad de los sistemas TIC en sus múltiples facetas**.

- **Procedimiento de designación**, el desempeño de las responsabilidades derivadas de esta Política de Seguridad y del E.N.S., se determinará por el **acceso a los diferentes cargos o destinos**, estatutarios o no, vinculadas a ellas.

- En estos avatares, el 30/10/2013, me operan de desprendimiento de retina ¿Es culpa de los trabajos? No, es mala suerte ☺

Algunas fechas claves en el proceso:

el 26/02/2014

En Consejo de Gobierno se aprueban el Plan de Adecuación y la Política de Seguridad de acuerdo a las exigencias del E.N.S.

Algunas fechas claves en el proceso: a partir del 26/02/2014

¿Qué queda ahora?
y
¿Qué se ha hecho?

Etapas y Fases del proyecto (S.I.C.)

ETAPAS PROYECTO		
Etapa II – Desarrollo del Plan de Adecuación	Fase III – Adecuación	• Implementación del Plan de Adecuación definido
	Fase IV - Despliegue	• Afianzamiento medidas de seguridad definidas en fase de adecuación

Desarrollo del Plan de Adecuación al E.N.S.

- Informe de Análisis de Riesgos
- Declaración de Aplicabilidad
- Política de Seguridad
- Documentos de Seguridad
- Documentación Operacional
- Especificaciones Técnicas de Seguridad
- Plan de Formación
- Plan de Mantenimiento, Revisión y auditoría
- Cuadro de Mando
- Informe de Auditoría

A partir del 26/02/2014

El mismo día 26 envío un borrador de "Normativa del uso de la Red y las Comunicaciones", dentro de los pasos a seguir según exige el E.N.S., para su estudio por el Comité y aprobación por el órgano correspondiente.

A primeros de marzo se nombra nueva Directora del S.T.I.C. pasando el anterior Director a Vicerrector de Infraestructuras, lo que va a influir en el devenir del proyecto.

Posteriormente el borrador se refunde en otro denominado "Normas de uso de las Redes de Comunicaciones", tomando la referencia del documento de las Normas de Seguridad en el E.N.S., y se pasa a su estudio por el Comité, ya dirigido por la nueva Directora.

A partir del 26/02/2014

Ya con antelación a la fecha de la aprobación, finales de enero, se habían empezado los contactos con las empresas que podían darnos soporte para la Implantación del Plan de Adecuación.

A pesar de que como dije antes Nextel había hecho un trabajo muy bueno, la cuantía del proyecto a desarrollar ahora, Implantación, independiente del anterior, exige que haya un procedimiento negociado y por lo tanto varias ofertas para su estudio.

Nos ponemos en contacto con Isotrol, Nextel, Sinergy y Start up, ya se han recibido las ofertas y se está con el estudio correspondiente y con la negociación; pero tenemos el problema económico de siempre.

Gracias por su atención.

¿Alguna pregunta?

Gustavo A. Rodríguez (gurodri@us.es)
Dtor. Técnico Área de Comunicaciones.

Maite Sierra Macía (maite@us.es)
Jefa Sección SIC.

Servicio de Informática y Comunicaciones (S.I.C.)
Universidad de Sevilla.