UNIVERSIDAD DE ALMERÍA

Implantación ENS en la Universidad de Almería

Diego Pérez Martínez
Servicio de Tecnologías de la Información y las Comunicaciones
Oct 2017

Breve introducción al ENS

¿Qué es el Esquema Nacional de Seguridad (ENS)?

- El ENS es:
  - Un Real Decreto (RD 03/2010) que se ocupa de la protección de los sistemas de información en las administraciones públicas. Actualizado por Real Decreto 951/2015, de 23 de octubre
  - Un marco de referencia en las AA.PP. para la creación de un proceso de gestión de la seguridad de la información acorde a buenas prácticas (ISO 27000)
  - Era un complemento de la Ley 11/2007 de eAdmon

¿A quién afecta el ENS?

- El ENS afecta:
  - A todas las Administraciones Públicas
  - A los ciudadanos en su relación con las AA.PP.
  - A la relación entre las AA.PP

- OJO, pero NO a todos los sistemas de información. A todos los sistemas de información de la AA.PP. salvo aquellos:
  - No relacionados con el cumplimiento de derechos/deberes del ciudadano
  - No relacionados con el acceso por medios electrónicos a información
  - No relacionados con el procedimiento administrativo

Existen por tanto excepciones

¿Cuándo entra en vigor el ENS?

Si te estás haciendo esa pregunta … vas tarde.

Hubo diversos plazos para la adaptación, pero tras la modificación del ENS con el Real Decreto 951/2015, de 23 de octubre, el plazo de adecuación acaba el 5 de noviembre.

Particularidades de cada AAPP

El ENS es uno, pero las administraciones públicas somos muchas y muy variadas, por tanto su implantación debe ser diferente

Particularidades de cada AAPP

- La seguridad es un ente con diversas caras:
  - Confidencialidad
  - Integridad
  - Disponibilidad
  - Trazabilidad
  - Autenticidad

- Las distintas facetas de la seguridad cobran una importancia también diferente en cada organización. Ej:
  - En un banco es vital la integridad
  - En un entorno militar la confidencialidad
  - … Pero en una Universidad es muy importante la Disponibilidad

Particularidades de cada AAPP

- Cada AAPP presta un tipo diferente de servicios. Ej:
  - En una Universidad es fundamental dar acceso a su red y a Internet a sus alumnos.
  - Eso es algo de lo que no debe preocuparse por ejemplo un Ministerio.
  - Ese servicio puede conllevar implicaciones de seguridad. Ej: Tienes personas externas a tu organización en tu red

Particularidades de cada AAPP

- No son comparables las consecuencias de un incidente de seguridad en un colegio público o en el Ministerio de Defensa.
- Por tanto la categorización de los niveles de seguridad de sus sistemas son muy diferentes.

Particularidades de cada AAPP

- La organización interna de cada AAPP es distinta.
- En algunos casos hay una estructura jerárquica piramidal clásica muy clara. Ej: Un Ministerio
- En otras administraciones, como una Universidad, la jerarquía es menos clara

Por todo ello:

El ENS es uno, pero las administraciones públicas somos muchas y muy variadas, por tanto su implantación debe ser diferente

El proyecto de adecuación al ENS en la UAL

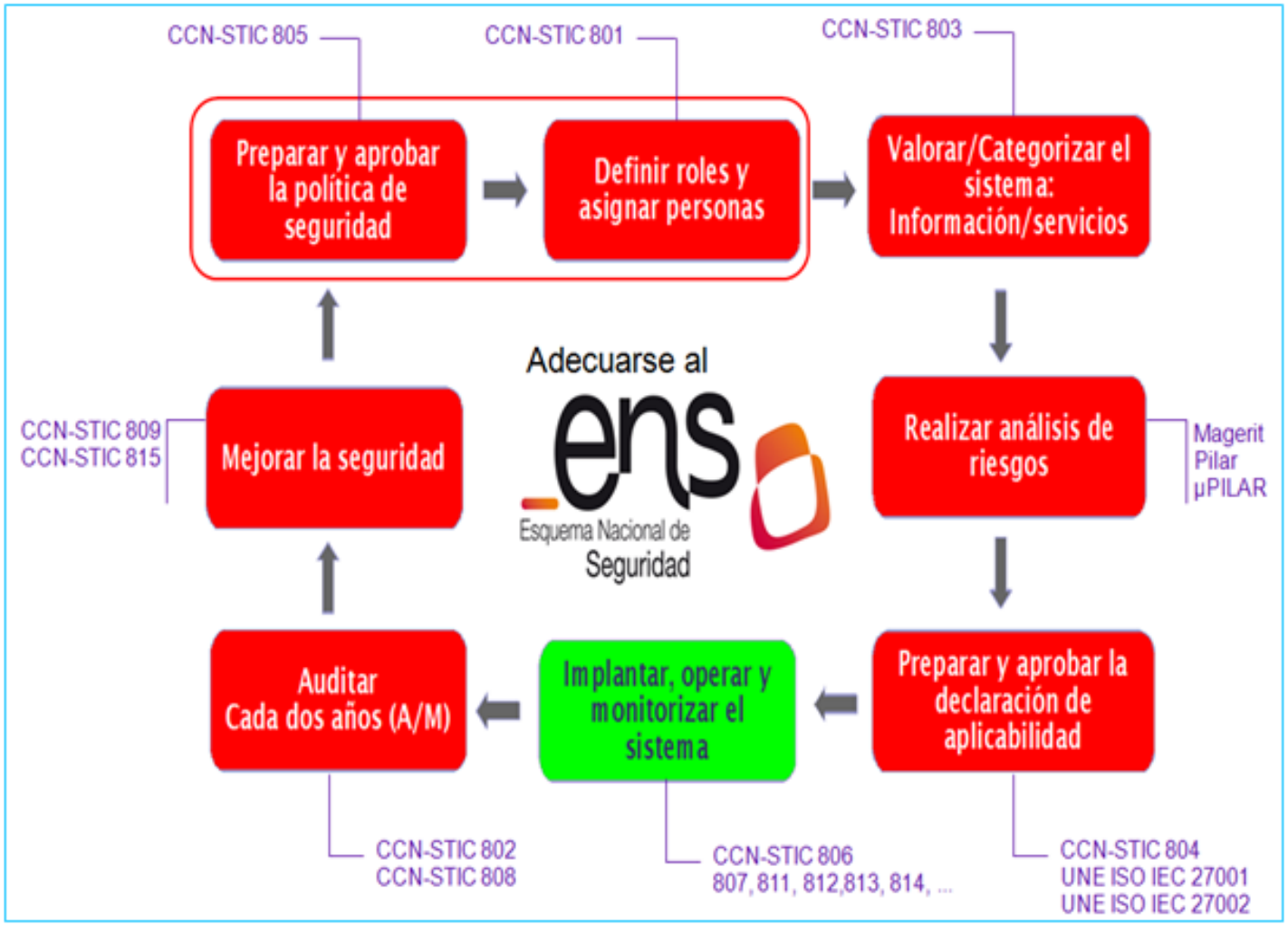
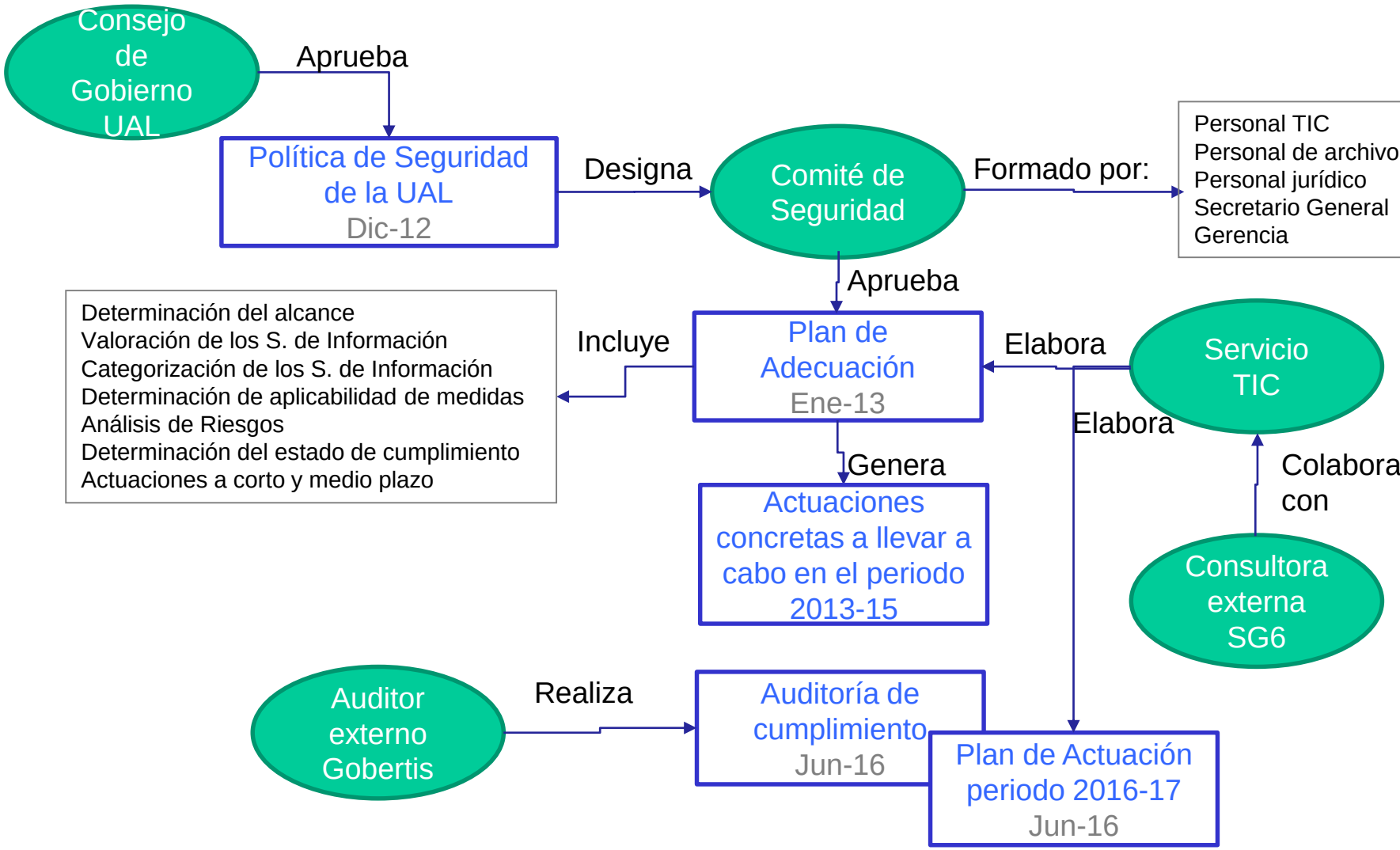


Figura: Adecuación al Esquema Nacional de Seguridad.


Consejo de Gobierno UAL
Aprueba
Política de Seguridad de la UAL
Dic-12
Designa
Comité de Seguridad
Formado por:
Personal TIC
Personal de archivo
Personal jurídico
Secretario General
Gerencia
Aprueba
Determinación del alcance
Valoración de los S. de Información
Categorización de los S. de Información
Determinación de aplicabilidad de medidas
Análisis de Riesgos
Determinación del estado de cumplimiento
Actuaciones a corto y medio plazo
Incluye
Plan de Adecuación
Ene-13
Elabora
Servicio TIC
Elabora
Genera
Actuaciones concretas a llevar a cabo en el periodo 2013-15
Colabora con
Consultora externa SG6
Auditor externo Gobertis
Realiza
Auditoría de cumplimiento
Jun-16
Plan de Actuación periodo 2016-17
Jun-16

El proyecto de adecuación al ENS en la UAL

- Inicio en marzo de 2012
- Participan: Vicerrectorado TIC y empresa consultora externa (SG6)
- Objetivo principal: Cumplir con la legalidad desarrollando un plan de adecuación al ENS.
- Objetivos secundarios o beneficios derivados del objetivo principal:
  - Desarrollo de un marco procedimental
  - Identificación y catalogación del sistema de información
  - Realización de análisis de riesgos
  - Identificación de insuficiencias y aspectos de mejora

El proyecto de adecuación al ENS en la UAL

- Principales resultados:
  - Política de Seguridad. Aprobada por Consejo de Gobierno en dic-2012. Incluye:
    - Definición del alcance, es decir, de los sistemas de información sobre los que aplica
    - Propuesta de nombramiento del Comité de Seguridad. Ya en funcionamiento previo por la LOPD. Miembros con perfil técnico, jurídico y de responsabilidad en la organización.
    - Propuesta de nombramiento del resto de figuras que aparecen en el RD: responsables de información, de sistema, de seguridad, etc.
  - Plan de Adecuación acorde al RD 3/2010. Aprobado en enero de 2013 por el Comité de Seguridad.
  - Publicitar en sede electrónica política de seguridad y plan de adecuación

El Plan de Adecuación al ENS

- Proceso desarrollado según la guía CCN-STIC 806 del Centro Criptológico Nacional.
  1. Determinación del alcance
  2. Identificación y valoración de los servicios de información de la UAL
  3. Categorización (agrupación de los servicios)
  4. Determinación de la aplicabilidad de las medidas del ENS a nuestros sistemas
  5. Análisis de riesgos de los sistemas de la UAL
  6. Determinación del estado en ese momento de cumplimiento de las medidas de seguridad del ENS
  7. Selección de las medidas de seguridad a implantar en los próximos 3 años

Plan de Adecuación al ENS.
Paso 1: Determinación del Alcance

- Se incluyen en el alcance
  - Servicios relacionados con el ejercicio de los derechos del ciudadado. (servicios referidos por la ley 11/2007)
  - Otros servicios de especial interés para la UAL (web y docencia virtual)

UNIVERSIDAD DE ALMERÍA

Plan de Adecuación al ENS.
Paso 2: Identificación y valoración de los servicios de información de la UAL

Servicio	Confidencialidad	Integridad	Autenticidad	Trazabilidad	Disponibilidad	Nivel Global
Gestión Académica	Medio	Medio	Medio	Medio	Bajo	Medio
Gestión Económica	Bajo	Medio	Medio	Medio	Bajo	Medio
Gestión de RRHH	Medio	Medio	Medio	Medio	Bajo	Medio
Gestión de la Investigación	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
Campus Virtual	Bajo	Medio	Medio	Bajo	Bajo	Medio
Web Institucional	Sin Valorar	Medio	Medio	Sin Valorar	Medio	Medio
Administración Electrónica	Medio	Medio	Medio	Medio	Bajo	Medio
Servicio de Atención al Usuario	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
Servicio de Calidad	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
Gestión de Espacios	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
Docencia Virtual	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo

Plan de Adecuación al ENS.
Paso 3: Categorización
(Agrupación de servicios en sistemas)

Sistema	Servicio	Aplicabilidad ENS
Sistema ERP	Gestión Académica	Aplica
Sistema ERP	Gestión Económica	Aplica
Sistema ERP	Gestión de RRHH	Aplica
Sistema ERP	Gestión de la Investigación	Aplica
Sistema ERP	Campus Virtual	Aplica
Sistema AE	Administración Electrónica	Aplica
Sistema Web Institucional	Web Institucional	Extensión
Sistema Servicios Universitarios	Servicio de Atención al Usuario	Aplica
Sistema Servicios Universitarios	Servicio de Calidad	Aplica
Sistema Servicios Universitarios	Servicio de Gestión de Espacios	Aplica
Sistema Servicios Universitarios	Servicio de Docencia Virtual	Aplica

Sistema	Confidencialidad	Integridad	Autenticidad	Trazabilidad	Disponibilidad	Nivel Global
Sistema ERP	Medio	Medio	Medio	Medio	Bajo	Medio
Sistema AE	Medio	Medio	Medio	Medio	Bajo	Medio
Sistema WEB	Sin Valorar	Medio	Medio	Sin Valorar	Medio	Medio
Sistema SU	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo

Plan de Adecuación al ENS.
Paso 3: Determinar la aplicabilidad de las medidas de seguridad del ENS a los sistemas de información de la UAL

En función de la valoración de las dimensiones de la seguridad de cada sistema, y acorde a lo indicado en el Anexo II del RD 3/2010, se determinan las medidas de seguridad a aplicar a cada sistema

Plan de Adecuación al ENS.
Paso 4: Realización de un análisis de riesgos
(con la herramienta PILAR del CCN)

- 1 Sistema de información está formado por X activos (redes, servidores, software, bases de datos, …)
- Para cada activo, PILAR, propone posibles riesgos y el STIC ha evaluado su probabilidad
- En función de la exposición a cada riesgo de cada activo de un sistema, se obtiene un valor que es el riesgo de ese sistema

Plan de Adecuación al ENS.
Paso 5: Determinación del estado actual

- Para cada medida de seguridad del Anexo II del ENS se ve la situación respecto a ella de los sistemas de información de la UAL
- En base a ese estudio se determinan las medidas de seguridad que se deben abordar a corto y medio plazo

Medidas a aplicar

- Durante 2013

org.3	Procedimientos de seguridad
op.pl.2	Arquitectura de seguridad
op.pl.3	Adquisición de nuevos componentes
op.pl.4	Dimensionamiento / Gestión de capacidades
op.acc.6	Acceso local (local logon)
mp.per.4	Formación
mp.eq.2	Bloqueo del puesto de trabajo
mp.info.2	Calificación de la información
mp.s.2	Protección de servicios y aplicaciones web
mp.s.8	Protección frente a la denegación de servicio

- En 2014 y 2015

op.ext.2	Gestión diaria
op.acc	Controles de acceso
op.ext	Servicios externos
mp.si	Medidas de protección de los soportes de información
mp.info	Medidas de limpieza de información y calificación de la información

Auditoría externa LOPD y ENS

- Realizada en junio de 2016. El auditor detecta medidas de seguridad que no se cumplen o que no se cumplen totalmente y genera las no conformidades correspondientes
- La UAL elabora un nuevo Plan de Actuación para subsanar las no conformidades
  - Recatalogación de sistemas y por tanto nuevo catálogo de medidas a aplicar
  - En la actualidad se trabaja en las medidas de ese plan de actuación

UNIVERSIDAD DE ALMERÍA

PROPUESTA DE ACTUACIÓN
Listado de acciones concretas a llevar a cabo

Nombre	Descripción	Corrige	Prioridad	Ejecuta	Aprueba
Recatalogación	Catalogar el sistema de información como de nivel básico, modificando la catalogación del sistema, la declaración de aplicabilidad de medidas y el análisis de riesgos de la organización.	NC01 NC09 (más algunas de las mejoras propuestas por el auditor)	1	STIC	Secretario General y Gerente
Procedimientos	Redacción y aprobación de procedimientos de seguridad siguiendo el modelo de las guías CCN-STIC	NC02 NC03 NC04 NC05 NC14	2	STIC	STIC
Registros	Definir cuál debe ser el nivel de trazabilidad para los sistemas de información, tomando como base los resultados del análisis de riesgos, y aplicarlo en sus servicios y aplicaciones afectadas por el cumplimiento del ENS	NC07 (más registro de accesos LOPD)	3	STIC	STIC
Notificación de deberes	Elaborar Deberes y Obligaciones del personal (en concreto clausulas de confidencialidad) y establecer el mecanismo para que sean aceptadas por los usuarios	NC10	3	STIC + GabJur	Comité segur.
Formación	Establecer un plan de concienciación a todo el personal de la UAL. Establecer un plan de formación a los trabajadores del STIC.	NC11 NC12	2	STIC	Comité segur. (STIC para plan de formación de su personal)
Recatalogación	Proponer una reducción del nivel de los ficheros al Comité de Seguridad para que sea valorada sus miembros.	Nivel Ficheros	3	Gabjur	Comité segur.

- Tras la última auditoría, en la actualidad se trabaja en:
  - Creación de nuevos procedimientos: de gestión de usuarios, de copias de respaldo y de clasificación y tratamiento de la información clasificada
  - Mejora de los sistemas de identificación de usuarios, eliminando por ejemplo cuentas genéricas

Estado actual

- El Centro Criptológico Nacional realizó en 2016 un estudio sobre cumplimiento del ENS en las Universidades Españolas.
- La Universidad de Almería alcanza un honroso 15º puesto entre las 50 Universidades públicas españolas, por delante de grandes potencias del Sistema Universitario Español.

Universidad	Comunidad Autónoma	Índice de Cumplimiento	Índice de Madurez
Universidad Rovira i Virgili	Cataluña	96%	92%
Universidad de Granada	Andalucía	95%	90%
Universidad de Burgos	Castilla y León	92%	84%
Universidad de Valencia	Comunidad Valenciana	89%	80%
Universidad Jaime I de Castellón	Comunidad Valenciana	87%	78%
UNED	Estado	80%	81%
Universidad de Málaga	Andalucía	75%	68%
Universidad de La Rioja	La Rioja	72%	70%
Universidad de Sevilla	Andalucía	66%	62%
Universidad Miguel Hernández	Comunidad Valenciana	65%	61%
Universidad Pompeu Fabra	Cataluña	63%	63%
Universidad de Jaén	Andalucía	61%	52%
Universidad País Vasco EHU - UPV	País Vasco	60%	57%
Universidad de Salamanca	Castilla y León	58%	55%
Universidad de Almería	Andalucía	56%	53%
Universidad Las Palmas de Gran Canaria	Islas Canarias	54%	49%
Universidad Rey Juan Carlos	Madrid, Comunidad de	54%	47%
Universidad Autónoma de Madrid	Madrid, Comunidad de	54%	47%
Universidad Politécnica de Cartagena	Murcia, Región de	53%	52%
Universidad Politécnica de Valencia	Comunidad Valenciana	51%	50%
Universidad de Alicante	Comunidad Valenciana	50%	47%

- Cuando finalicen las actuaciones que se están llevando a cabo en la actualidad esperamos seguir escalando algún puesto en esa clasificación

Gracias por vuestra atención

Diego Pérez Martínez
dperez@ual.es
Director del Servicio TIC
Universidad de Almería

UNIVERSIDAD DE ALMERÍA