Boletín Oficial de la Universidad de Jaén

Año XV – Número 114 – marzo y abril de 2015

I. ACUERDOS Y RESOLUCIONES DE LOS ÓRGANOS DE GOBIERNO

- Consejo de Gobierno nº 51
  26 de marzo de 2015

II. NOMBRAMIENTOS

- Personal de Administración y Servicios
- Personal Docente e Investigador

III. CONCURSOS Y OPOSICIONES

- Personal de Administración y Servicios
- Personal Docente e Investigador

IV. PUBLICADO EN OTROS BOLETINES OFICIALES

- Boletín Oficial del Estado
- Boletín Oficial de la Junta de Andalucía

V. INFORMACIÓN DE INTERÉS PARA LA COMUNIDAD UNIVERSITARIA

- Anuncios

∗ **Pulsar con el botón izquierdo del ratón sobre el apartado al que quiera ir y le llevará automáticamente**

I. ACUERDOS Y RESOLUCIONES DE LOS ÓRGANOS DE GOBIERNO

CONSEJO DE GOBIERNO

(Sesión extraordinaria nº 51)

Acuerdo del Consejo de Gobierno de la Universidad de Jaén, de 26 de marzo, por el que se aprueba el Documento de Seguridad para Ficheros de Datos de Carácter Personal de la Universidad de Jaén (Anexo 3)

Acuerdo del Consejo de Gobierno de la Universidad de Jaén, de 26 de marzo, por el que se conocen los Convenios suscritos por la Universidad de Jaén (Anexo 4)

INICIO SUBIR

II. NOMBRAMIENTOS

PERSONAL DE ADMINISTRACIÓN Y SERVICIOS

PERSONAL DOCENTE E INVESTIGADOR

INICIO SUBIR

III. CONCURSOS Y OPOSICIONES

PERSONAL DE ADMINISTRACIÓN Y SERVICIOS

Resolución de 7 de abril de 2015, de la Universidad de Jaén, por la que se convoca concurso público para la adjudicación de un contrato en régimen laboral con duración temporal, en la categoría profesional de Titulado Superior (perfil: cooperación internacional y desarrollo).

BOJA número 69, de 13/04/2015, páginas 20 a 24

PERSONAL DOCENTE E INVESTIGADOR

INICIO SUBIR

IV. PUBLICADO EN OTROS BOLETINES OFICIALES

BOLETÍN OFICIAL DEL ESTADO

Disposiciones y Resoluciones de interés publicadas en el BOE:

Resolución de 2 de marzo de 2015, de la Secretaría de Estado de Educación, Formación Profesional y Universidades, por la que se publica el importe de la compensación a las universidades públicas por la reducción de precios por servicios académicos a estudiantes pertenecientes a familias numerosas de tres hijos, del curso académico 2013-2014.

BOE número 62 de 13/03/2015, páginas 23503 a 23504

Resolución de 16 de marzo de 2015, de la Secretaría de Estado de Educación, Formación Profesional y Universidades, por la que se conceden ayudas de precios públicos por matrícula en programas de doctorado a beneficiarios de ayudas de Formación de Profesorado Universitario, correspondientes al curso 2013-2014

BOE número 68 de 20/03/2015, páginas 24844 a 24859

Resolución de 9 de febrero de 2015, de la Secretaría General de Universidades, por la que se publica el Acuerdo del Consejo de Ministros de 30 de enero de 2015, por el que se modifican determinados Acuerdos del Consejo de Ministros por los que se establece el carácter oficial de determinados títulos de Grado, Máster y Doctor y su inscripción en el Registro de Universidades, Centros y Títulos

BOE número 73 de 26/03/2015, páginas 26042 a 26067

Resolución de 6 de marzo de 2015, de la Dirección General de Política Universitaria, por la que se publica el Acuerdo de la Comisión Permanente del Consejo de Universidades por el que se designan miembros de las comisiones de acreditación nacional.

BOE número 74 de 27/03/2015, páginas 26503 a 26509

Resolución de 24 de marzo de 2015, de la Secretaría de Estado de Educación, Formación Profesional y Universidades, por la que se conceden ayudas por matrícula en programas de doctorado a beneficiarios del subprograma de formación del profesorado universitario, correspondientes al curso 2014-2015.

BOE número 77 de 31/03/2015, páginas 27372 a 27415

Resolución de 22 de abril de 2015, de la Dirección General de Investigación Científica y Técnica, por la que se publican las ayudas y subvenciones concedidas en el primer trimestre de 2015.

BOE número 103 de 30/04/2015, páginas 37946 a 37987

BOLETÍN OFICIAL DE LA JUNTA DE ANDALUCIA

Disposiciones y Resoluciones de interés publicadas en el BOJA:

Resolución de 24 de marzo de 2015, del Instituto de Estadística y Cartografía de Andalucía, por la que se publica el convenio de colaboración para la transmisión de información entre la Universidad de Jaén y el Instituto de Estadística y Cartografía de Andalucía para el desarrollo de actividades estadísticas contenidas en el Plan Estadístico y Cartográfico de Andalucía 2013-2017

BOJA número 63 de 01/04/2015, páginas de 147 a 149

Acuerdo de 17 de marzo de 2015, del Consejo de Gobierno, por el que se autoriza la modificación del Convenio-Marco suscrito entre las Consejerías de Salud y Educación y Ciencia y las Universidades de Almería, Cádiz, Córdoba, Granada, Huelva, Jaén, Málaga y Sevilla, para la utilización de las instituciones sanitarias en la investigación y la docencia.

BOJA número 66 de 08/04/2015, páginas de 30 a 33

Decreto 121/2015, de 7 de abril, por el que se declara el cese de don Manuel Parras Rosa como Rector Magnífico de la Universidad de Jaén. (BOJA número 67 de 09/04/2015, página 97)

De conformidad con lo establecido en el artículo 20.2 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y en el artículo 52.5 de los Estatutos de la Universidad de Jaén, aprobados por Decreto 230/2003, de 29 de julio, a propuesta del Consejero de Economía, Innovación, Ciencia y Empleo, y previa deliberación del Consejo de Gobierno en su reunión del día 7 de abril de 2015,

DISPONGO

Artículo único. Declarar el cese de don Manuel Parras Rosa como Rector Magnífico de la Universidad de Jaén, por finalización de su mandato, agradeciéndole los servicios prestados.

Sevilla, 7 de abril de 2015

SUSANA DÍAZ PACHECO.- Presidenta de la Junta de Andalucía, en funciones

JOSÉ SÁNCHEZ MALDONADO.- Consejero de Economía, Innovación, Ciencia y Empleo, en funciones

Decreto 122/2015, de 7 de abril, por el que se declara el nombramiento de don Juan Gómez Ortega como Rector Magnífico de la Universidad de Jaén. (BOJA número 67 de 09/04/2015, página 98)

De conformidad con lo establecido en el artículo 20.2 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y en el artículo 52 de los Estatutos de la Universidad de Jaén, aprobados por Decreto 230/2003, de 29 de julio, y una vez efectuada la proclamación de Rector, conforme al resultado de la elección efectuada a este respecto por la comunidad universitaria de la citada Universidad, a propuesta del Consejero de Economía, Innovación, Ciencia y Empleo, y previa deliberación del Consejo de Gobierno en su reunión del día 7 de abril de 2015,

DISPONGO

Artículo único. Nombrar Rector Magnífico de la Universidad de Jaén a don Juan Gómez Ortega, Catedrático de dicha Universidad.

Sevilla, 7 de abril de 2015

SUSANA DÍAZ PACHECO.- Presidenta de la Junta de Andalucía, en funciones

JOSÉ SÁNCHEZ MALDONADO.- Consejero de Economía, Innovación, Ciencia y Empleo, en funciones

Resolución de 8 de abril de 2015, de la Secretaría General de Universidades, Investigación y Tecnología, por la que se hacen públicas las subvenciones excepcionales concedidas en el primer trimestre del año 2015

BOJA número 69 de 13/04/2015, páginas de 129 a 130

INICIO SUBIR

V. INFORMACIÓN DE INTERÉS PARA LA COMUNIDAD UNIVERSITARIA

ANUNCIOS

Anuncio de la Universidad de Jaén por el que se convoca licitación pública para el suministro e instalación de butacas para el Aula Magna y Sala de Grados del Edificio de Transferencia del Conocimiento y Servicios Generales del Campus Científico-Tecnológico de Linares

BOE número 55, de 05/03/2015, páginas 9479 a 9480

Anuncio de la Universidad de Jaén por el que se convoca licitación pública para el suministro e instalación de mobiliario para despachos, salas de juntas y seminarios del edificio Oeste del Complejo I+D del campus Científico-Tecnológico de Linares

BOE número 56, de 06/03/2015, páginas 9620 a 9621

Anuncio de la Universidad de Jaén por el que se convoca licitación pública para el suministro e instalación de equipamiento de cocina y cafetería del edificio de transferencia del conocimiento y servicios generales del Campus Científico-Tecnológico de Linares

BOE número 57, de 07/03/2015, páginas 9820 a 9821

Anuncio del Centro de Profesorado "Sagrada Familia" de la Universidad de Jaén sobre extravío de título universitario.

BOE número 58, de 09/03/2015, páginas 10069

Anuncio de formalización de contratos de: Rectorado de la Universidad de Jaén. Objeto: Servicio de vigilancia y seguridad y auxiliares de instalaciones deportivas en instalaciones de la Universidad de Jaén. Expediente: 2014/20.

BOE número 63, de 11/03/2015, páginas 10991

Anuncio de la Universidad de Jaén por el que se convoca licitación pública para el suministro e instalación de mobiliario para laboratorios de la planta cuarta del edificio A-2. Centro de instrumentación científico-técnica.

BOE número 64, de 16/03/2015, páginas 11260 a 11261

Anuncio de la Fundación Campus Científico-Tecnológico de Linares por el que se convoca licitación pública para la contratación del servicio de limpieza de edificios e instalaciones del Campus Científico-Tecnológico de Linares

BOE número 70, de 23/03/2015, páginas 12272 a 12273

Anuncio de la Escuela Politécnica Superior de Jaén de la Universidad de Jaén sobre extravío de título universitario. (BOE número 88, de 13/04/2015, página 15806)

Se anuncia el extravío de título de Ingeniero Técnico Industrial. Mecánica de Jesús López Tripiana a efectos de lo establecido en la legislación vigente, con número de Registro Universitario 6923 y con número de Registro Nacional de Títulos 1999176836, de fecha de expedición 25 de febrero de 1999.

Jaén, 27 de marzo de 2015.- El Jefe del Servicio de Gestión Académica.

Anuncio de la Universidad de Jaén por el que se hace pública la formalización del contrato de suministro de publicaciones periódicas extranjeras

BOE número 88, de 13/04/2015, páginas 15757

Anuncio de la Universidad de Jaén por el que se hace pública la formalización del contrato de suministro e instalación de equipamiento para un laboratorio de Control Medioambiental en la Escuela Politécnica Superior de Linares

BOE número 89, de 14/04/2015, páginas 16021

Anuncio de la Facultad de Humanidades y Ciencias de la Educación de la Universidad de Jaén sobre extravío de título universitario. (BOE número 100, de 17/04/2015, página 18410)

Se anuncia el extravío de título de Maestra, especialidad de Educación Física de María del Rocío Pulido Jiménez a efectos de lo establecido en la legislación vigente, con número de Registro Universitario 21224 y con número de Registro Nacional de Títulos 2005150948, de fecha de expedición 1 de septiembre de 2004.

Jaén, 16 de abril de 2015.- El Jefe del Servicio de Gestión Académica.

.

INICIO SUBIR

DOCUMENTO DE SEGURIDAD PARA FICHEROS DE DATOS DE CARÁCTER PERSONAL

Universidad de Jaén

Contenido

1. Aprobación y entrada en vigor 3
2. Ámbito de aplicación y Recursos protegidos 3
2.1. Ficheros inscritos 3
3. Normas de Seguridad 3
3.1. Codificación de las normas y procedimientos de seguridad 3
3.2. Normas sobre locales, puestos de usuario, sistemas y contraseñas 4
3.2.1. Centros de tratamiento y locales 4
3.2.2. Puestos de usuario 5
3.2.3. Entorno de Sistema Operativo y de Comunicaciones 6
3.2.4. Sistema Informático o aplicaciones de acceso al Fichero 8
3.2.5. Salvaguarda y protección de las contraseñas personales 9
3.3. Normas sobre gestión de incidencias 10
3.4. Normas sobre gestión de soportes 11
3.5. Normas sobre la entrada y salida de datos por red 13
3.6. Normas sobre las copias de respaldo y recuperación 13
3.7. Normas sobre los datos personales en soporte papel 14
3.8. Normas sobre controles periódicos de verificación del cumplimiento 16
3.9. Procedimientos de Seguridad 18
4. Funciones y obligaciones del personal 18
Anexo I. Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición 21

1. Aprobación y entrada en vigor

Texto aprobado el día 26/03/2015 por el Consejo de Gobierno.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva versión de la misma.

2. Ámbito de aplicación y Recursos protegidos

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de la Universidad de Jaén, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en la Ley Orgánica de Protección de Datos y el Real Decreto 1720/2007, las personas que intervienen en el tratamiento y los locales en los que se ubican.

La protección de los datos de los ficheros frente a accesos no autorizados se deberá realizar mediante el control, de todas las vías por las que se pueda tener acceso a dicha información. Los recursos que, por servir de medio directo o indirecto para acceder a los ficheros, deberán ser controlados por esta normativa son:

- Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan.
- Los puestos de usuario, bien locales o remotos, desde los que se pueda tener acceso a los ficheros.
- Los servidores, si los hubiese, y el entorno de sistema operativo y de comunicaciones en el que se encuentran ubicados los ficheros.
- Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos.
- Los archivadores y salas, en donde se almacenen los documentos en papel que contengan datos de carácter personal.

2.1. Ficheros inscritos

En el enlace indicado a continuación se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afectan de manera particular:
http://www10.ujaen.es/conocenos/servicios-unidades/servinfo/protecci%C3%B3ndedatosdecaracterpersonal/ficherosinscritos

3. Normas de Seguridad

3.1. Codificación de las normas y procedimientos de seguridad

Las normas de seguridad definidas en este documento se identifican mediante una letra que las identifica como tales, y que indica el nivel de seguridad en que es aplicable la norma:

B	Norma de seguridad de nivel básico
M	Norma de seguridad de nivel medio
A	Norma de seguridad de nivel alto

A continuación se indica el tipo de norma, en función de si afecta a la seguridad física o a la seguridad lógica:

F – Seguridad Física
L – Seguridad Lógica

El siguiente código indica a qué tipo de usuarios les afecta la norma:

R – Responsable del Fichero
S – Responsable de Seguridad
I – Administradores y Personal de Informática
T – Todo el personal

Por último se especifica un número de orden de la norma.
Los procedimientos de seguridad definidos siguen una codificación equivalente, utilizando como primera letra identificativa siempre una **P**

3.2. Normas sobre locales, puestos de usuario, sistemas y contraseñas

3.2.1. Centros de tratamiento y locales

Los locales donde se ubiquen los ordenadores así como los archivadores, armarios o demás contenedores que contienen cada uno de los conjuntos de datos de carácter personal, que en adelante llamaremos el Fichero, deben ser objeto de especial protección que garantice la disponibilidad y confidencialidad de los datos protegidos, especialmente en el caso de que el Fichero esté ubicado en un servidor accedido a través de una red.

B	F	R	1	Los locales deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad del Fichero que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas.

M	F	R	2	El acceso a los locales donde se encuentre el fichero deberá estar restringido exclusivamente a los administradores del sistema que deban realizar labores de mantenimiento para las que sea imprescindible el acceso físico.

M	F	T	3	Como alternativa a la norma anterior, toda persona que tenga acceso a los locales deberá estar acompañada en todo momento por algún empleado autorizado, que supervisará su comportamiento.

En todas las salas se encuentran de manera habitual empleados autorizados de la propia entidad. Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre los centros de tratamiento y locales se encuentra en el **Procedimiento de Seguridad Física,** publicado para su lectura en Universidad Virtual.

3.2.2. Puestos de usuario

Son todos aquellos dispositivos desde los que se puede acceder a los datos del Fichero, como, por ejemplo, terminales u ordenadores personales.
Se consideran también puestos de usuario aquellos terminales de administración del sistema, como, por ejemplo, las consolas de operación, donde en algunos casos también pueden aparecer los datos protegidos del Fichero.

B	F	T	4	Cada puesto de usuario estará bajo la responsabilidad de una persona, manteniéndose por tanto una relación de puestos de usuario de acuerdo al **"Procedimiento de Seguridad Lógica"**. El responsable de un puesto de usuario garantizará que la información a la que accede o que muestra no pueda ser vista por personas no autorizadas. Esta precaución se extremará cuando existan visitas ajenas al departamento al que pertenece el fichero. La plantilla para construir la relación de puestos de usuario y de personal autorizado para acceder al fichero se encuentra en el **"Procedimiento de Seguridad Lógica"**.

.

B	F	T	5	La norma anterior implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de usuario deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

B	L	T	6	Queda prohibido el almacenamiento de cualquier tipo de documento con datos personales en los PC de usuario salvo usuarios autorizados. En caso de existir aplicaciones de gestión específicas para el tratamiento de Datos de Carácter Personal, el usuario deberá de almacenar y tratarlos mediante dichas aplicaciones. La revocación de esta prohibición será autorizada por el responsable del Fichero, quedando constancia de esta modificación en el Registro de Incidencias. En cualquier caso se garantizará el cumplimiento de las medidas de seguridad correspondientes en el PC de usuario, especialmente medidas de control de acceso.

				El procedimiento para establecer las contraseñas se especifica en el **“Procedimiento de Control de Accesos”**.

B	L	T	7	Cuando el responsable de un puesto de usuario lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente. El procedimiento para establecer el protector de pantalla se especifica en el “**Procedimiento de Control de Accesos**”.

B	F	T	8	En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos del Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

B	L	T	9	Las conexiones a redes o sistemas exteriores de los puestos de usuario desde los que se realiza el acceso al Fichero, se ajustarán a lo definido en el “**Procedimiento de Seguridad Lógica**”.

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre los puestos de usuario se encuentra en el **“Procedimiento de Seguridad Lógica”**.

3.2.3. Entorno de Sistema Operativo y de Comunicaciones

Aunque el método establecido para acceder a los datos protegidos del Fichero es el sistema informático referenciado en el apartado 2 del presente documento, al estar el Fichero ubicado en un ordenador con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otros ordenadores, es posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación.

Esta normativa debe, por tanto, regular el uso y acceso de las partes del sistema operativo, herramientas o programas de utilidad, o del entorno de comunicaciones, de forma que se impida el acceso no autorizado a los datos del Fichero.

B	L	R	10	El sistema operativo y de comunicaciones del Fichero deberá tener al menos un responsable, que como administrador deberá estar relacionado de acuerdo al **“Procedimiento de Seguridad Lógica”**.

				En el caso más simple, como es que el Fichero se encuentre ubicado en un ordenador personal y accedido mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente al Fichero. La plantilla para construir la relación de personal autorizado para acceder al Fichero se encuentra en el "**Procedimiento de Seguridad Lógica**".

B	F	I	11	El administrador deberá responsabilizarse de guardar en lugar protegido las copias de seguridad y respaldo del Fichero, de forma que ninguna persona no autorizada tenga acceso a las mismas.

B	L	I	12	Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, ficheros de "logging", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.

B	L	T	13	Los usuarios eliminarán los ficheros intermedios que pudieran haber creado para desarrollar su trabajo, una vez que no sean necesarios. En ningún caso se conservarán estos ficheros durante largos periodos de tiempo. En el caso de los puestos de usuario de tipo PC, con sistema operativo Windows, se eliminarán al finalizar cada jornada laboral los ficheros del directorio temporal del sistema (comúnmente C:\WINDOWS\TEMP\). El procedimiento para realizar esta eliminación se especifica en el "**Procedimiento de Protección de la Información**".

B	L	I	14	Si el ordenador en el que está ubicado el fichero está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al Fichero, el Administrador Responsable del Sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas. En cualquier caso, deberá identificarse de manera única a las personas acceden de forma remota.

B	L	I	15	En el caso de puestos con Sistema Operativo Windows, en ningún caso se compartirá en red el directorio del sistema, comúnmente C:\WINDOWS. Este directorio, entre otras cosas, almacena las contraseñas y el directorio para ficheros temporales.

				La revocación de esta prohibición será autorizada por el Responsable de Seguridad, quedando constancia de esta modificación en el Registro de Incidencias.

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre la red se recoge en el "**Procedimiento de Seguridad Lógica**".

3.2.4. Sistema Informático o aplicaciones de acceso al Fichero

Son todos aquellos sistemas informáticos, programas o aplicaciones con las que se puede acceder a los datos del Fichero, y que son usualmente utilizados por los usuarios para acceder a ellos. Estos sistemas pueden ser aplicaciones informáticas expresamente diseñadas para acceder al Fichero, o sistemas preprogramados de uso general como aplicaciones o paquetes disponibles en el mercado informático.

B	L	R	16	Los sistemas informáticos de acceso al Fichero deberán tener su acceso restringido mediante un código de usuario y una contraseña.

B	L	R	17	Todos los usuarios autorizados para acceder al Fichero deberán tener un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

B	L	I	18	Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

M	L	I	19	En cualquier caso se controlarán los intentos de acceso fraudulento al Fichero, limitando el número máximo de intentos fallidos, y cuando sea técnicamente posible, guardando en un fichero auxiliar la fecha, hora, código y claves erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

B	L	R I	20	En función de las posibilidades técnicas, se limitará el acceso de cada usuario al mínimo conjunto de recursos que necesite para desempeñar su trabajo, configurando de manera adecuada la aplicación y/o el sistema operativo.

M	L	I	21	Si durante las pruebas anteriores a la implantación o modificación de la aplicación de acceso al Fichero se utilizasen datos reales, se deberá aplicar

				a esos ficheros de prueba el mismo tratamiento de seguridad que se aplica al mismo Fichero.

A	L	SI	22	En los ficheros de nivel alto, se guardará en un registro de accesos la identificación del usuario, fecha y hora en la que se realizó el acceso, el fichero accedido, el tipo de acceso y si éste ha sido autorizado o denegado. En caso de haber sido autorizado se guardará información que permita identificar el registro accedido. Los datos de este registro deberán conservarse al menos durante dos años. Los mecanismos de registro de estos datos de acceso no podrán ser desactivados en ningún caso, y estarán siempre bajo control del responsable de seguridad competente.

3.2.5. Salvaguarda y protección de las contraseñas personales

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

B	L	R	23	Sólo las personas relacionadas de acuerdo al **"Procedimiento de Seguridad Lógica"** podrán tener acceso a los datos del Fichero.

B	L	R	24	La norma anterior se aplica también a los Administradores del sistema, incluyendo aquél personal técnico externo que de manera habitual pudiera colaborar en la administración de los sistemas.

B	L	T	25	Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio.

B	L	I	26	Los identificadores de usuario y las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determinan en el **"Procedimiento de Control de Accesos"**, asegurando que se mantiene la confidencialidad de ambos.

B	L	I	27	El archivo donde se almacenen las contraseñas deberá estar protegido y cifrado, y bajo la responsabilidad del Administrador del Sistema.

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre las contraseñas se encuentra en el "**Procedimiento de Control de Accesos**".

3.3. Normas sobre gestión de incidencias

Una incidencia es cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del Fichero, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

El mantenimiento de un registro de las incidencias que comprometan la seguridad de un Fichero es una herramienta imprescindible para la prevención de posibles ataques a esa seguridad, así como para persecución de los responsables de los mismos.

B	L	S	28	El Responsable de Seguridad del Fichero habilitará un Registro de Incidencias a disposición de todos los usuarios y administradores del Fichero con el fin de que se registre en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

B	L	T	29	Cualquier usuario que tenga conocimiento de una incidencia, es responsable del registro de la misma en el Registro de Incidencias del Fichero, entregándola por escrito al Responsable de Seguridad o al Responsable del Fichero, que serán los encargados de incorporarla al Libro.

B	L	T	30	El conocimiento de una incidencia y la falta de notificación o registro de la misma por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

B	L	T	31	La notificación o registro de una incidencia deberá constar al menos de los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que puede producir y una descripción detallada de la misma. El procedimiento y formulario para notificar una incidencia está descrito en el **"Procedimiento gestión de incidencias"**.

B	L	S	32	El Responsable de Seguridad se ocupará de gestionar cada incidencia para resolver los problemas que plantee de la mejor manera posible, en colaboración con el Responsable del Fichero. El procedimiento para gestionar una incidencia está descrito en el **"Procedimiento de gestión de incidencias"**.

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre la gestión de incidencias se encuentra en el **"Procedimiento Gestión de Incidencias".**

3.4. Normas sobre gestión de soportes

Soportes informáticos son todos aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona el Fichero.

Dado que la mayor parte de los soportes que hoy en día se utilizan, Memorias USB, DVDs o CD-ROMs, son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que para la seguridad de los datos del Fichero tiene el control de estos medios.

Aunque este apartado hace referencia a los soportes informáticos, también se establecen algunas normas para el caso de los soportes no informáticos, como los documentos impresos en papel.

B	L	T	33	Los soportes (Memorias USB, DVDs, CD-ROMs...) que contengan datos de carácter personal, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación. El procedimiento para identificar estos soportes se encuentra en el **“Procedimiento de Protección de la Información”**.

M	F	T	34	Aquellos medios que sean reutilizables, y que hayan contenido copias de datos del Fichero, deberán ser borrados físicamente antes de su reutilización o destrucción, de forma que los datos que contenían no sean recuperables. El procedimiento para reutilizar o destruir estos soportes se encuentra en el **“Procedimiento de Protección de la Información”**.

M	F	T	35	Los documentos impresos con datos personales, una vez que ya no sean necesarios, se destruirán físicamente de manera que no puedan recuperarse los datos que contenían (por ejemplo mediante una trituradora de papel). En ningún caso se reutilizarán este tipo de documentos (por ejemplo, no podrán ser utilizados para imprimir por la otra cara, si estuviera en blanco).

B	F	T	36	Los soportes que contengan datos del Fichero deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso del Fichero que no estén, por tanto, relacionadas de acuerdo al **“Procedimiento de Protección de la Información”**. En caso de ser posible, se utilizará un lugar protegido frente a incendios. En ningún caso se dejarán a la vista, como por ejemplo encima de una mesa.

B	L	T	37	Todos los soportes que se utilicen se incluirán en un inventario, en el que se indique, para cada soporte, la fecha de alta y de baja, indicando en este último caso si el soporte se destruye definitivamente o se reutiliza. La plantilla para construir el libro de inventario de soportes se encuentra en el **"Procedimiento de Protección de la Información"**.

B	F	T	38	Los documentos impresos con datos personales se almacenarán de manera que se mantenga la confidencialidad de los mismos en lugares a los que no tengan acceso personas no autorizadas. En ningún caso se dejarán a la vista, como por ejemplo encima de una mesa.

B	L	R	39	La salida de soportes informáticos que contengan datos del Fichero fuera de los locales donde está ubicado el Fichero deberá ser expresamente autorizada por el Responsable del Fichero. El procedimiento y formulario para la salida de soportes se encuentra en el **"Procedimiento de Protección de la Información"**.

M	L	R	40	El Responsable de Seguridad del Fichero o persona en quien delegue mantendrá un "**Registro de entrada y salida de soportes**" donde se guardarán los formularios de entradas y de salidas de soportes descritos en el capítulo "Locales, sistemas de tratamiento, aplicaciones y puestos de usuario", con indicación de tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío, destinatario, o persona responsable de la recepción que deberán estar debidamente autorizadas. El procedimiento y formulario para la entrada de soportes se encuentra en el **"Procedimiento de Protección de la Información"**.

M	L	T	41	Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

A	L	S	42	Se conservará una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente donde se encuentren los equipos informáticos que los tratan. Deberán cumplirse, en todo caso, las medidas de seguridad correspondientes al nivel de los datos contenidos en la copia.

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre la gestión de soportes se encuentra en el "**Procedimiento de Protección de la Información**".

3.5. Normas sobre la entrada y salida de datos por red

La transmisión de datos por red, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello merecen un tratamiento especial ya que, por sus características, pueden ser más vulnerables que los soportes físicos tradicionales.

M	L	R I	43	Todas las entradas y salidas de datos de carácter personal que se efectúen mediante correo electrónico se realizarán desde cuentas o direcciones de correo de la Universidad, estando prohibido el uso de cuentas personales. Igualmente si se realiza la entrada o salida de datos mediante sistemas de transferencia de ficheros por red, únicamente un usuario o administrador estará autorizado para realizar esas operaciones.

A	L	T	44	Cuando los datos del Fichero vayan a ser enviados por correo electrónico o por sistemas de transferencia de ficheros, a través de redes públicas o no protegidas, se recomienda que sean cifrados de forma que solo puedan ser leídos e interpretados por el destinatario. Si los datos son de nivel alto el cifrado es obligatorio.

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre la red en el **"Procedimiento de Seguridad Lógica"**.

3.6. Normas sobre las copias de respaldo y recuperación

La seguridad de los datos personales del Fichero no sólo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.
Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos del Fichero.

B	L	I	45	Existirá una persona, bien sea el administrador o bien otro usuario expresamente designado, que será responsable de obtener periódicamente una copia de seguridad del fichero, a efectos de respaldo y posible recuperación en caso de fallo. El procedimiento de realización de copias de seguridad se encuentra en el "**Procedimiento de Protección de la Información**".

B	L	I	46	Estas copias de seguridad deberán realizarse con una periodicidad, al menos, trimestral, salvo en el caso de que no se haya producido ninguna actualización de los datos.

M	L	I	47	Se evitará desgastar en exceso los soportes donde se realizan las copias de seguridad, rotándolos y renovándolos de forma periódica transcurridos un número determinado de grabaciones o un periodo de tiempo largo. El procedimiento para la rotación y renovación de soportes se encuentra en el "**Procedimiento de Seguridad Física**".

B	L	I	48	Los soportes destinados a copias de seguridad seguirán todas las normas definidas en el **"Procedimiento de gestión de Soportes"** (identificación, reutilización y eliminación, etc.).

B	L	I	49	En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban en el momento del fallo. El procedimiento de recuperación de datos se encuentra en el "**Procedimiento de Protección de información**".

B	L	R	50	Será necesaria la autorización por escrito del Responsable de Seguridad del Fichero para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación. El formulario para notificar una incidencia se encuentra en el "**Procedimiento de Protección de información**".

Una descripción más detallada acerca de las medidas de seguridad a aplicar sobre las copias de seguridad en el "**Procedimiento de Protección de información**".

3.7. Normas sobre los datos personales en soporte papel

El Real Decreto 1720/2007 regula las medidas de seguridad que es necesario implantar para asegurar la confidencialidad y la integridad de los datos personales almacenados en soporte papel (ficheros no automatizados).

Estas medidas afectan igualmente a las salas y archivadores destinadas al almacenamiento de los documentos que contengan datos personales, así como a los medios informáticos utilizados para su tratamiento, como pueden ser impresoras o fotocopiadoras.

B	L	T	51	Los documentos no automatizados que contengan datos de carácter personal, deberán almacenarse de manera que los empleados de la

				Universidad tendrán acceso únicamente a aquellos documentos en papel que precisen para el desarrollo de sus funciones. Deberá existir una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
B	L	T	52	Los documentos que contengan datos personales, deberán ser archivados de manera que se permita la correcta conservación de los documentos, la localización y consulta de la información, y que permitan la posibilidad del ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. En ningún caso se dejarán a la vista, como por ejemplo encima de una mesa.
B	F	T	53	Asimismo, los documentos deberán archivarse de modo que se permita identificar el tipo de información que contienen, debiendo estos ser etiquetados e inventariados.
B	F	T	54	Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.
B	F	T	55	Siempre que los documentos con datos personales no estén archivados, la persona que esté utilizando el documento, deberá custodiarlo y encargarse de asegurar la confidencialidad y la integridad de los datos que contiene, impidiendo el acceso a dicho documento por parte de usuarios no autorizados.
B	F	T	56	Siempre que se proceda al traslado físico de los documentos que contengan datos personales, deberán adoptarse las medidas que impidan el acceso por parte de usuarios no autorizados a la información trasladada, debiendo llevarse, además, un registro de los movimientos de los ficheros no automatizados realizados.
M	F	T	57	Los documentos impresos con datos personales, una vez que ya no sean necesarios, se destruirán físicamente de manera que no puedan recuperarse los datos que contenían (por ejemplo mediante una trituradora de papel). En ningún caso se reutilizarán este tipo de documentos (por ejemplo, no podrán ser utilizados para imprimir por la otra cara, si estuviera en blanco).

A	F	T	58	Las copias o reproducciones (fotocopias o impresos) de los documentos que contengan datos de carácter personal, sólo podrán ser realizadas por parte de personal autorizado, y han de ser destruidas físicamente y desechadas, una vez ya no sean útiles para la finalidad con la que fueron realizados.

A	F	T	59	Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero

A	F	T	60	Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos de nivel alto que puedan ser utilizados por múltiples usuarios. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

3.8. Normas sobre controles periódicos de verificación del cumplimiento

La veracidad de los datos contenidos en los apartados de este documento, así como el cumplimiento de las normas que contiene deberán ser periódicamente comprobados, de forma que puedan detectarse y subsanarse anomalías.

M	L	S I	61	El Responsable de Seguridad del Fichero comprobará, de acuerdo al procedimiento, que la lista de usuarios autorizados se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso al Fichero, para lo que recabará la lista de usuarios de la aplicación y sus identificadores al Administrador o administradores del Fichero. De igual manera, comprobará que los niveles de acceso de cada usuario se corresponden con las medidas técnicas habilitadas para limitar este acceso (restricción de funciones de las aplicaciones, configuración de permisos de carpetas, etc.). También comprobará que se realizan de manera adecuada los procedimientos de gestión de usuarios y contraseñas, especialmente la renovación periódica de las contraseñas.

				Además de estas comprobaciones periódicas, el Administrador comunicará al Responsable de seguridad, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado al Fichero.
M	L	S I	62	Se comprobará también al menos con periodicidad trimestral, la existencia de copias de respaldo correctas que permitan la recuperación de Fichero según lo estipulado en el capítulo “Normas sobre las copias de respaldo y recuperación” de este documento.
M	L	S I	63	A su vez, y también con periodicidad al menos trimestral, los Administradores del Fichero comunicarán al Responsable de Seguridad cualquier cambio que se haya realizado en los datos técnicos de los sistemas, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso al Fichero, procediendo igualmente a la actualización de dichos datos en el **Anexo I** y resto de documentos.
M	L	S I	64	Será responsabilidad de los usuarios que las configuraciones hardware y software de los puestos se ajusten a lo establecido por el Responsable de Seguridad, verificando que no se hayan instalado programas sin autorización. Se hará hincapié en no instalar programas especiales como herramientas de utilidad que permitan el acceso no controlado a los ficheros de datos.
M	L	S I	65	Será responsabilidad del usuario no almacenar documentos con datos personales en los PCs que no estén autorizados. De igual manera se eliminarán los ficheros temporales, tanto en los PCs de usuario como en el servidor.
M	L	S I	66	El Responsable de seguridad, verificará, con periodicidad al menos bienal, el cumplimiento de lo previsto en los capítulos “Normas sobre la entrada y salida de datos por red” y "Normas sobre las copias de respaldo y recuperación" de este documento en relación con las entradas y salidas de datos, sean por red o en soporte magnético.
M	L	R S	67	El Responsable de Seguridad analizará con periodicidad al menos bienal las incidencias registradas en el Registro correspondiente para, independientemente de las medidas particulares que se hayan adoptado en

				el momento que se produjeron, adoptar las medidas correctoras que limiten esas incidencias en el futuro.

A	L	S	68	El Responsable de Seguridad revisará periódicamente la información de control registrada en el registro de accesos, y elaborará un informe de las revisiones realizadas y los problemas detectados.

M	L	R S	69	Al menos cada dos años, se realizará una auditoría, externa o interna, que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de Desarrollo de la LOPD (RD 1720/2007), identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoría serán analizados por el Responsable de Seguridad, quien propondrá al Responsable del Fichero las medidas correctoras correspondientes.

M	L	R S	70	Los resultados de todos estos controles periódicos, así como de las auditorías serán efectuadas y tratadas de acuerdo al **"Procedimiento de Gestión de Seguridad de la Información**".

3.9. Procedimientos de Seguridad

- Procedimiento de Control de Accesos
- Procedimiento de Seguridad Física
- Procedimiento de Seguridad Lógica
- Procedimiento de Gestión de Incidencias
- Procedimiento de Gestión de la Seguridad de la Información
- Procedimiento de Protección de la Información
- Procedimiento de Gestión de la Continuidad
- Procedimiento de Gestión de la Seguridad del desarrollo de SW
- Procedimiento de Gestión de Proveedores
- Procedimiento de Gestión de Soportes
- Procedimiento de Gestión del personal

Todos los procedimientos son accesibles a través de la Universidad Virtual.

4. Funciones y obligaciones del personal

El personal afectado por esta normativa se clasifica en cuatro categorías:

R – Responsable del Fichero:

El Responsable del Fichero es el encargado jurídicamente de la seguridad del Fichero y de las medidas establecidas en el presente documento, implantará las medidas de seguridad establecidas en él, según su categoría, y adoptará las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.

Sus principales funciones y obligaciones son:

- Implantar las medidas de seguridad establecidas en este documento.
- Garantizar la difusión de este Documento entre todo el personal que vaya a utilizar el fichero.
- Mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, según el Reglamento de Desarrollo de la LOPD.
- Adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos.
- Designar uno o varios responsables de seguridad.

Encargado Interno del Tratamiento:

El Responsable del Fichero delegará para el cumplimiento de sus funciones y responsabilidades en un Servicio/Unidad de la Universidad nombrado en las disposiciones de creación de los ficheros. Dicho servicio será el Encargado interno del tratamiento y tomará las decisiones sobre dicho fichero (accesos autorizados, sistemas de tratamiento, flujos de información, etc.)

S – Responsable de Seguridad:

Es la persona designada por el responsable del fichero para coordinar y controlar las medidas de seguridad aplicables al Fichero. Debe ser una persona con los conocimientos suficientes para llevar a cabo esa función, por tanto, debe estar al día en temas técnico-informáticos y también en temas jurídicos relativos al documento de seguridad y a la propia normativa.

Sus principales funciones y obligaciones son:

- Coordinar la puesta en marcha de las medidas establecidas en la normativa y en el documento de seguridad.
- Colaborar con el responsable del fichero en la difusión del documento de seguridad y coordinase con éste en el cumplimiento de las medidas de seguridad.
- Habilitar el Registro de incidencias. Analizar las incidencias registradas y tomar las medidas oportunas.

I – Administradores de Sistemas y Personal de Informática: El administrador del sistema es el encargado de garantizar a los responsables y usuarios la seguridad de los datos que se procesan en la organización. Este rol puede ser desempeñado tanto por personal de la empresa como por una persona externa. Las funciones básicas del cargo de administrador de sistemas son:

- Proponer estándares y procedimientos relacionados con la seguridad.
- Desarrollar los planes de seguridad.
- Gestionar los perfiles de usuarios de los sistemas informáticos y los accesos de cada uno.
- Controlar y realizar el seguimiento de la seguridad física y lógica del entorno informático.
- Dar soporte a los usuarios en materia de seguridad.
- Evaluar los riesgos.

- Implantar equipos, dispositivos y paquetes relacionados con la seguridad física y lógica.
- Ofrecer a los usuarios finales los medios para posibilitar la actualización de los programas antivirus y canalizar las notificaciones de existencia de virus

T – Todo el personal. Usuarios: Los usuarios son todas aquellas personas que participan en alguna fase del tratamiento del Fichero. Entre sus obligaciones fundamentales se encuentran las siguientes:

- Proteger la información a la que tenga acceso en virtud de su puesto y funciones de acuerdo a lo establecido en las normas del presente Documento de Seguridad.
- No deben revelar nunca sus contraseñas ni mantenerlas escritas en lugares visibles de su puesto de trabajo.
- Son responsables ante la empresa de todas las actividades y accesos que se realicen con su código de usuario.
- Asimismo es responsable de la custodia y utilización del ordenador que le ha sido asignado.
- En el caso de las impresoras, deberá asegurarse que no quedan impresos en la bandeja de salida que contengan datos protegidos.
- Si el terminal es portátil, deberá ser guardado bajo llave o llevarlo consigo. Durante los viajes, no debe facturarse como equipaje en aeropuertos y estaciones.
- El usuario final es responsable exclusivo de la utilización del antivirus y la salvaguarda de los terminales.
- Ante cualquier incidencia, el usuario es responsable de la comunicación de la misma al Responsable de Seguridad. La falta de notificación de una incidencia conocida por un usuario, será considerada como falta contra la seguridad de los ficheros.
- Los usuarios firmarán por escrito que conocen y se comprometen a cumplir las políticas, normas, estándares y procedimientos establecidos en la empresa.

En el “Procedimiento de Control de Accesos” se detalla el registro de los nombramientos de cargos y usuarios que acceden a cada uno de los Ficheros.

Anexo I. Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición.

Las plantillas para ejercitar los derechos de acceso, rectificación, cancelación y oposición sobre los datos de carácter personal, en cumplimiento de los artículos del Título III del Real Decreto 1720/2007 de desarrollo de la LOPD, se encuentran disponibles en la página Web de la Universidad http://www10.ujaen.es/conocenos/servicios-unidades/servinfo/protecci%C3%B3ndedatosdecaracterpersonal/FormulariosDerechosARCO

PLAN DE ADECUACIÓN AL ENS

Universidad de Jaén

Contenido

1. Introducción 3
2. Términos y definiciones 3
3. Responsabilidades 3
4. Categoría del sistema 4
4.1. Criterios de Valoración de los Niveles 4
4.2. Valoración de Información y Servicios 9
5. Identificación de los activos 11
5.1. Hardware 11
5.2. Aplicaciones 12
5.3. Comunicaciones 12
5.4. Servicios Externos 12
5.5. Personal 12
5.6. Instalaciones 12
6. Valoración de los activos 13
7. Declaración de aplicabilidad 15
8. Análisis de riesgos 19
8.1. Metodología de análisis 20
8.2. Procedimientos 20
8.3. Nivel de riesgo potencial 21
8.4. Cálculo del riesgo actual 22
8.5. Medidas de protección actuales y previstas 24
8.6. Nivel de riesgo actual 28
8.7. Nivel de riesgo aceptable 29
8.8. Nivel de riesgo objetivo 29
9. Plan de mejora 31
9.1. Introducción 31
9.2. Objetivo 32
9.3. Alcance 32
9.4. Calendario 32
9.5. Responsabilidades 32
9.6. Seguimiento 32
9.7. Acciones de adaptación al ENS 33
9.8. Implantación de Medidas de Seguridad 34

1. Introducción

El presente plan de adecuación recoge todos los datos y documentación necesarios para declarar conformidad con el Esquema Nacional de Seguridad (ENS)
En este documento se identifican los principales activos de información de la UNIVERSIDAD DE JAÉN, que van a ser utilizados para la categorización de los sistema de acuerdo con el Esquema Nacional de Seguridad y posteriormente considerados en un análisis de riesgos, cuyo objeto será determinar el nivel de riesgo de la organización y las prioridades en cuanto al tratamiento de dicho riesgo.
Se recoge la Declaración de Aplicabilidad, con las medidas de seguridad aplicables según el ENS para los sistemas de la categoría correspondiente a los sistemas identificados.
Por último se referencia al Plan de Mejora desarrollado para ejecutar las tareas necesarias para que los sistemas de la UNIVERSIDAD DE JAÉN estén completamente adecuados al ENS.

2. Términos y definiciones

Para los fines de este documento se aplican los términos y conceptos incluidos en la guía **CCN-STIC-800, ESQUEMA NACIONAL DE SEGURIDAD, GLOSARIO DE TÉRMINOS Y ABREVIATURAS**.

3. Responsabilidades

Las principales responsabilidades dentro del ENS corresponden al responsable de seguridad, y a los de la información y los servicios. Es un requisito del ENS que estas responsabilidades estén definidas y diferenciadas para evitar conflictos de intereses que perjudiquen el nivel de seguridad. Puede darse el caso de que una misma persona cuente con responsabilidades de información y de servicio, pero el responsable de seguridad no debe tenerla sobre la prestación de los servicios.

- El **responsable de la información** es quien determinará los requisitos de la información tratada, aprobando formalmente las valoraciones de la misma. Por ello será asignado a quien tenga la responsabilidad del uso de la información.
- El **responsable del servicio** determinará los requisitos de seguridad de los servicios prestados, y aprobará formalmente las valoraciones de los mismos. Se propone a los responsables de los servicios de información para este rol. El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- El **responsable de seguridad** determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La Política de Seguridad identificará los responsables de la gestión de la seguridad, sus deberes y responsabilidades, el procedimiento para su designación y renovación así como la estructura y responsabilidades del comité de seguridad.

4. Categoría del sistema

4.1. Criterios de Valoración de los Niveles

Cada activo se valorará con los criterios definidos en la guía CCN-STIC-803, ESQUEMA NACIONAL DE SEGURIDAD, VALORACIÓN DE LOS SISTEMAS.

- **D: Disponibilidad**. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. Para valorar este criterio la pregunta a responder será: ¿Qué importancia tendría que el activo no estuviera disponible cuando se necesita?
- **I: Integridad**. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada Para valorar este criterio la pregunta a responder será: ¿Qué importancia tendría que el activo fuera alterado por alguien sin autorización?
- **C: Confidencialidad**. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. La pregunta a responder para valorar un activo en este criterio será: ¿Qué importancia tendría que el activo fuera revelado a personas no autorizadas?
- **A: Autenticidad**. Propiedad o característica consistente en que la entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. La pregunta aquí sería, ¿qué importancia tendría que el activo no fuera auténtico?
- **T: Trazabilidad**. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a la misma. La valoración de este criterio responde a la pregunta de ¿qué importancia tendría no poder identificar a quien haya ejecutado una acción?

Para valorar los activos en cada uno de estos criterios se utiliza una escala de tres puntos; bajo, medio y alto, como sigue.

4.1.1. Disponibilidad

Valor	Escala
Alto	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque la indisponibilidad de la información causaría un grave daño, de difícil o imposible reparación Porque la indisponibilidad de la información supondría el incumplimiento grave de una norma Porque la indisponibilidad de la información causaría un daño reputacional grave con los ciudadanos o con otras organizaciones Porque la indisponibilidad de la información podría desembocar en protestas masivas (alteración seria del orden público)

	Cuando el RTO (tiempo máximo que el servicio puede permanecer interrumpido) es inferior a 4 horas
Medio	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque la indisponibilidad de la información causaría un daño importante aunque subsanable Porque la indisponibilidad de la información supondría el incumplimiento material o formal de una norma Porque la indisponibilidad de la información causaría un daño reputacional importante con los ciudadanos o con otras organizaciones Porque su revelación podría desembocar en protestas públicas (alteración del orden público) Cuando el RTO (tiempo máximo que el servicio puede permanecer interrumpido) es de entre 4 y 24 horas (un día)
Bajo	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque la indisponibilidad de la información causaría algún perjuicio Porque la indisponibilidad de la información supondría el incumplimiento leve de una norma Porque la indisponibilidad de la información supondría pérdidas económicas apreciables Porque la indisponibilidad de la información causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones Porque la indisponibilidad de la información podría desembocar en múltiples protestas individuales Cuando el RTO se sitúa entre 1 y 5 días (una semana)
Sin valorar	Cuando la información es prescindible por tiempo indefinido Cuando el RTO es superior a 5 días laborables (una semana)

4.1.2. Integridad

Valor	Escala
Alto	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible reparación Porque su manipulación o modificación no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas Porque su manipulación o modificación no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones Porque su manipulación o modificación no autorizada podría desembocar en protestas masivas (alteración seria del orden público)

Medio	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable Porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma Porque su manipulación o modificación no autorizada causaría pérdidas económicas importantes Porque su manipulación o modificación no autorizada causaría un daño reputacional importante con los ciudadanos o con otras organizaciones Porque su manipulación o modificación no autorizada podría desembocar en protestas públicas (alteración del orden público)
Bajo	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque su manipulación o modificación no autorizada causaría algún perjuicio Porque su manipulación o modificación no autorizada supondría el incumplimiento leve de una norma Porque su manipulación o modificación no autorizada supondría pérdidas económicas apreciables Porque su manipulación o modificación no autorizada causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones Porque su manipulación o modificación no autorizada podría desembocar en múltiples protestas individuales
Sin Valorar	Cuando los errores en su contenido carecen de consecuencias o son fácil y rápidamente reparables

4.1.3. Confidencialidad

Valor	Escala
Alto	Porque la información debe conocerla un número muy reducido de personas Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque su revelación causaría un grave daño, de difícil o imposible reparación Porque su revelación supondría el incumplimiento grave de una norma Porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas Porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones Porque su revelación podría desembocar en protestas masivas (alteración seria del orden público)
Medio	Porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita

	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque su revelación causaría un daño importante aunque subsanable Porque su revelación supondría el incumplimiento material o formal de una norma Porque su revelación causaría pérdidas económicas importantes Porque su revelación causaría un daño reputacional importante con los ciudadanos o con otras organizaciones Porque su revelación podría desembocar en protestas públicas (alteración del orden público)
Bajo	Porque la información no deben conocerla personas ajenas a la organización Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque su revelación causaría algún perjuicio Porque su revelación supondría el incumplimiento leve de una norma Porque su revelación supondría pérdidas económicas apreciables Porque su revelación causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones Porque su revelación podría desembocar en múltiples protestas individuales
Sin valorar	Información de carácter público, accesible por cualquier persona

4.1.4. Autenticidad

Valor	Escala
Alto	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible reparación Porque su la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas Porque su la falsedad en su origen o en su destinatario causaría un daño reputacional grave con los ciudadanos o con otras organizaciones Porque su la falsedad en su origen o en su destinatario podría desembocar en protestas masivas (alteración sería del orden público)
Medio	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque su la falsedad en su origen o en su destinatario: causaría un daño importante aunque subsanable Porque su la falsedad en su origen o en su destinatario supondría el incumplimiento material o formal de una norma Porque su la falsedad en su origen o en su destinatario causaría pérdidas económicas importantes Porque su la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

	Porque su la falsedad en su origen o en su destinatario podría desembocar en protestas públicas (alteración del orden público)
Bajo	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque su la falsedad en su origen o en su destinatario causaría algún perjuicio Porque su la falsedad en su origen o en su destinatario supondría el incumplimiento leve de una norma Porque su la falsedad en su origen o en su destinatario supondría pérdidas económicas apreciables Porque su la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones Porque su la falsedad en su origen o en su destinatario podría desembocar en múltiples protestas individuales
Sin valorar	Cuando el origen es irrelevante o ampliamente conocido por otros medios Cuando el destinatario es irrelevante, por ejemplo por tratarse de información de difusión anónima

4.1.5. Trazabilidad

Valor	Escala
Alto	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque la incapacidad para rastrear un acceso a la información impediría la capacidad de subsanar un error grave Porque la incapacidad para rastrear un acceso a la información impediría la capacidad para perseguir delitos Porque la incapacidad para rastrear un acceso a la información facilitaría enormemente la comisión de delitos graves
Medio	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque la incapacidad para rastrear un acceso a la información dificultaría gravemente la capacidad de subsanar un error grave Porque la incapacidad para rastrear un acceso a la información impediría la capacidad de subsanar un error importante Porque la incapacidad para rastrear un acceso a la información dificultaría gravemente la capacidad para perseguir delitos. Porque la incapacidad para rastrear un acceso a la información facilitaría la comisión de delitos.
Bajo	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores.

	Porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad para perseguir delitos
Sin valorar	Cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios Cuando no se pueden perpetrar delitos relevante, o su investigación es fácilmente realizable por otros medios

4.2. Valoración de Información y Servicios

Para categorizar el Sistema según el ENS, se detallan a continuación las valoraciones de cada uno de los activos fundamentales (Información y Servicio). Como establece el ENS, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio. Consecuentemente, la categoría del Sistema viene dada por el valor máximo en cada parámetro.

Id	Servicio	Id	Información	D	I	C	A	T
CRUE_05_01	Web Institucional			Bajo	Medio	Bajo	Medio	Bajo
		IN01	Información General	Bajo	Medio	Bajo	Medio	Bajo
		IN02	Programas de asignaturas	Bajo	Bajo	Bajo	Medio	Bajo
SR02	Tablón de Anuncios			Bajo	Medio	Bajo	Medio	Bajo
		IN03	Resoluciones	Bajo	Medio	Bajo	Medio	Bajo
SR03	Perfil del contratante			Medio	Medio	Bajo	Medio	Medio
		IN04	Expedientes	Medio	Medio	Bajo	Medio	Medio
SR FirmaElec	Firma electrónica			Bajo	Medio	Medio	Medio	Bajo
		IN05	Certificados	Bajo	Medio	Medio	Medio	Bajo
SR05	Verifirma			Bajo	Medio	Bajo	Medio	Bajo
		IN06	Documentos firmados	Bajo	Medio	Bajo	Medio	Bajo
CRUE_03_43	Secretaria General. Registro			Medio	Bajo	Medio	Medio	Medio
		IN07	Quejas y sugerencias	Bajo	Bajo	Medio	Bajo	Bajo

		IN08	Archivo general	Bajo	Bajo	Bajo	Bajo	Bajo
		IN09	Estadísticas	Bajo	Bajo	Bajo	Medio	Bajo
CRUE_03_06	Gestión Académica. Becas			Bajo	Medio	Medio	Medio	Bajo
		IN10	Solicitudes de becas	Bajo	Medio	Medio	Medio	Bajo
CRUE_03_05	Gestión Académica. Automatrícula			Medio	Bajo	Medio	Bajo	Medio
		IN11	Solicitud de matrícula	Medio	Bajo	Medio	Bajo	Medio
		IN12	Resguardos de matrícula	Bajo	Bajo	Medio	Bajo	Bajo
		IN13	Información pruebas de acceso	Bajo	Bajo	Medio	Bajo	Bajo
CRUE_08_04	Autenticacion centralizada (SIDUJA)			Bajo	Medio	Medio	Medio	Bajo
		IN14	Cuenta de correo electrónico	Bajo	Medio	Medio	Medio	Bajo
		IN15	Expediente académico	Bajo	Medio	Medio	Medio	Bajo
CRUE_03_45	Secretaria General. Convenios			Bajo	Bajo	Bajo	Bajo	Bajo
		IN16	Convenios	Bajo	Bajo	Bajo	Bajo	Bajo
CRUE_03_36	Extensión Universitaria. Actividades Deportivas			Bajo	Bajo	Bajo	Bajo	Bajo
		IN17	Solicitud de utilización	Bajo	Bajo	Bajo	Bajo	Bajo
SR12	Investigación y transferencia: Portal del Investigador			Bajo	Bajo	Medio	Bajo	Bajo
		IN18	Información Investigación (Planes, Noticias, Memorias, Convocatorias)	Bajo	Bajo	Medio	Bajo	Bajo

Para simplificar la aplicación de medidas de seguridad, se diferencian tres sistemas de diferentes niveles:

Sistema	Servicio	D	I	C	A	T
Sistema1	CRUE_03_45 - Secretaria General. Convenios CRUE_03_36 - Extensión Universitaria. Actividades Deportivas	Bajo	Bajo	Bajo	Bajo	Bajo
Sistema2	CRUE_05_01 - Web Institucional SR02 - Tablón de Anuncios SR_FirmaElec - Secretaria General. Firma electrónica SR05 - Verifirma CRUE_03_06 - Gestión Académica. Becas CRUE_08_04 - Autenticacion centralizada (SIDUJA) SR12 - Investigación y transferencia: Portal del Investigador	Bajo	Medio	Medio	Medio	Bajo
Sistema3	SR03 - Gestión Económica. Perfil del contratante CRUE_03_43 - Secretaria General. Registro CRUE_03_05 - Gestión Académica. Automatrícula	Medio	Medio	Medio	Medio	Medio

5. Identificación de los activos

Los activos identificados se han agrupado en las siguientes categorías:

- **Hardware.** Hardware que compone los sistemas de información de la entidad.
- **Aplicaciones.** Software utilizado, gestionado y mantenido por la UNIVERSIDAD DE JAÉN.
- **Comunicaciones.** Líneas de comunicación necesarias para la prestación de los servicios
- **Servicios externos.** Servicios subcontratados que intervienen en la prestación del servicio.
- **Personal.** Personal que desarrolla sus labores en la UNIVERSIDAD DE JAÉN.
- **Instalaciones.** Edificios y oficinas en las que se desarrollan las labores de la entidad.

A continuación se relacionan los activos que dan soporte a los servicios de administración electrónica en la Universidad de Jaén:

5.1. Hardware

Id	Nombre	Descripción
273	www10_frontend	frontal www10
296	www10_backend	backend www10
102404	sabiote	sabiote
VIR_alma2	Alma2	Alma2
37535	jabato	jabato

5.2. Aplicaciones

Id	Nombre	Descripción
	www10.ujaen.es	www10.ujaen.es
	www.ujaen.es	www.ujaen.es
	Notario	Notario
	Portafirmas/Verifirma	Portafirmas/Verifirma
	UXXIAC	Académico
	Firma	Firma
	IDP Cluster	cluster IDP

5.3. Comunicaciones

Id	Nombre	Descripción
	RIUJA	red RIUJA

5.4. Servicios Externos

Id	Nombre	Descripción
	RICA-CICA	red RICA-CICA

5.5. Personal

Id	Nombre	Descripción
	Administradores	Administradores
	Usuarios	Usuarios

5.6. Instalaciones

Id	Nombre	Descripción
	CPD	Centro de proceso de datos

En la siguiente tabla se relacionan los activos de información con los servicios anteriormente identificados. En la casilla correspondiente aparecerá marcado si el activo es necesario para el correcto funcionamiento del servicio.

Servicios / Activos	CRUE_05_01	SR02	SR 03	SR_FirmaElec	SR 05	CRUE_03_43	CRUE_03_06	CRUE_03_05	CRUE_08_04	CRUE_03_45	CRUE_03_36	SR12
www10_frontend	■	■	■							■		
www10_backend	■	■	■							■		
Sabiote	■	■	■							■		
Alma2											■	
Jabato											■	
www10.ujaen.es	■	■	■							■		
www.ujaen.es	■	■	■							■		
Notario						■						
Portafirmas / Verifirma				■	■							
UXXIAC							■	■				
Firma				■	■	■						
IDP Cluster									■			
RIUJA	■	■	■	■	■	■	■	■	■	■	■	■
RICA-CICA	■	■	■	■	■	■	■	■	■	■	■	■
Administradores	■	■	■	■	■	■	■	■	■	■	■	■
Usuarios	■	■	■	■	■	■	■	■	■	■	■	■
CPD	■	■	■	■	■	■	■	■	■	■	■	■

6. Valoración de los activos

La valoración de los activos identificados en función de las cinco dimensiones de seguridad, Disponibilidad (D), Integridad (I) y Confidencialidad (C), Autenticidad (A) y Trazabilidad (T) se detallan en la siguiente tabla.

Los valores de los activos de administración electrónica se han deducido de las valoraciones recogidas para servicios e información y sus dependencias, de manera que se mantenga la coherencia con el resto de las valoraciones, según el siguiente criterio:

- Nivel Bajo (B) : 0-2
- Nivel Medio (M) : 3-5
- Nivel Alto (A): 6-8

Activo	D	I	C	A	T

Hardware					
www10_frontend (Sistema 3)	4	4	2	4	4
www10_backend (Sistema 3)	4	4	2	4	4
sabiote (Sistema 3)	4	4	2	4	4
Alma2 (Sistema 1)	2	2	2	2	2
jabato (Sistema 1)	2	2	2	2	2
Software					
www10.ujaen.es (Sistema 3)	4	4	2	4	4
www.ujaen.es (Sistema 3)	4	4	2	4	4
Notario (Sistema 3)	4	2	4	4	4
Portafirmas/Verifirma (Sistema 2)	2	4	4	4	2
UXXIAC (Sistema 3)	4	4	4	4	4
Firma (Sistema 3)	4	4	4	4	4
LOPD Cluster (Sistema 2)	2	4	4	4	2
Comunicaciones					
RIUJA (Sistema 3)	4	4	4	4	4
Servicios Externos					
RICA-CICA (Sistema 3)	4	4	4	4	4
Personal					
Administradores (Sistema 3)	4	4	4	4	4
Usuarios (Sistema 3)	4	4	4	4	4
Instalaciones					
CPD (Sistema 3)	4	4	4	4	4

7. Declaración de aplicabilidad

En la tabla se detallan las medidas de seguridad de entre las contenidas en el Anexo II del Esquema Nacional de Seguridad, con el estado en el que se encuentran teniendo en cuenta que las categorías de los sistemas y subsistemas.

Cada medida de seguridad tendrá uno de los dos estados siguientes:

- **No Aplica:** Control no seleccionado debido a que no es obligatorio según la categoría del Sistema.
- **Aplica:** Control seleccionado por requerimiento del ENS para la categoría del Sistema o para reducir alguno de los riesgos identificados. La medida puede estar ya implantada a la fecha de realización del presente Documento o bien se prevé implementar en los plazos determinados por el ENS, tal y como se define en el Plan de Mejora de la seguridad.

Dimensiones afectadas	Tipo de medida	Medida de seguridad	Sistema 1	Sistema 2	Sistema 3
	ORG	MARCO ORGANIZATIVO			
categoría	org.1	Política de seguridad	**Aplica – B**	**Aplica – B**	**Aplica – B**
categoría	org.2	Normativa de seguridad	**Aplica – B**	**Aplica – B**	**Aplica - B**
categoría	org.3	Procedimientos de seguridad	**Aplica – B**	**Aplica – B**	**Aplica – B**
categoría	org.4	Proceso de autorización	**Aplica – B**	**Aplica - B**	**Aplica – B**
	OP	MARCO OPERACIONAL			
	op.pl	Planificación			
categoría	op.pl.1	Análisis de riesgos	**Aplica – B**	**Aplica – M**	**Aplica – M**
categoría	op.pl.2	Arquitectura de seguridad	**Aplica – B**	**Aplica – B**	**Aplica - B**
categoría	op.pl.3	Adquisición de nuevos componentes	**Aplica – B**	**Aplica – B**	**Aplica - B**
D	op.pl.4	Dimensionamiento /Gestión de capacidades	**No Aplica**	**No Aplica**	**Aplica – M**
categoría	op.pl.5	Componentes certificados	**No Aplica**	**No Aplica**	**No Aplica**
	op.acc	Control de acceso			
A T	op.acc.1	Identificación	**Aplica – B**	**Aplica - B**	**Aplica – B**

I C A T	op.acc.2	Requisitos de acceso	**Aplica – B**	**Aplica – B**	**Aplica – B**
I C A T	op.acc.3	Segregación de funciones y tareas	**No Aplica**	**Aplica – M**	**Aplica – M**
I C A T	op.acc.4	Proceso de gestión de derechos de acceso	**Aplica – B**	**Aplica – B**	**Aplica – B**
I C A T	op.acc.5	Mecanismo de autenticación	**Aplica – B**	**Aplica – M**	**Aplica – M**
I C A T	op.acc.6	Acceso local (local logon)	**Aplica – B**	**Aplica – M**	**Aplica – M**
I C A T	op.acc.7	Acceso remoto (remotelogin)	**Aplica – B**	**Aplica – M**	**Aplica - M**
	op.exp	Explotación			
categoría	op.exp.1	Inventario de activos	**Aplica - B**	**Aplica - B**	**Aplica – B**
categoría	op.exp.2	Configuración de seguridad	**Aplica - B**	**Aplica – B**	**Aplica – B**
categoría	op.exp.3	Gestión de la configuración	**No Aplica**	**Aplica - M**	**Aplica - M**
categoría	op.exp.4	Mantenimiento	**Aplica – B**	**Aplica – B**	**Aplica – B**
categoría	op.exp.5	Gestión de cambios	**No Aplica**	**Aplica – M**	**Aplica – M**
categoría	op.exp.6	Protección frente a código dañino	**Aplica – B**	**Aplica – B**	**Aplica – B**
categoría	op.exp.7	Gestión de incidencias	**No Aplica**	**Aplica – M**	**Aplica – M**
T	op.exp.8	Registro de la actividad de los usuarios	**No Aplica**	**No Aplica**	**No Aplica**
categoría	op.exp.9	Registro de la gestión de incidencias	**No Aplica**	**Aplica – M**	**Aplica – M**
T	op.exp.10	Protección de los registros de actividad	**No Aplica**	**No Aplica**	**No Aplica**
categoría	op.exp.11	Protección de claves criptográficas	**Aplica – B**	**Aplica – B**	**Aplica – B**
	op.ext	Servicios externos			
categoría	op.ext.1	Contratación y acuerdos de nivel de servicio	**No Aplica**	**Aplica – M**	**Aplica – M**

categoría	op.ext.2	Gestión diaria	**No Aplica**	**Aplica – M**	**Aplica – M**
D	op.ext.9	Medios alternativos	**No Aplica**	**No Aplica**	**No Aplica**
	op.cont	Continuidad del servicio			
D	op.cont.1	Análisis de impacto	**No Aplica**	**No Aplica**	**Aplica – M**
D	op.cont.2	Plan de continuidad	**No Aplica**	**No Aplica**	**No Aplica**
D	op.cont.3	Pruebas periódicas	**No Aplica**	**No Aplica**	**No Aplica**
	Op.mon	Monitorización del sistema			
categoría	op.mon.1	Detección de intrusión	**No Aplica**	**No Aplica**	**No Aplica**
categoría	op.mon.2	Sistema de métricas	**No Aplica**	**No Aplica**	**No Aplica**
	MP	MEDIDAS DE PROTECCIÓN			
	mp.if	Protección de las instalaciones e infraestructuras			
categoría	mp.if.1	Áreas separadas y con control de acceso	**Aplica – B**	**Aplica – B**	**Aplica – B**
categoría	mp.if.2	Identificación de las personas	**Aplica – B**	**Aplica – B**	**Aplica – B**
categoría	mp.if.3	Acondicionamiento de los locales	**Aplica – B**	**Aplica – B**	**Aplica – B**
D	mp.if.4	Energía eléctrica	**Aplica – B**	**Aplica – B**	**Aplica – M**
D	mp.if.5	Protección frente a incendios	**Aplica – B**	**Aplica – B**	**Aplica - B**
D	mp.if.6	Protección frente a inundaciones	**No Aplica**	**No Aplica**	**Aplica – M**
categoría	mp.if.7	Registro de entrada y salida de equipamiento	**Aplica – B**	**Aplica – B**	**Aplica – B**
D	mp.if.9	Instalaciones alternativas	**No Aplica**	**No Aplica**	**No Aplica**
	mp.per	Gestión del personal			

categoría	mp.per.1	Caracterización del puesto de trabajo	**No Aplica**	**Aplica – M**	**Aplica – M**
categoría	mp.per.2	Deberes y obligaciones	**Aplica – B**	**Aplica – B**	**Aplica – B**
categoría	mp.per.3	Concienciación	**Aplica – B**	**Aplica - B**	**Aplica – B**
categoría	mp.per.4	Formación	**Aplica – B**	**Aplica – B**	**Aplica - B**
D	mp.per.9	Personal alternativo	**No Aplica**	**No Aplica**	**No Aplica**
	mp.eq	Protección de los equipos			
categoría	mp.eq.1	Puesto de trabajo despejado	**Aplica – B**	**Aplica – M**	**Aplica – M**
A	mp.eq.2	Bloqueo de puesto de trabajo	**No Aplica**	**Aplica – M**	**Aplica – M**
categoría	mp.eq.3	Protección de equipos portátiles	**Aplica – B**	**Aplica – B**	**Aplica – B**
D	mp.eq.9	Medios alternativos	**No Aplica**	**No Aplica**	**Aplica - M**
	mp.com	Protección de las comunicaciones			
categoría	mp.com.1	Perímetro seguro	**Aplica – B**	**Aplica – B**	**Aplica – B**
C	mp.com.2	Protección de la confidencialidad	**No Aplica**	**Aplica – M**	**Aplica – M**
I A	mp.com.3	Protección de la autenticidad y de la integridad	**Aplica – B**	**Aplica – M**	**Aplica – M**
categoría	mp.com.4	Segregación de redes	**No Aplica**	**No Aplica**	**No Aplica**
D	mp.com.9	Medios alternativos	**No Aplica**	**No Aplica**	**No Aplica**
	mp.si	Protección de los soportes de información			
C	mp.si.1	Etiquetado	**Aplica – B**	**Aplica – B**	**Aplica – B**
I C	mp.si.2	Criptografía	**No Aplica**	**Aplica – M**	**Aplica – M**
categoría	mp.si.3	Custodia	**Aplica – B**	**Aplica - B**	**Aplica – B**
categoría	mp.si.4	Transporte	**Aplica – B**	**Aplica – B**	**Aplica - B**

C	mp.si.5	Borrado y destrucción	**No Aplica**	**Aplica – M**	**Aplica – M**
	mp.sw	Protección de las aplicaciones informáticas			
categoría	mp.sw.1	Desarrollo	**No Aplica**	**Aplica – M**	**Aplica – M**
categoría	mp.sw.2	Aceptación y puesta en servicio	**Aplica – B**	**Aplica – M**	**Aplica – M**
	mp.info	Protección de la información			
categoría	mp.info.1	Datos de carácter personal	**Aplica – B**	**Aplica – B**	**Aplica – B**
C	mp.info.2	Calificación de la información	**Aplica – B**	**Aplica – M**	**Aplica – M**
C	mp.info.3	Cifrado	**No Aplica**	**No Aplica**	**No Aplica**
I A	mp.info.4	Firma electrónica	**Aplica – B**	**Aplica – M**	**Aplica – M**
T	mp.info.5	Sellos de tiempo	**No aplica**	**No aplica**	**No aplica**
C	mp.info.6	Limpieza de documentos	**Aplica – B**	**Aplica – B**	**Aplica – B**
D	mp.info.9	Copias de seguridad (back Up)	**No aplica**	**No aplica**	**Aplica – M**
	mp.s	Protección de los servicios			
categoría	mp.s.1	Protección del correo electrónico	**Aplica – B**	**Aplica – B**	**Aplica - B**
categoría	mp.s.2	Protección de servicios y aplicaciones web	**Aplica – B**	**Aplica – B**	**Aplica - B**
D	mp.s.8	Protección frente a la denegación de servicio	**No aplica**	**No aplica**	**Aplica – M**
D	mp.s.9	Medios alternativos	**No aplica**	**No Aplica**	**No Aplica**

8. Análisis de riesgos

El presente análisis de los riesgos fue desarrollado con el propósito de determinar cuáles de los activos utilizados por la UNIVERSIDAD DE JAÉN, tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos, identificando las causas potenciales que faciliten o impidan alcanzar los objetivos, calculando la probabilidad de su ocurrencia, evaluando sus probables efectos, y considerando el grado en que el riesgo puede ser controlado.

8.1. Metodología de análisis

Para la realización del análisis de riesgos se ha utilizado la herramienta PILAR, la cual utiliza la metodología Magerit, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información “Ministerio de Administraciones Públicas”.

Magerit cubre las actividades de análisis y tratamiento de riesgos facilitando una gestión de riesgos informada.

1. El análisis de riesgos le permite conocer su sistema: sus activos, su valor, y las amenazas a las que está expuesto.
2. El tratamiento de riesgos se centra en seleccionar medidas de seguridad para conjurar las amenazas.
3. La gestión de riesgos es el proceso integral de tratamiento de los riesgos descubiertos durante el análisis.

8.2. Procedimientos

Para el Análisis de riesgos

- Se identifican los Activos de la organización. Estos activos están expuestos a una serie de Amenazas que, cuando ocurren, degradan el valor del activo, causando un cierto Impacto.
- Se listan las Amenazas que afectan directa o indirectamente al Activo. Si estimamos la probabilidad de la amenaza, podemos concluir el Riesgo en el sistema, o la pérdida a la cual está expuesto.

La degradación y la probabilidad califican la vulnerabilidad del sistema frente a una amenaza.

Para la Gestión de riesgos

- Se desplegarán medidas de seguridad para hacer frente a las amenazas.
- Las medidas de seguridad mitigan los valores de impacto y riesgo dejándolos reducidos a unos valores residuales, que serán asumidos por la Organización.

La herramienta utilizada ha sido PILAR, que estima los riesgos según una escala de nueve valores:

PILAR presenta los niveles de criticidad con un decimal, de forma que se puede relativizar el riesgo relativo dentro de un mismo nivel.

8.3. Nivel de riesgo potencial

El riesgo potencial es el que presenta un activo antes de aplicarle ninguna medida de seguridad.

Activo	[D]	[I]	[C]	[A]	[T]
[B] Capa de negocio	{3,7}	{4,2}	{2,8}	{3,3}	{1,5}
[CRUE_05_01] Web Institucional	{3,7}	{4,2}	{1,6}	{3,3}	{1,5}
[SR02] Tablón de anuncios	{2,5}	{4,2}	{1,6}	{3,3}	{0,87}
[SR03] Gestión Económica. Perfil del contratante	{3,7}	{4,2}	{1,6}	{3,3}	{1,5}
[SR_FirmaElectronica] Secretaria General. Firma electrónica	{2,5}	{4,2}	{2,8}	{3,3}	{0,87}
[SR05] Verifirma	{2,5}	{4,2}	{1,6}	{3,3}	{0,87}
[CRUE_03_43] Secretaria General. Registro	{3,7}	{3,0}	{2,8}	{3,3}	{1,5}
[CRUE_03_06] Gestión Académica. Becas	{2,5}	{4,2}	{2,8}	{3,3}	{0,87}
[CRUE_03_05] Gestión Académica. Automatrícula	{3,7}	{3,0}	{2,8}	{2,1}	{1,5}
[CRUE_08_04] Autenticacion centralizada (SIDUJA)	{2,5}	{4,2}	{2,8}	{3,3}	{0,87}
[CRUE_03_45] Secretaria General. Convenios	{2,5}	{3,0}	{1,6}	{2,1}	{0,87}
[CRUE_03_36] Extensión Universitaria. Actividades Deportivas	{2,5}	{3,0}	{1,6}	{2,1}	{0,87}
[SR12] Investigación y transferencia: Portal del Investigador	{2,5}	{3,0}	{2,8}	{2,1}	{0,87}
[IN] Informacion	{3,7}	{4,2}	{4,5}	{4,2}	{1,5}
[IN01] Informacion General	{3,7}	{4,2}	{3,4}	{4,2}	{1,5}
[IN02] Programas de asignaturas	{3,7}	{4,2}	{3,4}	{4,2}	{1,5}
[IN03] Resoluciones	{2,5}	{4,2}	{3,4}	{4,2}	{0,87}
[IN04] Expedientes	{3,7}	{4,2}	{4,5}	{4,2}	{1,5}
[IN05] Certificados	{2,5}	{4,2}	{4,5}	{4,2}	{0,87}
[IN06] Documentos firmados	{2,5}	{4,2}	{3,4}	{4,2}	{0,87}
[IN07] Quejas y sugerencias	{3,7}	{3,0}	{4,5}	{4,2}	{1,5}
[IN08] Archivo General	{3,7}	{3,0}	{4,5}	{4,2}	{1,5}
[IN09] Estadísticas	{3,7}	{3,0}	{4,5}	{4,2}	{1,5}
[IN10] Solicitudes de becas	{2,5}	{4,2}	{4,5}	{4,2}	{0,87}
[IN11] Solicitud de matricula	{3,7}	{3,0}	{4,5}	{3,0}	{1,5}
[IN12] Resguardos de matricula	{3,7}	{3,0}	{4,5}	{3,0}	{1,5}
[IN13] Información pruebas de acceso	{3,7}	{3,0}	{4,5}	{3,0}	{1,5}
[IN14] Cuenta de correo electronico	{2,5}	{4,2}	{4,5}	{4,2}	{0,87}
[IN15] Expediente academico	{2,5}	{4,2}	{4,5}	{4,2}	{0,87}

[IN16] Convenios	{2,5}	{3,0}	{3,4}	{3,0}	{0,87}
[IN17] Solicitud utilizacion deportes	{2,5}	{3,0}	{3,4}	{3,0}	{0,87}
[IN18] Información Investigación (Planes, Noticias, Memorias, Convocatorias)	{2,5}	{3,0}	{4,5}	{3,0}	{0,87}
[IS] Servicios internos					
[E] Equipamiento	{3,7}	{4,2}	{3,9}	{3,3}	{1,5}
[SW] Aplicaciones					
[SW.SIS_www10.ujaen.es] www10.ujaen.es	{3,7}	{4,2}	{1,6}	{3,3}	{1,5}
[SW.SIS_www.ujaen.es] www.ujaen.es	{3,7}	{4,2}	{1,6}	{3,3}	{1,5}
[SW.SIS_Notario] Notario		{4,2}		{3,3}	
[SW.SIS_Portafirmas/Verifirma] Portafirmas/Verifirma	{2,1}	{3,9}	{3,9}	{3,3}	{0,87}
[SW.SIS_UXXIAC] UXXIAC	{3,7}	{3,9}	{3,9}	{3,3}	{1,5}
[SW.CLU_Firma] Firma	{3,7}	{2,1}	{2,8}		
[SW.CLU_IDP] Idp cluster	{2,5}	{3,9}	{3,9}	{3,3}	{0,87}
[HW] Equipos					
[HW.N/A-273] www10_frontend	{3,7}	{3,9}	{2,7}	{3,3}	{1,5}
[HW.N/A-296] www10_backend	{3,7}	{3,9}	{2,7}	{3,3}	{1,5}
[HW.102404] sabiote	{3,7}	{3,9}	{2,7}	{3,3}	{1,5}
[HW.VIR_alma2] alma2	{2,1}	{2,7}	{2,7}	{2,1}	{0,87}
[HW.37535] jabato	{2,1}	{2,7}	{2,7}	{2,1}	{0,87}
[COM] Comunicaciones					
[COM.SIS_RIUJA] RIUJA	{3,7}	{3,9}	{3,9}	{3,3}	{1,5}
[SS] Servicios subcontratados	{3,7}	{2,1}	{2,8}	{3,3}	{1,5}
[PRV_RICA-CICA] RICA-CICA	{3,7}	{2,1}	{2,8}	{3,3}	{1,5}
[L] Instalaciones	{3,3}	{2,8}	{2,8}		
[INS_CPD] CPD	{3,3}	{2,8}	{2,8}		
[P] Personal	{2,5}	{3,3}	{3,7}		
[PER_Administradores] Administradores	{1,8}	{3,3}	{3,7}		
[PER_Usuarios] Usuarios	{2,5}	{2,0}	{3,0}		

8.4. Cálculo del riesgo actual

El riesgo actual es el que presentan los activos considerando las medidas de seguridad (salvaguardas) implementadas en la organización.

Para el cálculo del riesgo actual se asigna un nivel de madurez al proceso asociado a la salvaguarda o medida de seguridad aplicable, de manera que el riesgo potencial al que está expuesto el activo se reduce en función de las medidas de seguridad aplicadas y el nivel de madurez de las mismas

Las salvaguardas actúan en el impacto y el riesgo, limitando el impacto de una amenaza, o reduciendo la probabilidad de que ocurra.
PILAR utiliza niveles de madurez para evaluar medidas de seguridad según la madurez de de proceso

Eficacia	Nivel	Significado
-	n.a.	no es aplicable
0%	L0	Inexistente
10%	L1	Inicial / ad hoc
50%	L2	Reproducible, pero intuitivo
90%	L3	Proceso definido
95%	L4	Gestionado y medible
100%	L5	Optimizado

L0 - Inexistente
En el nivel L0 de madurez no hay nada.
L1 - Inicial / ad hoc
En el nivel L1 de madurez, las medidas de seguridad existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta.
El éxito del nivel L1 depende de tener personal de la alta calidad.
L2 - Reproducible pero intuitivo
En el nivel L2 de madurez, la eficacia de las medidas de seguridad depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción heroica.
Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
L3 - Proceso definido
Se despliegan y se gestionan las medidas de seguridad. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado).
El éxito es algo más que buena suerte: se merece.
L4 – Gestionado y medible
Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las medidas de seguridad. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.
L5 - Optimizado

El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.
En este análisis de riesgos se han valorado las medidas de seguridad contempladas en el Esquema Nacional de Seguridad, usando para ello el Perfil de Seguridad incorporado en la herramienta PILAR.

8.5. Medidas de protección actuales y previstas

Código	Medida	Actual	Objetivo
C:org	Marco organizativo	L0-L1	L3
C:org.1	Política de Seguridad	L1	L3
C:org.2	Normativa de seguridad	L1	L3
C:org.3	Procedimientos de seguridad	L1	L3
C:org.4	Proceso de autorización	L0-1	L3
C:op	Marco operacional	_-L2	L3
C:op.pl	Planificación	_-L2	L3
C:op.pl.1	Análisis de riesgos	L0	L3
C:op.pl.2	Arquitectura de seguridad	L1-L2	L3
C:op.pl.3	Adquisición de nuevos componentes	L0	L3
C:op.pl.4	Dimensionamiento / Gestión de capacidades	L1	L3
C:op.pl.5	Componentes certificados	N/A	N/A
C:op.acc	Control de acceso	L1-L2	L3
C:op.acc.1	Identificación	L1	L3
C:op.acc.2	Requisitos de acceso	L1	L3
C:op.acc.3	Segregación de funciones y tareas	L2	L3
C:op.acc.4	Proceso de gestión de derechos de acceso	L1	L3
C:op.acc.5	Mecanismo de autenticación	L1	L3

C:op.acc.6	Acceso local (local logon)	L1	L3
C:op.acc.7	Acceso remoto (remote login)	L1-L2	L3
C:op.exp	Explotación	_-L2	L3
C:op.exp.1	Inventario de activos	L1-L2	L3
C:op.exp.2	Configuración de seguridad	L1	L3
C:op.exp.3	Gestión de la configuración	L0-L2	L3
C:op.exp.4	Mantenimiento	L1	L3
C:op.exp.5	Gestión de cambios	L1	L3
C:op.exp.6	Protección frente a código dañino	L0-L1	L3
C:op.exp.7	Gestión de incidencias	L0-L2	L3
C:op.exp.8	Registro de la actividad de los usuarios	N/A	N/A
C:op.exp.9	Registro de la gestión de incidencias	L2	L3
C:op.exp.10	Protección de los registros de actividad	N/A	N/A
C:op.exp.11	Protección de claves criptográficas	N/A	N/A
C:op.ext	Servicios externos	L0-L1	L3
C:op.ext.1	Contratación y acuerdos de nivel de servicio	L1	L3
C:op.ext.2	Gestión diaria	L0	L3
C:op.ext.9	Medios alternativos	N/A	N/A
C:op.cont	Continuidad del servicio	L0	L3
C:op.cont.1	Análisis de impacto	L0	L3
C:op.cont.2	Plan de continuidad	N/A	N/A
C:op.cont.3	Pruebas periódicas	N/A	N/A
C:op.mon	Monitorización del sistema	N/A	N/A
C:op.mon.1	Detección de intrusión	N/A	N/A
C:op.mon.2	Sistema de métricas	N/A	N/A

C:mp	Medidas de protección	L0-L2	L3
C:mp.if	Protección de las instalaciones e infraestructuras	L0-L2	L3
C:mp.if.1	Áreas separadas y con control de acceso	L0-L2	L3
C:mp.if.2	Identificación de las personas	L1	L3
C:mp.if.3	Acondicionamiento de los locales	L0	L3
C:mp.if.4	Energía eléctrica	L2	L3
C:mp.if.5	Protección frente a incendios	L2	L3
C:mp.if.6	Protección frente a inundaciones	L1	L3
C:mp.if.7	Registro de entrada y salida de equipamiento	L0	L3
C:mp.if.9	Instalaciones alternativas	N/A	N/A
C:mp.per	Gestión del personal	L0-L2	L3
C:mp.per.1	Caracterización del puesto de trabajo	L0	L3
C:mp.per.2	Deberes y obligaciones	L0	L3
C:mp.per.3	Concienciación	L1-L2	L3
C:mp.per.4	Formación	L1	L3
C:mp.per.9	Personal alternativo	N/A	N/A
C:mp.eq	Protección de los equipos	L0-L1	L3
C:mp.eq.1	Puesto de trabajo despejado	L0-L1	L3
C:mp.eq.2	Bloqueo del puesto de trabajo	L1	L3
C:mp.eq.3	Protección de equipos portátiles	L1	L3
C:mp.eq.9	Medios alternativos	L1	L3
C:mp.com	Protección de las comunicaciones	L1-L2	L3
C:mp.com.1	Perímetro seguro	L2	L3
C:mp.com.2	Protección de la confidencialidad	L1	L3
C:mp.com.3	Protección de la autenticidad y de la integridad	L1	L3

C:mp.com.4	Segregación de redes	N/A	N/A
C:mp.com.9	Medios alternativos	N/A	N/A
C:mp.si	Protección de los soportes de información	L0-L1	L3
C:mp.si.1	Etiquetado	L0	L3
C:mp.si.2	Criptografía	L0	L3
C:mp.si.3	Custodia	L1	L3
C:mp.si.4	Transporte	L0	L3
C:mp.si.5	Borrado y destrucción	L1	L3
C:mp.sw	Protección de las aplicaciones informáticas (SW)	L1-L2	L3
C:mp.sw.1	Desarrollo de aplicaciones	L1-L2	L3
C:mp.sw.2	Aceptación y puesta en servicio	L1	L3
C:mp.info	Protección de la información	L0-L1	L3
C:mp.info.1	Datos de carácter personal	L1	L3
C:mp.info.2	Calificación de la información	L1	L3
C:mp.info.3	Cifrado de la información	N/A	N/A
C:mp.info.4	Firma electrónica	L1	L3
C:mp.info.5	Sellos de tiempo	N/A	N/A
C:mp.info.6	Limpieza de documentos	L0	L3
C:mp.info.9	Copias de seguridad (backup)	L1	L3
C:mp.s	Protección de los servicios	L1-L2	L3
C:mp.s.1	Protección del correo electrónico (e-mail)	L2	L3
C:mp.s.2	Protección de servicios y aplicaciones web	L1	L3
C:mp.s.8	Protección frente a la denegación de servicio	L2	L3
C:mp.s.9	Medios alternativos	N/A	N/A

8.6. Nivel de riesgo actual

Activo	[D]	[I]	[C]	[A]	[T]
[B] Capa de negocio	{3,3}	{4,0}	{2,7}	{2,8}	{1,3}
[CRUE_05_01] Web Institucional	{3,3}	{4,0}	{1,5}	{2,8}	{1,3}
[SR02] Tablón de anuncios	{2,1}	{4,0}	{1,5}	{2,8}	{0,82}
[SR03] Gestión Económica. Perfil del contratante	{3,3}	{4,0}	{1,5}	{2,8}	{1,3}
[SR_FirmaElectronica] Secretaria General. Firma electrónica	{2,1}	{4,0}	{2,7}	{2,8}	{0,82}
[SR05] Verifirma	{2,1}	{4,0}	{1,5}	{2,8}	{0,82}
[CRUE_03_43] Secretaria General. Registro	{3,3}	{2,8}	{2,7}	{2,8}	{1,3}
[CRUE_03_06] Gestión Académica. Becas	{2,1}	{4,0}	{2,7}	{2,8}	{0,82}
[CRUE_03_05] Gestión Académica. Automatrícula	{3,3}	{2,8}	{2,7}	{1,4}	{1,3}
[CRUE_08_04] Autenticacion centralizada (SIDUJA)	{2,1}	{4,0}	{2,7}	{2,8}	{0,82}
[CRUE_03_45] Secretaria General. Convenios	{2,1}	{2,8}	{1,5}	{1,4}	{0,83}
[CRUE_03_36] Extensión Universitaria. Actividades Deportivas	{2,1}	{2,8}	{1,5}	{1,4}	{0,83}
[SR12] Investigación y transferencia: Portal del Investigador	{2,1}	{2,8}	{2,7}	{1,4}	{0,83}
[IN] Informacion	{3,5}	{4,1}	{4,4}	{3,8}	{1,5}
[IN01] Informacion General	{3,5}	{4,1}	{3,3}	{3,8}	{1,5}
[IN02] Programas de asignaturas	{3,5}	{4,1}	{3,3}	{3,8}	{1,5}
[IN03] Resoluciones	{2,4}	{4,1}	{3,3}	{3,8}	{0,85}
[IN04] Expedientes	{3,5}	{4,1}	{4,4}	{3,8}	{1,5}
[IN05] Certificados	{2,4}	{4,1}	{4,4}	{3,8}	{0,85}
[IN06] Documentos firmados	{2,4}	{4,1}	{3,3}	{3,8}	{0,85}
[IN07] Quejas y sugerencias	{3,5}	{2,9}	{4,4}	{3,8}	{1,5}
[IN08] Archivo General	{3,5}	{2,9}	{4,4}	{3,8}	{1,5}
[IN09] Estadísticas	{3,5}	{2,9}	{4,4}	{3,8}	{1,5}
[IN10] Solicitudes de becas	{2,4}	{4,1}	{4,4}	{3,8}	{0,85}
[IN11] Solicitud de matricula	{3,5}	{2,9}	{4,4}	{2,5}	{1,5}
[IN12] Resguardos de matricula	{3,5}	{2,9}	{4,4}	{2,5}	{1,5}
[IN13] Información pruebas de acceso	{3,5}	{2,9}	{4,4}	{2,5}	{1,5}
[IN14] Cuenta de correo electronico	{2,4}	{4,1}	{4,4}	{3,8}	{0,85}
[IN15] Expediente academico	{2,4}	{4,1}	{4,4}	{3,8}	{0,85}
[IN16] Convenios	{2,4}	{2,9}	{3,3}	{2,5}	{0,85}
[IN17] Solicitud utilizacion deportes	{2,4}	{2,9}	{3,3}	{2,5}	{0,85}

[IN18] Información Investigación (Planes, Noticias, Memorias, Convocatorias)	{2,4}	{2,9}	{4,4}	{2,5}	{0,85}
[IS] Servicios internos					
[E] Equipamiento	{3,6}	{4,0}	{3,8}	{2,9}	{1,3}
[SW] Aplicaciones					
[SW.SIS_www10.ujaen.es] www10.ujaen.es	{3,3}	{4,0}	{1,5}	{2,8}	{1,3}
[SW.SIS_www.ujaen.es] www.ujaen.es	{3,3}	{4,0}	{1,5}	{2,8}	{1,3}
[SW.SIS_Notario] Notario		{4,0}		{2,8}	
[SW.SIS_Portafirmas/Verifirma] Portafirmas/Verifirma	{2,0}	{3,8}	{3,8}	{2,8}	{0,85}
[SW.SIS_UXXIAC] UXXIAC	{3,3}	{3,7}	{3,7}	{2,8}	{1,3}
[SW.CLU_Firma] Firma	{3,6}	{1,9}	{2,7}		
[SW.CLU_IDP] Idp cluster	{2,1}	{3,6}	{3,6}	{2,8}	{0,81}
[HW] Equipos					
[HW.N/A-273] www10_frontend	{3,6}	{3,7}	{2,5}	{2,8}	{1,3}
[HW.N/A-296] www10_backend	{3,6}	{3,7}	{2,5}	{2,8}	{1,3}
[HW.102404] sabiote	{3,3}	{3,7}	{2,5}	{2,8}	{1,3}
[HW.VIR_alma2] alma2	{2,0}	{2,6}	{2,6}	{1,4}	{0,85}
[HW.37535] jabato	{2,0}	{2,6}	{2,6}	{1,4}	{0,85}
[COM] Comunicaciones					
[COM.SIS_RIUJA] RIUJA	{3,6}	{3,7}	{3,7}	{2,9}	{1,3}
[SS] Servicios subcontratados	{2,7}	{1,6}	{2,3}	{2,0}	{1,1}
[PRV_RICA-CICA] RICA-CICA	{2,7}	{1,6}	{2,3}	{2,0}	{1,1}
[L] Instalaciones	{3,3}	{2,0}	{2,2}		
[INS_CPD] CPD	{3,3}	{2,0}	{2,2}		
[P] Personal	{2,1}	{2,2}	{2,7}		
[PER_Administradores] Administradores	{1,3}	{2,2}	{2,7}		
[PER_Usuarios] Usuarios	{2,1}	{0,99}	{2,0}		

8.7. Nivel de riesgo aceptable

Se considera que el nivel de riesgo aceptable es 2,5

8.8. Nivel de riesgo objetivo

Activo	[D]	[I]	[C]	[A]	[T]
[B] Capa de negocio	{0,71}	{1,2}	{0,88}	{0,75}	{0,60}
[CRUE_05_01] Web Institucional	{0,70}	{1,2}	{0,64}	{0,75}	{0,60}
[SR02] Tablón de anuncios	{0,43}	{0,97}	{0,64}	{0,75}	{0,31}

[SR03] Gestión Económica. Perfil del contratante	{0,70}	{1,2}	{0,64}	{0,75}	{0,60}
[SR_FirmaElectronica] Secretaria General. Firma electrónica	{0,43}	{0,97}	{0,88}	{0,75}	{0,31}
[SR05] Verifirma	{0,43}	{0,97}	{0,64}	{0,75}	{0,31}
[CRUE_03_43] Secretaria General. Registro	{0,71}	{0,79}	{0,88}	{0,75}	{0,60}
[CRUE_03_06] Gestión Académica. Becas	{0,43}	{0,97}	{0,88}	{0,75}	{0,31}
[CRUE_03_05] Gestión Académica. Automatrícula	{0,71}	{0,79}	{0,88}	{0,26}	{0,60}
[CRUE_08_04] Autenticacion centralizada (SIDUJA)	{0,43}	{0,97}	{0,88}	{0,75}	{0,31}
[CRUE_03_45] Secretaria General. Convenios	{0,47}	{0,79}	{0,64}	{0,26}	{0,37}
[CRUE_03_36] Extensión Universitaria. Actividades Deportivas	{0,46}	{0,79}	{0,64}	{0,26}	{0,37}
[SR12] Investigación y transferencia: Portal del Investigador	{0,47}	{0,79}	{0,88}	{0,26}	{0,37}
[IN] Informacion	{0,65}	{1,8}	{2,2}	{1,2}	{0,67}
[IN01] Informacion General	{0,65}	{1,8}	{1,0}	{1,2}	{0,67}
[IN02] Programas de asignaturas	{0,65}	{1,8}	{1,0}	{1,2}	{0,67}
[IN03] Resoluciones	{0,42}	{1,8}	{1,0}	{1,2}	{0,43}
[IN04] Expedientes	{0,65}	{1,8}	{2,2}	{1,2}	{0,67}
[IN05] Certificados	{0,42}	{1,8}	{2,2}	{1,2}	{0,43}
[IN06] Documentos firmados	{0,42}	{1,8}	{1,0}	{1,2}	{0,43}
[IN07] Quejas y sugerencias	{0,65}	{0,92}	{2,2}	{1,2}	{0,67}
[IN08] Archivo General	{0,65}	{0,92}	{2,2}	{1,2}	{0,67}
[IN09] Estadísticas	{0,65}	{0,92}	{2,2}	{1,2}	{0,67}
[IN10] Solicitudes de becas	{0,42}	{1,8}	{2,2}	{1,2}	{0,43}
[IN11] Solicitud de matricula	{0,65}	{0,92}	{2,2}	{0,69}	{0,67}
[IN12] Resguardos de matricula	{0,65}	{0,92}	{2,2}	{0,69}	{0,67}
[IN13] Información pruebas de acceso	{0,65}	{0,92}	{2,2}	{0,69}	{0,67}
[IN14] Cuenta de correo electronico	{0,42}	{1,8}	{2,2}	{1,2}	{0,43}
[IN15] Expediente academico	{0,42}	{1,8}	{2,2}	{1,2}	{0,43}
[IN16] Convenios	{0,42}	{0,92}	{1,0}	{0,69}	{0,43}
[IN17] Solicitud utilizacion deportes	{0,42}	{0,92}	{1,0}	{0,69}	{0,43}
[IN18] Información Investigación (Planes, Noticias, Memorias, Convocatorias)	{0,42}	{0,92}	{2,2}	{0,69}	{0,43}
[IS] Servicios internos					
[E] Equipamiento	{0,70}	{1,2}	{1,0}	{0,77}	{0,60}
[SW] Aplicaciones					

[SW.SIS_www10.ujaen.es] www10.ujaen.es	{0,70}	{1,2}	{0,64}	{0,75}	{0,60}
[SW.SIS_www.ujaen.es] www.ujaen.es	{0,70}	{1,2}	{0,64}	{0,75}	{0,60}
[SW.SIS_Notario] Notario		{0,97}		{0,75}	
[SW.SIS_Portafirmas/Verifirma] Portafirmas/Verifirma	{0,34}	{0,96}	{0,96}	{0,75}	{0,25}
[SW.SIS_UXXIAC] UXXIAC	{0,67}	{1,0}	{1,0}	{0,75}	{0,53}
[SW.CLU_Firma] Firma	{0,67}	{0,34}	{0,50}		
[SW.CLU_IDP] Idp cluster	{0,43}	{0,92}	{0,92}	{0,75}	{0,21}
[HW] Equipos					
[HW.N/A-273] www10_frontend	{0,67}	{0,92}	{0,68}	{0,75}	{0,44}
[HW.N/A-296] www10_backend	{0,67}	{0,92}	{0,68}	{0,75}	{0,44}
[HW.102404] sabiote	{0,67}	{1,0}	{0,77}	{0,75}	{0,53}
[HW.VIR_alma2] alma2	{0,34}	{0,72}	{0,72}	{0,26}	{0,25}
[HW.37535] jabato	{0,34}	{0,72}	{0,72}	{0,26}	{0,25}
[COM] Comunicaciones					
[COM.SIS_RIUJA] RIUJA	{0,64}	{0,80}	{0,80}	{0,77}	{0,33}
[SS] Servicios subcontratados	{0,59}	{0,54}	{0,69}	{0,59}	{0,44}
[PRV_RICA-CICA] RICA-CICA	{0,59}	{0,54}	{0,69}	{0,59}	{0,44}
[L] Instalaciones	{0,67}	{0,53}	{0,53}		
[INS_CPD] CPD	{0,67}	{0,53}	{0,53}		
[P] Personal	{0,45}	{0,52}	{0,63}		
[PER_Administradores] Administradores	{0,31}	{0,52}	{0,63}		
[PER_Usuarios] Usuarios	{0,45}	{0,27}	{0,49}		

9. Plan de mejora

9.1. Introducción

En esta sección se identifican las tareas a llevar a cabo para cumplir con los requisitos planteados por el Esquema Nacional de Seguridad para los sistemas de información de la Universidad de Jaén que dan soporte a la Administración Electrónica.

El buen estado de la seguridad en la organización permitirá ajustarse a dichos requisitos sin excesivos esfuerzos humanos ni económicos.

Se han identificado dos principales carencias que consumirán la mayor parte de los recursos:

- **Documentación.** Existen numerosas tareas que se ejecutan sin que haya procedimientos formalmente aprobados ni quede constancia de su ejecución. El ENS requiere que exista un sistema documental que recoja la sistemática que se utiliza para gestionar la seguridad.

- **Formación.** El ENS requiere que todo el personal sea concienciado de sus responsabilidades en la medida que apliquen a su puesto de trabajo y que se reciba formación específica en seguridad.

9.2. Objetivo

El presente plan de actuación tiene como objetivo planificar la implantación de las medidas técnicas y organizativas que permitan cumplir con lo establecido en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad para los sistemas soportados por la Universidad de Jaén.
Este plan detalla las insuficiencias encontradas. Las anomalías detectadas provienen de:

- Incumplimiento de las medidas de seguridad que aplican según la categorización del sistema, recogidas en el presente Plan de Adecuación.
- Incumplimiento formal de las medidas de seguridad exigidas por el RD 1720/1997 para los datos de carácter personal tratados por el sistema
- Existencia de riesgos no asumibles por la entidad.

9.3. Alcance

Este plan comprende todos los activos recogidos en el Análisis de Riesgos de la entidad.

9.4. Calendario

El Esquema Nacional de Seguridad establece un plazo de un año desde su publicación (30 de Enero de 2010) para su cumplimiento. No obstante da un margen de tres años más para aquellas organizaciones que en ese plazo no puedan hacer frente a todas las tareas, en cuyo caso exige la elaboración del Plan de Adecuación.
Aunque la fecha límite para la elaboración del presente Plan de Adecuación era el 30 de Enero de 2011, se dispone de otros tres años adicionales, es decir, hasta el pasado 30 de Enero de 2014, para la completa implantación de todas las medidas definidas en el presente Plan.

9.5. Responsabilidades

El Responsable de Seguridad se encargará de la ejecución y supervisión en su caso de las distintas actividades.
El Responsable de los Servicios revisará y aprobará el Plan y los objetivos marcados en el mismo, proporcionando además los recursos necesarios para el cumplimiento del mismo.

9.6. Seguimiento

El Responsable de Seguridad verificará el cumplimiento del plan para el periodo establecido y lo irá actualizando conforme se vayan realizando las acciones. En caso de desviaciones se tomarán las medidas oportunas para corregirlas y en caso necesario se actualizará el plan para reflejar los cambios.

Una vez finalizado el periodo establecido por el ENS, se deberían haber finalizado todas las acciones.

9.7. Acciones de adaptación al ENS

9.7.1. Comité de seguridad de la Información

Definir y establecer los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo. Se debe determinar qué personas formarán parte del Comité de Seguridad de la Información, detallando su ámbito de responsabilidad y sus posibles relaciones con otros elementos de la organización.

9.7.2. Definir los procedimientos de seguridad

Diseñar y documentar procedimientos operativos de seguridad que cubran, al menos, los siguientes aspectos:

- Gestión de personal
- Procesos de autorización y control de accesos
- Protección de las instalaciones
- Protección de las telecomunicaciones
- Sistemas de registro
- Gestión de incidentes de seguridad
- Plan de continuidad del servicio
- Monitorización del sistema
- Plan de auditorías de seguridad

9.7.3. Implantar procedimientos

Una vez desarrollados los procedimientos, deben ponerse en funcionamiento. Debe controlarse la efectividad de la implantación así como la idoneidad de lo descrito en los procedimientos.

9.7.4. Programa de formación

De acuerdo al Esquema Nacional de Seguridad, todos los miembros de la Universidad de Jaén deben involucrarse en el proceso de seguridad de la información y conocer y comprender las normas y procedimientos establecidos.
La mejor manera es la realización de jornadas de formación sobre la política, normativa y procedimientos de seguridad de manera que el personal aprenda y asimile las indicaciones sobre las normas con las que deben trabajar.
Se deben evaluar los resultados obtenidos en relación a los objetivos perseguidos con las acciones formativas.

9.7.5. Monitorización y supervisión

El proceso de seguridad de la información es un proceso dinámico que requiere ser verificado de una manera continua para detectar posibles errores así como medidas, normas y/o elementos

que hayan podido quedar obsoletos y que provoquen que no se esté realizando una efectiva gestión de los riesgos en la organización.
Deben establecerse los mecanismos que permitan la detección de todos estos elementos variables, al menos:

- Auditorías de seguridad de la información
- Gestión de incidentes

9.7.6. Actualización y mantenimiento del sistema

El sistema debe mantenerse actualizado de acuerdo a los nuevos enfoques, tendencias, nuevas tecnologías y cumplimientos legales que se requieran en la Universidad de Jaén. Se deben establecer procedimientos para la gestión de desviaciones respecto a las normativas de seguridad y del propio Esquema Nacional de Seguridad.
Se deben elaborar planes de auditoría y de formación para mantener a todos los miembros de la Universidad de Jaén sensibilizados con el proceso de seguridad de la información implantado.

9.7.7. Programa de auditorías

El Esquema Nacional de Seguridad establece la necesidad de realizar una auditoría completa del sistema al menos cada dos años.
No obstante, en el proceso de desarrollo e implantación del ENS, será conveniente realizar auditorías con una mayor frecuencia, al menos hasta que se haya logrado un buen ajuste y una buena asimilación de los procesos dentro de la organización.

9.8. Implantación de Medidas de Seguridad

Se han definido bloques de actuación para la implantación de las medidas de seguridad, correspondientes a los distintos tipos de medidas a implantar según están definidas en la Declaración de Aplicabilidad.

9.8.1. Actuación 1: Marco organizativo

Medidas de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Política de seguridad	La Universidad de Jaén dispone de una versión en borrador de la Política general de seguridad de la información donde se integra los principios del ENS y la LOPD.	Se debería aprobar formalmente la Política de Seguridad de la Información y difundirla a todo el personal.	1-1
Normativa de seguridad	Solo existe una normativa de uso del correo electrónico.	Se deberían desarrollar, implementar y aprobar directrices que comprendan todos los puntos del Esquema Nacional de Seguridad, para el buen uso de los	1-2

		equipos, recursos, servicios, información e instalaciones. Asimismo deberán publicarse y comunicarse a todos los usuarios internos y externos de la universidad.	
Procedimientos de seguridad	Existen procedimientos de LOPD y de calidad.	Si bien se siguen procedimientos de actuación para algunas tareas (Documento de Seguridad LOPD), estos no están basados en el Esquema Nacional de Seguridad. No se han definido e implantado la totalidad de los Procedimientos de Seguridad.	1-3
Proceso de Autorización	Se cuenta algún proceso de autorización aunque no está definido formalmente.	No se han definido e implantado formalmente la totalidad de los Procesos de Autorización.	1-4

9.8.1.1. Acción 1-1 Aprobación y distribución de la Política de Seguridad

Se completará la documentación y aprobación formal de la Política de Seguridad y se distribuirá entre el personal. La Política debe cubrir todos los aspectos incluidos en las medidas de seguridad de la información (Gestión de comunicaciones, Seguridad física y lógica, Recursos Humanos, etc.)

La Política ha de ser aprobada por el órgano superior competente que corresponda y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

- Los objetivos o misión de la Universidad de Jaén.
- El marco legal y regulatorio en el que se desarrollarán las actividades.
- Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
- La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

La Política de Seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, de desarrollo de la Ley Orgánica de Protección de Datos, en lo que corresponda, lo que implica evitar duplicidades o incompatibilidades entre las directrices especificadas en uno y otro documento.

9.8.1.2. Acción 1-2 Elaboración de la Normativa de Seguridad

Se dispondrá de una serie de documentos, o se incorporarán a la Política de Seguridad, en los que se describa:

- Lo que se considerará uso indebido de los equipos que intervienen en el proceso de administración electrónica y otros procesos en el alcance.
- El uso correcto de equipos, servicios e instalaciones.
- La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Es decir, se establecerá una política de uso aceptable de los sistemas de información, que deberá ser respetada por el personal de la organización y de organizaciones externas que dispongan de acceso a los mismos. El personal deberá conocer esta 'política de uso aceptable', debiendo ser consciente de las actividades que no puede realizar con los sistemas de información porque puedan poner en peligro la integridad de los mismos.

9.8.1.3. Acción 1-3 Elaboración de los Procedimientos de Seguridad

Se elaborarán un conjunto de documentos (procedimientos) en los que se detallará la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad de la información. En estos procedimientos se indicará de forma clara y precisa:

- Cómo llevar a cabo las tareas habituales.
- Quién debe hacer cada tarea.
- Cómo identificar y reportar comportamientos inadecuados.

Ejemplo de procedimientos habituales en cuanto a seguridad de la información pueden ser: Procedimiento de Copias de Seguridad, Procedimiento de Control de Acceso Lógico, Procedimiento de Gestión de Incidencias, etc.

9.8.1.4. Acción 1-4 Definición del Proceso de Autorización

Se comprobará que se sigue un proceso formal de autorizaciones que cubra todos los elementos de los sistemas de información:

- Entrada de equipos en producción.
- Entrada de aplicaciones en producción.
- Establecimiento de enlaces de comunicaciones con otros sistemas.
- Utilización de instalaciones, habituales y alternativas.
- Utilización de medios de comunicación, habituales y alternativos.
- Utilización de soportes de información.
- Utilización de equipos móviles (portátiles, Smartphone, Tablet, etc.).

Las nuevas instalaciones de sistemas (si las hubiera), equipos o aplicaciones, así como el uso de instalaciones y equipamiento informático o soportes extraíbles será controlado y autorizado por parte de los Responsables competentes.

Se comprobará la existencia de registros que acrediten estas autorizaciones, por ejemplo, listas de usuarios autorizados para acceder a los sistemas, registros de entrada y salida de soportes, etc.

9.8.2. Actuación 2: Planificación

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Análisis de Riesgos	La universidad solo cuenta con un inventario de activos.	No se ha realizado un Análisis de Riesgos de los activos relacionados con la Administración Electrónica.	2-1
Arquitectura de seguridad	Existen diagramas de conexiones, esquemas de líneas de defensa y sistemas de identificación y autenticación de usuarios.	No se han realizado documentos que describan los controles técnicos internos y los sistemas de gestión de actualización y aprobación periódica. Será necesario definir un protocolo de revisiones / actualizaciones de la Arquitectura de Seguridad.	2-2
Adquisición de nuevos componentes	No existe un proceso formal para planificar la adquisición de nuevos componentes del sistema.	Se deberá elaborar y aprobar formalmente un proceso para planificar la adquisición de nuevos componentes atendiendo a las conclusiones de un análisis de riesgo previo y a necesidades formativas y financieras.	2-3
Dimensionamiento / Gestión de Capacidades	Cuando se planifican nuevos proyectos, se estiman las necesidades de capacidad de manera informal y se amplía según se necesite, pero no existe un proceso formal.	Se documentarán las sistemáticas de gestión de la capacidad. Con carácter previo a la explotación de un sistema se documentarán los requisitos de capacidad.	2-4
Componentes certificados	No se utilizan componentes certificados ni se da prioridad a estos componentes en las compras. Esta medida sólo es necesaria en sistemas de nivel alto.	No Aplica la medida de seguridad.	

9.8.2.1. Acción 2-1 Realización del Análisis de Riesgos

Se realizará un Análisis formal, utilizado la herramienta PILAR, que implementa la metodología MAGERIT. PILAR es una aplicación reconocida internacionalmente, a través de la cual se podrán seguir los siguientes pasos:

- Identificación y valoración de los activos del sistema.
- Identificación de las amenazas.
- Identificación y valoración de las medidas de seguridad que protegen dichas amenazas.
- Identificación y valoración de los riesgos residuales

9.8.2.2. Acción 2-2 Documentación de Arquitectura de Seguridad

Identificar y controlar la documentación que describa las instalaciones:

- Áreas donde se encuentran los sistemas de información.
- Puntos de acceso a las instalaciones.

Comprobar que la documentación que describe el sistema informático abarca:

- Equipos informáticos (puestos de usuario y servidores).
- Redes internas y conexiones al exterior.
- Puntos de acceso al sistema (puestos de trabajo y consolas de administración).
- Esquema de líneas de defensa.
- Puntos de interconexión a otros sistemas o a otras redes, en especial si se trata de Internet.
- Cortafuegos, DMZs, etc.
- Sistema de identificación y autenticación de usuarios.
- Controles técnicos internos (Validación de datos de entrada, salida e intermedios)

9.8.2.3. Acción 2-3 Adquisición de nuevos componentes

Se completará la documentación del proceso formal seguido para la adquisición de nuevos componentes del sistema, que se realizarán según las conclusiones del análisis de riesgo y a las necesidades técnicas, de formación y de financiación de la organización así como los requisitos planteados por el ENS.

9.8.2.4. Acción 2-4 Dimensionamiento y Gestión de la Capacidad

Se definirá el procedimiento, y se implantará formalmente, para garantizar que previamente a la puesta en marcha de nuevos sistemas de información se estudiarán las necesidades, recursos y capacidad del sistema, cubriendo aspectos como las necesidades de procesamiento, las de almacenamiento, las de comunicación, las de personal y las de instalaciones y medios auxiliares.

9.8.3. Actuación 3: Control de Accesos

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Identificación	Cada usuario cuenta con su propio identificador y clave de acceso. Con ellas accede a una serie de	Se deben revisar los derechos de accesos para evitar que personal que ya no está	3-1

	aplicaciones predeterminadas para su perfil, en función de los privilegios definidos por el jefe de servicio. Aun así se tienen algunas cuentas compartidas y se conservan habilitadas algunos servicios como el correo por política. No se le da de baja completa a ningún usuario, se mantienen el correo y la información (Ejemplo: guía de docentes), por política de retención de materiales.	autorizado siga accediendo a los recursos.	
Requisitos de acceso	Los accesos a los sistemas y la información están controlados, por usuario y contraseña en equipos y para los servicios de la administración electrónica mediante certificado del FNMT y DNIe permitiendo dichos accesos sólo a personal que lo necesite en función de su puesto y funciones. No obstante los usuarios tienen privilegios de administrador en sus propios equipos, por lo que podrían cambiar la configuración de este sin autorización del servicio de informática, realmente sólo se controla el acceso a los componentes de las aplicaciones.	Todo el personal PDI y PAS tienen permisos de administración local, lo que podría suponer un riesgo si modifican permisos de manera no autorizada.	3-2
Segregación de funciones y tareas	Las tareas se encuentran segregadas y los entornos de desarrollo están separados de las de pruebas y producción, así como las funciones de configuración y mantenimiento.	No existen insuficiencias	
Proceso de gestión de derechos de acceso	Los privilegios no necesariamente se limitarán a lo necesario para cumplir con sus obligaciones. Los usuarios mayormente acceden a la información que necesiten para el desarrollo de sus funciones, de acuerdo a su perfil, previa autorización.	No hay un proceso formal generalizado para gestión de derechos y revisión de privilegios.	3-3

Mecanismo de autenticación	Los usuarios acceden con usuario y contraseña, aunque no se puede controlar la generación y uso de contraseña. No se atiende a la seguridad de los autenticadores, por ejemplo hay contraseñas que son compartidas por varios usuarios y que no se deshabilitan cuando la entidad que autentica termina su relación con el sistema, solo se limitan los permisos. No existen Normativas de cuentas personales (PAS y PDI).	No se aplican reglas básicas de calidad para la creación de contraseñas y no se puede controlar los cambios y uso de las mismas, debido a que los usuarios tienen privilegios de administradores sobre sus ordenadores. Asimismo hay contraseñas compartidas por varios usuarios, y que no se deshabilitan cuando termina su relación con el sistema.	3-4
Acceso local (local logon)	Al no contar con un directorio activo no se pueden controlar los accesos.	Los usuarios PAS y PDI disponen de permisos de administración, por lo que no se pueden controlar los accesos.	3-5
Acceso remoto (remote login)	Las conexiones remotas, que se realizan vía web a las aplicaciones y por VPN a los servidores.	Documentar el control de acceso remoto y las medidas de seguridad asociadas.	3-6

9.8.4. Acción 3-1 Identificación de los usuarios

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

- Se asignará un identificador singular para cada entidad (usuario o proceso) que accede al sistema, de tal forma que se pueda garantizar la imputabilidad de las operaciones.
- Las cuentas de usuario se gestionarán de la siguiente forma:
    - Cada cuenta estará asociada a un identificador único.
    - Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario.
    - Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas.

9.8.5. Acción 3-2. Requisitos de acceso

Se definirá un Procedimiento de Control de accesos para definir los requisitos de acceso a los componentes del sistema y a sus ficheros y registros de configuración, así como a la información procesada a través del sistema. Los derechos de acceso de cada recurso, se establecerán según

las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad.

9.8.6. Acción 3-3. Proceso de gestión de derechos de acceso

Se revisarán los derechos de acceso de cada usuario y se implantarán teniendo en cuenta las siguientes consideraciones:

- Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones.
- Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.
- Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos.

9.8.7. Acción 3-4. Mecanismos de autenticación

Los mecanismos de autenticación frente al sistema se adecuarán según las siguientes consideraciones:

- Los autenticadores estarán bajo el control exclusivo del usuario.
- El usuario reconocerá que los ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
- Los autenticadores se cambiarán con una periodicidad marcada por un procedimiento formal.
- Los autenticadores se retirarán y serán deshabilitados cuando el usuario que autentica termina su relación con el sistema.
- No se recomendará el uso de claves concertadas.
- Se recomendará el uso de otro tipo de mecanismos del tipo dispositivos físicos (tokens) o componentes lógicos tales como certificados software u otros equivalentes o biométricos.
- Para las contraseñas se aplicarán políticas más rigurosas de calidad de la contraseña y renovación frecuente.

9.8.8. Acción 3-5. Mecanismo de Acceso local

El Mecanismo de acceso local al sistema de información se adecuará a las siguientes consideraciones:

- Se prevendrán ataques que puedan revelar información del sistema sin llegar a acceder al mismo.
- El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos. Es recomendable no conceder más de 3 intentos de acceso a los usuarios antes de bloquearse los equipos.
- Se registrarán los accesos con éxito, y los fallidos.
- El sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso.

- Se informará al usuario del último acceso efectuado con su identidad.

9.8.9. Acción 3-6. Mecanismo de Acceso Remoto

Se establecerá una política específica de lo que puede hacerse remotamente, requiriéndose autorización positiva a través de medios seguros.

9.8.10. Actuación 4: Explotación

Medida de seguridad	Situación Actual	Insuficiencia del Sistema	Acc.
Inventario de activos	Existe un Inventario de activos de la entidad relacionados con los servicios electrónicos así como de los elementos TIC en la herramienta de gestión de la CMDB.	No existen insuficiencias.	
Configuración de seguridad	No existen cuentas y contraseñas "estándar" sólo en servidores. No se aplica reglas mínima funcionalidad, todos los usuarios tienen permiso de admiración en sus ordenadores.	No hay pautas para la configuración de servidores y equipos y no se aplica la regla de mínima funcionalidad (No proporcionar funciones gratuitas, ni de operación ni de operación, etc.).	4-1
Gestión de la configuración	Existe documentación sobre la configuración inicial de los equipos.	No se puede garantizar que los usuarios no hagan cambios en los equipos. Se han de realizar auditorías de control de la CMDB.	4-1
Mantenimiento	El servicio de informática realiza las actividades de mantenimiento de los equipos.	Debe documentarse las actividades que se ejecutan durante los mantenimientos preventivos/correctivos a equipos y servidores. Se deben registrar los mantenimientos de los servidores.	4-1
Gestión de cambios	Se intenta analizar los cambios anunciados por los fabricantes o proveedores para determinar su conveniencia antes de ser	No se realiza un control de cambios de manera estructurada (no se analizan los riesgos para saber si los cambios son	4-1

	incorporados. Sólo lo servidores disponen de entorno de pre producción.	relevantes para la seguridad) y formal. Se debe documentar el proceso. Se debe disponer de un sistema para controlar las versiones de las aplicaciones desarrolladas internamente.	
Protección frente a código dañino	La Universidad de Jaén dispone de un sistema antivirus perimetral, en los equipos, aunque el usuario al tener permiso de administrador lo puede eliminar. A nivel de red: 1IDS, 1 anti spam, 1 antivirus, 2 firewall en cascada de diferentes fabricantes.	No se puede controlar que los usuarios tenga activo y actualizado el sistema antivirus perimetral instalados en sus equipos, por lo que no se puede garantizar la seguridad de los sistemas de información.	4-1
Gestión de incidencias	La gestión de incidencias no se encuentra implantada, aunque la definición de "incidencia de seguridad" está incluida en el Documento de Seguridad de la LOPD.,	No se cuenta con una sistemática establecida para gestionar adecuadamente las incidencias que aplican al Esquema Nacional de Seguridad. Sería recomendable integrar los conceptos y las actividades ya definidas hasta ahora para dar cumplimiento a la Ley Orgánica de Protección de Datos.	4-1
Registro de la actividad de los usuarios	No aplica esta medida para la categoría de los sistemas identificada. Aplica a categoría Alta.	No Aplica esta medida de seguridad.	
Registro de la gestión de incidencias	Se dispone de una aplicación para la gestión de las incidencias.	Concretar la sistemática para registrar las incidencias que aplican al Esquema Nacional de Seguridad.	4-1
Protección de los registros de actividad	No aplica esta medida para la categoría de los sistemas identificada. Aplica a categoría Alta.	No Aplica esta medida de seguridad.	

9.8.10.1. Acción 4-1 Formalizar la seguridad en la explotación

Plasmar documentalmente todos los procesos necesarios para una gestión de la seguridad en la explotación acorde con los requisitos de la entidad y del ENS, aprobarlos formalmente, difundirlos e implantarlos tales como:

- **Gestión del Inventario de activos:** Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su propietario; es decir, la persona que es responsable de las decisiones relativas al mismo.
- **Gestión de la Configuración de seguridad:** Se van a configurar los equipos previamente a su entrada en operación y se va a gestionar de forma continuada esta configuración de forma que se mantengan en todo momento las reglas de «funcionalidad mínima» y «seguridad por defecto», el sistema se adapte a las nuevas necesidades, previamente autorizadas y reacciones tanto a vulnerabilidades reportadas como a incidencias. Previo a estas actividades la universidad debería plantearse desarrollar algunas de estas alternativas:
    - Migrar todos los equipos de usuarios a un directorio activo, de forma que se pueda centralizar en el servicio de informática el control de acceso y la gestión de la configuración de la seguridad sobre los equipos, aplicaciones y la información.
    - eliminar de los equipos los permisos de administración de los usuarios, y configurar manualmente la seguridad en cada equipo.
    - Realizar auditorías por muestreo de la configuración de los equipos.
- **Gestión del Mantenimiento.** Cómo se va a mantener el equipamiento físico y lógico teniendo en cuenta las especificaciones de los fabricantes, haciendo un seguimiento continuo de los anuncios de defectos y la sistemática y criterios a seguir para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.
- **Gestión de cambios.** Para controlar de manera continua los cambios realizados en el sistema, de forma que sean analizados para determinar su conveniencia o no para ser incorporados, comprobando el funcionamiento de las nuevas versiones antes de ponerlas en entornos de producción y planificando el paso a producción para reducir su impacto en los servicios. Además el procedimiento deberá contemplar la realización de un análisis de riesgos, para determinar si los cambios afectan al nivel de seguridad del sistema y si el riesgo es alto, deberán ser aprobados explícitamente de forma previa a su implantación.
- **Gestión de la Protección frente a código dañino.** En este procedimiento se detallarán los mecanismos de prevención y reacción frente a código dañino, como realizar los mantenimientos de acuerdo a las recomendaciones del fabricante o el uso de aplicaciones antivirus.
- **Gestión de incidencias.** Es necesario tener un procedimiento claro para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluirá la recogida de la información necesaria para analizar las causas y las consecuencias del incidente y determinar los métodos para evitar que se repita.

9.8.11. Actuación 5: Servicios Externos

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.

Contratación y acuerdos de nivel de servicio	Hay algún acuerdo de nivel de servicio con proveedor, pero no se describen en el todas las características del servicio.	No se ha establecido una sistemática de revisión de los contratos y acuerdos, común a todos los servicios subcontratados. Asimismo no se supervisa el cumplimiento de los mismos.	5-1
Gestión diaria	En caso de fallo se medir el cumplimiento de las obligaciones de servicio, pero no diariamente.	No se cuenta con un sistema rutinario para medir el cumplimento de las obligaciones de servicio y las actividades a realizar para neutralizar cualquier desviación.	5-1
Medios alternativos	No aplica esta medida para la categoría de los sistemas identificada. Aplica a categoría Alta.	No Aplica esta medida de seguridad.	

9.8.11.1. Acción 5-1 Establecer las pautas para la seguridad en los servicios externos

Documentar los procedimientos necesarios para la gestión de los servicios externos, de manera que los contratos incorporen acuerdos de nivel de servicio, los mecanismos para controlar el cumplimiento de los mismos, y como se van a gestionar los incumplimientos.

9.8.12. Actuación 6: Continuidad del Servicio

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Análisis de Impacto	No se ha realizado un análisis de impacto de los requisitos de disponibilidad del servicio.	Para los sistemas de nivel Bajo y Medio aplica la media de Análisis de Impacto, pero no la de Plan de Continuidad y pruebas periódicas, aunque son recomendables.	6-1
Plan de continuidad	No aplica esta medida para la categoría de los sistemas identificada. Aplica a categoría Alta.		6-2
Pruebas periódicas	No aplica esta medida para la categoría de los sistemas		6-3

	identificada. Aplica a categoría Alta.		

9.8.12.1. Acción 6-1: Documentar el Análisis de Impacto y el Plan de Continuidad

Debe realizarse un análisis de impacto sobre los componentes del sistema que dan soporte a los servicios de administración electrónica, de manera que se identifiquen las principales amenazas y se determinen unos tiempos de recuperación máximos en caso de fallos por materialización de las amenazas.
Como resultado de este análisis de impacto se elaborará un Plan de Continuidad que permita recuperar el servicio en los tiempos máximos previstos, si bien este plan de continuidad estará supeditado a la contratación de un centro de respaldo.
Planificar y realizar pruebas para comprobar la viabilidad y eficacia del Plan de Continuidad.

9.8.12.2. Acción 6-2: Plan de continuidad

Es recomendable desarrollar un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.

9.8.12.3. Acción 6-3: Pruebas periódicas

Es recomendable elaborar un plan de pruebas de continuidad y que se ejecutaran las pruebas necesarias para comprobar la viabilidad y eficacia del Plan de Continuidad.

9.8.13. Actuación 7: Monitorización del Sistema

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Detección de intrusión	No aplica esta medida para la categoría de los sistemas identificada. Aplica a categoría Alta.	No Aplica esta medida de seguridad.	
Sistema de métricas	No aplica esta medida para la categoría de los sistemas identificada. Aplica a categoría Alta.	No Aplica esta medida de seguridad.	

9.8.14. Actuación 8: Protección de las instalaciones e infraestructuras

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.

Áreas separadas y con control de acceso	Los sistemas de información se encuentran en áreas separadas. Existe servicio de vigilancia, videovigilancia, control de accesos, etc.	No se cuenta con un procedimiento de accesos físicos.	8-1
Identificación de las personas	Se identifica a todas las personas que acceden al CPD, pero no se registran todas la entradas y salidas del mismo. Los despachos quedan cerrados con llave.	Las entradas al CPD son registradas por el sistema al utilizar las llaves de acceso y, aunque las salidas no se registran, mediante la cámara de seguridad se pueden controlar.	8-1
Acondicionamiento de los locales	Las salas de CPD cuentan con sistemas de control de temperaturas y humedad, así como de detección y extinción de incendios. En el CPD principal se dispone de suelo técnico.	No existen insuficiencias. Pero sería recomendable tener en cuenta las amenazas del análisis de riesgo ara mejorar la seguridad física.	8-1
Energía eléctrica	Se garantiza el suministro de la potencia eléctrica necesaria para el funcionamiento de los equipos mediante Sistemas de Alimentación Ininterrumpida (S.A.I.) y Grupo electrógeno. Los servidores lanzan una alarma a los administradores de sistemas en caso de fallo del suministro eléctrico general.	No existen insuficiencias.	
Protección frente a incendios	Se aplica la normativa existente para la protección de incendios (extintores, salidas de incendios,…).	No existen insuficiencias.	
Protección frente a inundaciones	El CPD cuenta con suelo técnico y detectores de humedad (agua).	No existen insuficiencias.	
Registro de entrada y salida de equipamiento	No se controlan las entradas y salidas de los equipos.	No se registran las entradas y salidas de los equipos ni la identificación de las personas que	8-1

		autoriza el movimiento ya sea por mantenimiento o por eliminación.	
Instalaciones alternativas	No aplica esta medida para la categoría de los sistemas identificada. Aplica a categoría Alta.	No Aplica esta medida de seguridad. Aunque sería recomendable tener en cuenta este control en el diseño del Plan de Continuidad del Servicio.	8-1

9.8.14.1. Acción 8-1 Documentar Protección de las Instalaciones y definir instalaciones alternativas

Se implantará un procedimiento de seguridad física que normalice estos aspectos.
Documentar en el plan de continuidad cuáles serán las instalaciones alternativas en caso de desastre.

9.8.15. Actuación 9: Gestión de Personal

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Caracterización del puesto de trabajo	No se han definido las responsabilidades de cada puesto de trabajo en materia de seguridad. No se verifican los antecedentes laborales, de formación y otras referencias a la hora de seleccionar el personal.	Es necesario definir las responsabilidades relacionadas con el ENS.	9-1
Deberes y obligaciones	El personal propio o subcontratado no ha sido informado de sus deberes y responsabilidades de su puesto de trabajo en materia de seguridad.	No se ha informado a los usuarios de sus deberes y obligaciones en materia de ENS.	9-2
Concienciación	Se han llevado a cabo acciones de concienciación/formación en materia de protección de datos de carácter personal.	Es preciso definir las acciones necesarias de formación y concienciación en el ENS.	9-3
Formación	El personal no recibe formación continua en materias que requieran para el desempeño de sus funciones.	No se establecido una sistemática para la realización de la formación continua del personal.	9-3

Personal alternativo	No aplica para la categoría del sistema definida, si bien se considera recomendable definirlo en el Plan de Continuidad de la actividad.	No Aplica esta medida de seguridad.	

9.8.15.1. Acción 9-1 Formalizar las responsabilidades en seguridad

Documentar cada puesto de trabajo con sus responsabilidades incluidas las de seguridad. Difundir la definición de los puestos a los empleados de manera formal.
Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias.

9.8.15.2. Acción 9-2: Deberes y Obligaciones

Se informará a cada persona de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, para lo cual:

- Se especificarán las medidas disciplinarias a que haya lugar.
- Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
- Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.

En caso de personal contratado a través de un tercero:

- Se establecerán los deberes y obligaciones del personal.
- Se establecerán los deberes y obligaciones de cada parte.
- Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

9.8.15.3. Acción 9-3 Llevar a cabo acciones de concienciación y formativas

Definir las acciones de concienciación y formación necesarias para cada grupo de usuarios de los servicios y planificar la realización de las mismas de manera que llegue a toda la audiencia potencial.
Se recordará regularmente, bien mediante charlas formativas, cursos, o mediante la distribución de normativas o correo electrónico:

- La normativa de seguridad relativa al buen uso de los sistemas.
- La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- El procedimiento de reporte de incidencias de seguridad.

9.8.16. Actuación 10: Protección de los Equipos

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Puesto de trabajo despejado	No se controla que los puestos de trabajo se mantengan despejados y que los usuarios guarden todo el material en lugar cerrado cuando no lo estén utilizando.	No existe una normativa de puestos de trabajo despejado.	10-1
Bloqueo de puesto de trabajo	Los equipos del personal se configuran para bloquearse tras un periodo de inactividad, pero al tener permisos de administradores, podrían quitarlo, por lo cual no se puede controlar que se aplique dicha medida. Para el uso de la VPN si se cumple.	No se aplica esta medida de seguridad en todos los casos.	10-1
Protección de equipos portátiles	No hay control sobre los equipos portátiles, pero si se encuentran inventariados en EasyVista. Existe un canal de comunicación de incidencias al servicio de informática.	No existe control sobre los equipos portátiles ni normativa que establezca las condiciones de uso.	10-2
Medios alternativos	Los servidores están balanceados y replicados. Para equipos hay alguno de reemplazo. No se ha definido un tiempo máximo de entrada en funcionamiento aunque se lleva a cabo pruebas con buenos indicadores.	No se han documentado los procedimientos a seguir en caso de desastre.	10-3

9.8.16.1. Acción 10-1 Proteger el puesto de trabajo

Definir normas para que todos los puestos de trabajo permanezcan despejados y que los equipos se bloqueen tras un tiempo de inactividad. Esta información se difundirá en las acciones formativas.

Se recomienda que tras un tiempo establecido de inactividad se cancelen las sesiones abiertas desde dicho puesto de trabajo.

9.8.16.2. Acción 10-2 Proteger los equipos portátiles

Se documentarán las acciones que se siguen para la protección de los portátiles.

- Se llevará un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.
- Se establecerá un canal de comunicación para informar, al servicio de gestión de incidencias, de pérdidas o sustracciones.
- Se establecerá un sistema de protección perimetral que minimice la visibilidad exterior y controle las opciones de acceso al interior cuando el equipo se conecte a redes, en particular si el equipo se conecta a redes públicas.
- Se evitará, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.

9.8.16.3. Acción 10-3 Definir las necesidades de equipos alternativos

Realizar un estudio de los equipos que serían necesarios en caso de no contar con los que habitualmente se utilizan para prestar los servicios y documentar la estrategia a seguir en el Plan de Continuidad.

9.8.17. Actuación 11: Protección de las Comunicaciones

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Perímetro seguro	La red interna dispone de dos dispositivos firewall para protegerla del exterior.	No existen procedimientos documentados que definan las medidas de seguridad relacionadas con la protección de las comunicaciones.	11-1
Protección de la confidencialidad	La red se encuentra protegida por firewall y las conexiones desde fuera se hacen mediante VPN.		
Protección de la autenticidad y de la integridad	Las medidas de seguridad de las redes internas cubren los aspectos requeridos para los servicios de sistemas de nivel medio.		
Segregación de redes	No aplica esta medida para la categoría de los sistemas identificada. Aplica a categoría Alta. Aunque sería recomendable que las redes se encuentran segregadas según las		

	necesidades de los servicios y los usuarios.		
Medios alternativos	No aplica esta medida para la categoría de los sistemas identificada. Aplica a categoría Alta. Aun así es recomendable documentar los procedimientos a seguir en caso de desastre, aunque no aplique en la categoría del sistema definido.		

9.8.17.1. Acción 11-1 Formalizar la protección de las comunicaciones

Documentar los procedimientos necesarios de manera que las acciones realizadas para la protección de las comunicaciones se gestionen adecuadamente.

9.8.18. Actuación 12: Protección de los Soportes de Información

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Etiquetado	No se etiquetan los soportes de información.	No existe una normativa para el etiquetado de soportes.	12-1
Criptografía	No hay cifrado.	En el transporte de soportes removibles se deben aplicar mecanismos criptográficos.	12-2
Custodia	Existe un proceso de custodia de soportes.	No existen insuficiencias.	
Transporte	No existe un procedimiento de entrada y salida de soportes. No se emplea cifrado en el transporte de información.	No se puede garantizar que los dispositivos satisfacen los requisitos de seguridad cuando están siendo desplazados de un lugar a otro.	12-1
Borrado y destrucción	No hay definido un procedimiento de borrado ni de destrucción seguro.	No se ha establecido la sistemática de borrado y destrucción de soportes (medios electrónicos y no electrónicos).	12-1

9.8.18.1. Acción 12-1: Protección de soportes

Se establecerán procedimientos para:

- Definir normas de etiquetado de soportes de forma que se pueda conocer el nivel de seguridad de la información contenida. Los usuarios se capacitarán para entender el significado de las etiquetas.
- Aplicar mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida en los soportes removibles, siendo estos los CD, DVD, discos USB. Sobre todo si salen de las instalaciones y en especial para las copias de seguridad en segunda ubicación.
- Custodiar los soportes y almacenarlos con las debidas medidas de seguridad.
- Tomar las medidas adecuadas para el transporte de los soportes. Registrar las entradas y salidas.
- Establecer medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado:
    - En el caso de que sean magnéticos se pueden utilizar desmagnetizados.
    - Grabación de varias pasadas con un contenido aleatorio para que no sea legible el contenido anterior.

9.8.18.2. Acción 12-2: Cifrado de soportes

Se debe definir e implantar un proceso para el cifrado de todos aquellos soportes que contengan información y especialmente sobre los soportes que contienen las copias de seguridad.

9.8.19. Actuación 13: Protección de las Aplicaciones Informáticas

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Desarrollo	El entorno de desarrollo está separado al de producción. Los desarrollos internos se realizan utilizando una metodología incremental pero no está documentada al 100%. Hay guías de buenas prácticas. Se integran al diseño del sistema mecanismos de identificación y autenticación. Se utilizan copias de datos reales y se asegura el nivel de seguridad.	No existe un procedimiento de seguridad en el desarrollo de software que incluya los controles de seguridad a tener en cuenta.	13-1
Aceptación y puesta en servicio	Se ponen en producción los sistemas que han sido probados previamente en un entorno de pruebas.	No se realizan análisis de vulnerabilidades ni pruebas de penetración.	13-1

	Existe un procedimiento de pruebas con datos reales.		

9.8.19.1. Acción 13-1 Seguridad en los desarrollos informáticos.

Documentar e implantar los procedimientos necesarios con los criterios y tareas para el desarrollo de aplicaciones y su posterior puesta en producción de acuerdo a lo estipulado por el ENS.

Se realizarán las siguientes inspecciones previas a la entrada en servicio de un nuevo servicio así como de los actuales:

- Análisis de vulnerabilidades.
- Pruebas de penetración.

Estas medidas de seguridad deben aplicarse para todas las aplicaciones desarrolladas que intervienen en la prestación del servicio.

9.8.20. Actuación 14: Protección de la Información

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Datos de carácter personal	La entidad ha registrado los ficheros de datos de carácter personal y cuenta con un Documento de Seguridad, pero se está modificando.	No existen insuficiencias.	14-1
Calificación de la información	Existe una clasificación de la información por niveles de seguridad, según lo definido en la LOPD (nivel básico, medio y alto). Asimismo se cuenta con una política de seguridad pero que se encuentra en versión borrador.	A excepción de lo previsto en la LOPD, no se ha calificado la información utilizada en la entidad.	14-2
Cifrado	No aplica esta medida para la categoría de los sistemas identificada. Aplica a categoría Alta.	No aplica esta medida para la categoría de los sistemas identificada. Aplica a categoría Alta.	
Firma electrónica	Se dispone de una Política de Firma Electrónica @firma.	No se cuenta con una Normativa Reguladora de los procedimientos de obtención, revocación y suspensión de certificados electrónicos de empleado público en la Universidad de Jaén.	14-3

Sellos de tiempo	El uso de los sellos de tiempo sólo es obligatorio para los sistemas de categoría alta.	No Aplica esta medida de seguridad si bien es un requisito obligatorio legalmente (Ley de Contratos Públicos), por lo que debería ser considerada esta medida.	14-5
Limpieza de documentos	En principio no se hace limpieza de documentos. Pero comprueban si el gestor de contenidos lo hace.	No existen normas en la entidad para eliminar datos innecesarios de los documentos antes de transmitirlos y los documentos que se descargan de la sede electrónica pueden contener meta-datos ó campos ocultos.	14-4
Copias de seguridad (back Up)	Se realizan copias de seguridad regular y sistemáticamente de la documentación almacenada en los servidores, de los datos de configuración, de aplicaciones, de claves, etc., pero no de los Sistemas Operativos	No se ha documentado la sistemática establecida para la realización de las diferentes copias de seguridad.	14-6

9.8.20.1. Acción 14-1: Auditoría LOPD

Se deberá concluir con la revisión y actualización de los ficheros y del documento de seguridad, para realizar luego la auditoría bienal sobre el cumplimiento de la Ley Orgánica de Protección de Datos y del Reglamento de Medidas de Seguridad que la desarrolla.

9.8.20.2. Acción 14-2: Calificación de la información

Se establecerá una clasificación de la información, según lo establecido legalmente sobre la naturaleza de la misma, y se le asignará a cada información manejada por el sistema un Responsable, que será reflejado en la Política de Seguridad, donde, además, se recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido (dentro de lo establecido en cuanto a la categorización de los sistemas).
Se redactarán los procedimientos necesarios que describan, en detalle, la forma en que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere; y precisando cómo se ha de realizar:

- Su control de acceso.
- Su almacenamiento.
- La realización de copias.
- El etiquetado de soportes.
- Su transmisión telemática.
- Y cualquier otra actividad relacionada con dicha información.

9.8.20.3. Acción 14-3: Firma electrónica

Se verificará la correcta aplicación de la Política de Firma y Certificados de la Administración General para asegurarse de que los sistemas de administración electrónica cumplen con la misma.
Si no fuese así se valorará la posibilidad de elaborar una Política de Firma propia.

9.8.20.4. Acción 14-4: Limpieza de documentos

Se implantarán procedimientos que describan la meta-información que debe de ser objeto de limpieza en los archivos a publicar y que vayan a ser transmitidos fuera de la organización.

9.8.20.5. Acción 14-5: Sellos de Tiempo

Se evaluará la posibilidad de emplear sellos de tiempo para prevenir la posibilidad del repudio posterior. Se utilizarán productos certificados o servicios externos admitidos.

9.8.20.6. Acción 14-6: Copias de seguridad

Con respecto al Procedimiento de copias de seguridad, además de dejarlo documentado, se tendrán en cuenta los siguientes puntos:

- Se establecerán procedimientos de copiado de la información de configuración (máquinas virtuales).
- Se realizarán pruebas de recuperación de las copias de seguridad.
- Se establecerán métodos de cifrado para los soportes que almacenen información sensible y especialmente para las copias de seguridad que se conservan en segunda ubicación.

9.8.21. Actuación 15: Protección de los Servicios

Medida de seguridad	Situación actual	Insuficiencia del Sistema	Acc.
Protección del correo electrónico	Se protege el correo electrónico con antivirus y antispam de manera automatizada, se cuenta con acuerdo con Gmail para ello. Existen normativas de uso y algún curso de Outlook.	No existen insuficiencias.	
Protección de servicios y aplicaciones web	Si se controla internamente pero nunca se ha hecho una auditoría. Se siguen buenas prácticas para el cumplimiento. De la parte institucional si se controla, del resto no hay tanto control.	No se ha verificado que se cumplen todas las medidas de seguridad, ya que no se tiene un control total sobre todo todos los servicios. Se debería definir un procedimiento con las medidas a aplicar asignado las responsabilidades necesarias.	15-1

Protección frente a la denegación de servicio	Se han tomado medidas para evitar ataques de denegación de servicios mediante la gestión de la capacidad, balanceadores y las reglas del firewall.	No existen insuficiencias.	15-2
Medios alternativos	Es recomendable documentar los procedimientos a seguir en caso de desastre, aunque sólo obligatorio para sistemas de categoría Alta.	No Aplica esta medida de seguridad.	

9.8.21.1. Acción 15-1 Protección de servicios y aplicaciones web

1) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:
    - Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
    - Se prevendrán ataques de manipulación de URL.
    - Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como «cookies».
    - Se prevendrán ataques de inyección de código.
2) Se prevendrán intentos de escalado de privilegios.
3) Se prevendrán ataques de «cross site scripting».
4) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como «proxies» y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como «cachés».

9.8.21.2. Acción 15-1 Protección frente a la denegación de servicio

Es recomendable documentar las medidas preventivas y reactivas frente a ataques de denegación de servicio.

- Se planificará y dotará al sistema de capacidad suficiente para atender a la carga prevista con holgura.
- Se desplegarán tecnologías para prevenir los ataques conocidos.

Realizar un estudio de los medios que serían necesarios en caso de no contar con los que habitualmente se utilizan para prestar los servicios y documentar en el Plan de Continuidad la estrategia a seguir.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Universidad de Jaén

Contenido

1. Aprobación y entrada en vigor 3
2. Introducción 3
2.1. Prevención 3
2.2. Detección 4
2.3. Respuesta 4
2.4. Recuperación 4
3. Alcance 4
4. Declaración de la política de seguridad de la información 5
5. Misión de la Universidad de Jaén 5
6. Marco Normativo 5
7. Organización de la seguridad 6
7.1.Comité: Funciones y Responsabilidades 6
7.2. Roles: Funciones y Responsabilidades 7
7.3. Procedimientos de designación 7
7.4. Revisión de la Política de Seguridad de la Información 7
8. Datos de carácter personal 8
9. Gestión de riesgos 8
10. Desarrollo de la Política de Seguridad de la Información 8
11. Obligaciones del personal 8
12. Terceras partes 9
Anexo I: Funciones y responsabilidades 10
Anexo II: Normativa de Seguridad de los Sistemas de Información 13
II.1. Política de uso aceptable 13
II.2. Seguridad de la gestión de recursos Humanos 13
II.3. Seguridad física y del entorno 14
II.4. Gestión de comunicaciones y operaciones 14
II.5. Control de accesos 16
II.6. Uso de la información fuera de la Universidad 17
II.7. Gestión de incidencias 17
II.8. Continuidad del servicio 18

1. Aprobación y entrada en vigor

Texto aprobado el día 26/03/2015 por el Consejo de Gobierno.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva versión de la misma.

2. Introducción

La Universidad de Jaén depende de los sistemas de Información (SI) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los Sistemas de Información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La Universidad de Jaén debe cerciorarse de que la seguridad es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para todos los proyectos que se relacionen con los Sistemas de Información.

La Universidad de Jaén debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1. Prevención

La Universidad de Jaén debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, se debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. Respuesta

La Universidad de Jaén:

- Establecerá mecanismos para responder eficazmente a los incidentes de seguridad.
- Designará un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecerá protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, la Universidad de Jaén dispondrá de planes de continuidad de los sistemas de Información como parte de su plan general de continuidad del servicio y actividades de recuperación.

3. Alcance

Esta política se aplica a los sistemas de Información de la Universidad de Jaén y a todos los miembros de la organización, que tengan relación con los servicios de administración electrónica:

- Web Institucional (CRUE_05_01)
- Tablón de Anuncios (SR02)
- Gestión Económica. Perfil del contratante (SR03)
- Secretaria General. Firma electrónica (SR_FirmaElec)
- Verifirma (SR05)

- Secretaria General. Registro (CRUE_03_43)
- Gestión Académica. Becas (CRUE_03_06)
- Gestión Académica. Automatrícula (CRUE_03_05)
- Autenticacion centralizada (SIDUJA) (CRUE_08_04)
- Secretaria General. Convenios (CRUE_03_45)
- Extensión Universitaria. Actividades Deportivas (CRUE_03_36)
- Investigación y transferencia: Portal del investigador (SR12)

4. Declaración de la política de seguridad de la información

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de administración electrónica de la Universidad de Jaén.

Es la política de esta entidad asegurar que:

- La información y los servicios están protegidos contra pérdidas de disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad.
- La información está protegida contra accesos no autorizados.
- Se cumplen los requisitos legales aplicables.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.
- Se establecen procedimientos para cumplir con esta Política.
- El Responsable de Seguridad de la Información será el encargado de mantener esta política, los procedimientos y de proporcionar apoyo en su implementación.
- El Responsable de Servicio será el encargado de implementar esta Política y sus correspondientes procedimientos.
- Cada empleado es responsable de cumplir esta Política y sus procedimientos según aplique a su puesto.
- La Universidad de Jaén implementa, mantiene y realiza un seguimiento del Esquema Nacional de Seguridad.

5. Misión de la Universidad de Jaén

La misión de la Universidad de Jaén se encuentra detallada en http://www10.ujaen.es/conocenos/organos-gobierno/ptransparencia/informacion-institucional/mision-vision-y-valores

6. Marco Normativo

La Legislación aplicable a la Universidad se encuentra detallada en el siguiente enlace: http://www10.ujaen.es/conocenos/servicios-unidades/sinformatica/calidad/legislacion

7. Organización de la seguridad

7.1. Comité: Funciones y Responsabilidades

El Comité de Seguridad de la Información estará formado por:

Presidente: La persona designada como Responsable de la Información.

Secretario: La persona designada como Responsable de Seguridad, quién se encargará de convocar, preparar, redactar las actas de reunión del Comité y realizar el seguimiento de las decisiones adoptadas.

Vocales:

La persona designada como Responsable del Fichero

La persona designada como Responsable de Servicios

La persona designada como Responsable del Sistema

Dos personas designadas como Responsables de Seguridad delegados

Vicerrector TIC o quien tenga atribuidas las funciones.

Se han definido las siguientes responsabilidades:

- Responsable de la Información (ENS) - Rector
- Responsable de Seguridad (ENS y LOPD) - Secretario General delegado en jefe del Servicio de Información y Asuntos Generales
- Responsable del Fichero (LOPD) - Secretario General
- Responsable de los Servicios (ENS) - Gerente
- Responsable del Sistema (ENS) - Jefa del servicio de informática
- Responsable de Seguridad delegados - Jefes de cada Servicio

El Comité de Seguridad de la Información coordina la seguridad de la información en la Universidad de Jaén.

El Comité de Seguridad reportará al Consejo de Dirección de la Universidad de Jaén y tendrá las siguientes funciones:

- Informar regularmente del estado de la seguridad de la información al Consejo de Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Universidad de Jaén en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por el Consejo de Dirección.
- Proponer la normativa de seguridad de la información al Equipo de Gobierno para su aprobación.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- elaborar Planes de concienciación y formación
- Monitorizar los principales riesgos residuales asumidos por la Universidad de Jaén y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Universidad de Jaén. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos de implantación de sistemas de información desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas de información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Coordinar y aprobar Planes de continuidad.

7.2. Roles: Funciones y Responsabilidades

Las funciones y responsabilidades se detallan en el **Anexo I**

7.3. Procedimientos de designación

El Consejo de Dirección designará las personas que ocuparan los roles definidos en esta Política así como la composición del Comité de Seguridad de la Información.

Los nombramientos se revisarán o renovarán con la revisión de la Política de Seguridad.

7.4. Revisión de la Política de Seguridad de la Información

Será misión del Comité de Seguridad de la información la revisión bienal de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Consejo de Gobierno y difundida para que la conozcan todas las partes afectadas.

8. Datos de carácter personal

Todos los sistemas de información de la Universidad de Jaén que contienen datos de carácter personal han adoptado las medidas de seguridad exigidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.

Los ficheros afectados y los responsables correspondientes se encuentran recogidos en el Documento de Seguridad que se puede consultar en Universidad Virtual (https://uvirtual.ujaen.es)

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la Universidad de Jaén.

9. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

10. Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad complementa las políticas de seguridad en diferentes materias. Se desarrollará en la normativa descrita en el **Anexo II** y por medio de procedimientos de seguridad que afrontan aspectos específicos. Los procedimientos de seguridad deben ser conocidos por aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Los procedimientos de seguridad estarán disponibles en Universidad Virtual (https://uvirtual.ujaen.es)

11. Obligaciones del personal

Todos los miembros de la Universidad de Jaén tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se realizarán periódicamente acciones de concienciación y sensibilización en materia de seguridad de la información que afecte a todos los miembros de la Universidad de Jaén. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en que la

necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12. Terceras partes

Cuando la Universidad de Jaén preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Universidad de Jaén utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Anexo I: Funciones y responsabilidades

Función	Responsabilidades
Responsable del Fichero	• Notificar los ficheros ante el Registro General de Protección de Datos para que se proceda a su inscripción. • Asegurarse de que los datos sean adecuados y veraces, obtenidos lícita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados. • Garantizar el cumplimiento de los deberes de secreto y seguridad. • Informar a los titulares de los datos personales en la recogida de éstos. • Obtener el consentimiento para el tratamiento de los datos personales. • Facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación. • Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto en la LOPD. • Cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que le sea de aplicación. • Notificar los ficheros ante el Registro General de Protección de Datos. • Garantizar el cumplimiento de los deberes de secreto y seguridad. • Garantizar derechos ARCO.
Responsable de la Información	• Velar por el buen uso de la información y, por tanto, de su protección, incluidos los ficheros de datos de carácter personal. • Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad. • Establecer los requisitos de la información en materia de seguridad. • Determinar los niveles de seguridad de la información. • Determinación de los niveles de seguridad requeridos en cada dimensión junto con el responsable del servicio. • Aceptación del riesgo residual junto con el responsable del servicio.
Responsable del Servicio	• Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad. • Determinar los niveles de seguridad de los servicios.
Responsable de Seguridad	• Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.

	● Promover la formación y concienciación en materia de seguridad de la información y protección de datos de carácter personal. ● Determinación de la categoría del sistema. ● Análisis de riesgos. ● Declaración de aplicabilidad. ● Medidas de seguridad adicionales. ● Elaborar configuración de seguridad. ● Documentación de seguridad del sistema. ● Elaborar y aprobar procedimientos operativos de seguridad. ● Elaborar planes de mejora de la seguridad junto con el responsable del sistema. ● Elaborar planes de concienciación y formación. ● Validar planes de continuidad. ● Aprobar ciclo de vida de los sistemas de información: especificación, arquitectura, desarrollo, operación, cambios.
Responsable del Sistema	● Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. ● Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. ● Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. ● La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información. ● La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información. ● La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado. ● La aplicación de los Procedimientos Operativos de Seguridad. ● Aprobar los cambios en la configuración vigente del Sistema de Información. ● Asegurar que los controles de seguridad establecidos son cumplidos estrictamente. ● Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información. ● Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes. ● Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de

	auditoría técnica implementados en el sistema y reportarlos el responsable de seguridad. ● Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad. ● Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución. ● Aplicar configuración de seguridad. ● Implantación de las medidas de seguridad. ● Aplicar procedimientos operativos de seguridad. ● Monitorizar el estado de la seguridad del sistema y los reporta al responsable de seguridad. ● Elaborar y realizar ejercicios periódicos de los planes de continuidad. ● Elaborar Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios.

Anexo II: Normativa de Seguridad de los Sistemas de Información

II.1. Política de uso aceptable

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios. No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de la Universidad de Jaén (sólo los administradores de sistemas están autorizados a ello).
- No vigilar los diferentes tipos de licencias de todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y no mantener los derechos que la ley de propiedad intelectual le confiera.
- Queda prohibido el uso de equipos, redes y servicios para fines personales. En tal caso, será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios restringidos a personas no autorizadas.
- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso adrede. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus

II.2. Seguridad de la gestión de recursos Humanos

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información secreta.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede.

Cuando se termine la relación laboral o contractual con empleados o personal externo (exceptuando los casos autorizados por el Responsable de Seguridad), se les retirarán los

permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

II.3. Seguridad física y del entorno

Para que una seguridad lógica sea efectiva es primordial que las instalaciones mantengan una correcta seguridad física para evitar los accesos no autorizados así como cualquier otro tipo de daño o interferencia externa.

II.3.1. Áreas restringidas

La Universidad de Jaén tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones restringidas.

La totalidad de las instalaciones de la Universidad de Jaén cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen.

Los lugares donde se ubican los servidores y el cableado se considerarán áreas restringidas.

Las ventanas y puertas deberán permanecer cerradas cuando las instalaciones estén vacías.

Para la prevención de fugas de agua e inundaciones será necesaria la revisión periódica de la grifería, sanitarios y demás instalaciones que puedan causar daños de este tipo.

II.3.2. Seguridad de los equipos

Los equipos informáticos son un activo importante del que depende la continuidad de las actividades, por lo que serán protegidos de manera adecuada y eficaz.

Los equipos informáticos críticos de la Universidad de Jaén estarán protegidos contra posibles fallos de energía u otras anomalías eléctricas, para ello se habilitarán sistemas de alimentación ininterrumpida.

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello deben someterse a las revisiones recomendadas por el suministrador.

Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación.

También será necesario adoptar las medidas de precaución necesarias en caso de los equipos deban abandonar las instalaciones para su mantenimiento.

II.4. Gestión de comunicaciones y operaciones

II.4.1. Procedimientos operativos y responsabilidades

La Universidad de Jaén controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red de la Universidad de Jaén y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red de la Universidad de Jaén existirán mecanismos para cubrir los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los empleados autorizados para el manejo de información automatizada deberán estar registrados como usuarios del sistema. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal. Esta contraseña caducará periódicamente.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo a estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

II.4.2. Protección frente a código malicioso y código móvil

El Administrador del Sistema instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

II.4.3. Copias de seguridad

La salvaguarda de la información almacenada en los PC será responsabilidad del usuario del mismo.

Para la salvaguarda de la información almacenada en servidores, se definirán procedimientos de copias de datos. Estas copias estarán claramente identificadas y depositadas en sitio seguro. También se desarrollarán procedimientos para recuperar los datos a partir de las copias de seguridad. Hay que asegurarse periódicamente de que la información se guarda correctamente y permite recuperar un nivel mínimo de servicio en caso necesario.

II.4.4. Gestión de la seguridad de la red

Los elementos de red (switch, router...) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema.

Existirá una gestión gráfica de la red de forma que su mantenimiento pueda resultar más cómodo.

II.4.5. Gestión de soportes

Los usuarios aplicarán las mismas medidas de seguridad a los soportes (tanto papel como digitales) que contengan información sensible que a los ficheros de donde han sido extraídos.

Los soportes que contengan información sensible deben permanecer en cajones o armarios cerrados bajo llave. Cuando alguna persona autorizada deba utilizarla para realizar alguna gestión relacionada con las labores propias de la Universidad de Jaén, ésta se hará responsable del buen cuidado de los soportes. No los dejará encima de su mesa cuando abandone su puesto

de trabajo ni los colocará en cualquier otro lugar donde una persona sin autorización pueda verlos o apropiarse de ellos.

Los soportes reutilizables cuya información ya no se necesite deberá borrarse, siempre que se cuente con la autorización precisa. Esta eliminación debe hacerse de forma segura para que los datos que contiene no se filtren a otras personas.

Siempre será necesario registrar la eliminación de soportes que contengan información sensible para mantener una pista de auditoría.

II.4.6. Intercambio de información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, fax, etc.).

II.4.7. Seguimiento

Según se considere necesario, se establecerán los mecanismos que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos así como para recomendar cualquier cambio que se estime necesario.

II.5. Control de accesos

II.5.1. Requisitos del servicio para el control de accesos

La información debe estar protegida contra accesos no autorizados. El Responsable del Servicio definirá las necesidades de acceso a la información a dos niveles, para el conjunto del área y las de cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

También deben protegerse los puntos de entrada y salida de correo postal.

En el caso de que visitantes o personal no autorizado acceda a las instalaciones restringidas o a la información de la Universidad de Jaén deberá ir siempre acompañado por un miembro responsable de la Organización que controlará en todo momento que la seguridad de los recursos está garantizada.

II.5.2. Gestión de accesos a los sistemas de información

El administrador del sistema es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, así como el acceso lógico especializado de los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.

Los autenticadores se cambiarán con una periodicidad.

Cada usuario deberá estar asociado a un perfil, de acuerdo a las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a Información y sistemas que no le son necesarios para las competencias de su trabajo.

II.5.3. Control de acceso a los equipos

Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado así como otros posibles daños. Éstos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.

Los usuarios velarán por la seguridad en el acceso a su equipo informático y habilitarán contraseñas a tal efecto. De igual forma, es necesario configurar los equipos informáticos para que éstos queden bloqueados cuando el usuario no se encuentra en su puesto de trabajo de forma que sea necesario introducir una contraseña para acceder a los datos que se almacenan en el terminal.

También deben protegerse las máquinas de fax y las impresoras que no se encuentren atendidas por alguna persona de la Universidad de Jaén.

II.5.4. Control de acceso a la red

No se permitirá el acceso a la red oficial, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con la Universidad de Jaén para mantener el nivel de seguridad que se determine.

II.6. Uso de la información fuera de la Universidad

En caso de necesitar trabajar fuera de la Universidad con información en soporte electrónico o papel, se transportará con el debido cuidado.

Debido a los riesgos de seguridad en Internet, la transmisión de información de la organización al exterior, se realizará mediante una conexión segura (VPN). Antes de usar cualquier información hay que asegurarse de que el equipo en el que va a ser tratada está libre de virus o código malicioso.

Cuando los equipos o la información propiedad de la Universidad de Jaén están fuera de las instalaciones, el responsable de su seguridad es el empleado que los está utilizando y debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento.

II.7. Gestión de incidencias

Se habilitará un sistema de gestión de incidencias de seguridad que facilitará que cualquier empleado comunique las incidencias que sospeche u observe, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.).

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

II.8. Continuidad del servicio

Es imprescindible para la Universidad de Jaén establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad de la actividad en estos casos, la Universidad de Jaén dispondrá de planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del servicio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del servicio se documentará, partiendo de los riesgos detectados y de los controles definidos en consecuencia que deberán probarse y actualizarse regularmente para comprobar su idoneidad.

La gestión de la continuidad del servicio se incorporará a los procesos de la Universidad de Jaén y será responsabilidad de una o varias personas dentro de la entidad.

Servicio de Información y Asuntos Generales

CONVENIOS SESIÓN CONSEJO DE GOBIERNO 51/15

TÍTULO	FECHA	IMPORTE
CONVENIO DE COLABORACIÓN ENTRE LA DIPUTACIÓN PROVINCIAL DE JAÉN Y LA UJA, PARA LA REALIZACIÓN DEL PROGRAMA DE FORMACIÓN Y PRÁCTICAS UNIVERSITARIAS EN PROYECTOS EN COOPERACIÓN AL DESARROLLO (IV EDICIÓN)	16/12/2014	58.188,25 €
CONVENIO MARCO DE COLABORACIÓN ENTRE LA UJA Y LIDERKIT, S.L	06/11/2014	
CONVENIO MARCO DE COOPERACIÓN ACADÉMICA ENTRE LA UJA (ESPAÑA) Y UNIVERSIDADE ESTUAL DO OESTE DO PARANÁ (BRASIL)	17/11/2014	
ANEXO AL CONVENIO MARCO DE COOPERACIÓN ACADÉMICA ENTRE LA UJA (ESPAÑA) Y LA UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ (BRASIL)	17/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y RODRIGUEZ MORILLAS ASESORES SCA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	21/10/2014	
CONVENI DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y PERSONAL MARK S.L B62920962 PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	23/10/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA YLICO CORPORACIÓN OPERADOR DE BANCA-SEGUROS VINCULADO, S.A PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	24/10/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y MANUEL ANGUITA CÁMARA (AREAESENCIAL) PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	30/10/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y AYUNTAMIENTO DE BAÓS DE LA ENCINA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	29/10/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y FUNDACIÓN PURÍSIMA CONCEPCIÓN PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	30/10/2014	
CONVENI DE COOPERACIÓN EDUCTIVA ENTRE LA UJA Y DISTRIBUIDORA INTERNACIONAL DE ALIMENTACIÓN (DIA SA) PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	29/10/2014	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COOPERACIÓN ACADÉMICA ENTRE LA UJAY LA UNIVERSIDAD INTERNACIONAL DE ANDALUCÍA PARA IMPARTIR EL MÁSTER INTERUNIVERSITARIO EN INTERVENCIÓN ASISTIDA CON ANIMALES	23/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y INEFEX SOLUCIONES ENERGÉTICAS S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	03/09/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y CONTRATAS SERVILIM, S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	04/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y RESTAURACIÓN EL GAMBERO S.A PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	29/10/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y AYUNTAMIENTO DE ÓRGIVA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	04/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y AUTOESCUELAPÉREZ GARCÍA S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	16/10/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENRE LA UJA Y MARIA DOLORES MARTÍNEZ ROLDÁN PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	04/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y SOCIEDAD COOPERATIVA ANDALUZA DE TRANSPORTES DODETRAN PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	06/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y CONSUELO ASTASIO PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	17/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y JUAN PULIDO GONZÁLEZ PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	12/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJAE E INSTITUTO DE INNOVACIÓN CIENCIA Y EMPRESA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y D.A. MOLINA CONSULTORES TÉCNICOS S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	18/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y GREGORIO F GARCÍA SEGURA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	19/11/2014	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y ANTONIO MORALLÓN RODRÍGUEZ PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	25/11/2014	
ANEXO AL CONVENIO MARCO DE COOPERACIÓN ACADÉMICA ENTRE LA UJA (ESPAÑA) Y UNIVERSIDAD DE CIENCIAS FORESTALES U-ESNACIFOR (HONDURAS)	03/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y ASOCIACIÓN RECREATIVA CULTURAL EL MENTIDERO PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	25/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y GERMAN RAMÍREZ GONZÁLEZ PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	29/10/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y GESTIÓN Y DESARROLLO DE IMAGEN CORPORATIVA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	29/10/2014	
STUDENT EXCAHNGE PROGRAM AGREEEMENT BETWEEN UNIVERSIDAD DE JAÉN AND UNIVERSITY OF REGINA	15/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA CONSEJERÍA DE EDUCACIÓN, CULTURA Y DEPORTE DE LA JUNTA DE ANDALUCÍA Y LA UJA, PARA EL DESARROLLO DE LAS PRÁCTICAS ACADÉMICAS EXTERNAS UNIVERSITARIAS DEL PRACTICUM DEL MÁSTER DE FORMACIÓN DEL PROFESORADO DE EDUCACIÓN SEDUNDARIA OBLIGATORIA, BACHILLERATO, FORMACIÓN PROFESIONAL Y ENSEÑANZA DE IDIOMAS	26/01/2015	
PROTOCOLO GENERAL DE COLABORACIÓN ENTRE LA CONSEJERÍA DE FOMENTO Y VIVIENDA DE LA JUNA DE ANDALUCÍA Y LA UNIVERSIDAD DE JAÉN	23/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS ENTRE LA UJA Y EL AYUNTAMIENTO DE CÓRDOBA	30/10/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y LABORALIA ETT SCA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	17/10/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y PATOLOGÍA Y NUTRICIÓN VEGETAL S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	12/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y LLEDO Y SEDA NOTARIOS ASOCIADOS PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	12/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y SAMUEL LÓPEZ FERNÁNDEZ LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	12/11/2014	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y LULIA MORENO MADUEÑO PARA LA REALICACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	10/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y HNOS. RUANO S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	04/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y DESTILERIA SANTO REINO, S.L PARA LA REALIZACIÓN DE PRÁCTICAS EN EMPRESAS	25/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y GEMA MORENO CORTECERO PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	17/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA YCINCOCINA SL PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	27/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y ANTONIO SÁNCHEZ MILLA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y FISCALIA PROVINCIAL JAÉN PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	27/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJAY FUNDACIÓN ARCOS DEL CASTILLO PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	17/11/2014	
CONVENIO MARCO DE COLABORACIÓN ENTRE LA UJA Y ASOCIACIÓN HUMANITARIA AMIGOS DE JAÉN	28/01/2015	
CONVENIO DE COLABORACIÓN ENTRE LA DIPUTACIÓN PROVINCIAL DE JAÉN Y LA UJA, PARA LA PARTICIPACIÓN EN LA III EDICIÓN DE LA COMPETICIÓN INTERUNIVERSITARIA MOTOSDUDENT	27/11/2014	6.762,56 €
CONVENIO DE COOPERACIÓN ACADÉMICA ENTRE LAS UNIVERSIDADES DE CÁDIZ, HUELVA Y JAÉN PARA LA IMPARTICIPACIÓN DEL TÍTULO CONJUNTO MÁSTER EN ECONOMÍA Y DESARROLLO TERRITORIAL POR LA UNIVERSIDAD DE CÁDIZ, LA UNIVERSIDAD DE HUELVA Y LA UJA	26/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y NPF-ITAERS, S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	04/05/2014	
CONVENIO DE COLABORACIÓN ENTRE LA UJA Y LA EMPRESA SYNEMET WEATHER SOLUTIONS S.L. PARA EL FOMENTO DE LA CONTRATACIÓN LABORAL DE TITULADOS DE LA UJA	15/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTE LA UNIVERSIDAD DE JAÉN Y AYUNTAMIENTO DE GUARROMAN PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	01/12/2014	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COOPERACIÓN EDUCATIVA ENTE LA UNIVERSIDAD DE JAÉN Y ASESORÍA Y GESTION DIAZ, S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	17/11/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y AYUNTAMIENTO DE BULLASPARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/10/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CAMILO JOSE CHICA TORRES PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	25/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTE LA UNIVERSIDAD DE JAÉN Y ROSARIO FERNÁNDEZ LÓPEZ PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	01/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTE LA UNIVERSIDAD DE JAÉN Y FISIOTERAPIA-OSTEOPATÍA-RECUPERACIÓN DEPORTIVA ALTHEA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	05/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y DELEGACION TERRITORIAL DE FOMENTO, VIVIENDA, TURISMO Y COMERCIO EN JAEN. JUNTA DE ANDALUCÍA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	01/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y EULEN FLEXIPLÁN PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	27/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ASPIRA-CENTRO DE PSICOLOGÍA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	10/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y HOTEL ZODIACO LIBRA S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	05/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y YOLANDA DOMÍNGUEZ GARCÍA DE LA MORA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	02/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTER LA UNIVERSIDAD DE JAÉN Y ASOCIACIÓN RECREATIVA CULTURAL EL MENTIDERO PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	25/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTE LA UNIVERSIDAD DE JAÉN Y CARLOS CAÑETE BARRIOS PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	05/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y S.C.A DEL CAMPO SAN JUAN PARA LA RALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	01/12/2014	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y HIJOS DE ANTONIO MUÑOZ S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	07/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CASTILLO DE SABIOTE S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	07/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y BEATRIZ MONTES BERGES PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	14/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTE LA UNIVERSIDAD DE JAÉN Y DAP ONCE CORDOBA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	31/10/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ASOCIACIÓN SAN RAFAEL DE ALZHEIMER Y OTRAS DEMENCIAS PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	16/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y REAL JAÉN C.F. SAD PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	15/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y PEDRO PULIDO DELGADO PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	17/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y HURTADO Y VILLAR, S.L. PARA LA REALIZACIÓN DE PRÁCTICAS EXTERNAS	17/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ANTONIO MANUEL CÁMARA LENDÍNEZ Y OTROS CB PARA	17/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y MAR LIÑAN MUÑOZ PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	13/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ABACO CENTRO DE PSICOLOGIA Y LENGUAJE PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	16/12/2014	
CONVENIO DE COOPERACIÓN ENTRE LA UNIVERSIDAD DE JAÉN Y GCPMEDIA ESTRATEGIAS DE COMUNICACIÓN S.L. PARA LA REALIZACIÓN DE LAS PRÁCTICAS ACADÉMICAS EXTERNAS	14/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y SMART MATERIALS 3D PRINTING SL LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	09/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y S2A INT. SERVICES OF AUDIT,S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	10/12/2014	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CAMARA OFICIAL DE COMERCIO E INDUSTRIA DE LINARESPARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	09/12/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y FUNDACIÓN CANARIA YRICHEN PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	01/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y COYMA FUEGO,S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	12/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y MANPOWER TEAM,E.T.T.,S.A.U. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	19/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y JOSÉ CARLOS LINDEZ JURADO PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	11/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y COLEGIO NUESTRA SEÑORA DE LAS MERCEDES PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	12/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y FRANCISCO JAVIER BARRANCO ORTEGA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	18/12/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y EMPREINGENIA S.L.U. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CENTRO COMUNICA LOGOPEDIA Y PSICOPEDAGOGÍA,ANA MARIN MUNUERA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	18/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CENTRO COMUNICA LOGOPEDIA Y PSICOPEDAGOGÍA,ANA MARIN MUNUERA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	18/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ASESORÍA Y ADMINISTRACIONES LIÑAN,S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	13/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ASOCIACIÓN DE FAMILIARES Y ENFERMOS MENTALES DE ANDÚJAR Y COMARCA "AFEMAC" PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	05/12/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y AUDITORES JAÉN S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	22/10/2014	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y VINIIOLIS DISEÑO S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	17/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y FRANCISCO JOSE ORTAL RODRIGUEZ PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	22/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y MONTSERRAT AMARO ALARCON PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	13/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y SIERRA HOTEL D.V. S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	29/10/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CELESTINO RUIZ ROMERO PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	13/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ACTIVIA MUTUA 2008 PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	13/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y JOSE LUIS MARTINEZ MARIN PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	12/01/2015	
ADDENDA AL CONVENIO DE COLABORACIÓN ENTRE LA DIPUTACIÓN PROVINCIAL DE JAÉN Y LA UJA, PARA LA REALIZACIÓN DEL PROYECTO "ESTUDIOS GEOLÓGICOS Y GEODÉSICOS PARA LA EVALUACIÓN DEL POTENCIAL SÍSMICO Y MICROZONIFICACIÓN SÍSMICA EN EL CURSO ALTO DEL GUADALQUIVIR (GUADALGEO)"	13/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y V & L ASESORES BAILÉN,S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	26/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y MARÍA GARCÍA-FÉRRIZ DE LOS ÁNGELES PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	14/01/2015	
CONVENIO DE COOPERACIÓN ENTRE LA UNIVERSIDAD DE JAÉN Y ORG.NACIONAL DISCAPACITADOS ESP.Y EUR. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	22/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y LOPEZ ROBLES Y DOS MAS, C.B. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	25/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y SOCIEDAD DE PREVENCIÓN FRATERNIDAD MUPRESPA,S.L.U PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	07/01/2015	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CENTRO DE INICIATIVAS PARA LA REALIZACIÓN BATA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	07/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y GESCIT CONSULTING CB PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y GRUPO COREMSA FORMACIÓN Y TECNOLOGÍA,S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	19/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ALBEN ASESORES, S.C.A. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	13/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CENTRO DE TERAPIA Y ORIENTACIÓN PSICOLÓGICA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	07/01/2015	
CONVENIO ESPECÍFICO PARA EL CURSO 2015-2016 DEL ACUERDO MARCO GENERAL SUSCRITO ENTRE FUNDACIÓN CAROLINA Y UNIVESIDAD DE JAÉN . MÁSTER EN OLIVAR, ACEITE DE OLIVA Y SALUD	02/02/2015	5.908,20 €
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y SOLUCIONES SICNOVA S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/03/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y EXPOMOTO JAÉN S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	22/01/2015	
CONVENIO ESPECÍFICO PARA EL CURSO 2015-2016 DEL ACUERDO MARCO GENERAL SUSCRITO ENTRE FUNDACIÓN CAROLINA Y UNIVERSIDAD DE JAÉN. MÁSTER EN ENERGÍAS RENOVABLES	02/02/2015	5.908,20 €
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y AGRICOLA DE BAILEN VIRGEN DE ZOCUECA SCA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	27/11/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y YELMO MOTOR S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	29/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y SERVICIOS GENERALES DEL FUTBOL ANDALUZ S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	09/12/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ASOCIACIÓN A FAVOR DE PERSONAS CON DISCAPACIDAD INTELECTUAL DE GRANADA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	29/01/2015	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y AYESTA INGIENERÍA Y ARQUITECTURA S.A PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	13/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y PURIFICACIÓN AGUILA GONZALEZ PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	15/12/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y JOAQUÍN GARCÍA GUIRADO S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	15/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ÍTACA SALUD S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	22/01/2015	
CONVENIO DE COLABORACIÓN PARA LA TRANSMISIÓN DE INFORMACIÓN ENTRE LA UJA Y EL INSTITUTO DE ESTADÍSTICA Y CARTOGRAFÍA DE ANDALUCÍA PARA EL DESARROLLO DE ACTIVIDADES ESTADÍSTICAS CONTENIDAS EN EL PLAN ESTADÍSTICO Y CARTOGRÁFICO DE ANDALUCÍA 2013-2017	20/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y TAGHLEEF INDUSTRIALES S.L.U PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	17/12/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CONSULTING DE NEGOCIOS S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	22/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y PILAR RUIZ DE ADANA JURADO PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	03/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y JULIO HIGUERAS HERRADOR PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	29/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDA DE JAÉN Y ENRIQUE RUIZ CANTOS PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	30/01/2015	
CONVENIO MARCO DE COLABORACIÓN ENTRE LA UJA Y TERNUM GROUP, S.L	02/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y EUROPREVENJAEN PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	06/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CLARTON HORN, S.A.U. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	02/02/2015	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COOPERACIÓN ENTRE LA UNIVERSIDAD DE JAÉN Y INFORMÁTICA CANO GRANADA, S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	02/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y DESARROLLOS TECNOLÓGICOS INTELEC S.L PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	26/08/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y JAIME TORIBIO MORENO PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	08/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CONSTRUCCIONES CALDERÓN PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	07/10/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y MORENO CRUZ ASESORES C.B., PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	03/02/2015	
CONVENIO DE COOPERACIÓN ENTRE LA UNIVERSIDAD DE JAÉN Y METUBER S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	22/10/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ANTONIO ALVAREZ PUERTA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	02/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CATALINA FUSTER PSICOLOGÍA Y COACHING PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	04/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y HLG CONSTRUCCIONES TEMPLE S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	19/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y PORTINOX S.A PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	30/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y FEDERACIÓN DE SERVICIOS PUBLICOS DE UGT PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	22/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CLINICA DE FISIOTERAPIA MIGUEL ÁNGEL LÉRIDA ORTEGA S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	03/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CONGELADOS DEL MAR EL CARMEN S.L., PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	31/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y FUNDACIÓN FUENTE AGRIA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	09/02/2015	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y MANUEL CABANES RODRIGUEZ S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	18/12/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ALBERTO ORTEGA APONTE, PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y HEFAGRA, S. COOP.AND. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	06/11/2014	
CONVENIO DE COOPERACIÓN ENTRE LA UNIVERSIDAD DE JAÉN Y AYUNTAMIENTO DE LOPERA PARA LA REALIAZCIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	07/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y AUDUFOTO AUDIOVISUAL GROUP, SL. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/01/2015	
CONVENIO DE COOPERACIÓN ENTRE LA UNIVERSIDAD DE JAÉN Y AYUNTAMIENTO DE ÁLORA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/11/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y INSTALACIONES NEGRATIN SL PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	11/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CB ASESORIA MOLINA LARA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	11/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y JULIO JOSÉ MURILLO LECHUGA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	10/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y RESIDENCIA DE MAYORES "NUESTRA SEÑORA DE LOS DESAMPARADOS" PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	05/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y PEDRO JOAQUÍN CHICA JIMÉNEZ Y DOS MÁS,C.B. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	19/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y SHARING SENSES PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	19/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y TECOMED, S.C.A. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/02/2015	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y JUANA MARÍA GILA LEON PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y MC SPA SOCIEDAD DE PREVENCIÓN SLU PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	19/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ASESORÍA MARIA GONZALEZ S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	13/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ALBA PERALTA MARIA DEL PILAR, PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	11/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y SERGIO BERRIOS MESA PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/03/2013	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y STO ASERVITECO SUR 2000, SL PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	28/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y PREMAP SEGURIDAD Y SALUD SLU PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	17/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y EXCMO. COLEGIO OFICIAL DE GRADUADOS SOCIALES DE MADRID PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ASESORAMIENTO INMOBILIARIO ROAN, S.A., PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	10/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y MINCATEC, S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	11/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y PELLENC IBERICA SL PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	10/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y MARIA DE LA PALOMA RUIZ SANCHEZ PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	13/11/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ASESORIA GARCIA-PLATA, S.L. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	24/02/2015	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y E.I.I.T S.A PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	04/12/2014	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y GARRIDO-ESPINOSA ASESORES S.L., PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	13/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y VEGACEITES S.L., PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	26/01/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y SCA NUESTRA SEÑORA DE LA PAZ PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	20/02/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y CRISTINA APARICIO BARROSO, PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	29/01/2015	
CONVENIO DE COLABORACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y LA EMPRESA GRUPO DE AUDITORES PÚBLICOS S.A. PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS	10/02/2015	
CONVENIO ESPECÍFICO DE COLABORACIÓN ENTRE LA UJA Y LA EXCMA. DIPUTACIÓN PROVINCIAL DE JAÉN PARA LA REALIZACIÓN DEL PROYECTO "SECUENCIA DEL GENOMA DEL OLIVO"	09/03/2015	
CONVENIO ESPECÍFICO DE COLABORACIÓN ENTRE LA UJA Y LA EXCMA. DIPUTACIÓN PROVINCIAL DE JAÉN PARA LA REALIZACIÓN DE UN PROYECTO DE INVESTIGACIÓN SOBRE RIESGOS ASOCIADOS A LAS INFRAESTRUCTURAS VIARIAS DE LA PROVINCIA DE JAÉN	09/03/2015	50.000,00 €
PROTOCOLO DE COLABORACIÓN ENTRE LA DIPUTACIÓN PROVINCIAL DE JAÉN Y LA UJA, PARA LA REALIZACIÓN DEL PROYECTO "SECUENCIA DEL GENOMA DEL OLIVO"	09/03/2015	
PROTOCOLO DE COLABORACIÓN ENTRE LA DIPUTACIÓN PROVINCIAL DE JAÉN Y LA UJA, PARA LA REALIZACIÓN DEL PROYECTO "SECUENCIA DEL GENOMA DEL OLIVO"	09/03/2015	
CONVENIO MARCO DE COOPERACIÓN ACADÉMICA ENTRE LA UJA (ESPAÑA) Y STRATHOMORE UNIVERSITY (KENIA)	07/11/2011	
CONVENIO MARCO DE COOPERACIÓN INTERINSTITUCIONAL ENTRE EL TRIBUNAL CONSTITUCIONAL DEL PERÚ Y LA UJA DE ESPAÑA	12/03/2015	
ACTA DE ENTREGA Y DONACIÓN DE OBRA DE ARTE A LA UJA	26/02/2015	6.000,00 €
CONVENIO ESPECÍFICO DE COLABORACIÓN ENTRE LA UJA Y LA UNIVERSIDAD DE GUADALAJARA (MÉXICO)	27/02/2015	
CONVENIO MARCO DE COOPERACIÓN ACADÉMICA ENTRE LA UJA (ESPAÑA) Y EL PONTIFICIO INSTITUTO AMBROSIANO DE MÚSICA SACRA (ITALIA)	02/02/2015	

TÍTULO	FECHA	IMPORTE
CONVENIO MARCO DE COLABORACIÓN ENTRE LA UNIVERSIDAD DE JAÉN Y EL CENTRO DE PSICOLOGÍA CLÍNICA-ESCOLAR-JURÍDICA "DAVID SÁNCHEZ"	20/05/2013	
CONVENIO MARCO DE COLABORACIÓN ENTRE LA UNIVERSIDAD DE JAÉN Y EL CENTRO DE ESTUDIOS SOCIALES Y JURÍDICOS SUR DE EUROPA	04/12/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y EL MUSEO PROVINCIAL DE JAÉN, S.L. PARA LA REALIZACIÓN DEL/DE LAS PRÁCTICUM/PRÁCTICAS DEL MÁSTER EN TURISMO, ARQUEOLOGÍA Y NATURALEZA	24/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y EL MUSEO PROVINCIAL DE JAÉN, S.L. PARA LA REALIZACIÓN DEL/DE LAS PRÁCTICUM/PRÁCTICAS DEL MÁSTER EN TURISMO, ARQUEOLOGÍA Y NATURALEZA	24/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y LA ASOCIACIÓN SOLIDARIDAD DON BOSCO PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS EN EL CURSO DE EXPERTO/A EN COOPERACIÓN INTERNACIONAL AL DESARROLLO CON ÁFRICA SUBSAHARIANA Y EN EL PROGRAMA DE FORMACIÓN Y PRÁCTICAS UNIVERSITARIAS EN PROYECTOS DE COOPERACIÓN AL DESARROLLO	12/06/2014	
CONVENIO MARCO DE COOPERACIÓN ENTRE LA ASOCIACIÓN CAMINAMOS, MOVIMIENTO ASOCIATIVO POR LAS PERSONAS CON CAPACIDADES INTELECTUALES DIFERENTES Y LA UNIVERSIDAD DE JAÉN	24/06/2014	
CONVENIO MARCO DE COOPERACIÓN ENTRE LA ASOCIACIÓN SOCIAL Y CULTURAL EN PRO A LA DISCAPACIDAD "LA INTEGRAL" Y LA UNIVERSIDAD DE JAÉN	26/09/2014	
CONVENIO MARCO DE COOPERACIÓN ENTRE LA ASOCIACIÓN ASPACE JAÉN Y LA UNIVERSIDAD DE JAÉN	25/06/2014	
CONVENIO MARCO DE COOPERACIÓN ENTRE LA FUNDACION ALIATAR Y LA UNIVERSIDAD DE JAÉN	24/06/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y RESTING DOÑANA CAMPING, S.L. PARA LA REALIZACIÓN DEL/DE LAS PRÁCTICUM/PRÁCTICAS DE MÁSTER EN TURISMO, ARQUEOLOGÍA Y NATURALEZA	30/06/2014	
CONVENIO MARCO DE COOPERACIÓN ENTRE LA ASOCIACIÓN HERMANDAD DE DONANTES DE SANGRE DE JAÉN Y LA UNIVERSIDAD DE JAÉN	01/07/2014	
CONVENIO MARCO DE COOPERACIÓN ENTRE LA ASOCIACIÓN PARA LA LUCHA CONTRA LAS ENFERMEDADES DE LA SANGRE DE PADRES DE NIÑOS CON CÁNCER Y LA UNIVERSIDAD DE JAÉN	08/07/2014	

TÍTULO	FECHA	IMPORTE
CONVENIO MARCO DE COOPERACIÓN ENTRE LA ASOCIACION EN DEFENSA DE LA ANOREXIA NERVIOSA Y LA BULIMIA Y LA UNIVERSIDAD DE JAÉN	08/07/2014	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y EL MUSEO PROVINCIAL DE JAÉN, S.L. PARA LA REALIZACIÓN DEL/DE LAS PRÁCTICUM/PRÁCTICAS DEL MÁSTER EN TURISMO, ARQUEOLOGÍA Y NATURALEZA	17/02/2015	
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UNIVERSIDAD DE JAÉN Y ASOCIACIÓN SOLIDARITY AFRICA PRACTICAL PROJECTS (SAPP) PARA LA REALIZACIÓN DE PRÁCTICAS ACADÉMICAS EXTERNAS EN EL CURSO DE EXPERTO/A EN COOPERACIÓN INTERNACIONAL AL DESARROLLO CON ÁFRICA SUBSAHARIANA Y EN EL PROGRAMA DE FORMACIÓN Y PRÁCTICAS UNIVERSITARIAS EN PROYECTOS DE COOPERACIÓN AL DESARROLLO	12/06/2014	
CONVENIO CON HEREDEROS DE DIEGO TORRES MARTÍNEZ, S.L (CANON) PARA EL PATROCINIO DEL VII PREMIO AL EMPRENDIMIENTO	15/09/2014	
CONVENIO DE COLABORACIÓN ENTRE LA UNIVERSIDAD DE JAÉN Y CAJA RURAL DE JAÉN PARA LA CELEBRACIÓN DEL VII PREMIO AL EMPRENDIMIENTO	15/09/2014	3.000,00 €
CONVENIO MARCO DE COOPERACIÓN ENTRE LA ASOCIACIÓN DE FAMILIAS DE AYUDA A DROGODEPENDIENTES (AFAD) Y LA UNIVERSIDAD DE JAÉN	21/10/2014	
CONVENIO MARCO DE COOPERACIÓN ENTRE LA ONGD FARMACÉUTICOS MUNDI Y LA UNIVERSIDAD DE JAÉN	28/10/2014	
EXCAVACIONES ARQUEOLÓGICAS EN EL CASTILLO DE VILLARDOMPARDO 2015. CONVENIO ESPECÍFICO DE COLABORACIÓN ENTRE EL EXCMO. AYUNTAMIENTO DE VILLARDOMPARDO Y LA UNIVERSIDAD DE JAÉN PARA LA PRESTACIÓN DE SERVICIOS DE ASESORAMIENTO CIENTÍFICO-TÉCNICO	08/01/2015	
AL CONVENIO ESTABLECIDO ENTRE LA UNIVERSIDAD DE JAÉN Y LA EMPRESA LABORATORIO HIGEA (ANTES LABORATORIO ARJONA, S.L.), PARA LA REALIZACIÓN DEL PRACTICUM DEL MÁSTER OFICIAL EN OLIVAR, ACEITE DE OLIVA Y SALUD (DE FECHA 29 DE NOVIEMBRE DE 2006)	26/11/2014	
ANÁLISIS DE ALIMENTOS. MASTER OFICIAL AVANCES EN SEGURIDAD DE LOS ALIMENTOS . CONTROLAB	11/02/2015	
UJA-CAJA RURAL PREDIMED PLUS. CONVENIO ESPECÍFICO DE COLABORACIÓN ENTRE LA UNIVERSIDAD DE JAÉN Y FUNDACIÓN CAJA RURAL DE JAÉN	30/01/2015	10.000,00 €
CONVENIO DE COLABORACIÓN ENTRE LA UNIVERSIDAD DE JAÉN Y LA DIPUTACIÓN PROVINCIAL DE JAÉN, PARA EL IMPULSO DE LA CÁTEDRA DE PLANIFICACIÓN ESTRATÉGICA TERRITORIAL, DESARROLLO LOCAL Y GOBERNANZA (RENOVACIÓN)	01/02/2015	

TÍTULO	FECHA	IMPORTE
CONVENIO DE COOPERACIÓN EDUCATIVA ENTRE LA UJA Y FUNDACIÓN ANDALTEC I+D+I, PARA LA REALIZACIÓN DEL/DE LAS PRÁCTICUM/PRÁCTICAS DE MÁSTER "AVANCES EN SEGURIDAD DE LOS ALIMENTOS"	08/01/2015	