DOCUMENTO DE SEGURIDAD DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

ELABORACIÓN	APROVACIÓN
Unidad de Comunicación, Innovación y Gestión de la Calidad	Dirección
Fecha: 4 de marzo de 2015	Fecha:
Firma:	Firma:

Documento presentado y aprobado por el Patronato del IISPV: 28 de junio de 2010

Documento presentado al Comité Científico Interno del IISPV: 1 de julio de 2010

Documento revisado por la Comisión de Seguimiento: xxxx 2015

Control de versiones

Fecha	Modificado por	Comentarios	Aprobado por	Versión
22/01/13	Unidad de gestión de la calidad, innovación y comunicación	Cambios en usuarios y ubicación fichero manual	IISPV	1.0
02/09/13	Unidad de gestión de la calidad, innovación y comunicación	Inscripción fichero ATT	IISPV	2.0
04/03/15	Unidad de gestión de la calidad, innovación y comunicación	Inscripción de ficheros del BIOBANC IISPV	IISPV	3.0

ÍNDICE DE CONTENIDOS

ABREVIATURAS Y SIGLAS 5

ÁMBITO DE APLICACIÓN DEL DOCUMENTO DE SEGURIDAD 6

A.1. ÁMBITO JURÍDICO 6
A.2. ÁMBITO PERSONAL 9

1. ESTRUCTURA DE LOS FICHEROS DEL IISPV 10

ENCARGADO DE TRATAMIENTO 11

2. MEDIDAS, NORMAS, PROCEDIMIENTOS REGLAS Y ESTÁNDARES DE SEGURIDAD ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS 12

2.1. Identificación y autenticación 12
2.2. Control de accesos 13
2.3. Registro de accesos 13
2.4. Gestión de soportes y documentos 14
2.4.1. Medidas de seguridad aplicables a los ficheros y tratamientos automatizados de nivel mediano y alto 14
2.4.2. Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados 15
2.5. Acceso a datos a través de redes de comunicaciones 15
2.6. Régimen de trabajo fuera de los locales de la ubicación del fichero 16
2.7. Traslado de documentación (solo ficheros no automatizados) 16
2.8. Ficheros temporales o copias de trabajo de documentos 16
2.9. Copias de respaldo y recuperación 16
2.10. Responsable de Seguridad 17
2.11. Control interno y auditoría 17

3. PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL 18

4. FUNCIONES Y OBLIGACIONES DEL PERSONAL 18

5. PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS 19

6. PROCEDIMIENTOS DE REVISIÓN 20

7. CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD 20

8. ANEXOS AL DOCUMENTO DE SEGURIDAD DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DEL IISPV 21

ANEXO I. DESCRIPCIÓN DE FICHEROS 22

I.A. DESCRIPCIÓN DE LOS FICHEROS 22
I.B. TIPOLOGÍA DE USUARIOS 32
RELACIÓN DE USUARIOS (PERSONAL IISPV) CON ACCESO AUTORIZADO 32
I.C. PROCEDIMIENTO DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS 36
I.D. PROCEDIMIENTO DE ASIGNACIÓN, DISTRIBUCIÓN Y ALMACENAMIENTO DE CONTRASEÑAS .37
I.E. SISTEMA UTILIZADO PARA LIMITAR EL ACCESO A LOS USUARIOS, ÚNICAMENTE A AQUELLOS DATOS Y RECURSOS QUE PRECISEN PARA EL DESARROLLO DE SUS FUNCIONES 38
I.F. FORMULARIOS DE LA DECLARACIÓN DE LOS FICHEROS A LA AEPD 39
I.G. REGISTRO DE ACCESOS A LOS FICHEROS NO AUTOMATIZADOS 44

ANEXO II. NOMBRAMIENTOS 45

II.A. NOMBRAMIENTOS 45
II.B. OBLIGACIONES DE TODO EL PERSONAL DEL IISPV 47
II.C. CONSECUENCIAS EN CASO DE INCUMPLIMIENTO 51
II.D. RECIBÍ DEL ACCESO AL DOCUMENTO DE SEGURIDAD IISPV 52
II.E. MODELO DE DOCUMENTO DE CONFIDENCIALIDAD 54

ANEXO III. AUTORIZACIONES DE SALIDA O RECUPERACIÓN DE DATOS 55

MODELO DE SOLICITUD DE RECUPERACIÓN DE DATOS 58

ANEXO IV. DELEGACIONES DE AUTORIZACIONES 59

ANEXO V. INVENTARIOS DE SOPORTES 60

MODELO DE INVENTARIO DE SOPORTES 62

ANNEXO VI. REGISTRO DE INCIDENCIAS 63

ANEXO VII. ENCARGADOS DE TRATAMIENTO 66

ANEXO VIII. REGISTRO DE ENTRADA Y SALIDA DE SOPORTES 69

MODELO DE REGISTRO DE ENTRADA DE LOS SOPORTES 69
MODELO DE REGISTRO DE SALIDA DE LOS SOPORTES 70

ANEXO IX. MEDIDAS ALTERNATIVAS 71

CAPÍTULO: COMPROBACIONES PARA LA REALIZACIÓN DE LA AUDITORÍA DE SEGURIDAD 72

ABREVIATURAS Y SIGLAS

- Art.: Artículo
- AGPD: Agencia Española de Protección de Datos
- BOE: Boletín Oficial del Estado
- FURV: Fundació URV
- HJ23: Hospital Universitari de Tarragona Joan XXIII
- HUSJR: Hospital Universitari Sant Joan de Reus
- HTVC: Hospital de Tortosa Verge de la Cinta
- ICS: Institut Català de la Salut
- IISPV: Institut d'Investigació Sanitària Pere Virgili
- IPM: Institut Pere Mata
- ISCIII: Instituto de Salud Carlos III
- LOPD: Ley de Protección de Datos de Carácter Personal
- RMS: Reglamento de Medidas de Seguridad
- RLOPD: Real Decreto por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal
- URV**:** Universitat Rovira i Virgili
- VITRO SA: VITRO

ÁMBITO DE APLICACIÓN DEL DOCUMENTO DE SEGURIDAD

A.1. Ámbito jurídico

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el Real Decreto 1720/2007 (RD LOPD[1]), de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en adelante RDLOD, recoge las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la LOPD[2].

El presente Documento de Seguridad es de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad del Instituto de Investigación Sanitaria Pere Virgili (IISPV), con sede en la c/ Escorxador, s/n – 43007 de Tarragona, con CIF número G-43814045, 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 normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Las medidas de seguridad se clasifican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

- **NIVEL ALTO**, se aplicarán a los ficheros o tratamientos de datos:
  - de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;
  - recabados con fines policiales sin consentimiento de las personas afectadas; y
  - derivados de actos de violencia de género.
- **NIVEL MEDIO**, se aplicarán a los ficheros o tratamientos de datos:
  - relativos a la comisión de infracciones administrativas o penales;
  - que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito);
  - de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;

[1] https://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf

[2] https://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/Ley-15_99.pdf

- de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros;
- de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;
- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;
- que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y
- de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización[3].

- **NIVEL BÁSICO**, se aplicarán a cualquier otro fichero que contenga datos de carácter personal.

  - También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando: los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;
  - se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero;
  - y en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

Estructura del Instituto de Investigación Sanitaria Pere Virgili

El IISPV es un Instituto creado en el marco de un convenio de colaboración científica interinstitucional (Registre de Convenis). Las instituciones constituyentes son (en, adelante Instituciones):

- ICS: HJ23, HTVC, Àrea d'Atenció Primària de Tarragona y Àrea d'Atenció Primària de Terres de l'Ebre
- URV
- Grup SAGESSA: HUSJR, Àrea d'Atenció Primària de SAGESSA
- Grup Pere Mata: Hospital Psiquiàtric Universitari Institut Pere Mata (IPM)

[3] Para esta categoría de ficheros además deberá disponerse de un registro de accesos.

Las Instituciones acogen y agrupan la actividad investigadora epidemiológica, clínica, básica y asistencia sanitaria, realizada por el personal investigador y el personal investigador del IISPV.

Estas Instituciones disponen de espacios e infraestructura específicos para llevar a cabo actividades de investigación y prestar los servicios de apoyo necesarios para los investigadores y grupos de investigación de las diferentes Instituciones y unidades asociadas.

El IISPV utiliza los espacios de investigación, docencia y de infraestructura básica de investigación (laboratorios, equipamientos, otras instalaciones, etc.) de las Instituciones y requiere de las mismas para desarrollar su actividad de investigación y poder concurrir a convocatorias públicas.

El IISPV ha recibido, por parte de las Instituciones, el encargo de diseñar y ejecutar el proyecto de transformación de la actividad de investigación sanitaria y biomédica que las instituciones llevan a cabo individualmente hacia un modelo común e integrado de producción, gestión y explotación de excelencia y altamente competitivo de investigación sanitaria y biomédica en el Camp de Tarragona y las Terres de l'Ebre. Para lograr este objetivo, se ha trabajado en el Manual de Gestión de la IISPV, en el que se referencia el Documento de Seguridad de la IISPV (apartado 1.4.2.). Se define una estrategia a seguir para poder cumplir los objetivos que marca la LOPD.

El IISPV ha elaborado el presente un Documento de Seguridad siendo este cumplimentado con el Documento de Seguridad de cada Institución fundadora y el Documento del Encargado de Tratamiento (FURV, VITRO y detallado en el punto específico **Encargado de Tratamiento**). Siendo dichos documentos conocidos por todo el personal investigador del IISPV. Con ello y de acuerdo con los puntos de obligado cumplimiento del proceso de acreditación del ISCIII, en concreto los apartados: 1.4.2. Verificación del cumplimiento de disposiciones vigentes en materia de I+D+i (ensayos clínicos, Declaración de Helsinki, Convenio de Oviedo, Protección de datos personales, etc.) y 1.4.2.aEl el Instituto respeta la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. El IISPV documenta e informa de las bases de datos con información personal y actúa de forma acorde a la legislación tanto en proyectos nacionales como internacionales.

El IISPV dispone, también, de los documentos: Código de Buenas Prácticas Científicas del IISPV aprobado por el Comité Científico Interno del IISPV (26.06.09) y gestionado por la misma Dirección Científica del IISPV, el Comité de Integridad de la Investigación y la Unidad de Gestión de la Calidad y la Guia de bona pràctica en la recerca de la salut de l'ICS, aprobada por la reunión de Directores Científicos del ICS en junio de 2014.

A.2. Ámbito personal

Este documento es de obligado cumplimiento para todo el personal del IISPV. El RLOPD establece que estas medidas de seguridad serán conocidas, aceptadas y respetadas por todo el personal del IISPV. Por este motivo, el IISPV ha elaborado un documento que está debidamente comunicado y aceptado por todos y cada uno de los trabajadores del IISPV.

Con esta finalidad, se incluirá un extracto a la documentación a entregar al personal en el momento de la contratación, con el objetivo de dar el debido cumplimiento a la obligación contenida en el Art. 8 del RLOPD.

1. ESTRUCTURA DE LOS FICHEROS DEL IISPV

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

NOMBRE DEL FICHERO	FINALIDAD DEL FICHERO	NIVEL	GESTIÓN
FICHERO AUTOMATIZADO			
A3NOM - **Personal**	Fichero destinado a la gestión de la relación contractual de los trabajadores	Medio	Encargado de Tratamiento
FÉNIX - **Clientes (Internos y Externos)** - **Proveedores**	Fichero empleado para la gestión de los clientes y la gestión de los procesos contables de cobros de los proveedores del IISPV y pago de las facturas que éstos emiten.	Bajo	Encargado de Tratamiento
ATT APLICATIU DE TRANSFERÈNCIA DE TECNOLOGIA	Fichero destinado a la gestión de la contratación de proyectos de transferencia de tecnología o conocimiento.	Bajo	Encargado de Tratamiento
FICHERO MIXTO			
BIOBANC IISPV – GPM	Gestión de datos asociados a muestras biológicas para su uso en la investigación biomédica	Alta	Encargado de Tratamiento
BIOBANC IISPV – HUSJR	Gestión de datos asociados a muestras biológicas para su uso en la investigación biomédica	Alta	Encargado de Tratamiento
BIOBANC HJ23 (Nodo HTVC)	Gestión de datos asociados a muestras biológicas para su uso en la investigación biomédica	Alta	Encargado de Tratamiento
FICHERO NO AUTOMATIZADO			
PROYECTOS Y CONTRATOS R+D+i	Fichero de almacenaje de las solicitudes de proyectos y contratos R+D+i (de acuerdo con la gestión de proyectos del ISCIII).	Bajo	IISPV

En el Anexo I.A. se describen detalladamente cada uno de los ficheros y tratamientos, junto con los aspectos que les afecten de manera particular.

En el Anexo I.F. se incorpora una copia de los impresos de las notificaciones remitidos al Registro de la Agencia Española de Protección de Datos.

Encargado de Tratamiento

El 01.10.08 se firmó una adenda al contrato (01.10.07) entre la URV, FURV y el IISPV para la prestación de servicios informáticos. En fecha 15.05.2013 se renovó dicha adenda de encargado de tratamiento. En este mismo documento el IISPV autoriza a la FURV a ser el Encargado de Tratamiento de los datos según los artículos 20-22 del Real Decreto por el cual se aprueba el Reglamento de Desarrollo de la Ley Orgánica 16/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal (BOE, núm. 17 de 19.01.2008).

El Contracte de prestació de serveis entre VITRO, SA i l'IIPSV (Manteniment software BIOBANC IISPV) Con la empresa VITRO, SA el IISPV firmó en julio de 2012 el Contracte de prestació de serveis entre VITRO, SA i l'IIPSV (Manteniment software BIOBANC IISPV) como Encargado de Tratamiento. Este convenio se renueva anualmente.

Dichos documentos se encuentran en el Anexo VII.

En fecha 16.06.2013 la Fundació IISPV firmó un contrato de encargado de tratamiento de datos con la Asociació Pol de Coneixement Catalunya Sud de la URV.

El plan de seguridad del IISPV contempla las medidas, normas y procedimientos recogidos en el presente documento con el fin de garantizar el nivel de seguridad exigido por el RMS.

Con dicho objetivo se incluyen en el presente documento una serie de medidas que 8.2.b del citado texto legal y, en particular, a los datos y ficheros de carácter personal utilizados por el IISPV.

Asimismo, el RMS establece que estas medidas de seguridad deberán ser conocidas, aceptadas y respetadas por todo el personal del IISPV. Para ello el IISPV ha elaborado un documento que ha sido debidamente comunicado y aceptado por todos y cada uno de los empleados del IISPV.

2. MEDIDAS, NORMAS, PROCEDIMIENTOS REGLAS Y ESTÁNDARES DE SEGURIDAD ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS

Las medidas de seguridad adoptadas se circunscriben a los siguientes ámbitos:

2.1. Identificación y autenticación

El procedimiento de identificación y autenticación de los usuarios para la asignación y gestión de contraseñas asociadas a cada usuario con acceso a los sistemas de información del IISPV, para los ficheros FENIX, A3NOM@, ATT, BIOBANC IISPV – HUSJR, BIOBANC IISPV –GPM, BIOBANC HJ23 (NODO HTVC), garantizando confidencialidad e integridad es desarrollado por el Encargado de Tratamiento.

El Responsable de Ficheros del IISPV se encarga de que exista una relación actualizada de usuarios que tengan acceso autorizado a los sistemas de información. Dicha relación se integra en el presente Documento de Seguridad como Anexo I.B.

El Responsable de Ficheros del IISPV custodia y el Encargado de Tratamiento actualiza la relación de todos los usuarios de la red que tienen acceso autorizado a los sistemas de información. Es competencia del Responsable de Seguridad que la atribución y asignación de contraseñas, así como la custodia de la relación de usuarios se realice de forma que se garantice su confidencialidad e integridad.

Los identificadores de usuario y contraseñas asignadas a cada usuario de la red corporativa del IISPV son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse del mal uso, divulgación o pérdida de los mismos. Cuando un usuario sospeche que alguien conoce su contraseña, será responsable de cambiar la contraseña.

Cada una de las aplicaciones que contienen datos de carácter personal del IISPV genera un procedimiento de identificación y autenticación independiente para cada uno de los ficheros. Dichos procedimientos deben ser revisados y actualizados por el Responsable de Seguridad y que el Encargado de Tratamiento deberá documentar en su Documento de Seguridad.

Las normas contenidas en los Anexo I.C. y Anexo I.D. del presente documento regulan los procedimientos mencionados.

2.2. Control de accesos

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El Responsable del Fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

Únicamente el personal autorizado descrito (Anexo I.B.) en el presente Documento de Seguridad podrá conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el Responsable del Fichero. En este mismo anexo se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos facilitado por el Encargado del Tratamiento. Esta lista se actualizará y el procedimiento utilizado de solicitud de alta, modificación y baja de las autorizaciones de acceso a los datos se actualizará según lo establecido en el Anexo I.E..

Toda la información albergada en la red corporativa del IISPV, de forma estática o circulando en forma de mensaje de correo electrónico, es propiedad del IISPV y tiene carácter confidencial.

De existir personal ajeno al Responsable del Fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

2.3. Registro de accesos

a. Ficheros automatizados y mixtos

El mecanismo que permita este registro estará bajo control del Responsable de Seguridad (Proyectos y Contratos R+D+i) y el Encargado de Tratamiento (Fenix, A3NOM@, ATT, BIOBANC IISPV-HSUJR-IPM y BIOBANC HJ23 (NODO HTVC).

El Responsable de Seguridad revisará la información de control.

Los usuarios tienen acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

El procedimiento utilizado para limitar el acceso en función de los privilegios otorgados a cada usuario se describe el Anexo I.E. del presente documento.

Sólo el personal autorizado para ello, citado en el documento, podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el Responsable del Fichero.

Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido.

b. Ficheros no automatizados

El acceso a la documentación se limita exclusivamente al personal autorizado. El procedimiento utilizado para limitar el acceso en función de los privilegios otorgados a cada usuario se describe el Anexo I.G. del presente Documento.

Los usuarios tienen acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

Sólo el personal autorizado para ello en el presente Documento de Seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el Responsable del Fichero.

2.4. Gestión de soportes y documentos

2.4.1. Medidas de seguridad aplicables a los ficheros y tratamientos automatizados de nivel mediano y alto

La adenda al contrato entre la FURV y el IISPV para la prestación de servicios informáticos y LOPD de 1.10.2009, establece la autorización a la FURV por parte del IISPV a ser el Encargado de Tratamiento para los ficheros FENIX, A3NOM@ y ATT. El contrato entre VITRO y el IISPV para para la prestación de servicios informáticos y LOPD de julio 2012, establece la autorización a VITRO por parte del IISPV a ser el Encargado de Tratamiento para los ficheros BIOBANC IISPV-HSUJR-IPM y BIOBANC HJ23 (NODO HTVC). En este mismo documento se incluyen los servicios de hosting y housing y de copias de seguridad de los ficheros que contienen datos de carácter personal y los sistemas que los gestionen indicados en el convenio.

En el Anexo V se describe el procedimiento de identificación, inventario y custodia de soportes informáticos del IISPV que contengan datos de carácter personal. El objetivo de dicho procedimiento es permitir identificar el tipo de información que contienen dichos soportes, ser inventariados y almacenados en un lugar de acceso restringido al personal autorizado que se detalla en el Anexo I.B Dicho procedimiento, para los ficheros FENIX, A3NOM@, ATT y BIOBANC IISPV – HSUJR, BIOBANC IISPV - GPM y BIOBANC HJ23 (NODO HTVC) es responsabilidad del Encargado de Tratamiento.

Únicamente el Responsable del Fichero, o aquel en que se hubiera delegado, podrán autorizar la salida de soportes informáticos que contengan datos personales, fuera de los locales en los que esté ubicado el fichero, de acuerdo con el procedimiento detallado en el

Anexo III. En este mismo anexo, se incluyen los documentos de autorización relativos a la salida de soportes que contengan datos personales.

Los soportes o cualquier documento que vayan a ser desechados (ficheros FENIX, A3NOM@, ATT, BIOBANC IISPV – HSUJR, BIOBANC IISPV - GPM y BIOBANC HJ23 (NODO HTVC)) que incluyan datos de carácter personal, se han de destruir o borrar mediante el procedimiento previsto en el Anexo III de forma que no sea posible el acceso a la información contenida en ellos o su recuperación posterior, dicho procedimiento la responsabilidad es el Encargado de Tratamiento.

Es responsabilidad del Encargado de Tratamiento cuidar el traslado de la documentación adoptando las medidas previstas en su Documento de Seguridad para evitar la sustracción, pérdida o acceso indebido a la información.

2.4.2. Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en la legislación. Estos criterios garantizarán la correcta conservación de los documentos, la localización y consulta de la información y posibilitarán el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal dispondrán de mecanismos que obstaculicen su apertura. Cuando sus características físicas no permitan adoptar esta medida, el responsable adoptará medidas que impidan el acceso a la información de personas no autorizadas.

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamientos indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso a personas no autorizadas.

En el Anexo I.E se han descrito las formas y acceso al archivo.

2.5. Acceso a datos a través de redes de comunicaciones

En el caso del IISPV, para los ficheros FENIX, A3NOM@, ATT, BIOBANC IISPV – HSUJR, BIOBANC IISPV - GPM y BIOBANC HJ23 (NODO HTVC) es el Encargado de Tratamiento que garantiza las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones, sean públicas o no. También garantizarán un nivel de seguridad equivalente al exigido para los accesos en modo local. Cada una de las

instituciones dispone de sus propios sistemas de seguridad, que contempla los servicios de autenticación, confidencialidad e integridad de los datos. Para el fichero Contratos y Proyectos R+D+i el IISPV es quien adopta todas las medidas.

2.6. Régimen de trabajo fuera de los locales de la ubicación del fichero

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada explícitamente por el Responsable del Fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

El procedimiento para la autorización se realizará mediante correo electrónico enviado por el Responsable de Fichero.

2.7. Traslado de documentación (solo ficheros no automatizados)

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse las medidas para impedir el acceso o manipulación de la información objeto de traslado, siguiendo las instrucciones descritas en el presente Documento para el fichero Contratos y Proyectos R+D+i es el IISPV.

2.8. Ficheros temporales o copias de trabajo de documentos

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el RDLOPD, y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

2.9. Copias de respaldo y recuperación

Es el Encargado de Tratamiento es el órgano encargado de realizar las copias de respaldo para los ficheros FENIX, A3NOM@, ATT, BIOBANC IISPV – HSUJR, BIOBANC IISPV - GPM y BIOBANC HJ23 (NODO HTVC).

Respecto los ficheros parcialmente automatizados no se aplica, no existen este tipo de ficheros actualmente.

El Responsable del Fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Se conserva una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentran los equipos informáticos que los tratan, cumpliendo, en todo caso, las medidas de seguridad exigidas en el RLOPD.

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información.

Dichos procedimientos son los que relacionan en el Anexo III.

2.10. Responsable de Seguridad

El Responsable de Seguridad, con carácter general, se encargará de coordinar y controlar las medidas definidas en este documento de seguridad. En ningún caso, la designación supone la exoneración de la responsabilidad que corresponde a al Responsable del Fichero y al Encargado de Tratamiento como Responsable del Fichero (FENIX, A3NOM@, ATT, BIOBANC IISPV – HSUJR, BIOBANC IISPV - GPM y BIOBANC HJ23 (NODO HTVC)), de acuerdo con el RLOPD.

El Responsable de Seguridad desempeñará las funciones encomendadas durante el periodo de 2 años. Una vez transcurrido este plazo, se podrá nombrar al mismo o a otro diferente.

En el Anexo II.A se describe la relación de los Responsables de Seguridad, y en su caso de ausencia por enfermedad, vacaciones o ejercicio de permiso legal, sus sustitutos directos son os Responsables de Fichero correspondientes.

2.11. Control interno y auditoría

Control Interno:

Con una frecuencia mínima de una vez al año, el Responsable de Seguridad llevará a cabo un seguimiento para verificar el cumplimiento de lo dispuesto en el presente Documento de Seguridad.

Auditoría:

A partir del nivel medio, los sistemas de información e instalaciones del tratamiento y almacenamiento de datos se someterán, al menos cada dos años a una auditoria interna o externa que verifique el cumplimiento del RLOPD y de los procedimientos e instrucciones vigentes en materia de seguridad de datos.

En el capítulo específico “Comprobaciones para la realización de la auditoria de seguridad” se detallan los puntos a seguir para la realización de la auditoría, interna o externa, según convenga, para la verificación del cumplimiento del Título VIII del RLOPD, referente a las

medidas de seguridad, según lo indicado en sus artículos 96 y 110 respecto de ficheros automatizados y no automatizados respectivamente, y que debe realizarse al menos cada dos años.

Con carácter extraordinario deberá realizarse también cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas, con el objetivo de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado anteriormente.

El informe analizará la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias.

Los informes de auditoría han de ser analizados por el Responsable de Seguridad, que elevará las conclusiones al Responsable del Fichero para que adopte las medidas correctoras y quedará a disposición de la AGPD, o en su caso, de las autoridades de control de las Comunidades Autónomas.

3. PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas para cada fichero en la parte del Anexo II.B. correspondiente.

Para asegurar que todas las personas conocen la seguridad que afectan al desarrollo de las funciones, así como las consecuencias legales, que pudieran ser exigidas, del incumplimiento de las mismas serán informadas de acuerdo con el documento de confidencialidad (Anexo II.E.), en el que se exponen las normas que debe cumplir y las consecuencias de su omisión (Anexo II.C.).

4. FUNCIONES Y OBLIGACIONES DEL PERSONAL

Funciones y obligaciones de carácter general:

Todo el personal (Anexo II.B.), incluido el Encargado de Tratamiento, que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al Responsable del Fichero las incidencias de seguridad de las que tenga conocimiento respecto a los recursos protegidos, según los

procedimientos establecidos en este Documento de Seguridad del IISPV, y en concreto en lo descrito en el Anexo VI.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo. En consecuencia, todo el personal de la oficina técnica del IISPV ha firmado un documento de confidencialidad, cuyo modelo se encuentra en el Anexo II.E.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan, o a los recursos del sistema de información.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto de aquellos datos que hubiera podido conocer durante la prestación del servicio.

En el Anexo IV se encuentra el procedimiento en el que se explica cómo se delegan las autorizaciones en los usuarios relacionados.

5. PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal citados en el Anexo I.A.

El análisis y descripción detallada de este procedimiento se refleja en el Anexo VI. No obstante, el registro de incidencias de los ficheros FENIX, A3NOM@ y ATT se gestionará mediante lo convenido con el Encargado de Tratamiento, también lo serán los ficheros BIOBANC IISPV – HSUJR, BIOBANC IISPV - GPM y BIOBANC HJ23 (NODO HTVC).

Con independencia a lo referente en el punto anterior, en el registro de incidencias se consignarán: los procedimientos de recuperación de los datos que se han realizado, (indicando la persona que ejecutó el proceso), los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. Para la ejecución de los procedimientos de recuperación se precisará la autorización por escrito del Responsable del Fichero. En el Anexo III se incluyen los documentos de autorización de recuperación de datos.

6. PROCEDIMIENTOS DE REVISIÓN

Revisión del Documento de Seguridad

El documento se mantendrá actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Asimismo, se adecuará a las disposiciones vigentes en materia de seguridad de los datos de carácter personal. Las modificaciones serán propuestas por el Responsable de Seguridad y aprobadas por el Responsable de Ficheros y comunicadas por el mismo a las personas afectadas.

7. CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por parte del personal implicado, será sancionable de acuerdo con la normativa laboral, independientemente de las responsabilidades civiles y penales que pudieran ser exigidas. Ver Anexo II.C.

8. ANEXOS AL DOCUMENTO DE SEGURIDAD DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DEL IISPV

ANEXO I	I.A. Descripción de Ficheros
	I.B. Tipología de usuarios y Relación actualizada de usuarios con acceso autorizado
	I.C. Procedimiento de identificación y autenticación de usuarios
	I.D. Procedimiento de asignación, distribución y almacenamiento de contraseñas
	I.E. Sistema utilizado para limitar el acceso de los usuarios, únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones
	I.F. Formularios declaración ficheros a la AGPD
	I.G. Registro de accesos a los ficheros no automatizados
ANEXO II	II.A. Nombramientos
	II.B. Obligaciones del personal
	II.C. Consecuencias en caso de incumplimiento
	II.D. Documento de acceso al Documento de Seguridad
	II.E. Modelo de Documento de Confidencialidad
ANEXO III	Procedimiento de realización de copias de respaldo y recuperación de datos
	Modelo de salida de soportes físicos
	Modelo de recuperación de datos
ANEXO IV	Delegación de autorizaciones
ANEXO V	Procedimiento utilizado para la gestión de soportes informáticos
	Modelo de inventario de soportes
ANEXO VI	Notificación, gestión y respuesta ante incidencias
ANEXO VII	Responsabilidades del Encargado de Tratamiento
	Modelo de acuerdo de confidencialidad y tratamiento de los datos de carácter personal
ANEXO VIII	Registro de entrada y salida de soportes
ANEXO IX	Medidas alternativas

ANEXO I. DESCRIPCIÓN DE FICHEROS

I.A. Descripción de los ficheros

Denominación del fichero: APLICATIVO DE GESTIÓN ECONÓMICA Y ADMINISTRATIVA (FÉNIX)		**Nivel de Seguridad:** BÁSICO **Identificador AEPD:** 2103011019
Responsable: Gerencia	**Área:** Unidad de Gestión de Proyectos I+D+i y Unidad de Gestión Económica Servicio subcontratado (Convenio para la prestación de servicios FURV)	
Descripción: Fichero empleado para la gestión contable y de tesorería		
Finalidad del fichero y usos previstos: Gestión contable, fiscal y administrativa		
Personas o colectivos: Personal directivo, técnico, de servicios y administrativo del IISPV. Personal Investigador del IISPV que tiene contratado un proyecto de investigación y/o formación a través del IISPV		
Sistema / Aplicación: Servidores Centrales		**Entorno:** ORACLE
Tipo de conexión remota: Red corporativa, Internet, Intranet		
Sistema de tratamiento: Mixto (automatizado y no automatizado)	**Periodicidad del cambio de contraseñas**: como mínimo una vez al año	
Trato de los datos: Uso interno; gestión de clientes, contable, fiscal y administrativa		
Procedencia de los datos: El propio interesado o su representante legal	**Procedimiento de recogida de los datos:** Formularios o cupones; el propio documento emitido por el interesado	

Estructura y descripción de los datos: NIF/DNI. Nombre y Apellidos. Dirección. Teléfono. Ingresos, rentas. Datos bancarios. Datos económicos de nómina. Datos de deducciones impositivas/impuestos. Bienes y Servicios suministrados por el afectado. Bienes y Servicios recibidos por el afectado. Transacciones Financieras.	
Cesión o comunicación: Comunicación	**Transferencia de datos:** Organismos de la Seguridad Social; Administración Tributaria; Registros Públicos; Organizaciones o personas directamente relacionadas
Descripción detallada de las copias de respaldo y recuperación: – De acuerdo con la adenda al contrato de prestación de servicios informáticos con el Encargado de Tratamiento	

Denominación del fichero: GESTIÓN DE NÓMINAS A3NOM	**Nivel de Seguridad:** MEDIO **Identificador AEPD:** 2103011008
Responsable: Gerencia	**Área:** Recursos Humanos y Formación y Unidad de Gestión de Proyectos I+D+i. Servicio subcontratado (Convenio para la prestación de servicios FURV)
Descripción: Destinado a la gestión de la relación contractual de los trabajadores	
Finalidad del fichero y usos previstos: Gestión contractual de los trabajadores	
Personas o colectivos: Empleados y becarios	
Sistema / Aplicación: Ordenadores personales	**Entorno:** SQL SERVER
Tipo de conexión remota: No	
Sistema de tratamiento: Mixto (automatizado y no automatizado)	**Periodicidad del cambio de contraseñas**: como mínimo una vez al año
Sistema de tratamiento: Manual	
Trato de los datos: Uso interno y organismo competente, Unidad de RRHH y Formación.	
Procedencia de los datos: El propio interesado o su representante legal	**Procedimiento de recogida de los datos:** Soporte papel; Vía telemática
Estructura y descripción de los datos: Salud. NIF/DNI. Núm. SS. Nombre y Apellidos. Dirección. Teléfono. Datos de Estado Civil. Datos de Familia. Lugar y Fecha de Nacimiento. Edad. Sexo. Nacionalidad. Profesión. Puesto de Trabajo. Datos no económicos de nómina. Ingresos, rentas. Datos bancarios. Datos económicos de nómina. Compensaciones / indemnizaciones. Bienes y servicios suministrados por el afectado. Bienes y servicios recibidos por el afectado. Transacciones financieras.	
Cesión o comunicación: Comunicación	**Transferencia de datos:** Organismos de la Seguridad Social; Administración Tributaria.

Descripción detallada de las copias de respaldo y recuperación:

- De acuerdo con la adenda al contrato de prestación de servicios informáticos con el Encargado de Tratamiento.

Denominación del fichero: ATT – APLICATIU DE TRANSFERÈNCIA DE TECNOLOGIA	**Nivel de Seguridad**: BÀSICO
Responsable: Gerencia	**Identificador AEPD**: 2132171500
Titular: Dirección	**Área:** Unitat de Gestió de Projectes I+D+i
Descripción: Destinado a la gestión de la contratación de proyectos de transferencia de tecnología o conocimiento	
Finalidad del fichero y utilidades previstas: proyectos de transferencia de tecnología (datos económicos, facturación y presupuesto), fines estadísticos, históricos o científicos, otras finalidades.	
Persones o colectivos: Personal contratado	
Sistema / Aplicación: Ordenadores personales	**Entorno:** ORACLE/ACCESS
Tipo de conexión remota: Red corporativa	
Sistema de tratamiento: Mixto (automatizado y no automatizado)	**Periodicidad del cambio de contraseñas**: como mínimo una vez al año
Sistema de tratamiento: Mixta	
Tratamiento de los datos: Uso interno; gestión de la transferencia de tecnología	
Procedencia de los datos: El propio interesado o su representante legal	**Procedimiento de recogida de los datos:** Soporte papel; Vía telemática
Estructura y descripción de los datos: NIF/DNI. Núm. SS. Nombre y Apellidos; Dirección; Teléfono; Profesión; Lugar de trabajo	
Cesión o comunicación: N/A	**Transferencia de datos:** N/A

Ubicación de datos: Servidor de la URV

Descripción detallada de las copias de seguridad y recuperación:

– De acuerdo con la adenda al contrato de prestación de servicios informáticos con el Encargado de Tratamiento.

Denominación del fichero: PROYECTOS Y CONTRATOS I+D+i	**Nivel de Seguridad:** BAJO **Identificador AEPD:** 2103011021
Responsable: Gerencia	**Área:** Unidad de Gestión de Proyectos I+D+i y Unidad de Gestión Económica.
Descripción: Fichero destinado a la gestión de proyectos y contratos de I+D+i.	
Finalidad del fichero y usos previstos: Gestión económica y científica de proyectos y contratos de I+D+i.	
Personas o colectivos: Empleados.	
Sistema / Aplicación: n/a	**Entorno:** Soporte papel.
Tipo de conexión remota: No.	
Sistema de tratamiento: Manual.	
Trato de los datos: Uso interno; Unidad de Gestión de Proyectos I+D+i; Unidad de Gestión Económica	
Procedencia de los datos: El propio interesado o su representante legal	**Procedimiento de recogida de los datos:** Soporte papel; Vía telemática
Estructura y descripción de los datos: NIF/DNI. Nombre y Apellidos. Dirección. Teléfono. Lugar y Fecha de Nacimiento. Edad. Sexo. Nacionalidad. Profesión. Y otros datos relacionados con su actividad profesional	
Cesión o comunicación: Comunicación	**Transferencia de datos:** Organismos oficiales competentes en función de la convocatoria; Cliente Externo contratante
Descripción detallada de las copias de respaldo y recuperación: – Digitalización de dichos proyectos y contratos. Su ubicación es la base de datos Fenix	

Denominación del fichero: BIOBANC IISPV – HUSJR	Nivel de Seguridad: ALTO
Responsable: BIOBANC IISPV (HUSJR – GPM)	**Identificador AEPD**: 2131901959
Titular: Dirección	**Área:** Biobanc IISPV
Descripción: Gestión de datos asociados a muestras biológicas para su uso en la investigación biomédica	
Finalidad del fichero y utilidades previstas: Investigación epidemiológica y actividades análogas	
Persones o colectivos: Pacientes, Padres o Tutores; Representante legal	
Sistema / Aplicación: Ordenadores personales	**Entorno:** ORACLE
Tipo de conexión remota: Red corporativa	
Sistema de tratamiento: Mixta	
Tratamiento de los datos: Investigación epidemiológica y actividades análogas	
Procedencia de los datos: El propio interesado o su representante legal	**Procedimiento de recogida de los datos:** Soporte papel; Vía telemática
Estructura y descripción de los datos: Origen racial o étnico; Salud; Dirección Teléfono	
Cesión o comunicación: Investigación biomédica (datos codificados)	**Transferencia de datos:** N/a
Ubicación de datos: VITRO, SA **Descripción detallada de las copias de seguridad y recuperación:** – De acuerdo el contrato de prestación de servicios informáticos con el Encargado de Tratamiento.	

Denominación del fichero: BIOBANC IISPV – GPM	**Nivel de Seguridad**: ALTO
Responsable: BIOBANC IISPV (HUSJR – GPM)	**Identificador AEPD**: 2132480037
Titular: Dirección	**Área:** Biobanc IISPV
Descripción: Gestión de datos asociados a muestras biológicas para su uso en la investigación biomédica	
Finalidad del fichero y utilidades previstas: Investigación epidemiológica y actividades análogas	
Persones o colectivos: Pacientes, Padres o Tutores; Representante legal	
Sistema / Aplicación: Ordenadores personales	**Entorno:** ORACLE
Tipo de conexión remota: Red corporativa	
Sistema de tratamiento: Mixta	
Tratamiento de los datos: Investigación epidemiológica y actividades análogas	
Procedencia de los datos: El propio interesado o su representante legal	**Procedimiento de recogida de los datos:** Soporte papel; Vía telemática
Estructura y descripción de los datos: Origen racial o étnico; Salud; Dirección Teléfono	
Cesión o comunicación: Investigación biomédica (datos codificados)	**Transferencia de datos:** N/a
Ubicación de datos: VITRO, SA **Descripción detallada de las copias de seguridad y recuperación:** – De acuerdo el contrato de prestación de servicios informáticos con el Encargado de Tratamiento.	

Denominación del fichero: BIOBANC HUJ23 (NODO HTVC)	Nivel de Seguridad: **ALTO**
Responsable: BIOBANC IISPV (HJ23)	**Identificador AEPD**: 2131150043
Titular: Dirección	**Área:** Biobanc IISPV
Descripción: Gestión de datos asociados a muestras biológicas para su uso en la investigación biomédica	
Finalidad del fichero y utilidades previstas: Investigación epidemiológica y actividades análogas	
Persones o colectivos: Pacientes, Padres o Tutores; Representante legal	
Sistema / Aplicación: Ordenadores personales	**Entorno:** ORACLE
Tipo de conexión remota: Red corporativa	
Sistema de tratamiento: Mixta	
Tratamiento de los datos: Investigación epidemiológica y actividades análogas	
Procedencia de los datos: El propio interesado o su representante legal	**Procedimiento de recogida de los datos:** Soporte papel; Vía telemática
Estructura y descripción de los datos: Origen racial o étnico; Salud; Dirección Teléfono	
Cesión o comunicación: Investigación biomédica (datos codificados)	**Transferencia de datos:** N/a
Ubicación de datos: VITRO, SA **Descripción detallada de las copias de seguridad y recuperación:** – De acuerdo el contrato de prestación de servicios informáticos con el Encargado de Tratamiento.	

I.B. Tipología de usuarios

Tipología de usuarios	Perfiles y privilegios
Personal de la Oficina del IISPV y personal de los servicios subcontratados	En función su perfil de trabajo tendrá acceso a los *software* de gestión declarados
Personal contratado y becado por el IISPV (no de la Oficina)	Puede tener acceso, ó no, a la aplicación Web Consulta de Saldos Fenix, en función de las tareas para las que le haya contratado. Consulta de datos referentes a la ATT. Acceso mediante un l*ogin y password*
Personal del IISPV (Catálogo de Personal IISPV) que tiene contratado un proyecto de investigación a través del IISPV	Acceso a: Consulta del estado económico de un proyecto Fénix. Accede mediante un *login* y *password*

Relación de usuarios (Personal IISPV) con acceso autorizado

FENIX	
ÀREA DE TREBAJO	**PRIVILEGIOS**
Gerencia	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización
Técnico/a de Gestión, Recursos Humanos y Formación	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización
Técnico/a de Promoción y Desarrollo	☒ consulta ☒ actualización ☒ inserción ☐ borrado ☐ autorización
Administrativo/a de Proyectos y Contratos de R+D+i	☒ consulta ☒ actualización ☒ inserción ☐ borrado ☐ autorización
Administrativo/a, Facturación de Clientes	☒ consulta ☒ actualización ☒ inserción ☐ borrado ☐ autorización

Administrativo/a, Facturación de Proveedores	☒ consulta ☒ actualización ☒ inserción ☐ borrado ☐ autorización

A3 NOM	
ÁREA DE TRABAJO	**PRIVILEGIOS**
Gerencia	☒ consulta ☐ actualización ☐ inserción ☐ borrado ☐ autorización
Técnico/a de Gestión, Recursos Humanos y Formación	☒ consulta ☐ actualización ☐ inserción ☐ borrado ☐ autorización
Unidad de RRHH (Responsable)	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización
Unidad de RRHH (Soporte Administrativo)	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización

PROYECTOS Y CONTRATOS DE R+D+i	
ÀREA DE TREBAJO	**PRIVILEGIOS**
Gerencia	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización
Técnico/a de Gestión, Recursos Humanos y Formación	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización
Administración de Proyectos y Contratos de I+D+i	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☐ autorización

Administración, Facturación de Clientes	☒ consulta ☒ actualización ☒ inserción ☐ borrado ☐ autorización
Administración, Facturación de proveedores	☒ consulta ☒ actualización ☒ inserción ☐ borrado ☐ autorización

ATT - APLICATIU DE TRANSFERÈNCIA DE TECNOLOGIA	
ÀREA DE TREBAJO	**PRIVILEGIOS**
Gerencia	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización
Técnico/a de Gestión, Recursos Humanos y Formación	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización
Administrativo/a de Proyectos y Contratos de R+D+i	☒ consulta ☒ actualización ☒ inserción ☐ borrado ☐ autorización
Administrativo/a, Facturación de Clientes	☒ consulta ☒ actualización ☒ inserción ☐ borrado ☐ autorización
Administrativo/a, Facturación de Proveedores	☒ consulta ☒ actualización ☒ inserción ☐ borrado ☐ autorización

BIOBANC IISPV - GPM	
ÁREA DE TRABAJO	**PRIVILEGIOS**
BIOBANC IISPV – HOSPITAL UNIVERSITARI SANT JOAN DE REUS	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización

BIOBANC IISPV - HUSJR	
ÁREA DE TRABAJO	**PRIVILEGIOS**
BIOBANC IISPV – HOSPITAL UNIVERSITARI SANT JOAN DE REUS	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización

BIOBANC HJ23 (NODO HTVC)	
ÁREA DE TRABAJO	**PRIVILEGIOS**
BIOBANC IISPV – HOSPITAL UNIVERSITARI DE TARRAGONA JOAN XXIII	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización
BIOBANC IISPV – HOSPTIAL DE TORTOSA VERGE DE LA CINTA	☒ consulta ☒ actualización ☒ inserción ☒ borrado ☒ autorización

I.C. Procedimiento de identificación y autenticación de usuarios

En el presente anexo se describe el sistema utilizado por el Encargado de Tratamiento (Ficheros FENIX, A3NOM@ y ATT) y por el IISPV (Proyectos y Contratos de I+D+i) para la identificación y autenticación de los usuarios autorizados que acceden a los sistemas.

El sistema utilizado para la identificación y autenticación de los usuarios autorizados que acceden a los sistemas por el Encargado de Tratamiento VITRO (BIOBANC IISPV - HUSJR / BIOBANC IISPV – GPM / BIOBANC HJ23 (NODO HTVC) está detallado en el Documento de Seguridad de VITRO.

El sistema utilizado para la identificación y autenticación de los usuarios autorizados que acceden al fichero Proyectos y Contratos de I+D+i está detallado en el presente Documento de Seguridad.

Dichos procedimientos irá de acuerdo con la tipología de usuarios y privilegios definidos en el Anexo I.B.

Procedimiento de Identificación

- Todos los usuarios del sistema informático del IISPV son identificados en el momento de cursar el alta, mediante el contrato laboral el personal contratado por el IISPV y el personal investigador del IISPV mediante su adscripción a un grupo de investigación.

Procedimiento de Autenticación

- A cada usuario del sistema se le asigna un identificador y una clave.
- Las claves de acceso asignadas a cada usuario de la red corporativa del IISPV son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que puedan derivarse del mal uso, divulgación o pérdida de los mismos. Cuando un usuario del IISPV sospeche que alguien conoce o puede conocer su contraseña será responsable de cambiar dicha contraseña.
- Se cambian mensualmente de forma obligatoria las claves de acceso de los usuarios listados en el Anexo I.B.

I.D. Procedimiento de asignación, distribución y almacenamiento de contraseñas

En este anexo se describe el sistema utilizado por el Encargado de Tratamiento (Ficheros FENIX y A3NOM@) el Encargado de Tratamiento (BIOBANC IISPV - HUSJR / BIOBANC IISPV – GPM / BIOBANC HJ23 (NODO HTVC) y por el IISPV (Proyectos y Contratos R+D+i) para la asignación, distribución y almacenamiento de las contraseñas de los usuarios autorizados que acceden a sus sistemas. Dicho procedimiento irá de acuerdo con la tipología de usuario y privilegios descritos en el Anexo I.B.

Asignación de contraseñas

Se asignará inicialmente una contraseña.

Es competencia del Responsable de Seguridad y de ficheros establecer y comprobar que el procedimiento de asignación y atribución de contraseñas, así como la custodia de la relación de usuarios, se realice de forma que se garantice su confidencialidad e integridad.

Distribución de contraseñas

La distribución de contraseñas se realizará de manera que sólo el usuario pueda visualizar la clave asociada a su identificador mediante correo electrónico o una carta.

Almacenamiento de contraseñas

Las contraseñas se almacenan encriptadas por el sistema.

Las contraseñas no deben desvelarse. En el momento en que un usuario sospeche que alguien conoce su contraseña de acceso deberá cambiarla lo antes posible.

I.E. Sistema utilizado para limitar el acceso a los usuarios, únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones

En este anexo se describe el sistema utilizado por el Encargado de Tratamiento (ficheros FENIX y A3NOM@), por el Encargado de Tratamiento (BIOBANC IISPV - HUSJR / BIOBANC IISPV – GPM / BIOBANC HJ23 (NODO HTVC) y por el IISPV (fichero Proyectos y Contratos R+D+i) para limitar el acceso a los diferentes sistemas y áreas de los mismos en función de los privilegios de cada usuario.

El Responsable de Seguridad y de los Ficheros elaborará una relación actualizada de usuarios que tengan acceso autorizado al sistema de información.

El Responsable de Seguridad custodiará y actualizará la relación de todos los usuarios de la red que tienen acceso autorizado al sistema de información.

Control de acceso al sistema:

- Al iniciar el proceso de arranque de cada ordenador conectado a la red corporativa del IISPV, el sistema solicitará la clave de acceso al usuario.
- Una vez introducida la clave de acceso por el usuario, el sistema operativo arrancará y se solicitará el identificador de usuario y la clave de acceso a la red corporativa.
- Cada identificador tendrá unos privilegios asociados, en función del cargo y las funciones del usuario que solicita el acceso.

Cada identificador de usuario tendrá unos privilegios asociados, en función de los cuales podrá acceder únicamente a aquellos datos y recursos que precise para el desarrollo de sus funciones.

I.F. Formularios de la declaración de los ficheros a la AEPD

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

O12/D 569718/2010

DAVID MARTIN FRIGOLS
INSTITUT D'INVESTIGACIO SANITARIA PERE VIRGILI (IISPV)
C/ SANT LLORENÇ, 21
43201 REUS
TARRAGONA ESPAÑA

Nº Reg. Salida: 569718/2010

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, ha acordado en virtud de las competencias que le atribuyen el artículo 60 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre y en el artículo 12.2.a del Real Decreto 428/1993 de 26 de marzo, vigente de conformidad con lo dispuesto en la Disposición Transitoria Tercera de la citada Ley Orgánica 15/1999, **proceder a la inscripción** del fichero notificado con el nombre APLICATIVO DE GESTION ECONOMICA Y ADMINISTRATIVA (FENIX) en el que figura como responsable INSTITUT D'INVESTIGACIO SANITARIA PERE VIRGILI (IISPV), asignándole el código de inscripción 2103011019.

La inscripción de un fichero en el Registro General de Protección de Datos, únicamente acredita que se ha cumplido con la obligación de notificación dispuesta en la Ley Orgánica 15/1999, sin que de esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en dicha Ley y demás disposiciones reglamentarias. De conformidad con lo dispuesto en el artículo 58 del citado Reglamento, esta inscripción deberá encontrarse actualizada en todo momento.

Contra esta Resolución, que pone fin a la vía administrativa, podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, de conformidad con lo previsto en el artículo 46.1 del referido texto legal.

Madrid, 28 de Octubre de 2010
EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

O12/D 569707/2010

DAVID MARTIN FRIGOLS
INSTITUTO DE INVESTIGACION SANITARIA PERE VIRGILI (IISPV)
C/ SANT LLORENÇ, 21
43201 REUS
TARRAGONA ESPAÑA

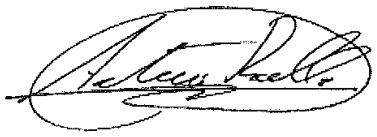
Nº Reg. Salida: 569707/2010

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, ha acordado en virtud de las competencias que le atribuyen el artículo 60 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre y en el artículo 12.2.a del Real Decreto 428/1993 de 26 de marzo, vigente de conformidad con lo dispuesto en la Disposición Transitoria Tercera de la citada Ley Orgánica 15/1999, **proceder a la inscripción** del fichero notificado con el nombre GESTION DE NOMINAS A3NOM en el que figura como responsable INSTITUT D'INVESTIGACIO SANITARIA PERE VIRGILI (IISPV), asignándole el código de inscripción 2103011008.

La inscripción de un fichero en el Registro General de Protección de Datos, únicamente acredita que se ha cumplido con la obligación de notificación dispuesta en la Ley Orgánica 15/1999, sin que de esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en dicha Ley y demás disposiciones reglamentarias. De conformidad con lo dispuesto en el artículo 58 del citado Reglamento, esta inscripción deberá encontrarse actualizada en todo momento.

Contra esta Resolución, que pone fin a la vía administrativa, podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, de conformidad con lo previsto en el artículo 46.1 del referido texto legal.

Madrid, 28 de Octubre de 2010
EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS



Fdo.: Artemi Rallo Lombarte

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

O12/D 569720/2010

DAVID MARTIN FRIGOLS
INSTITUT D'INVESTIGACIO SANITARIA PERE VIRGILI (IISPV)
C/ SANT LLORENÇ, 21
43201 REUS
TARRAGONA ESPAÑA

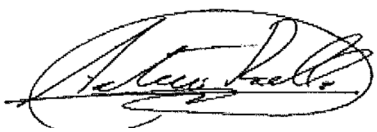
Nº Reg. Salida: 569720/2010

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, ha acordado en virtud de las competencias que le atribuyen el artículo 60 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre y en el artículo 12.2.a del Real Decreto 428/1993 de 26 de marzo, vigente de conformidad con lo dispuesto en la Disposición Transitoria Tercera de la citada Ley Orgánica 15/1999, **proceder a la inscripción** del fichero notificado con el nombre PROYECTOS Y CONTRATOS I+D+I en el que figura como responsable INSTITUT D'INVESTIGACIO SANITARIA PERE VIRGILI (IISPV), asignándole el código de inscripción 2103011021.

La inscripción de un fichero en el Registro General de Protección de Datos, únicamente acredita que se ha cumplido con la obligación de notificación dispuesta en la Ley Orgánica 15/1999, sin que de esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en dicha Ley y demás disposiciones reglamentarias. De conformidad con lo dispuesto en el artículo 58 del citado Reglamento, esta inscripción deberá encontrarse actualizada en todo momento.

Contra esta Resolución, que pone fin a la vía administrativa, podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, de conformidad con lo previsto en el artículo 46.1 del referido texto legal.

Madrid, 28 de Octubre de 2010
EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS



FIRMADO ELECTRÓNICAMENTE por : Agencia Española de Protección de Datos. A fecha : 05/09/2013 19:34:16.
CSV : APDRE93E207680A543B22E98E0-59599
El documento consta de un total de 2 páginas. Página 1 de 2.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

NSTITUT D'INVESTIGACIO SANITARIA PERE VIRGILI (IISPV)
AVDA. UNIVERSIDAD, 1 - CENTRE DE R+D+I EN NUTRICION Y SALUD, 2A PLANTA
43204 REUS
TARRAGONA

Nº Registro Salida: 236958/2013

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, ha acordado en virtud de las competencias que le atribuyen los artículos 60 y 61 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre y el artículo 12.2.a del Real Decreto 428/1993 de 26 de marzo, vigente de conformidad con lo dispuesto en la Disposición Transitoria Tercera de la citada Ley Orgánica 15/1999, proceder a la/s siguiente/s inscripción/es en el Registro General de Protección de Datos correspondiente/s al/los fichero/s en el/los que figura como responsable INSTITUT D'INVESTIGACIO SANITARIA PERE VIRGILI (IISPV):

CÓDIGO INSCRIPCIÓN	NOMBRE FICHERO	OPERACIÓN
2132480037	BIOBANC IISPV - GPM	ALTA

Las inscripciones en el Registro General de Protección de Datos únicamente acreditan que se ha cumplido con la obligación de notificación dispuesta en la Ley Orgánica 15/1999, sin que de esta anotación se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en dicha Ley y demás disposiciones reglamentarias (estas obligaciones se pueden consultar en *www.agpd.es/portalwebAGPD/Deberes.html*). De conformidad con lo dispuesto en el artículo 58 del citado Reglamento, la inscripción del fichero deberá encontrarse actualizada en todo momento.

Contra esta Resolución, que pone fin a la vía administrativa, podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, de conformidad con lo previsto en el artículo 46.1 del referido texto legal.

El Director de la Agencia Española de Protección de Datos,
José Luis Rodríguez Álvarez

C/ Jorge Juan 6
28001 - Madrid

www.agpd.es
sedeagpd.gob.es

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

INSTITUTO DE INVESTIGACION SANITARIA PERE VIRGILI (IISPV)
AVDA. UNIVERSIDAD, 1 - CENTRO DE R+D+I EN NUTRICION Y SALUD, 2A PLANTA
43204 REUS
TARRAGONA

Nº Registro Salida: 193815/2013

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, ha acordado en virtud de las competencias que le atribuyen los artículos 60 y 61 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre y el artículo 12.2.a del Real Decreto 428/1993 de 26 de marzo, vigente de conformidad con lo dispuesto en la Disposición Transitoria Tercera de la citada Ley Orgánica 15/1999, proceder a la/s siguiente/s inscripción/es en el Registro General de Protección de Datos correspondiente/s al/los fichero/s en el/los que figura como responsable DIRECCION INSTITUTO DE INVESTIGACION SANITARIA PERE VIRGILI (IISPV):

CÓDIGO INSCRIPCIÓN	NOMBRE FICHERO	OPERACIÓN
2131901959	BIOBANC IISPV - HUSJR	ALTA

Las inscripciones en el Registro General de Protección de Datos únicamente acreditan que se ha cumplido con la obligación de notificación dispuesta en la Ley Orgánica 15/1999, sin que de esta anotación se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en dicha Ley y demás disposiciones reglamentarias (estas obligaciones se pueden consultar en *www.agpd.es/portalwebAGPD/Deberes.html*). De conformidad con lo dispuesto en el artículo 58 del citado Reglamento, la inscripción del fichero deberá encontrarse actualizada en todo momento.

Contra esta Resolución, que pone fin a la vía administrativa, podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, de conformidad con lo previsto en el artículo 46.1 del referido texto legal.

El Director de la Agencia Española de Protección de Datos,
José Luis Rodríguez Álvarez

FIRMADO ELECTRÓNICAMENTE por : Agencia Española de Protección de Datos. A fecha : 05/07/2013 20:17:20.
CSV : APOREWCCTEHATCB171C86F6EC0-48408
El documento consta de un total de 2 páginas. Página 1 de 2.

C/ Jorge Juan 6
28001 - Madrid
www.agpd.es
sedeagpd.gob.es

I.G. Registro de accesos a los ficheros no automatizados

Solo el personal autorizado, citado en el Anexo I.B. tendrá acceso al archivo no automatizado PROYECTOS Y CONTRATOS R+D+i. Esta base de datos, en soporte de papel, se encuentra en la Fundación URV (Avinguda dels Països Catalans, 43007 Tarragona) en la planta sótano, debidamente custodiada y con las medidas de seguridad adecuadas para su conservación.

Cada Institución dispone de su protocolo de destrucción de ficheros no automatizados, que se encuentran recogidos en cada documento de seguridad correspondiente. En la sede de la oficina IISPV se dispone de una máquina destructora de papel para los ficheros no automatizados.

ANEXO II. NOMBRAMIENTOS

II.A. Nombramientos

FENIX, A3NOM, ATT y PROYECTOS Y CONTRATOS I+D+i

RESPONSABLE DE SEGURIDAD
Dirección IISPV

RESPONSABLE DE FICHEROS
Gerencia IISPV

ENCARGADO DE TRATAMIENTO
Fundació URV

RESPONSABLE DE ATENCIÓN AL AFECTADO
Unidad de Comunicación, Innovación y Gestión de la Calidad

BIOBANC IISPV – GPM y BIOBANC IISPV – HUSJR

RESPONSABLE DE SEGURIDAD
VITRO, SA

RESPONSABLE DE FICHEROS
Dirección IISPV
RESPONSABLE DE FICHEROS
Coordinadora Técnica del Biobanc IISPV – HUSJR – GPM

ENCARGADO DE TRATAMIENTO
VITRO, SA

RESPONSABLE DE ATENCIÓN AL AFECTADO
Biobanc IISPV

BIOBANC HJ23 (NODO HTVC)

RESPONSABLE DE SEGURIDAD
VITRO, SA

RESPONSABLE DE FICHEROS
Dirección IISPV
RESPONSABLE DE FICHEROS
Coordinador Técnico del Biobanc HJ23 (NODO HTVC)

ENCARGADO DE TRATAMIENTO
VITRO, SA

RESPONSABLE DE ATENCIÓN AL AFECTADO
Biobanc IISPV

II.B. Obligaciones de todo el personal del IISPV

Con objeto de dar debido cumplimiento a lo establecido en el Art. 8.2.c del Real Decreto 994/1999, de 11 de junio, el IISPV comunica a su personal el cumplimiento de las siguientes obligaciones, las cuales, tal y como se establece en el Art. 9 del mismo texto legal, han de ser conocidas, aceptadas y respetadas por todo el personal.

- **Identificadores de usuario y contraseña**

Queda prohibido comunicar a otra persona el identificador de usuario y la clave de acceso. Si el usuario sospecha que otra persona conoce su identificador y contraseña deberá cambiar su contraseña para garantizar la confidencialidad de la misma. Ante una baja o ausencia temporal del usuario, el responsable del área de trabajo podrá solicitar, en casos justificados y bajo su responsabilidad, al Responsable del Fichero el cambio de la contraseña de dicho usuario para poder acceder a recursos bajo su propiedad durante su ausencia.

El usuario está obligado a utilizar la red corporativa del IISPV y sus datos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos del IISPV o de terceros, o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas.

Están expresamente prohibidas las siguientes actividades:

- Compartir o facilitar el identificador de usuario y la contraseña para acceder a los sistemas de información del IISPV a otra persona física o jurídica, incluido el personal del propio el IISPV[4]. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada el identificador del usuario.
- Intentar distorsionar o falsear los registros LOG del sistema.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos del IISPV.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios. (Esta actividad puede constituir un delito de interceptación de las telecomunicaciones, previsto en el artículo 197 del Código Penal).
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos del IISPV o de terceros.

[4] Sólo en casos excepcionales se autorizará la cesión de la contraseña a personal técnico para la realización de tareas de mantenimiento, al final de las cuales el usuario deberá cambiar la contraseña. Dicha autorización deberá realizarla el responsable del área al que pertenece el usuario.

– Intentar aumentar el nivel de privilegios de un usuario en el sistema.

- **Utilización de los sistemas informáticos**

Los usuarios de Internet deben esforzarse en hacer y promover un uso eficiente de las redes a fin de evitar tráfico innecesario en la red e interferencias con el trabajo de otros usuarios o con otras redes asociadas ni con los servicios que éstas ofrecen.

En concreto, están expresamente prohibidas las siguientes actividades:

– Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos del IISPV o de terceros. (Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal).

– Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos del IISPV, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.

– Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario (Spam).

– Introducir voluntariamente programas, virus, macros, *applets*, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros. El usuario tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.

– Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por el IISPV, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.

– Instalar copias ilegales de cualquier programa, incluidos los corporativos.

– Borrar cualquiera de los programas instalados legalmente.

– Utilizar los recursos telemáticos del IISPV, incluido el acceso a la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.

– Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para las finalidades propias del IISPV, en la red corporativa del mismo.

– Enviar o reenviar mensajes en cadena o de tipo piramidal.

- **Confidencialidad de la información**

– Queda prohibido enviar información confidencial del IISPV al exterior, mediante soportes materiales, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso[5].

– Los usuarios de los sistemas de información corporativos deberán guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o el IISPV los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral con el IISPV, tanto en soporte material como electrónico. Esta obligación continuará vigente tras la extinción del contrato laboral.

– Ningún colaborador deberá poseer, para usos no propios de su responsabilidad, ningún material o información propiedad del IISPV, tanto ahora como en el futuro.

– En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado entre en posesión de información confidencial bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le otorgue derecho alguno de posesión, o titularidad o copia sobre la referida información. Asimismo, el trabajador deberá devolver dichos materiales al IISPV inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación laboral. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento del IISPV, no supondrá, en ningún caso, una modificación de esta cláusula. El incumplimiento de esta obligación puede constituir un delito de revelación de secretos, previsto en el artículo 197 y siguientes del Código Penal y dará derecho al IISPV a exigir al usuario una indemnización económica.

- **Incidencias**

– Es obligación de todo el personal del IISPV comunicar al responsable del sistema cualquier incidencia que se produzca en los sistemas de información a que tengan acceso. El procedimiento de comunicación de incidencias se encuentra relacionado en el Anexo VI.

– Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.

[5] Esta prohibición no se aplicará al envío de información confidencial a empresas o profesionales subcontratados, siempre que en los contratos establecidos con dichas terceras empresas se contemple lo establecido en el artículo 12 de la Ley de Protección de Datos de Carácter Personal.

Protección de datos

- La creación, modificación o supresión de los ficheros automatizados que contengan datos de carácter personal deberá notificarse a la Agencia de Protección de Datos. Asimismo, se notificará cualquier cambio que afecte a la finalidad del fichero, a su responsable o a la ubicación del mismo.
- El IISPV notificará a las personas sobre las cuales se recaben datos y en el momento de recabar dichos datos:
  - Existencia del fichero.
  - Finalidad de la recogida de datos.
  - Destinatarios de la información.
  - Posibilidad para el cliente de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
  - Identidad y dirección del Responsable del Fichero.
  - Consecuencias de no suministrar la información requerida y el carácter obligatorio o no de las respuestas a las preguntas realizadas.
- La recogida de datos sensibles que afecten a ideología, afiliación sindical, religión y creencias, origen racial, salud y vida sexual requerirá el consentimiento expreso y por escrito de los afectados a quienes se les ha solicitado dichos datos.
- Se realizarán las cesiones o comunicaciones de datos de carácter personal de acuerdo con los siguientes requisitos:
  - Con consentimiento previo del cliente.
  - Cumpliendo fines directamente relacionados con las funciones legítimas del IISPV y de sus cesionarios.
- No será necesario recabar dicho consentimiento:
  - Cuando la cesión está autorizada por Ley.
  - Cuando se trate de datos recogidos de una fuente accesible al público (repertorios telefónicos, censo promocional, diarios y boletines oficiales, medios de comunicación y listas de grupos profesionales).
  - Cuando el tratamiento responda a una relación jurídica cuyo cumplimiento y control implique la conexión con ficheros de terceros.
- Se consideran actos prohibidos:
  - Crear ficheros de datos personales sin la correspondiente notificación previa a la

Agencia de Protección de Datos.

- Utilizar los datos personales para finalidades incompatibles con aquellas para las que los datos hubieran sido recabados o para finalidades distintas a las comunicadas a la Agencia de Protección de Datos.
- Cruzar información relativa a datos de diferentes ficheros o servicios con el fin de establecer perfiles de personalidad, hábitos de consumo o cualquier otro tipo de preferencias, sin la autorización expresa del Responsable del Fichero, así como del afectado en el caso de encontrarnos en alguno de los supuestos establecidos en el apartado 3 anterior.
- Cualquier otra actividad expresamente prohibida en este documento o en las normas sobre protección de datos e Instrucciones de la Agencia de Protección de Datos.

II.C. Consecuencias en caso de incumplimiento

El incumplimiento de las obligaciones anteriormente expuestas tendrá la consideración de falta sancionable de acuerdo con la normativa laboral, independientemente de las responsabilidades civiles y penales que pudieran ser exigidas.

II.D. Recibí del acceso al Documento de Seguridad IISPV

IISPV INSTITUT D'INVESTIGACIÓ SANITÀRIA PERE VIRGILI

Rebut documentació

En / Na. .....

Mitjançant la signatura del present document faig constar que he rebut:

☐ L'original del meu contracte com a personal laboral que he subscrit amb l'IISPV.
☐ El Manual d'Acollida de l'IISPV.
☐ Accés al Document de Seguretat de l'IISPV (LOPD).
☐ Accés a la Intranet de l'IISPV.

Aquesta documentació és per a la meva lectura i coneixement, a fi de tenir presents les normes de funcionament, les quals hem comprometo a complir i respectar com a treballador de l'IISPV.

Reus / Tarragona, de de 200

Signatura:

(RETORNAR SIGNAT CONFORME HA REBUT ELS DOCUMENTS CITATS)

IISPV INSTITUT D'INVESTIGACIÓ SANITÀRIA PERE VIRGILI

(ES LLIURARÀ I ELS TREBALLADROS EL SIGNARAN, QUAN ES FACILITI L'ACCÉS AL DOCUMENT DE SEGURETAT,)

Nom i Cognoms del treballador

Mitjançant la signatura del present document, es manifesta que l'Institut d'Investigació Sanitària Pere Virgili (IISPV) ha posat a la meva disposició el "Documento de Seguridad de datos de carácter personal" aplicable, per a la meva lectura i coneixement, a fi de conèixer les normes de Seguretat de l'IISPV, i especialment, les funcions i obligacions que com usuari dels equips informàtics de l'ISIPV i que m'apliquen en relació amb el tractament de dades de caràcter personal, les quals em comprometo a complir i respectar.

Signatura

II.E. Modelo de documento de confidencialidad

CONFIDENCIALITAT DE LA INFORMACIÓ I LLEI ORGÀNICA DE PROTECCIÓ DE DADES

En / Na en qualitat de treballadora de l'Institut d'Investigació Sanitària Pere Virgili (IISPV),

MANIFESTA:

- Que coneix que la informació i les dades a les que té accés com a conseqüència de la seva feina a l'IISPV té un caràcter confidencial i, com a tal, està subjecta al que es disposa en la legislació vigent en matèria de protecció de dades.
- Que es compromet a mantenir la confidencialitat de la informació i de les dades a les quals tingui i/o hagi tingut accés durant l'execució de la seva feina.
- Que, una vegada utilitzada aquesta informació i/o dades per a la feina que té encomanada, ha de ser íntegrament emmagatzemada a les bases de dades de l'IISPV i/o destruïda i que, en cap cas, es pot utilitzar per a cap altre fi que no sigui relacionat directament amb la feina que li pertoca fer a l'IISPV.
- Que, pel que fa a les dades de caràcter personal corresponents al propi treballador/a, coneix i autoritza que la informació que ha proporcionat, en relació a la seva persona, i les que es vagi'n incorporant mentre duri la seva relació laboral amb l'empresa, estigui emmagatzemada en bases de dades propietat del propi IISPV, amb domicili social al carrer de l'Escorxador, s/n, 43007 de Tarragona.
- Que, d'acord al que s'estableix en la Llei Orgànica 15/1999 de Protecció de Dades de Caràcter Personal, el treballador/a ha estat informat i autoritza de que les seves dades personals estan sent tractades de manera automatitzada pel Servei de Recursos Humans de l'IISPV amb la finalitat de portar a terme l'adequat desenvolupament, compliment, gestió, control de la relació laboral existent en l'actualitat, així com per a altres serveis relacionats amb la seva carrera professional
- Finalment, que s'ha posat en el seu coneixement el seu dret d'accés, rectificació, oposició i, en cas de finalitzar la relació laboral, cancel·lació de les seves dades personals, que podrà exercitar mitjançant sol·licitud escrita dirigida al Servei de Recursos Humans de l'IISPV, que pot exercitar a través de la següent adreça electrònica: qualitat.iispv@iispv.cat

Data: 4 / març / 2015

ANEXO III. AUTORIZACIONES DE SALIDA O RECUPERACIÓN DE DATOS

Procedimiento de realización de copias de respaldo y recuperación de datos

Es el Encargado de Tratamiento quien tiene establecido el procedimiento de realización de las copias de respaldo y recuperación de datos, mediante lo establecido los contratos firmados. Todo ello queda reflejado en el Documento de Seguridad del Encargado de Tratamiento.

Copias de respaldo y recuperación:

En el caso de petición de copias de seguridad o recuperación de los datos a los servidores corporativos, esta vendrá solicitada por el Responsable de Seguridad del IISPV (formulario de solicitud de recuperación de datos, disponible en la intranet del IISPV), el cual realizará una petición escrita (por correo electrónico, vía formulario web) al Encargado de Tratamiento. La petición será revisada y tramitada al Responsable de Fichero y/o Responsable de Seguridad del IISPV, el cual indicará su aprobación o denegación, teniendo presente y garantizando la reconstrucción de los datos al estado en que se encontraban al tiempo de perderse o destrucción de las mismos. La respuesta por parte del Encargado de Tratamiento se hará llegar al solicitante y a la misma vez a los técnicos de seguridad.

En este mismo procedimiento también se contempla el correcto inventariado y etiquetado con los siguientes identificadores: de soporte y de registro.

Estos identificadores proporcionan el acceso al registro dónde se guardan: usuario, fecha, hora, procedencia de los datos y el nivel de las mismas, indicando si ha sido un proceso de copia o restauración.

Proceso de restauración de datos:

En el caso que se realice un proceso de restauración de las copias, se ha de notificar al Responsable de Seguridad del IISPV y éste al Responsable del Fichero y éste a los técnicos del Encargado de Tratamiento, haciendo constar los siguientes campos:

- Operador
- Datos Restaurados (datos, ubicación, servidor/sistema)
- Hora y Fecha
- Solicitante
- Identificador de soporte
- Status del proceso

Recordar que todo este proceso solo se podrá realizar en el caso de que el Responsable de Fichero del IISPV lo autorice, mediante el formulario correspondiente de Restauración de Datos.

Sistema de backup:

Las copias de seguridad que el Encargado de Tratamiento realiza mediante Servicio de Recursos Informáticos y TIC de la URV (Convenio de *Hosting y Hausing* firmado entre estas dos entidades subcontratando esta primera el servicio) realiza utilizando el sistema de Backup centralizado, en el que se recopilan los siguientes parámetros:

CLASE:	Grupo de máquinas con la misma política de backup.
PROGRAMACIÓN:	Cada cuanto se hace el backup por clase.
ACTIVO:	Especifica si se hace el backup para una clase.
CUA:	Se indica el conjunto de cintas que se utilizan.
FRECUENCIA:	Cada cuanto se hace el backup de aquella clase.
RETENCIÓN:	Tiempo que se guardan las cintas.
INCLUSIONES:	Los directorios que se hace el backup.
EXCLUSIONES:	Los directorios que no se hace el backup.
DÍA:	Día de la semana que se hace le backup.

Backup normal: 4 veces al mes, retención de 6 meses.

Backup históricos: 2 veces al año, retención de 5 años.

La política de realización de copias de seguridad, incluye un servicio de salvaguarda de cintas en una ubicación remota segura, para aquellos ficheros que lo requieran.

El Responsable de Seguridad y de los Ficheros será el encargado de que el inventario de copias de respaldo y recuperación permanezca correctamente actualizado.

Modelo de autorización de salida de los soportes físicos

AUTORIZACIÓN DE SALIDA DE SOPORTES	
Fecha de salida del soporte	

SOPORTE	
Identificación	
Contenido	
Ficheros de donde proceden los datos	
Fecha de creación	

FINALIDAD Y DESTINO	
Finalidad	
Destino	
Destinatario	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN	
Persona que autoriza	
Cargo / Puesto	
Observaciones	
Firma	

Modelo de solicitud de recuperación de datos

DATOS DE REGISTRO:

Nº de SOLICITUD:	*(Debe ser rellenado por el Responsable Técnico)*		
Fecha de la solicitud:		**Hora de la solicitud:**	

Datos restaurados	
Fichero objeto de la copia	
Identificación soporte:	
Datos:	
Ubicación:	
Servidor / sistmea:	
Operador:	
Identificación soporte:	
Satus del proceso:	

INFORMACIÓN SOBRE LA COMUNICACIÓN:

Persona(s) que realiza la petición:	
Persona(s) a quien(es) se comunica:	
APROBACIÓN ☐	**DENEGACIÓN** ☐

Persona que realiza la petición:

Fdo.:

ANEXO IV. DELEGACIONES DE AUTORIZACIONES

En este anexo se describe el sistema utilizado por el Encargado de Tratamiento del IISPV para limitar el acceso a los diferentes sistemas y áreas de los mismos en función de los privilegios de cada usuario.

El Responsable de Seguridad y de los Ficheros del IISPV elaborará, custodiará y actualizará una **relación actualizada de los usuarios** que tengan acceso autorizado al sistema de información.

Control de acceso al sistema: Es realizado por el procedimiento que el Encargado de Tratamiento tiene establecido en su Documento de Seguridad.

Control de acceso a los datos: Cada identificador de usuario tendrá unos privilegios asociados, en función de los cuales podrá acceder únicamente a aquellos datos y recursos que precise para el desarrollo de sus funciones. Dichos privilegios irán en función de la tipología de usuario, definida en el Anexo I.B.

ANEXO V. INVENTARIOS DE SOPORTES

Descripción del procedimiento utilizado para la gestión de soportes informáticos

Es el Encargado de Tratamiento quien describe el procedimiento utilizado para identificar, inventariar y almacenar en un lugar con acceso restringido, los soportes informáticos que contienen datos de carácter personal y queda recogido en su Documento de Seguridad.

Los soportes que alberguen datos personales serán etiquetados e identificados de forma diferenciada, con el fin de distinguirlos de los demás soportes.

El acceso a la ubicación donde se almacenan los soportes que contengan datos de carácter personal y la salida de los mismos, estará restringido al personal autorizado, según el Anexo I.B.

Inventario:

El Responsable de Seguridad y el Responsable de Ficheros del IISPV, conjuntamente con el Encargado de Tratamiento, llevarán una relación detallada de la entrada y salida de los soportes que contengan datos personales y permita conocer directa o indirectamente:

- Motivo de la salida
- El tipo de soporte
- Fecha y hora de entrada o salida
- Emisor
- Número de soporte
- Tipo de información que contienen
- Forma de envío
- Persona responsable de la recepción

Almacenamiento:

Los únicos soportes homologados para albergar datos de carácter personal en el IISPV, son los siguientes:

- Disco duro del servidor en el que se encuentra el fichero maestro (soporte permanente).
- Soportes homologados por el IISPV para realizar copias de respaldo y recuperación.
- Soportes homologados por el IISPV para realizar cesiones autorizadas a otras empresas o entidades.

Distribución de soportes:

La persona solicitante de un soporte con datos de carácter personal deberá seguir el siguiente procedimiento:

a. Solicitará por escrito, al Responsable de Seguridad del IISPV, (correo electrónico) mediante el formulario de petición de copias de seguridad y de restauración de datos (Anexo III) disponible en la Intranet del IISPV.
b. El Responsable de Fichero solicitará al Responsable de Seguridad la autorización para poder realizar la acción solicitada.
c. En caso que el Responsable de Fichero desestime la petición, el Responsable de Seguridad así lo notificará al solicitante, indicando la imposibilidad de poder realizar la acción.
d. En caso afirmativo, el Responsable de Seguridad del IISPV lo indicará al Encargado de Tratamiento.
e. Así mismo, el Responsable de Seguridad hará el inventario (Formulario - Inventario de Soportes) y etiquetaje de la copia realizada.

Modelo de inventario de soportes

MODELO DE INVENTARIO DE SOPORTES

Fichero:					
ALTAS		**BAJAS**			
Núm. de orden	**Fecha de copia**	**Motivo**			**Fecha**
		Reutilización	**Destrucción**	**Otros**	
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /
/	/ /				/ /

ANNEXO VI. REGISTRO DE INCIDENCIAS

En este anexo se describe el sistema utilizado por el IISPV y por el Encargado de Tratamiento para la notificación, gestión y respuesta ante las incidencias, en función de la ubicación física de los ficheros notificados a la AGPD.

El IISPV dispone de equipos informáticos, en los que el *hardware* y el *software* están gestionados por el Encargado de Tratamiento.

Procedimiento de Notificación y gestión de incidencias (Ficheros FÉNIX y A3NOM)

Estos ficheros están ubicados físicamente en las instalaciones de la URV (servicio de hosting y housing contratado por el Encargado de Tratamiento). El IISPV, mediante la petición de servicios al Encargado de Tratamiento solicita el control administrativo para la resolución de incidencia por parte de los técnicos autorizados.

Notificación:

Cualquier persona que forme parte de la plantilla del IISPV o se halle prestando sus servicios temporalmente en la misma deberá notificar inmediatamente al Responsable de Fichero cualquier anomalía que detecte y que afecte o pueda afectar a la seguridad de los datos, mediante el formulario de comunicación de incidencias de seguridad disponible en la intranet del IISPV.

Gestión:

El Encargado de Tratamiento recibirá las notificaciones, dicha comunicaron será en forma escrita (correo electrónico).

Respuesta:

El Encargado de Tratamiento se asegurará de dar respuesta a la incidencia detectada en el periodo de tiempo dispuesto para ello. Además supervisará el trabajo de subsanación de la anomalía detectada.

Registro:

El Encargado de Tratamiento, de conformidad con el art. 10 del Real Decreto 994/1999, mantiene un registro de las incidencias en el cual se hace constar la siguiente información relativa a las incidencias en el formulario de comunicación de incidencias de seguridad LOPD:

- Tipo de incidencia.
- Momento en el cual se ha producido la incidencia.
- Persona que realiza la notificación (solicitante).
- Descripción y análisis detallado de la incidencia.

- Solución de la incidencia.
- Información sobre la comunicación de la incidencia.

Es obligación del Responsable del Fichero es asegurarse de que el registro de incidencias se mantiene actualizado.

Consulta y control del Registro de Incidencias:

El control de las incidencias se realizará de una forma periódica, en un plazo no superior a 2 meses des de la última revisión.

El Encargado de Tratamiento hará el seguimiento del Registro de Incidencias a fin de poder detectar las incidencias repetitivas de carácter no grave.

También se revisarán las incidencias que hasta el momento estén abiertas y se comprobará el porqué de esta circunstancia.

Las conclusiones de estas revisiones, si se consideran graves, serán notificadas al Responsable de Fichero.

Modelo de formulario de comunicación de incidencias de seguridad LOPD

MODELO DE INVENTARIO DE SOPORTES

INCIDENCIA Núm.:	*(Rellenado por el Encargado de Tratamiento)*
Fichero objeto de la incidencia:	
Fecha de notificación:	

Información sobre la incidencia:

Tipo de Incicencia:	*(Anotar todos los detalles de interés de la incidencia)*		
Descripción detallada de la incidencia:			
Fecha de la incidencia:		Hora de la incidencia:	
Solución de la incidencia:			
Tiempo de resolución:			

Información sobre la comunicación:

Persona(s) que realiza la comunicación:	
Persona(s) a quien(es) se comunica:	

Persona que realiza la comuniación:

Fdo.:

ANEXO VII. ENCARGADOS DE TRATAMIENTO

Definición: el Encargado del Tratamiento se dará cuando hay el acceso de un tercero a los datos, cuando sea necesario para la prestación de un servicio y no se considera que exista comunicación de datos. En este caso, el encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal.

En el presente anexo se recoge la adenda al Contrato entre la URV, FURV e IISPV, para la prestación de servicios informáticos y protección de datos de carácter personal, en este consta por escrito que el IISPV autoriza a la FURV a ser el Encargado de Tratamiento.

El Encargado de Tratamiento ha redactado el Documento de Seguridad FURV, en el que figuran todos los procedimientos que permiten acreditar que tratará los datos conforme a las instrucciones del Responsable de Seguridad y Fichero del IISPV según las medidas de seguridad a que se refiere el artículo 9 de la LOPD.

En caso de que una empresa, sea autorizada por parte del IISPV a realizar una prestación de servicios, se firmará un acuerdo de confidencialidad y tratamiento de los datos de carácter personal. En el documento se deben recoger los siguientes aspectos:

I. *ACUERDAN*

Que ambas partas, a los efectos de cumplimiento con la obligación recogida en el artículo 12.2. de la Ley Orgánica 15/01, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) y en el artículo 20 del Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal (en adelante RLOPD), declaran y manifiestan que están interesada en la celebración de un acuerdo en virtud del cual se regule el régimen y naturaleza del tratamiento de Datos de Carácter Personal que se realiza como consecuencia de la Protección de Servicios acordada entre ambas partes.

….

II. *OBJETO*

El objeto del presente acuerdo es establecer el deber de confidencialidad que debe mantener en su calidad de Encargado de Tratamiento de Datos de Carácter Personal.

III. *CONFIDENCIALIDAD*

La EMPRESA reconoce que la legislación sobre protección de datos personales establece una serie de obligaciones en el tratamiento de datos de carácter personal aplicables a los encargados del tratamiento. A tal efecto, EMPRESA:

a) Únicamente accederá a los datos personales de personas físicas relacionadas con EMPRESA si tal acceso fuese necesario para cumplir con las obligaciones establecidas para EMPRESA en el presente contrato.

b) Se compromete a:

Utilizar los datos de carácter personal a los que tenga acceso único y exclusivamente para cumplir con sus obligaciones contractuales para con EMPRESA.

Implantar, en los sistemas informáticos que alberguen dichos datos, las medidas de seguridad definidas por el RD 994/1999 como de nivel Alto.

A no ceder en ningún caso a terceras personas los datos de carácter personal a los que tenga acceso, ni tan siquiera a efectos de su conservación. En cualquier caso, si EMPRESA precisase subcontratar con terceras empresas la totalidad o parte de los servicios objeto del presente contrato, o debiese facilitar a terceros proveedores acceso a los datos personales objeto del presente contrato, EMPRESA estará autorizada a actuar en nombre de EMPRESA a tal efecto, a condición de que dichos subcontratistas o terceros proveedores se comprometan ante EMPRESA, expresamente y por escrito, a asumir obligaciones idénticas a las establecidas para EMPRESA en virtud del presente contrato.

Una vez terminada la vigencia del presente contrato, los datos de carácter personal deberán ser destruidos por EMPRESA o devueltos a EMPRESA, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

Las obligaciones establecidas para EMPRESA en la presente cláusula serán también de obligado cumplimiento para sus empleados, colaboradores, tanto externos como internos, y subcontratistas, por lo que EMPRESA responderá frente a EMPRESA si tales obligaciones son incumplidas por tales empleados, colaboradores y subcontratistas.

El incumplimiento por parte del PROVEEDOR de cualesquiera de las obligaciones de establecidas en el presente compromiso, generará en favor de EMPRESA la facultad de iniciar cuantas acciones legales estime oportunas para el resarcimiento de los daños causados.

Las obligaciones de confidencialidad establecidas en el presente contrato tendrán una duración indefinida, manteniéndose en vigor con posterioridad a la finalización, por cualquier causa, de la relación entre las EMPRESAS.

IV. *PRINCIPIO DE INFORMACIÓN A TERCEROS*

La EMPRESA informará a su personal, colaboradores y subcontratistas de las obligaciones establecidas en el presente contrato sobre confidencialidad, así como de las obligaciones relativas al tratamiento de datos de carácter personal. EMPRESA realizará

cuantas advertencias y suscribirá cuantos documentos sean necesarios con su personal y colaboradores, con el fin de asegurar el cumplimiento de tales obligaciones.

V. *FINALIDAD DE LOS DATOS*

VI. *MEDIDAS DE SEGURIDAD*

LA *EMPRESA* se compromete, tras la extinción del presente contrato, a no conservar copia alguna de Información Confidencial.

VII. *PRINCIPIO DE NO CESIÓN DE DATOS*

VIII.*EJERCICIO DE DERECHOS POR EL INTERESADO*

IX. *INCUMPLIMIENTO*

X. *AUDITORIA*

XI. *DURACIÓN*

ANEXO VIII. REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

Modelo de registro de entrada de los soportes

REGISTRO DE ENTRADA DE SOPORTES	
Fecha y hora de entrada de soporte	

SOPORTE	
Tipo de soporte y número	
Contenido	
Fecha de creación	

ORIGEN Y FINALIDAD	
Finalidad	
Origen	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN	
Persona responsable de la recepción	
Cargo / Puesto	
Observaciones	
Firma	

Modelo de registro de salida de los soportes

REGISTRO DE ENTRADA DE SOPORTES	
Fecha y hora de entrada de soporte	

SOPORTE	
Tipo de soporte y número	
Contenido	
Fecha de creación	

ORIGEN Y FINALIDAD	
Finalidad	
Origen	

FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN	
Persona responsable de la recepción	
Cargo / Puesto	
Observaciones	
Firma	

ANEXO IX. MEDIDAS ALTERNATIVAS

No aplica.

CAPÍTULO: COMPROBACIONES PARA LA REALIZACIÓN DE LA AUDITORÍA DE SEGURIDAD [6]

Objetivo:

Determinar si se han establecido, si son adecuadas y si se cumplen las medidas de seguridad recogidas en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Su realización es obligatoria para ficheros de nivel medio y alto. Puede ser interna o externa. Debe realizarse al menos cada dos años. Excepcionalmente, si se han realizado modificaciones sustanciales en el sistema de información, deberá realizarse una auditoría para comprobar la adecuación, adaptación y eficacia de las medidas de seguridad. Esta auditoría iniciará el cómputo de dos años.

Determinación del alcance de la auditoría:

Se debe establecer cuáles son los ficheros con datos de carácter personal objeto de la auditoría, tratamientos sobre los mismos, sistemas de tratamiento, procedimientos, etc.

Planificación:

Determinar los recursos necesarios para llevar a cabo la auditoría, las fuentes de información, la ubicación del fichero o las instalaciones, etc.

Recolección de datos:

- Relación de ficheros, estructura y contenido.
- Políticas de seguridad y procedimientos (registro de incidencias, copias de respaldo y recuperación, Identificación y autorización, borrado de soportes, cifrado, etc.).
- Documento de Seguridad y auditorías anteriores (si las hubiese).
- Diseño físico y lógico de los sistemas de información.
- Relación de usuarios, accesos autorizados y sus funciones.
- Inventario de soportes y registro de entrada y salida de soportes.
- Registros de acceso e informes de revisión de los mismos.
- Entrevistas a usuarios, técnicos de sistemas, responsables, etc.

[6] Esta guía de ayuda se podrá utilizar con el fin de facilitar las revisiones periódicas de seguridad en la empresa, y de verificar el cumplimiento de los controles establecidos por el Reglamento de Seguridad. No es, por tanto, obligatoria la utilización de dicha guía por el responsable de seguridad, ya que puede utilizar otros medios para verificar el cumplimiento de estos controles, de obligada aplicación para los ficheros de nivel medio y alto.

- Inspección visual.
- etc.

Evaluación de las pruebas:

Se relacionan a continuación algunas comprobaciones que se pueden realizar para verificar el cumplimiento de las disposiciones del Reglamento:

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	ASPECTOS GENERALES	
TODOS	¿La clasificación del nivel de seguridad es adecuada respecto a la naturaleza de la información contenida en cada uno de los ficheros y su finalidad?	BÁSICO
	¿Se han creado, modificado o suprimido ficheros con datos de carácter personal desde la última auditoría?	
	ENCARGADO DE TRATAMIENTO	
TODOS	¿Se realiza el tratamiento por persona distinta al responsable del fichero?, ¿se ha formalizado mediante contrato conforme lo establecido el artículo 12 de la LOPD?	BÁSICO
	Si la realización de este encargo se realiza en los locales del responsable ¿se ha hecho constar esta circunstancia en el Documento de Seguridad?, ¿consta por escrito en el contrato el compromiso del personal del encargado de tratamiento respecto al cumplimiento de las medidas de seguridad recogidas en el Documento de Seguridad del responsable?	
	Cuando el tratamiento se realiza mediante acceso remoto a los sistemas del responsable ¿se le ha prohibido al encargado de tratamiento la incorporación de los datos a sistemas o soportes distintos de los del responsable?, ¿se ha hecho constar tal circunstancia en el Documento de Seguridad del responsable?	
	Si la prestación se hace en locales propios del encargado de tratamiento (distintos de los del responsable) ¿ha elaborado el encargado el documento de seguridad?, ¿identifica el fichero o tratamiento y el responsable del mismo?, ¿detalla las medidas de seguridad a implementar en relación con su tratamiento?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
PRESTACIÓN DE SERVICIO SIN ACCESO A DATOS PERSONALES		
TODOS	Si el tratamiento no afecta a datos personales ¿se han adoptado las medidas necesarias para limitar el acceso del personal a los datos personales, soportes y recursos?	BÁSICO
	Si se trata de personal ajeno ¿recoge el contrato la prohibición expresa de acceder a los datos personales, así como la obligación de secreto respecto a los datos que hubieran podido conocer con motivo de la prestación de servicio?	
DELEGACIÓN DE AUTORIZACIONES		
TODOS	¿Se han delegado las autorizaciones que el Reglamento atribuye al responsable en otras personas?, ¿se ha hecho constar en el Documento de Seguridad las personas habilitadas para otorgar estas autorizaciones y las personas en quienes recae dicha delegación?	BÁSICO
RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO		
TODOS	El almacenamiento de datos personales en dispositivos portátiles o los tratamientos fuera de los locales del responsable o del encargado ¿han sido autorizados expresamente por el responsable del fichero?, ¿consta dicha autorización en el Documento de Seguridad?	BÁSICO
	¿Se garantiza el nivel de seguridad correspondiente al tipo de fichero tratado?	
FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS		
TODOS	¿Cumplen el nivel de seguridad correspondiente?	BÁSICO
	¿Se han destruido o borrado cuando ya no han sido necesarios para los fines que motivaron su creación?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
FUNCIONES Y OBLIGACIONES DEL PERSONAL		
TODOS	Están las funciones y obligaciones del personal con acceso a datos de carácter personal y los sistemas de información claramente definidos?	BÁSICO
	¿Están documentadas y reflejadas en el documento de seguridad?	
	¿Se han definido las funciones de control o autorizaciones delegadas por el responsable del fichero?	
	¿Conoce el personal las medidas de seguridad que afectan al desarrollo de sus funciones?	
	¿Conoce las consecuencias de su incumplimiento?	
REGISTRO DE INCIDENCIAS		
TODOS	¿Existe un procedimiento de notificación y gestión de incidencias de seguridad?, ¿el procedimiento está bien diseñado y es eficaz? ¿Conoce todo el personal afectado dicho procedimiento?	BÁSICO
	¿Existe un registro de incidencias donde se reflejen todos los datos exigidos en el Reglamento?, ¿se han registrado todas las incidencias ocurridas?	
	¿Se revisa periódicamente el registro de incidencias para su análisis y adopción de medidas correctoras de las incidencias anotadas?	
AUTOMATIZADO	¿Se han anotado las ejecuciones de los procedimientos de recuperación de datos realizados?	
	¿Figuran en estas anotaciones los datos exigidos por el Reglamento?	MEDIO
	¿Existe la autorización por escrito del responsable del fichero?	
CONTROL DE ACCESO		
TODOS	¿Los accesos autorizados de los usuarios se corresponden exclusivamente a los datos y recursos que precisan para el desarrollo de sus funciones?	BÁSICO
	¿Existen mecanismos que impidan que los usuarios accedan a datos o recursos distintos de los autorizados?	
	¿Existe una relación de usuarios?, ¿especifica qué datos y recursos tiene autorizados para cada uno de ellos? ¿Está actualizada?	
	¿La concesión, alteración o anulación de accesos autorizados sobre datos y recursos la realiza exclusivamente el personal autorizado para ello en el Documento de Seguridad?	
	¿Ha establecido el responsable del fichero los criterios conforme a los cuales se otorga la autorización de los accesos a los datos y a los recursos?	
	El personal ajeno al responsable que tiene acceso a los datos y recursos de éste ¿se encuentra sometido a las mismas condiciones y obligaciones que el personal propio?	
AUTOMATIZADO	¿El acceso a los locales donde se encuentran ubicados los sistemas de información se realiza exclusivamente por el personal autorizado en el Documento de Seguridad?	MEDIO

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	DOCUMENTO DE SEGURIDAD	
TODOS	¿Ha elaborado el responsable del fichero el Documento de Seguridad?	BÁSICO
	¿Contiene los aspectos mínimos exigidos por el Reglamento?	
	¿Está el documento actualizado?, ¿se ha revisado cuando se han producido cambios relevantes desde la auditoría anterior?	
	¿Está su contenido adecuado a la normativa vigente en este momento en materia de seguridad de los datos de carácter personal?	
	¿Se ha indicado con qué periodicidad se deben cambiar las contraseñas?, ¿es inferior o igual a un año?	
	¿Se especifica cuál es el personal autorizado para la concesión, alteración o anulación de accesos autorizados sobre datos o recursos?	
	¿Se especifica cuál es el personal autorizado para acceder a los lugares donde se almacenan los soportes informáticos?	
	Si el tratamiento se realiza por cuenta de terceros ¿se han reflejado los ficheros afectados por el encargo, con referencia expresa al contrato, así como la identificación del responsable y el periodo de vigencia?	
	¿Se ha reflejado en el Documento de Seguridad si los datos personales se incorporan y tratan exclusivamente en los sistemas del encargado?	
	¿Se ha delegado en el encargado del tratamiento la llevanza del Documento de Seguridad para los ficheros objeto del contrato?, ¿se ha reflejado esta circunstancia en el contrato?	
	¿Establece la identidad del responsable o responsables de seguridad?, ¿se especifica si la designación es única para todos los ficheros o está diferenciada según el sistema de tratamiento utilizado?	MEDIO
	¿Contiene los procedimientos y controles periódicos a realizar para verificar el cumplimento de lo dispuesto en el propio documento?	
	¿Especifica qué medidas hay que adoptar en caso de desechado o reutilización de soportes?	
	¿Relaciona las personas que están autorizadas a acceder físicamente a los locales donde se ubican los sistemas de información?	

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	GESTION DE SOPORTES Y DOCUMENTOS	
TODOS	¿Está identificado el tipo de información contenido en el soporte o documento?	BÁSICO
	¿Existe y se mantiene un inventario de soportes?	
	¿Se almacenan los soportes o documentos en lugares de acceso restringido?	
	¿Existen mecanismos por los que solamente puedan acceder las personas autorizadas en el Documento de Seguridad?, ¿funcionan adecuadamente estos mecanismos?	
	¿Se ha dejado constancia en el Documento de Seguridad, si fuera el caso, de la imposibilidad de cumplir con las obligaciones establecidas en el Reglamento sobre identificación, inventariado y acceso a los soportes dadas sus características físicas?	
	¿La salida de soportes y documentos fuera de los locales donde se ubica el fichero está siendo autorizada por el responsable del fichero o está debidamente autorizada en el Documento de Seguridad?	
	¿Se están tomando las medidas adecuadas en el traslado de documentación para evitar la sustracción, perdida o acceso indebido durante su transporte?	
	Cuando se desecha un soporte o documento conteniendo datos de carácter personal ¿se adoptan las medidas adecuadas para evitar el acceso a la información o su recuperación posterior cuando se procede a su destrucción o borrado?, ¿son adecuadas estas medidas?	
	¿Se dan de baja en el inventario estos soportes o documentos desechados?	
	Para los soportes con datos de carácter personal considerados especialmente sensibles por la organización ¿se utilizan sistemas de etiquetado que permitan la identificación de su contenido a las personas autorizadas y dificulten su identificación al resto?, ¿son adecuados y cumplen su finalidad?	
	¿Existe un registro de entrada de soportes o documentos?, ¿y un registro de salida?	MEDIO
	¿Contienen estos registros de entrada y salida de soportes toda la información exigida en el Reglamento?	
	¿Las personas encargadas de la recepción y la entrega de soportes están debidamente autorizadas?, ¿Consta en el Documento de Seguridad dicha autorización?	
	¿Se han anotado todas las entradas y salidas de soportes?	
	IDENTIFICACIÓN Y AUTENTICACIÓN	
AUTOMATIZADO	¿Existe una relación de usuarios con acceso autorizado?, ¿se mantiene actualizada?	BÁSICO
	¿Existen procedimientos de identificación y autenticación para dicho acceso?, ¿garantiza la correcta identificación del usuario?	
	El mecanismo de acceso y verificación de autorización de los usuarios ¿les identifica de forma inequívoca y personalizada?	
	¿Existe un procedimiento de asignación, distribución y almacenamiento de contraseñas?, ¿garantiza su confidencialidad e integridad?	
	¿Se cambian las contraseñas con la periodicidad establecida en el documento de seguridad?	
	¿Se almacenan las contraseñas de forma ininteligible mientras están en vigor?	
	¿Se limita el intento reiterado de acceso no autorizado al sistema?, ¿se anotan estos intentos en el registro de incidencias?	MEDIO

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
COPIAS DE RESPALDO Y RECUPERACIÓN		
AUTOMATIZADO	¿El responsable del fichero ha definido los procedimientos de realización de copias de respaldo y recuperación de los datos?, ¿es adecuada esta definición?	BÁSICO
	¿Están reflejados estos procedimientos en el Documento de Seguridad?	
	¿Ha verificado el responsable del fichero la correcta aplicación de estos procedimientos?, ¿realiza esta verificación cada seis meses?	
	¿Garantizan los procedimientos establecidos la reconstrucción de los datos al estado en que se encontraban antes de producirse la pérdida o destrucción?	
	Si esta pérdida o destrucción afecta a ficheros parcialmente automatizados ¿se ha procedido a grabar manualmente los datos?, ¿queda constancia motivada de este hecho en el Documento de Seguridad?	
	¿Se realizan copias de respaldo al menos semanalmente? Si no es así ¿se debe a que no ha habido actualizaciones en ese periodo?	
	¿Las pruebas previas a la implantación o modificación de los sistemas de información se realizan con datos reales? En caso afirmativo, ¿se están aplicando las mismas medidas de seguridad que las que le corresponde por la naturaleza de los datos que contiene?, ¿se anota su realización en el Documento de Seguridad?, ¿se hacen copias de seguridad previas a la realización de pruebas con datos reales?	
	¿Se conserva una copia de respaldo y de los procedimientos de recuperación de datos en lugar diferente al de los equipos que los tratan?	ALTO
	¿Cumple este lugar las medidas de seguridad exigidas en el Reglamento?	
ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES		
AUTOMATIZADO	¿Los accesos a datos mediante redes de comunicaciones garantizan un nivel de seguridad equivalente a los accesos en modo local?	BÁSICO
AUTOMATIZADO	¿La transmisión de datos a través de redes se realiza de forma cifrada (o por cualquier otro mecanismos que garantice que la información no sea inteligible ni manipulada por terceros)?, ¿este mecanismo de cifrado es eficaz?	ALTO

SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	AUDITORÍA	
TODOS	¿Se realiza la actual auditoría en el plazo establecido desde la anterior?	MEDIO
	Si ha habido modificaciones sustanciales en el sistema de información ¿se ha realizado a continuación una auditoría para verificar la adaptación, adecuación y eficacia de las medidas de seguridad?	
	¿Los informes de las auditorías anteriores incluían los datos, hechos y observaciones en los que se basaban sus dictámenes?	
	¿Se han implementado las medidas correctoras propuestas por auditorías anteriores?, ¿han sido eficaces y han corregido las deficiencias encontradas?	
	CRITERIOS DE ARCHIVO	
TODOS	¿Existe legislación específica con criterios para el archivo de soportes o documentos?, ¿garantizan estos criterios la conservación de documentos, la localización y consulta de la información?, ¿posibilitan el ejercicio de los derechos de oposición, acceso, rectificación y cancelación?	BÁSICO
	En caso de no existir legislación específica ¿ha establecido el responsable del fichero los criterios y procedimientos de actuación para el archivo de documentos?, ¿es adecuado este procedimiento?	
	ALMACENAMIENTO DE LA INFORMACIÓN	
NO AUTOMATIZADO	¿Los dispositivos de almacenamiento de documentos disponen de mecanismos que obstaculicen su apertura? Si sus características físicas no permiten adoptar esta medida ¿ha adoptado el responsable medidas que impidan el acceso de personas no autorizadas?	BÁSICO
	CUSTODIA DE SOPORTES	
NO AUTOMATIZADO	¿Se custodia correctamente la documentación cuando ésta no se encuentra archivada en los dispositivos de almacenamiento por estar en revisión o tramitación?, ¿se impide en todo momento que sea accedida por persona no autorizada?	BÁSICO

Elaboración del informe (dictamen):

- Adecuaciones de las medidas y controles establecidas en lo dispuesto en el Título VIII del Reglamento.
- Identificación de deficiencias y propuesta de medidas correctoras o complementarias.
- Incluirá los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.
- Será analizado por el responsable de seguridad, y elevará sus conclusiones al Responsable del Fichero para que adopte las medidas adecuadas.
- Deberá quedar a disposición de la Agencia Española de Protección de Datos.

DOCUMENTO DE SEGURIDAD DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

INSTITUT D'INVESTIGACIÓ SANITÀRIA PERE VIRGILI (IISPV)

Febrero 2015