Hospital Regional Universitario
CARLOS HAYA
Servicio Andaluz de Salud
CONSEJERÍA DE SALUD

MANUAL DE CALIDAD

LABORATORIO DE ANÁLISIS CLÍNICO

Manual de Seguridad del Sistema Informático del Laboratorio (SIL)

Código	**Fecha emisión/última revisión**	**Revisado**	**Aprobado**
GI 04 Ed 01	29/04/2010	Julio Diaz Ojeda	Dr. Vidal Pérez Valero.
Edición	**Fecha próxima revisión**		
I		Fdo:	Fdo:

1. Política de Seguridad

En este documento, que es el **Manual de Seguridad del Sistema Informático del Laboratorio** (en adelante Manual), están definidas las reglas de actuación en la Unidad de Gestión Clínica (UGC) del Laboratorio del Hospital Regional Universitario Carlos Haya de Málaga (en adelante LABORATORIO), asegurando un adecuado equilibrio entre las necesidades de los usuarios, las exigencias de Seguridad y el respeto a las leyes vigentes. El presente Manual está inspirado en el Manual de Seguridad de del Hospital Regional Universitario de Málaga de Mayo de 2009 y que es el documento que recoge todos los demás aspectos necesarios no especificados este Manual propio del LABORATORIO

La aplicación de estas reglas permitirá garantizar la protección de la información y forman parte del conjunto de medidas, controles y procedimientos destinados a garantizar el cumplimiento de la legalidad vigente en términos de salvaguarda de la confidencialidad, integridad y disponibilidad de la información

Todos los empleados deberán colaborar en el cumplimiento de las reglas de Política de Seguridad de la Información Corporativa que aquí se regulan, y como consecuencia de ello asumen un deber de colaboración con el LABORATORIO en el interés de que no se produzcan alteraciones o violaciones de estas reglas.

Este documento es conocido por todas las personas que prestan sus servicios en el LABORATORIO, por lo que todos conocen las obligaciones que asumen respecto del uso correcto de los recursos informáticos.

Estas normas serán efectivas desde el mes de Mayo de 2010, hasta la fecha en que puedan ser modificadas parcial o totalmente. Cada una de las modificaciones que se realicen o adendas que se incorporen al presente documento serán comunicadas a todos los empleados, mediante inserción en la Intranet del LABORATORIO.

El Manual actualizado y vigente será el que se encuentre en cada momento en la Intranet del LABORATORIO.

2. Objeto del documento.

El presente documento desarrolla la política de seguridad definida por LABORATORIO en materia de Sistemas de Información.

Además responde a la obligación establecida en el artículo 88 del Real Decreto 1720/2007 de 21de Diciembre en el que se regulan las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, así como lo dispuesto en la Ley Orgánica 15/1999 de 13 de diciembre.

Y establece los métodos y procedimientos a seguir por parte del personal del LABORATORIO, tendentes a conseguir una adecuada protección de los Activos de Información (entre ellos los datos personales), así como su obtención, tratamiento, transmisión, etc.

La Seguridad de la Información consiste en un conjunto de medidas, controles, procedimientos y acciones destinados a cumplir con los tres aspectos básicos esenciales para el buen servicio al ciudadano, el cumplimiento de la legalidad vigente y la imagen de la propia entidad:

- **Confidencialidad:** la información debe ser conocida exclusivamente por las personas autorizadas, en el momento y forma prevista.
- **Integridad:** la información tiene que ser completa, exacta y válida, siendo su contenido el previsto de acuerdo con unos procesos predeterminados, autorizados y controlados.
- **Disponibilidad:** la información debe estar accesible y ser utilizable por los usuarios autorizados en todo momento, debiendo estar garantizada su propia persistencia ante cualquier eventualidad.

3. Ámbito de aplicación.

3.1 Ámbito funcional

Este Manual se aplicará en el Laboratorio y en todas sus áreas de influencia tanto dentro del recinto hospitalario como fuera del mismo interesando a los recursos de información y conocimiento, en la extensión y detalle que se describen en el mismo.

El documento hace especial hincapié en la política de seguridad definida por la organización para los ficheros que contienen datos de carácter personal, aunque dicha política se aplica a todos aquellos ficheros y recursos, protegidos o no, que contengan o traten datos automatizados, sin olvidar que la protección alcanza al tratamiento de datos no automatizados, es decir, que se encuentren en soportes físicos.

3.2 Ámbito personal

La Política de Seguridad contenida en el presente Manual es de obligado cumplimiento para todos los profesionales vinculados o relacionados con el LABORATORIO o con su actividad. Este Manual se encuentra inserto en la Intranet del LABORATORIO, debiéndose proceder a su lectura, y en el caso que no entendiesen algunos de los aspectos que en él se regulan, o tuviesen dudas sobre su contenido, deberán ponerlo en conocimiento del Director del Laboratorio o persona en quien se delegue a efecto de que estas dudas puedan ser resueltas, y, como consecuencia de ello, se alcance una mayor eficacia en el cumplimiento de las obligaciones que aquí se recogen.

Por principio, todo el personal del LABORATORIO está obligado a guardar la debida discreción cuando hable con terceros de asuntos relacionados con ella.

Todas las personas que tengan acceso a datos de Ficheros de carácter personal, bien a través del sistema informático habilitado para acceder al mismo, o bien a través de cualquier otro medio automatizado de acceso al Fichero, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

3.3 Ámbito Material

Los Sistemas de Información del LABORATORIO están compuestos por: el *hardware* considerado como el continente o soporte informático y los activos de Información considerados como el contenido. En los activos de información se incluye tanto el *software* como los datos.
Las presentes normas de seguridad son de aplicación a todo el conocimiento del LABORATORIO, se encuentre en formato digital, papel o cualquier otro.
Asimismo, estas normas recogen aspectos de seguridad física que deben disponer aquellos lugares, instalaciones, muebles, etc. donde se almacene información sensible del LABORATORIO.

4. Definiciones.

- **Información:**

Expresión genérica para indicar todos los datos que pueden ser procesados por cualquier medio y que tienen un determinado valor para el LABORATORIO.

- **LOPD:**

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- **Dato de carácter personal:**

Cualquier información concerniente a personas físicas identificadas o identificables. (Artículo 3 LOPD).

• **Fichero de datos de carácter personal**:
Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. (Artículo 3 LOPD).
De cara a su aplicación entendemos fichero como la aplicación informática que recoge y transforma los datos para proporcionar información.

• **Responsable del Fichero o Tratamiento:**
Persona física o jurídica, de naturaleza pública o privada, u organismo administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

• **Encargado del tratamiento:**
La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

• **Declarante:**
Persona física que cumplimenta la solicitud de preinscripción y actúa como mediador entre la Agencia y el titular/responsable del Fichero. No debe necesariamente coincidir con el titular/responsable.

• **Tratamiento de datos**:
Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, visualización, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. (Artículo 3 LOPD).

• **Afectado o interesado**:
Persona física titular de los datos que sean objeto del tratamiento. (Artículo 3 LOPD)

• **Procedimiento de disociación**:
Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

• **Bloqueo de datos:**
La identificación y reserva de los datos con el fin de impedir su tratamiento.

• **Soporte informático**:
Objeto físico susceptible de ser tratado en un sistema de información y sobre el cuál se puede grabar o recuperar datos.

• **Incidencia**:
Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

• **Consentimiento del interesado**:
Es toda manifestación de voluntad, libre inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. (Artículo 3 LOPD).

• **Cesión o comunicación de datos**:
Es toda revelación de datos realizado a una persona distinta del interesado. (Artículo 3 LOPD).

5. Recursos protegidos.

La protección de la información corporativa frente a accesos no autorizados, se deberá realizar mediante el control de todas las vías por las que se pueda tener acceso a ella.

Los recursos, que por servir de medio directo o indirecto para acceder a la información corporativa, que deberán ser controlados por esta normativa son:

1. Los locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan. La Unidad de Sistemas de Información tiene una Sala adecuada para ubicar los equipos y Servidores de todo el Complejo hospitalario y esta regulado en el Manual de seguridad del H R. Carlos Haya
2. Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso al Fichero.
3. Los servidores, si los hubiese, y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el Fichero, que está descrito en el Anexo D (Sistemas de información del fichero).
4. Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos.

6. Funciones y obligaciones del personal.

6.1Definición de perfiles.

La definición de perfiles que a continuación se describe responde a la exigencia que marca la LOPD, por una parte, y por otra, a la necesidad de implantar en el S.A.S. una política de seguridad que abarque no solo la información de carácter personal, sino toda la información corporativa.
El personal afectado por esta normativa queda clasificado en las siguientes categorías:

• **Responsable del Fichero**, *persona física o jurídica de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*. (Artículo 3 LOPD). Internamente esta figura se concreta en el titular del centro directivo o representante legal del centro del que dependa el fichero.

• **Responsable de Seguridad** cuyas funciones serán las de coordinar y controlar las medidas definidas en el documento, sirviendo al mismo tiempo de enlace con el Responsable del Fichero, sin que esto suponga en ningún caso una delegación de la responsabilidad que corresponde a este último. (Artículo 16 RD 994/1999).

• **Responsable de Sistemas y Tecnologías de la Información**, será la persona o entidad administrativa del propio organismo encargada de las tecnologías de la Información y Comunicaciones corporativas. También puede acumular las funciones de Responsable de Seguridad.

• **Usuario Responsable de la Aplicación/Fichero**[1], persona física u órgano específico del LABORATORIO, que por delegación del Responsable del Fichero tiene bajo su responsabilidad todo lo concerniente a la recogida, grabación, conservación, elaboración, modificación, visualización, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. Mantiene contacto diario con la aplicación, conoce su funcionamiento, vela por la seguridad de la misma y trabaja en coordinación con el Responsable de Sistemas y Tecnologías de la Información.
Los Usuarios Responsables de la Aplicación serán los responsables de los Centros, Áreas o Servicios que tienen bajo su responsabilidad información de carácter personal, cualquiera que sea su formato.

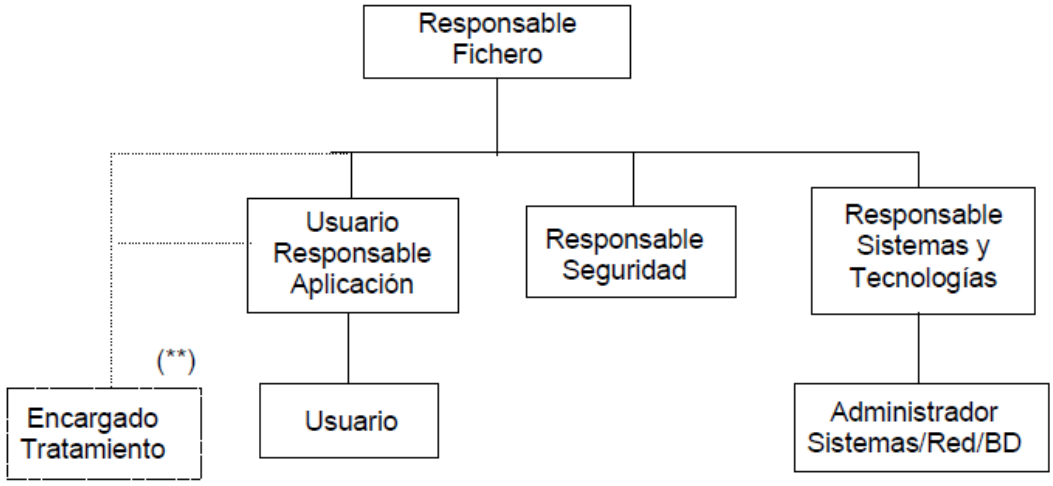
• **Encargado del Tratamiento**, la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos por cuenta del Responsable del Fichero. (Artículo 3 LOPD).
Figura creada para el caso de contratación a terceros del tratamiento de los datos. Todas las empresas contratadas por el LABORATORIO y que dispongan de cualquier base de datos del LABORATORIO para el trabajo que tienen que realizar, tienen la consideración de Encargados del Tratamiento.

• **Administradores de Bases de Datos/Red/Sistema**, encargados de administrar o mantener el entorno operativo de la información corporativa. Este personal, será dependiente del Área de Sistemas ya que por sus funciones pueden utilizar herramientas de administración que permitan el acceso a los datos protegidos.
Deberán además atenerse a aquellas normas, más extensas y estrictas, que se referencian en este documento, y que atañen, entre otras, al tratamiento de los respaldos de seguridad, normas para el alta de usuarios y contraseñas, así como otras normas de obligado cumplimiento en la unidad administrativa a la que pertenece la información.

[1] Esta interpretación es la que se ha recogido en el presente Manual. Algunos tratadistas lo denominan “Responsable Propietario del Fichero”, para indicar a la persona jurídica o física que tenga a su cargo el tratamiento de los datos.

• **Usuarios**, o personal que usualmente utiliza el sistema informático de acceso a la información corporativa.

6.2 Organización de Seguridad



**El Encargado del Tratamiento depende legalmente, a través del contrato de prestación del servicio correspondiente, del Responsable del Fichero, sin embargo será el Usuario responsable de la Aplicación correspondiente, quien vele y le exija el estricto cumplimiento de las normas de seguridad sobre los datos que gestiona.

6.3 Todo el Personal

FUNCIONES Y OBLIGACIONES

Todo el personal está obligado a conocer el Manual de Seguridad del Sistema Informático. Además de lo que se especifica a continuación y, de manera más específica, es de obligado cumplimiento el llevar a cabo la ***RESOLUCIÓN de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía***, adjuntado en el Anexo F de este manual.

Las funciones y obligaciones que afectan a todo el personal son:

6.3.1 Confidencialidad de la Información

1. Guardarán la debida reserva sobre las materias clasificadas a las que hayan tenido acceso en razón a su puesto de trabajo u otra circunstancia.
2. Impedirán el acceso de personas no autorizadas al conocimiento de información, en cuya gestión, tramitación o custodia participe.
3. *El Responsable del Fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.* (Artículo 10 LOPD)
4. Queda prohibido extraer datos de un fichero de datos de carácter personal ya existente, o crear un fichero de datos personales aprovechando los datos de un fichero ya existente, sin la autorización del Responsable del Fichero.
5. Queda prohibido utilizar archivos con datos personales que el LABORATORIO no haya comunicado y registrado ante la Agencia de Protección de Datos.

6. Respecto de aquellos archivos que el LABORATORIO haya comunicado y registrado en la Agencia de Protección de Datos, se prohíbe 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.

6.3.2 Salvaguarda y protección de las contraseñas personales

1. Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio o que ésta sea cambiada por el Administrador de Red/Sistemas.
2. Solamente para aquellos casos excepcionales en los que sea necesario continuar con las funciones que realizaba la persona ausente (debido a una baja o ausencia temporal no prevista), será el responsable del Centro, Área, o en caso de ficheros de carácter personal, el Usuario Responsable de la Aplicación/Fichero, el que podrá solicitar a los administradores el acceso a sus datos, dejando constancia en la aplicación de Mantenimiento del Sistema de Información.
3. Toda clave cumplirá unas normas mínimas, según detalla en el Anexo A, apartado 9 el Procedimiento de Acceso al Sistema de Información.
4. En el caso de que el Administrador de Sistemas solicite la contraseña/*password* para tareas de mantenimiento, la misma deberá ser cambiada inmediatamente después que se termine con dichas tareas.

6.3.3 Puesto de trabajo

1. El puesto de trabajo estará bajo la responsabilidad de un usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.
Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.
Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos.
2. Todos los puestos de trabajo estarán configurados de forma que el tiempo máximo que una máquina permanecerá desbloqueada será de 60 minutos a partir del momento en que se usó por última vez. Obsérvese que esto no entra en conflicto con el hecho de que el usuario pueda tener configurado un tiempo menor de bloqueo.
3. En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos correspondientes, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
4. Queda expresamente prohibida la conexión desde los puestos de trabajo en los que se realiza el acceso a la información corporativa, a redes o sistemas exteriores a través de dispositivos que no estén controlados por el sistema de seguridad de la Red Corporativa de Transmisión de Datos de la Junta de Andalucía. En concreto módem, enlaces de radiofrecuencia, tarjetas inalámbricas, *routers* o *bridges* WIFI. La revocación de esta prohibición será autorizada por el Responsable del Fichero, quedando constancia como incidencia.
5. Los puestos de trabajo desde los que se tiene acceso a la información corporativa tendrán una configuración fija en sus aplicaciones, sistemas operativos que sólo podrá ser cambiada por el Administrador de Sistema, el cual deberá solicitar autorización al Responsable de Sistemas y Tecnologías, existiendo unas normas de unificación de todos los terminales informáticos.
Por tanto queda prohibida la instalación, por parte del usuario, de cualquier tipo de Aplicaciones/Programas (*software*) en los puestos de trabajo, así como borrar cualquiera de los programas instalados.
6. Queda prohibido abrir los equipos o máquinas (*hardware*) para realizar cualquier tarea sobre ellos sin autorización previa y por escrito del Administrador de Red/Sistemas. Asimismo tampoco se podrán agregar o retirar partes o componentes de los mismos.
7. No se podrán retirar los equipos de cualquier edificio del LABORATORIO sin previa autorización escrita.

6.3.4 Sistema Informático y Telemático de Acceso a la Información

1. Todos los recursos telemáticos e informáticos del LABORATORIO, incluido por tanto Internet y el correo electrónico, serán usados con fines profesionales directamente relacionados con el puesto de trabajo del usuario.
2. Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial.

6.3.5 Otros Recursos

1. El empleado, en el momento en que finalice su contrato con el LABORATORIO deberá entregar a los responsables de los Centros, Áreas o Servicios cualesquiera dibujos, anotaciones, memorandos, especificaciones, esquemas, fórmulas, y documentos, junto con todas las copias de los mismos, y cualquier otro material que contenga o revele cualquier Invención de la Empresa, Información de Terceras Partes o Información clasificada del LABORATORIO. Asimismo deberá devolver todos aquellos instrumentos de trabajo que le han sido puestos a disposición por la compañía: teléfono móvil, tarjetas de acceso a edificios y CPD, ordenadores portátiles, etc., que son propiedad del LABORATORIO.

6.3.6 Gestión de Incidencias

1. Es obligación de todo el personal del LABORATORIO notificar cualquier incidencia que afecte a la seguridad de los datos, o presunción/sospecha de la misma, que se produzca en los sistemas de información a los que tenga acceso y recopilar toda la información posible para optimizar el procedimiento de detección del problema.
2. Es obligación de todo el personal del LABORATORIO notificar al Responsable de Seguridad cualquier otra incidencia, de naturaleza no técnica, que atente o pueda atentar contra la seguridad de la información corporativa.
3. El conocimiento y la no notificación de una incidencia por parte de un usuario será considerada como una falta del mismo contra la Seguridad del Fichero por parte de éste.

6.3.7 Gestión de soportes

1. Los soportes que contengan datos, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, qué tipo de datos contiene, proceso que los ha originado y fecha de creación.
2. Aquellos medios que sean reutilizables, y que hayan contenido copias de datos no públicos, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.
3. Los soportes que contengan datos no públicos deberán estar almacenados en lugares a los que sólo tengan acceso personas autorizadas.
4. Cualquier movimiento total o parcial de un fichero de carácter personal, ya sea en soporte físico o transferencia telemática, fuera de los locales donde está ubicado el fichero deberá ser autorizada por el Responsable del Fichero (artículo 13.2 del RD 994/1999).
5. Cuando los datos de un fichero de carácter personal deban ser enviados fuera del recinto físicamente protegido donde se encuentra ubicado el Fichero, bien sea mediante un soporte físico de grabación de datos o bien sea mediante correo electrónico, deberán ser cifrados de forma que sólo puedan ser leídos e interpretados por el destinatario.
6. Se deberán registrar en el Registro de Entrada/Salida los correos electrónicos o transferencia de datos de carácter personal por red, de forma que se pueda siempre identificar su origen, tipo de datos, formato, fecha y hora del envío y destinatario de los mismos.

6.3.8 Copias de Respaldo y Recuperación

1. El Administrador de Red/Sistemas/Base de Datos se responsabiliza de realizar las copias de seguridad de los servidores, y en ningún caso de los ordenadores personales. Esto implica que la información corporativa debe siempre guardarse en el espacio de servidor habilitado para los profesionales y/o Áreas concretas.

6.4 Responsable del Fichero

FUNCIONES

1. El Responsable del Fichero es el encargado jurídicamente de la seguridad del fichero y de las medidas establecidas en el presente documento, implantará las medidas de seguridad establecidas en él y adoptará las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones. (Artículos 88.1 y 89.2 RD 1720/2007).
2. Designará al Responsable de Seguridad.
3. Notificará a los Usuarios Responsables de Aplicación/Fichero, Responsable de Sistemas y Tecnologías de la Información, las responsabilidades que asumen al tomar posesión de sus cargos en lo que respecta a la Seguridad de la Información.
4. El Responsable del Fichero *se concreta en el titular del centro directivo o representante legal del centro del que dependa el fichero.*

OBLIGACIONES

6.4.1 Política de Seguridad de la Información Corporativa
Implantar las medidas de seguridad establecidas en este documento y garantizar la difusión de este Documento, a todo el personal relacionado con la información corporativa.

6.4.2 Declaración de Ficheros de Carácter Personal
1. Solicitará a la Subdirección de Tecnología y Sistemas de Información del Hospital R. Univ. Carlos Haya, la creación de los ficheros que contengan datos de carácter personal y que sean necesarios para el funcionamiento del LABORATORIO
2. Notificará a la Agencia de Protección de Datos los ficheros creados mediante Orden de la Consejería y publicados en el BOJA.

6.4.3 Ejercicio de derechos de oposición, acceso, rectificación o cancelación de Datos de Carácter Personal
El Responsable del Fichero habilitará los mecanismos para cumplir el procedimiento de ejercicio del derecho de oposición, acceso, rectificación y cancelación que la Ley otorga, en los casos que proceda, dejando registro de dicha solicitud.

6.4.4 Gestión de soportes
Cualquier movimiento total o parcial de un fichero de carácter personal, ya sea en soporte físico o transferencia telemática, fuera de los locales donde esta ubicado el fichero deberá ser autorizado por el Responsable del Fichero. (Artículo 92.2 del RD 1720/2007).
El Responsable del Fichero delega esta gestión del movimiento en el Responsable de Seguridad.

6.4.5 Controles periódicos de verificación del cumplimiento
Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del reglamento de seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoría serán analizados por el Responsable de Seguridad, quien propondrá al Responsable del Fichero las medidas correctoras correspondientes. (Artículo 96 RD 1720/2007).

6.5 Responsable de Seguridad

FUNCIONES

Sus funciones serán las de coordinar y controlar las medidas definidas en el documento, sirviendo al mismo tiempo de enlace con el Responsable del Fichero. (Artículo 95 RD 1720/2007).

OBLIGACIONES

6.5.1 Política de Seguridad de la Información Corporativa

1. El Responsable de Seguridad coordinará la puesta en marcha de las medidas de seguridad, colaborará con el Responsable del Fichero en la difusión y el cumplimiento del Documento de Seguridad.
2. Deberá mantenerlo actualizado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
3. Deberá adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos, y asegurar que el nuevo documento llega a todo el personal afectado.

6.5.2 Declaración de Ficheros de Carácter Personal

1. El responsable de Seguridad analizará la viabilidad de crear un nuevo fichero o solicitar las modificaciones a ficheros ya declarados.
2. Para la creación del fichero se solicitará:
   - Disposición de creación del fichero a la Consejería de Salud
   - Declaración a la Agencia de Protección de Datos

Según establece el procedimiento de Declaración de Ficheros de Carácter Personal.

3. El Responsable de Seguridad mantendrá siempre actualizado el Anexo B de este documento donde se relacionan los ficheros que contengan datos de carácter personal, con indicación de las referencias: escrito de remisión a la Consejería de Salud, publicación en BOJA, remisión a la Agencia de Protección de datos, etc.

6.5.3 Ejercicio de Derechos de Oposición, Acceso, Rectificación y Cancelación de Datos de Carácter Personal

1. El Responsable de Seguridad vigilará el correcto cumplimiento en cuanto a la notificación del tratamiento de datos de carácter personal al afectado, según establece el procedimiento para el ejercicio de derechos de oposición, acceso, rectificación y cancelación de datos de carácter personal.
2. En caso de recibir una solicitud para ejercer sus derechos, el responsable del Registro de Entrada/Salida hará llegar una copia del impreso al Responsable de Seguridad, el cual a su vez lo reencaminará al Usuario Responsable de la Aplicación/Fichero correspondiente al Centro, Área o Servicio (que tiene a su cargo la manipulación del fichero en cuestión).
3. El Responsable de Seguridad controlará si se están gestionando adecuadamente las reclamaciones, los tiempos y si pueden ser causa de algún tipo de sanción por parte de la Agencia de Protección de Datos.

6.5.4 Gestión de incidencias

1. El Responsable de Seguridad implantará las medidas necesarias, según el Procedimiento de Registro de Incidencias de Seguridad de la Información Corporativa, que estarán a disposición de todos los usuarios y administrador de Red/Sistemas/BD con el fin de que se registre, cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.
2. El Responsable de Seguridad, analizará con periodicidad al menos trimestral las incidencias registradas, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, adoptar las medidas correctoras que limiten esas incidencias en el futuro.

6.5.5 Gestión de Soportes

El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en el procedimiento de Gestión de Soportes.

6.5.6 Copias de Respaldo y Recuperación

1. Al Responsable de Seguridad le corresponde la supervisión de los soportes de grabación de las copias de respaldo y de las relaciones con las empresas externas (siempre que éstas lleven a cabo labores de copias de respaldo y desarrollen la labor de custodia y aseguramiento de las copias de respaldo), toda vez que se cumpla con las garantías contractuales y legales necesarias para garantizar la seguridad y confidencialidad de las copias de respaldo, marcando las responsabilidades de cada parte en estas funciones.
2. Participará en la recuperación de los datos en la forma descrita en el procedimiento de respaldo y recuperación.
3. Realizará la auditoría del sistema de copias de respaldo, según establece el procedimiento correspondiente, dos veces al año, documentando el resultado.

6.5.7 Descripción del Uso del Sistema de Información Corporativa

Al menos una vez al trimestre revisará, conjuntamente con el Responsable de Sistemas y Tecnologías de la Información, que los sistemas estén actualizados según recomendaciones de los fabricantes.

6.5.8 Control de Accesos

El Responsable de Seguridad comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados se corresponde con los usuarios que realmente deben estar autorizados para el acceso a la aplicación.

6.5.9 Registro de Accesos

1. El Responsable de Seguridad y Responsable de Sistemas y Tecnologías de la Información son los responsables de determinar los registros de accesos que se llevarán a cabo en el LABORATORIO.
2. El Responsable de Seguridad revisará periódicamente la información registrada elaborando un informe de incidencias al menos una vez al mes. (Artículo 103.5 RD 1720/2007)

6.5.10 Controles Periódicos de Verificación del Cumplimiento

1. Al menos cada dos años, se realizará una auditoría, externa o interna que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoría serán analizados por el Responsable de Seguridad, quien propondrá al Responsable del Fichero las medidas correctoras correspondientes. (Artículo 96 RD 1720/2007).
2. Los resultados de las auditorías serán documentados.

6.6 Responsable Sistemas y Tecnologías de la Información

FUNCIONES

1. Es el responsable de los sistemas tecnológicos, que dan soporte a la información corporativa, es decir, de las operaciones y procedimientos técnicos de carácter automatizado que permiten la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, de la información corporativa.
2. Designará a los Administradores del Sistema/Red/Base de datos, y cuya actividad coordinará.

OBLIGACIONES

6.6.1 Política de Seguridad de la Información Corporativa

1. Implantación de todas las medidas recogidas en este Documento y velar por la confidencialidad, disponibilidad, consistencia e integridad de los datos.

6.6.2 Sistema Informático y Telemático de Acceso a la Información

1. Autorizará, a propuesta del Administrador de Sistemas/Red/Base de Datos, los cambios en el *software* y en el equipamiento informático y de comunicaciones.
2. Comunicará al Responsable de Seguridad cualquier cambio que se haya realizado en la configuración de *hardware* o *software*, procediendo igualmente a la actualización de este documento si procede.

6.6.3 Gestión de Incidencias

Se encargará de que se dé solución a las incidencias ocurridas y registradas en la aplicación de Mantenimiento del Sistema de Información.

6.6.4 Descripción del Uso del Sistema de Información Corporativa

1. Velará por el cumplimiento de los requisitos de documentación de los sistemas, establecidos en el Anexo A, apartado 8 de *Descripción del Uso del Sistema de Información Corporativa*.
2. Al menos una vez al trimestre revisará, conjuntamente con el Responsable de Seguridad, que los sistemas estén actualizados según recomendaciones de los fabricantes.

6.6.5 Control de Accesos

Se encargará de que los sistemas informáticos tengan su acceso restringido mediante un código de usuario y una contraseña y con las características que establece en el Anexo A, apartado 9, *Procedimiento de Acceso al Sistema de Información*.

6.6.6 Registro de accesos

El Responsable de Seguridad y Responsable de Sistemas y Tecnologías de la Información son responsables de determinar los registros de accesos que se llevarán a cabo en el LABORATORIO

6.7 Usuario Responsable de la Aplicación/Fichero

FUNCIONES

1. Contacto directo con la explotación diaria de la aplicación y conociendo su funcionamiento pormenorizado vele por el mantenimiento de seguridad de la misma, trabaje en coordinación con el Responsable de Sistemas y Tecnologías de la Información, siguiendo las pautas de seguridad dictadas por el Responsable de Seguridad.
2. Se corresponde con el responsable, del LABORATORIO, de la actividad correspondiente.

OBLIGACIONES

6.7.1 Ejercicio de Derechos de Oposición, Acceso, Rectificación y Cancelación de Datos de Carácter Personal

1. El Usuario Responsable de la Aplicación/Fichero estudiará la reclamación y elaborará un escrito de comunicación al reclamante, en sentido aprobatorio o denegatorio, indicando en este último caso las causas, haciéndole ver que pueden ejercitar el derecho de reclamación ante la Agencia de Protección de Datos. El escrito deberá ir firmado por el Responsable del Fichero. Se deberá tener muy en cuenta los plazos fijados por la normativa a aplicar.
2. En caso de que se proceda a hacer efectivo alguno de los derechos el Usuario Responsable de la Aplicación/Fichero analizará si existieron cesiones para notificarlo a quien trate los datos cedidos y notificará los cambios al Encargado del Tratamiento en caso de que exista.
3. El Usuario Responsable de la Aplicación/Fichero será el encargado de hacer efectivo el derecho reclamado en la forma y plazo que establece el procedimiento para el ejercicio de oposición, acceso, rectificación y cancelación de datos de carácter personal.

6.7.2 Gestión de Soportes

1. El Usuario Responsable de la Aplicación/Fichero creará un inventario de soportes y transferencias donde registrará cada soporte que contenga información de carácter personal o confidencial, o cualquier transferencia telemática de dicha información, según el procedimiento de gestión de soportes
2. La preparación de soportes informáticos para su posterior envío, con información clasificada como confidencial o personal de nivel alto, ya sea en formato físico (disquete, CDROM, listado, etc.) o en formato electrónico (correo electrónico), será realizada por el Usuario Responsable de la Aplicación/Fichero[2]. La autorización de la salida la llevará a cabo el Responsable del Fichero. (Artículo 92.2 RD 1720/2007).

6.7.3 Copias de Respaldo y Recuperación

1. Para poder proceder a la recuperación de información, a partir de las copias de respaldo, se tendrá que recabar la autorización previa del Usuario Responsable de la Aplicación/Fichero[3] (Artículo 100.2 RD 1720/2007).

6.7.4 Control de Accesos

1. Proponer las altas y bajas de acceso de usuarios a su aplicación y/o información correspondiente en la aplicación de Mantenimiento del Sistema de Información, según establece el Anexo A, apartado 9 de *Procedimiento de Acceso al Sistema de Información.*
Es importante resaltar la obligatoriedad de notificar la baja, en el momento que se conozca, del personal que deba dejar de tener acceso a la información corporativa.
2. El Usuario Responsable de la Aplicación/Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados de su Área o Sede se corresponde con la

[2] El RD 994/1999 establece en su artículo 13.2 que la autorización será del Responsable del Fichero. Sin embargo para una más ágil operativa se establece en el S.A.S. que la autorización será del Usuario Responsable de la Aplicación/Fichero por ser quien vela en su operativa diaria por el cumplimiento de las normas establecidas sobre la información que trata.

[3] El RD 994/1999 establece que la autorización será por parte del Responsable del Fichero. En el S.A.S. se establece que dicha autorización se delega al Usuario Responsable de la Aplicación/Fichero, como persona más en contacto con la operativa diaria.

lista de los usuarios realmente autorizados en la aplicación de acceso a la información corporativa, para lo que recabará la lista de usuarios y su identificador de acceso al administrador, notificando toda variación (alta/baja/modificación) según se determina en apartados anteriores.

6.7.5 Externalización de Servicios

En caso de externalizar el servicio o tratamiento de su responsabilidad, velar por el cumplimiento de las obligaciones contractuales del Encargado del Tratamiento que corresponda.

6.8 Encargado del Tratamiento

FUNCIONES

Tratamiento de la información corporativa conforme a las instrucciones que expresamente figuran en este Manual.

RESPONSABILIDADES

El Encargado del Tratamiento adquiere una responsabilidad contractual con el LABORATORIO si menoscaba alguna de las normas que se relacionan en el presente manual.

OBLIGACIONES

1. Cumplir las instrucciones del Usuario Responsable de la Aplicación/Fichero y la finalidad señalada en el contrato.
2. Preservar que sólo tengan acceso, y a la información correspondiente, las personas autorizadas para ello, actuando únicamente con el alcance que le haya sido fijado: sólo consulta, modificación, etc.
Para ello propondrá las altas y bajas de acceso de usuarios a su aplicación y/o información correspondiente en la aplicación de Mantenimiento del Sistema de Información, según establece el Anexo A, apartado 9 de *Procedimiento de Acceso al Sistema de Información*.
Es importante resaltar la obligatoriedad de notificar la baja, en el momento que se conozca, del personal que deba dejar de tener acceso a la información corporativa.
3. Hacer cumplir todas las funciones, obligaciones y recomendaciones que se recogen en el apartado 6.3 del presente Manual, respecto a todos sus usuarios que traten la información corporativa del LABORATORIO.
4. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al Usuario Responsable de la Aplicación/Fichero, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

6.9 Administradores de Bases de Datos/Sistemas/Red

FUNCIONES

1. Mantener los sistemas de acceso a la información corporativa.
2. Dispondrán de los máximos privilegios. Tendrán acceso al *software* (programas y datos) del sistema, a las herramientas necesarias para su trabajo y a los ficheros o bases de datos necesarios para resolver los problemas que surjan.

OBLIGACIONES

6.9.1 Sistema Informático y Telemático de Acceso a la Información

1. Impedirá que existan herramientas o programas de utilidad que permitan accesos no autorizados a información corporativa.
En la norma anterior se incluye cualquier medio de acceso en bruto, es decir no elaborado o editado, a los datos, como los llamados "*queries*", editores universales, analizadores de ficheros, etc., que deberán estar bajo el control de los administradores autorizados.
2. Será responsabilidad del Administrador de Red/Sistemas/Base de Datos mantener completamente actualizados los sistemas, en todo momento, con las actualizaciones que recomiende el fabricante, a fin de eliminar todas aquellas vulnerabilidades, en cuanto a seguridad, que sean posibles.
3. Si la aplicación o sistema de acceso a la información corporativa utilizase usualmente ficheros temporales, ficheros de "*log*", o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse de que esos datos no son accesibles posteriormente por personal no autorizado.
4. Se asegurará en todo caso que el sistema de eliminación de ficheros temporales establecido en el LABORATORIO funciona correctamente.
5. Si en un ordenador está ubicada información corporativa no pública, y el ordenador está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso a la información corporativa, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.
6. Los Administradores de Red/Sistemas/Base de Datos ejecutarán, previa autorización del Responsable de Sistema y Tecnologías de la Información y del Usuario Responsable de la Aplicación/Fichero correspondiente, cualquier cambio en la configuración del *hardware* y *software* de acceso a la información corporativa, procediendo igualmente a la actualización de la documentación correspondiente.

6.9.2 Copias de Respaldo y Recuperación

1. El Administrador de Sistema/Red/BD es el responsable de realizar las copias de respaldo, de realizar la verificación de que las copias se hayan hecho de forma correcta y de realizar las recuperaciones de la información, así como de tener un registro en el que se anotarán todas las posibles incidencias que ocurran al realizar las copias y todas las recuperaciones de información que se tengan que hacer.
2. En caso de fallo del sistema con pérdida total o parcial de los datos aplicará los procedimientos, informáticos o manuales, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos al estado en que se encontraban en el momento del fallo. (Artículo 94.2 RD 1720/2007).
3. Al menos con periodicidad trimestral, realizará una recuperación de las copias de respaldo que permitan la recuperación de la información corporativa, según lo estipulado en el procedimiento de Respaldo y Recuperación.
4. El administrador deberá responsabilizarse de inventariar, identificar, registrar y guardar en lugar protegido las copias de seguridad y respaldo según establece el procedimiento de respaldo y recuperación.

6.9.3 Descripción del Sistema de acceso a la Información Corporativa

Los Administradores de Red/Sistemas/Base de Datos ejecutarán, previa autorización del Responsable de Sistemas y Tecnologías de la Información y del Usuario Responsable de la Aplicación/Fichero correspondiente, cualquier cambio en la configuración del *hardware* y *software* de acceso a la información corporativa, procediendo igualmente a la actualización de la documentación correspondiente.

6.9.4 Control de Accesos

1. Ejecutará las solicitudes del Usuario Responsable de la Aplicación/Fichero, para el cambio de permisos de accesos a la información corporativa, altas y bajas, según el *Procedimiento de Acceso al Sistema de Información* (Anexo A, apartado 9).
2. Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el *Procedimiento de Acceso al Sistema de Información* (Anexo A, apartado 9). Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.
3. El Administrador de Sistemas/Red realizará el seguimiento y control del funcionamiento de la administración de contraseñas del sistema.

6.9.5 Registro de Accesos

1. El Administrador de Sistemas/Red/Base de Datos designado, será el encargado de activar el sistema de registro de accesos según establece el procedimiento de *Registro de Accesos* (Anexo A, apartado 10).
2. Se controlarán los intentos de acceso fraudulento a la información corporativa, limitando el número máximo de intentos fallidos según determine el *Procedimiento de Acceso al Sistema de Información* (Anexo A, apartado 9), y, cuando sea técnicamente posible, guardando en un fichero auxiliar la fecha, hora, código y clave erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.
3. Será necesario también, cuando se autorice el acceso a un fichero con datos de carácter personal y considerado de nivel alto, guardar la información que permita identificar el registro accedido.

Anexo A. Normas y Procedimientos de Seguridad

1. Seguridad de la Sala de Servidores.
(Ver Manual de Seguridad Informática HRU Carlos Haya; Pág. 36)

2. Procedimiento de Declaración de Ficheros de Carácter Personal.
(Ver Manual de Seguridad Informática HRU Carlos Haya; Pág. 43)

3. Procedimiento para el Ejercicio de los Derechos de Oposición, Acceso, Rectificación o Cancelación de Datos de Carácter Personal.
(Ver Manual de Seguridad Informática HRU Carlos Haya; Pág. 45)

4. Procedimiento de Relaciones Contractuales con Empresas Externas con Acceso a Información Corporativa.

5. Registro de Incidencias de Seguridad de la Información Corporativa.
(Ver Manual de Seguridad Informática HRU Carlos Haya; Pág. 60)

6. Procedimiento de Gestión de Soportes.
(Ver Manual de Seguridad Informática HRU Carlos Haya; Pág. 64)

7. Procedimientos de Respaldo y Recuperación.
(Ver Manual de Seguridad Informática HRU Carlos Haya; Pág. 68)

8. Descripción del Uso del Sistema de Información Corporativa.
(Ver Manual de Seguridad Informática HRU Carlos Haya; Pág. 80)

9. Procedimiento de Acceso al Sistema de Información.

10. Registro de Accesos.
(Ver Manual de Seguridad Informática HRU Carlos Haya; Pág. 87)

11. Controles Periódicos de Verificación del Cumplimiento.
(Ver Manual de Seguridad Informática HRU Carlos Haya; Pág. 89)

4. **Procedimiento de Relaciones Contractuales con Empresas Externas con Acceso a Información Corporativa.**

OBJETIVO

Describir las cláusulas que deben inscribirse en todos los contratos que realice el LABORATORIO con otras empresas que necesiten acceso a información corporativa para ejercer el servicio contratado.

DESCRIPCIÓN

Se determinan tres clases de empresas que tienen relación contractual con el LABORATORIO:

- Empresas que realizan tareas de Encargados de Tratamiento.
- Empresas que prestan servicios sanitarios o de otra índole y a las que se les proporcionan determinados datos para que puedan prestar el servicio.
- Empresas que no tienen relación con información corporativa (limpieza, recogida de residuos, electricidad, fontanería, etc.).

a. Encargados de Tratamiento

1. *La realización de tratamiento por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del Usuario Responsable de la Aplicación/Fichero, que no los aplicará o utilizará con un fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.* (Artículo 12.2 LO 15/1999).
2. En el contrato se estipulará, asimismo, las medidas de seguridad que el Encargado del Tratamiento está obligado a implementar. (Artículo 12.2 LO 15/1999).
3. *En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también Usuario Responsable de la Aplicación/Fichero, respondiendo de las infracciones en que hubiera incurrido personalmente*.
(Artículo 12.4 LO 15/1999).

i. Cláusulas a Incorporar en el Contrato

1. El **contratista** estará obligado a conocer, respetar y asegurar que se cumplan en el desarrollo de su trabajo, todas las normas, pautas, procedimientos, recomendaciones, etc., que se fijan en el Manual de Seguridad de la Información Corporativa del **LABORATORIO**, que tras la firma del contrato le será proporcionado por el Responsable de Seguridad del LABORATORIO (se le proporcionarán los aspectos del Manual que le hagan falta para el desarrollo de su labor).
2. El **contratista** estará obligado a adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos facilitados por el LABORATORIO y eviten su alteración, pérdida, tratamiento o acceso no autorizado, todo ello en consonancia con el nivel de seguridad exigible de acuerdo con la información que trate. Para el caso de una interrupción de los servicios informáticos, el contratista dispondrá de otras instalaciones de características similares en donde podrá realizar, durante el tiempo de avería, el servicio mínimo que se considera imprescindible para el S.A.S
3. El **contratista** estará obligado a tratar los datos siguiendo las instrucciones que le fije el Usuario Responsable de la Aplicación/Fichero, para el fichero o los ficheros, con datos de carácter personal u otro tipo de información del **LABORATORIO**, que tenga que tratar en el desarrollo de sus funciones.
4. El **contratista** se compromete a no aplicar, ni utilizar, los datos de carácter personal que se le hayan proporcionado para el desarrollo de su labor, a un fin distinto al que figura en el contrato.
5. El **contratista** y todo el personal que trabaje para él estarán sujetos al deber de confidencialidad en el ejercicio de sus funciones, cuando trabajen para el **LABORATORIO.**, configurándose este deber como la prohibición de la revelación de datos de las personas que se conocen en virtud del ejercicio de la actividad que desempeñan, respondiendo, en

consecuencia, de los perjuicios que del incumplimiento puedan derivarse para el **LABORATORIO.**

6. El **contratista** no comunicará ningún tipo de datos, propiedad del **LABORATORIO.**, ni siquiera para su conservación, a otras personas o entidades.

7. Antes de comenzar a ofrecer el Servicio de Información contratado, el **contratista** deberá presentar a las Gerencias/Direcciones del **LABORATORIO**. los procedimientos que va a emplear, con objeto de comprobar que se cumplen los requisitos de seguridad exigidos en la legislación vigente en materia de protección de datos de carácter personal.

8. Una vez cumplida la prestación contractual, toda la información corporativa del **LABORATORIO** deberá ser destruida o devuelta al Usuario Responsable de la Aplicación/Fichero, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal u otra información objeto del tratamiento. (Artículo 12.3 LO 15/1999).

9. El S.A.S será el propietario de los datos que se traten en los diferentes servicios contratados.

10. Toda información, de carácter confidencial que el S.A.S. conozca, en virtud del contrato, acerca de las técnicas y metodologías empleadas por el **contratista** en la ejecución de estos servicios informáticos no podrá comunicarla a terceros ni emplearla en uso propio, respondiendo, en consecuencia, de los prejuicios que del incumplimiento de esta cláusula se pudieran derivar para el contratista.

11. El **contratista** no podrá trabajar para la competencia ni para quienes realicen actividades afines.

12. En el caso de los datos de carácter personal serán, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre (LOPD), responsables de los datos tanto el responsable del fichero como el encargado del tratamiento.

13. El **contratista** informará al **S.A.S,** antes de realizarlas, de todas las modificaciones que se vayan a hacer en la estructura de los ficheros que contengan datos de carácter personal, así como de la intención de suprimir o crear ficheros que contengan dicha clase de datos a fin de que el **S.A.S.- HRUCH,** como titular de dichos ficheros, pueda notificar con la debida antelación a la Agencia de Protección de Datos dichas variaciones.

14. Si a causa del incumplimiento por parte del **contratista** de lo regulado por la Ley, el **S.A.S.** fuese sancionado por la Agencia de Protección de Datos, dicha sanción será inmediatamente repercutida al contratista, debiendo ser abonada por este. Asimismo, resarcirá al S.A.S. por los daños y perjuicios que esta sanción, aparte de la multa, le hubiese ocasionado. En el caso de que no por haber sido debidamente informado fuese sancionado el **S.A.S. - HRUCH** por la Agencia de Protección de Datos, el contratista pagará la sanción que corresponda y asimismo resarcirá al **S.A.S.** por los daños y perjuicios que dicha omisión pudiera causarle.

15. El **contratista** deberá incluir en los contratos que tenga establecidos con sus trabajadores una cláusula de confidencialidad por la que estos se comprometan a no revelar ni emplear en uso propio o de terceros la información que conozcan en función de su cometido tanto durante el tiempo que dure su contrato, ya sea laboral o de cualquier otro tipo de los admitidos en derecho, como posteriormente al finalizar dicha relación, especialmente en los casos contemplados en el artículo 10 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD).

16. El **S.A.S. - HRUCH** podrá, si lo considera necesario, ordenar, una vez al año, la realización de una Auditoria de los Sistemas de Seguridad del Centro Informático del **contratista** y éste deberá posibilitar el acceso de los auditores informáticos y facilitarles las pruebas que soliciten para cubrir el objetivo de la auditoria. Asimismo los auditores informáticos podrán verificar si se cumplen los estándares de calidad.

17. El **contratista** se compromete a implementar las aplicaciones de forma que se puedan realizar en ellas Auditorias Informáticas, especialmente en aquellos ficheros que contengan datos de carácter personal y que pueden, en su día, ser auditados por los inspectores de la Agencia de Protección de Datos.

b. Empresas, Prestatarias de Servicios Sanitarios o de otra índole, a las que se les proporcionan determinados datos para que puedan prestar el servicio.

Este tipo de empresas, en principio, no representan al Encargado del Tratamiento pero necesitan conocer cierta información para desempeñar el servicio que prestan. Ejemplo: en transporte programado, las ambulancias a las que hay que facilitar el nombre y dirección del paciente.

i. Cláusulas a Incorporar en el Contrato

1. El **contratista** estará obligado a conocer, respetar y asegurar que se cumplan en el desarrollo de su trabajo, todas las normas, pautas, procedimientos, recomendaciones, etc., que se fijan en el Manual de Seguridad de la Información Corporativa del **LABORATORIO**., que tras la firma del contrato, le será proporcionado por el Responsable de Seguridad correspondiente del **LABORATORIO**. (se le proporcionarán los aspectos del Manual que le hagan falta para el desarrollo de su labor).
2. El **contratista** y todo el personal que trabaje para él estarán sujetos al deber de confidencialidad en el ejercicio de sus funciones, cuando trabajen para el **LABORATORIO**., configurándose este deber como la prohibición de la revelación de datos de las personas que se conocen en virtud del ejercicio de la actividad que desempeñan, respondiendo, en consecuencia, de los perjuicios que del incumplimiento puedan derivarse para el **LABORATORIO.**
3. El **contratista** se compromete a no aplicar, ni utilizar, los datos personales que se le hayan proporcionado para el desarrollo de su labor, para un fin distinto al que figura en el contrato.
4. El **contratista** no comunicará ningún tipo de datos, propiedad del **LABORATORIO**., ni siquiera para su conservación, a otras personas o entidades.
5. Si las tareas sanitarias que realiza el **contratista**, tanto para el **LABORATORIO.** como para otras instituciones sanitarias, las gestiona en una base de datos propia, presentará previamente la creación y notificación del fichero correspondiente ante la Agencia de Protección de Datos al S.A.S., así como las medidas de seguridad que amparan la gestión del citado fichero.
6. El **contratista** en el ejercicio de la cláusula anterior, tendrá la característica de Responsable del Fichero a los efectos de la Ley Orgánica de Protección de Datos y al Reglamento de Medidas de Seguridad.
7. El **contratista** estará obligado a adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal, proporcionados por el LABORATORIO, y eviten su alteración, pérdida, tratamiento o acceso no autorizado, todo ello en
consonancia con el nivel de seguridad exigible de acuerdo con los datos que trate.
8. El **S.A.S. - HRUCH** será el propietario de los datos que se traten en los diferentes servicios contratados.
9. Toda información, de carácter confidencial que el **S.A.S. - HRUCH** conozca, en virtud del contrato, acerca de las técnicas y metodologías empleadas por el **contratista** en la ejecución de estos servicios no podrá comunicarla a terceros ni emplearla en uso propio, respondiendo, en consecuencia, de los prejuicios que del incumplimiento de esta cláusula se pudieran derivar para el contratista.
10. El **contratista** no podrá trabajar para la competencia ni para quienes realicen actividades afines.
11. El **contratista** deberá incluir en los contratos que tenga establecidos con sus trabajadores una cláusula de confidencialidad por la que estos se comprometan a no revelar ni emplear en uso propio o de terceros la información que conozcan en función de su cometido tanto durante el tiempo que dure su contrato, ya sea laboral o de cualquier otro tipo de los admitidos en derecho, comoposteriormente al finalizar dicha relación, especialmente en los casos contemplados en el artículo 10 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD).
12. En el caso de los datos de carácter personal serán, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre (LOPD), responsables de los datos tanto el responsable del fichero como el encargado del tratamiento.

13. El **contratista** informará al **S.A.S. - HRUCH,** antes de realizarlas, de todas las modificaciones que se vayan a hacer en la estructura de los ficheros que contengan datos de carácter personal, así como de la intención de suprimir o crear ficheros que contengan dicha clase de datos a fin de que el **S.A.S. - HRUCH,** como titular de dichos ficheros, pueda notificar con la debida antelación a la Agencia de Protección de Datos dichas variaciones.
14. Si a causa del incumplimiento por parte del **contratista** de lo regulado por la Ley, el **S.A.S. – HRUCH** fuese sancionado por la Agencia de Protección de Datos, dicha sanción será inmediatamente repercutida al contratista, debiendo ser abonada por este. Asimismo, resarcirá al **S.A.S. – HRUCH** por los daños y perjuicios que esta sanción, aparte de la multa, le hubiese ocasionado. En el caso de que no por haber sido debidamente informado fuese sancionado el **S.A.S. - HRUCH** por la Agencia de Protección de Datos, el contratista pagará la sanción que corresponda y asimismo resarcirá al **S.A.S. - HRUCH** por los daños y perjuicios que dicha omisión pudiera causarle.

c. Otras Empresas que trabajen para el LABORATORIO

Consideramos en este apartado a todas aquellas empresas que en principio no tratan información corporativa, pero que por sus características, pueden llegar a tener acceso a ella, como es el caso de empresas de limpieza, mantenimiento, etc.

i. Cláusulas a Incorporar en el Contrato

1. El **contratista** estará obligado a conocer, respetar y asegurar que se cumplan en el desarrollo de su trabajo, todas las normas, pautas, procedimientos, recomendaciones, etc., que se fijan en el Manual de Seguridad de la Información Corporativa, que tras la firma del contrato le será proporcionado por el Responsable de Seguridad correspondiente del **LABORATORIO**. (se le proporcionarán los aspectos del Manual que le hagan falta para el desarrollo de su labor).
2. El **contratista** se compromete a no aplicar, ni utilizar, los datos personales que se le hayan proporcionados para el desarrollo de su labor, para un fin distinto al que figura en el contrato.
3. El **contratista** y todo el personal que trabaje para él estarán sujetos al deber de confidencialidad en el ejercicio de sus funciones, cuando trabajen para el **LABORATORIO**., configurándose este deber como la prohibición de la revelación de datos de las personas que se conocen en virtud del ejercicio de la actividad que desempeñan.
4. El **contratista** no comunicará ningún tipo de datos, propiedad del **LABORATORIO.,** ni siquiera para su conservación, a otras personas o entidades.
5. El **S.A.S. - HRUCH** será el propietario de los datos que se traten en los diferentes servicios contratados.
6. Toda información, de carácter confidencial que el **S.A.S. - HRUCH** conozca, en virtud del contrato, acerca de las técnicas y metodologías empleadas por el **contratista** en la ejecución de estos servicios no podrá comunicarla a terceros ni emplearla en uso propio, respondiendo, en consecuencia, de los prejuicios que del incumplimiento de esta cláusula se pudieran derivar para el contratista.
7. El **contratista** no podrá trabajar para la competencia ni para quienes realicen actividades afines.
8. El **contratista** deberá incluir en los contratos que tenga establecidos con sus trabajadores una cláusula de confidencialidad por la que estos se comprometan a no revelar ni emplear en uso propio o de terceros la información que conozcan en función de su cometido tanto durante el tiempo que dure su contrato, ya sea laboral o de cualquier otro tipo de los admitidos en derecho, como posteriormente al finalizar dicha relación, especialmente en los casos contemplados en el artículo 10 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD).

9. **Procedimiento de Acceso al Sistema de Información**

OBJETIVO

Describir el control de acceso a la información corporativa implantado, garantizando que *los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones*. (Artículo 91.1 RD1720/2007).

DESCRIPCIÓN

a. Identificación y Autenticación

El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado (Artículo 93.2 RD1720/2007).

1. El Sistema de Información, que facilita el acceso a información corporativa, tendrá su acceso restringido mediante un código de usuario y una contraseña.

La contraseña es una serie arbitraria y secreta de caracteres que hay que suministrar para poder acceder a sistemas, subsistemas, aplicaciones, programas, funciones, etc.

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

2. Todos los usuarios autorizados para acceder a determinada información corporativa, deberán tener un código de usuario que será único, y que estará asociado a su contraseña individual correspondiente, que sólo será conocida por el propio usuario.

3. Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio o que ésta sea cambiada por el Administrador de Red/Sistemas.

4. Solamente, para aquellos casos excepcionales en los que sea necesario continuar con las funciones que realizaba la persona ausente (debido a una baja o ausencia temporal no prevista), el Subdirector del Centro, Área o Servicio o en caso de ficheros de carácter personal el Usuario Responsable de la Aplicación/Fichero, podrá solicitar a los administradores el acceso a sus datos, dejando constancia en el registro de Mantenimiento del Sistema de Información.

5. En el caso de que el Administrador de Sistemas solicite la contraseña/*password* para tareas de mantenimiento, la misma deberá ser cambiada inmediatamente después que se termine con dichas tareas.

6. Cada usuario tiene un perfil determinado. Introduciendo su usuario y contraseña podrá acceder al Sistema de Información del LABORATORIO donde estarán aquellas aplicaciones a las que tiene acceso en virtud del perfil asignado.

7. Tras tres intentos de acceso fallidos, por equivocación del usuario al introducir su clave, se bloqueará su cuenta durante un periodo de una hora. En caso de ser necesaria su activación inmediata se solicitará el desbloqueo al Administrador de Red/Sistemas/Base de Datos, por parte del propio usuario.

Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información (Artículo 18.2 RD 994/1999).

b. Características del Identificador de Usuario y Contraseña

Dependerá de las restricciones técnicas de los sistemas operativos y de las restricciones funcionales de cada aplicación.

a) El identificador de usuario y contraseña que tiene el conjunto de aplicaciones del Sistema Informatico del Laboratorio, consistee en lo siguiente:
    1) Permiso/No permiso (si se le concede permiso o no se le concede permiso para acceder como usuario)
    2) Perfil: Es el perfil de usuario (FEA, TEL, …)

3) Aplicación: Dependiendo del perfil de cada usuario, este podrá acceder a una aplicación u otra

El mecanismo de identificación es el siguiente:
Un usuario que quiera acceder al sistema de gestión del Laboratorio, tendrá que autenticarse introduciendo su login y su password. El password se encuentra encriptado.

a) Para el nombre de usuario se sigue la siguiente nomenclatura: Se cogen las primeras letras del nombre y los apellidos, en caso de nombre compuesto serán dos las iniciales del nombre. Si se encontrara repetido se añadiría un número secuencial que va desde 01 hasta 99.
b) El usuario es el encargado de ecribir la contraseña (password) la primera vez que entra en el sistema. Dicha contraseña tiene una configuración libre en número de caracteres alfanuméricos
c) Se recomienda cambiar de contraseña periódicamente

c. Altas de Usuarios

1. La solicitud de alta de un nuevo usuario en los Sistemas del Laboratorio se realizará a través de la página de la intranet del Laboratorio
Nunca, bajo ningún concepto, se dará de alta a un usuario mediante una solicitud telefónica.
2. La solicitud de alta de un nuevo usuario no perteneciente al Laboratorio (personal Asistencia especializa o Atención primaria) se realizará a través de la pagina WEB del Laboratorio.
Nunca, bajo ningún concepto, se dará de alta a un usuario mediante una solicitud telefónica.
3. En la solicitud deberán aparecer como mínimo los siguientes datos:
- Nombre
- Primer Apellido
- Segundo Apellido
- DNI
- CNP (codigo numérico personal)
- Centro de Trabajo o Servicio Médico

d. Bajas de Usuarios

1. Será función del Área de Recursos Humanos comunicar las bajas del personal del Laboratorio, a través de los registros de Mantenimiento del Sistema de Información, a fin de anular todos los permisos de acceso a la información corporativa.
Nunca se aceptará una notificación telefónica de baja de usuario.
2. Será función del responsable del personal subcontratado comunicar las bajas de su personal que presta servicios para el Laboratorio, a través de los registros de Mantenimiento del Sistema de Información, a fin de anular todos los permisos de acceso a la información corporativa.
Nunca se aceptará una notificación telefónica de baja de usuario.
3. En caso de usuarios que causen bajas temporales, o personal contratado por periodos se bloqueará la cuenta hasta la nueva alta del profesional.

e. Modificación de Permisos

1. Cualquier modificación en los permisos de acceso de un usuario a información corporativa deberá ser solicitado, por el responsable correspondiente de la información a la que afecte, en los registros de Mantenimiento del Sistema de Información.
2. En la solicitud de modificación de permisos deberán aparecer los siguientes datos:
- Nombre
- Primer Apellido
- Segundo Apellido
- DNI
- CNP (codigo numérico personal)
- Centro de Trabajo o Servicio Médico

3. En el caso de que la administración de algún recurso compartido (carpetas públicas, carpetas compartidas, etc.) esté delegada a su correspondiente responsable funcional (Usuario

Responsable de la Aplicación/Fichero) no hará falta el registro de la incidencia correspondiente haciéndose responsable de la correcta asignación de permisos al propio responsable.

f. Almacenamiento de Contraseñas

1. *Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad* (Artículo 93.3 RD 1720/2007).
2. *Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible* (Artículo 93.4 RD 1720/2007).
3. El Administrador de Sistemas/Red realizará el seguimiento y control del funcionamiento de la administración de contraseñas del sistema.

g. Auditoría de Permisos de Acceso

1. El Usuario Responsable de la Aplicación/Fichero comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados de su Área o Sede se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso a la información corporativa, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador, notificando toda variación (alta/baja/modificación) según se determina en apartados anteriores.
2. El Responsable de Seguridad comprobará, con una periodicidad al menos trimestral, que la lista de usuarios autorizados se corresponde con los usuarios que realmente deben estar autorizados para el acceso a la aplicación

ANEXO E. REFERENCIAS LEGALES

En el presente Anexo se relacionan las Leyes, Reales Decretos, Sentencias del Tribunal Constitucional, Instrucciones de la Agencia de Protección de Datos y cuantas normas se publiquen para el desarrollo de todos los aspectos contemplados en la Ley Orgánica 15/1999 (LOPD), de 13 de diciembre, de Protección de Datos de Carácter Personal.
En la actualidad todo el proceso normativo se encuentra en sus inicios, por lo que en los próximos años se desarrollarán, con normas de diferentes rangos, los aspectos de la LOPD anteriormente citados.
La publicación de las diferentes normas, en el futuro, podrá dar lugar a modificaciones en el presente Manual.

RELATIVA A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, que declara la inconstitucionalidad de algunos incisos correspondientes a los apartados del artículo 21.1 y 24.1de la LOPD.
- Real Decreto 1720/2007, 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.
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.
- Real Decreto 156/1996, de 2 de febrero, por el que se modifica el Estatuto de la Agencia de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, para designar a la Agencia de Protección de Datos como representante español en el grupo de protección de personas previsto en la Directiva 95/46/CE de 24 de octubre.
- Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las personas físicas en lo que respecta al Tratamiento de Datos Personales y a la libre circulación de estos datos.
- Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
- Instrucción 1/1998, de 19 de Enero, de La Agencia de Protección de Datos, relativa al Ejercicio de los Derechos de Acceso, Rectificación y Cancelación.
- Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.
- RESOLUCION de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía.

RELATIVO A LA LEGISLACIÓN SOBRE LA SALUD

- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y derechos y obligaciones en materia de información y documentación clínica.
- Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Seguridad Pública.
- Ley 14/1986, de 25 de abril, General de Sanidad.
- Ley 2/1998, de 15 de junio, de Salud de Andalucía.
- Ley 8/1986, de 6 de mayo, de creación del Servicio Andaluz de Salud *(en los aspectos vigentes).*
- Ley 2/1994, de 24 de marzo, de creación de la Empresa Pública de Emergencias Sanitarias de Andalucía.
- Decreto 88/1994, de 19 de abril. Empresa Pública de Emergencias Sanitarias. Estatutos.

ANEXO F ANEXO F BOJA NÚM. 200 DEL 13 DE OCTUBRE DE 2004

Con la extensión de las nuevas tecnologías en la Administración de la Junta de Andalucía, se ha puesto a disposición de sus trabajadores una serie de recursos informáticos, cuyo uso ha de ser realizado de forma ordenada y enfocado al desempeño de su actividad laboral. Por ello, es necesario poner en conocimiento de los empleados públicos cuál es el modo correcto de utilización de las nuevas tecnologías en el ámbito de la Junta de Andalucía, con el fin de que obtengan un uso más eficiente de las mismas en el desarrollo de sus tareas, lo que repercutirá positivamente en la gestión administrativa y en los servicios prestados al ciudadano, además de prevenir las prácticas abusivas que de una utilización particular de los medios informáticos públicos se pudieran producir, y sobre todo de aquéllas que puedan poner en riesgo la seguridad de los sistemas informáticos.

Considerando, igualmente, que se ha de garantizar la legalidad, eficacia y eficiencia de la utilización de los sistemas de información y la fluidez de las comunicaciones informáticas, internas y externas en la Administración de la Junta de Andalucía, así como la protección de las bases de datos que contengan datos personales de las ciudadanas y ciudadanos, para la gestión de los distintos procedimientos administrativos, y aquellos otros archivos sensibles para el funcionamiento de la Administración Andaluza, resulta necesario establecer las pautas de comportamiento de utilización de los sistemas y equipos informáticos por los empleados públicos.

Finalmente, también se ha de asegurar que el uso de los distintos programas informáticos se haga respetando las condiciones establecidas en sus licencias de uso, garantizando de esta manera los derechos de los proveedores que participan en el desarrollo informático de la Junta de Andalucía.

En virtud de las competencias atribuidas en el artículo7 del Decreto 200/2004, de 11 de mayo, por el que se establece la Estructura Orgánica de la Consejería de Justicia y Administración Pública, se aprueban las instrucciones contenidas en el Manual para usuarios de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía que se adjunta como Anexo a la presente Resolución.

Sevilla, 27 de septiembre de 2004.-El Secretario General para la Administración Pública, Pedro José Pérez González-Toruño.

ANEXO

MANUAL DE COMPORTAMIENTO DE LOS EMPLEADOS PUBLICOS EN EL USO DE LOS SISTEMAS INFORMATICOS Y REDES DE COMUNICACIONES DE LA ADMINISTRACION DE LA JUNTA DE ANDALUCIA.

1. Objeto.

1.1. Facilitar el máximo aprovechamiento de los medios informáticos en la actuación de la Administración de la Junta de Andalucía.

1.2. Asegurar la protección de los derechos de los ciudadanos en sus relaciones con la Administración, de las personas que tienen acceso a los recursos informáticos y de la propia Junta de Andalucía.

1.3. Mejorar los servicios que la Administración de la Junta de Andalucía presta a los ciudadanos, propiciando una gestión eficiente de los procesos incluidos en sus sistemas de información y redes de comunicaciones con las que opera.

1.4. Prevenir a los sistemas de información y a los datos a ellos incorporados de los riesgos o daños que puedan deberse a la acción humana, referente a conductas incorrectas o inadecuadas.

2.Definiciones.

A los efectos del presente Manual se entenderá por:

2.1. Administración de la Junta de Andalucía. Todos los servicios dependientes de la Administración de la Junta de Andalucía y de sus Organismos Autónomos. Asimismo, se consideran incluidas las empresas y otras entidades contempladas en los artículos 6 y 6 bis de la Ley 5/1983, de 19 de julio, General de la Hacienda Pública de la Comunidad Autónoma de Andalucía, cuando utilicen sistemas de información y/o redes de comunicación propiedad o bajo supervisión de la Administración de la Junta de Andalucía, como quedan definidas en este punto.

2.2. Redes de comunicación. Infraestructura de telecomunicación accesible por los usuarios, tanto de acceso a red interna o intranet como de acceso a red externa o extranet, correo electrónico e-mail o cualquier otro instrumento de transmisión telemática o acceso a la información, mediante la conexión de medios informáticos, que sean propiedad o estén bajo supervisión de la Administración de la Junta de Andalucía.
2.3. Usuarios. Será toda persona física que tenga autorizado el acceso a los sistemas de información o redes de comunicaciones de la Administración de la Junta de Andalucía.
2.4. Recursos informáticos. Todos los medios de cualquier naturaleza, físicos, lógicos humanos, que intervienen en los sistemas de información y en las redes de comunicaciones.
2.5. Aplicación informática. Programa o conjunto de programas informáticos que tienen por objeto el tratamiento electrónico de la información.

3. Ámbito de aplicación.
3.1. Las reglas que comprenden este Manual serán de aplicación a todas los usuarios, cualquiera que sea el nivel o función que ejerza.
3.2. Las reglas que comprenden este Manual serán de aplicación para todo uso de los sistemas de información y redes de comunicación de la Administración de la Junta de Andalucía.

4. Utilización de los equipos informáticos.
4.1. La Administración de la Junta de Andalucía será quién ponga a disposición de los usuarios los medios y equipos informáticos para el cumplimiento de sus obligaciones laborales. En consecuencia, dichos equipos informáticos no están destinados al uso personal o extraprofesional de los usuarios, por tanto, éstos deben conocer que no gozan del uso privativo de los mismos.
4.2. Los usuarios deberán destinar los equipos informáticos de que sean proveídos, a usos compatibles con la finalidad de las funciones del servicio al que se encuentren adscritos y que correspondan a su trabajo.
4.3. Los usuarios deberán cuidar los equipos informáticos que les sean facilitados, no procediendo a alterarlos o modificarlos.
4.4. Los usuarios no tienen permitido conectar a los equipos informáticos que se les provea, otros equipos distintos de los que tengan instalados.
4.5. Los usuarios en ningún caso podrán acceder físicamente al interior de los PC's que tengan asignados para el ejercicio de sus funciones, sólo personal autorizado podrá realizarlo para labores de reparación, instalación o mantenimiento.
4.6. Los usuarios sólo podrán usar equipos que estén directamente especificados por la Administración de la Junta de Andalucía.
4.7. Los usuarios deberán abstenerse de manipular los mecanismos de seguridad instalados en los PC's.

5. Utilización de las aplicaciones informáticas.
5.1. Los usuarios deben hacer uso exclusivamente de las aplicaciones informáticas o versiones de software instalados en sus equipos por la Administración de la Junta de Andalucía.
Además, están obligados a seguir las instrucciones o normas que la misma establezca para su empleo. En todo caso, la utilización de las aplicaciones informáticas tiene una finalidad profesional, es decir, destinadas a satisfacer las obligaciones laborales y con el propósito para el que fueron diseñadas e implantadas, por lo que no son idóneas para un uso personal o privado.
5.2. La Administración de la Junta de Andalucía será la responsable de configurar el sistema operativo, definir las aplicaciones informáticas de uso estandarizado y proceder a su instalación o desinstalación. Sólo tras autorización expresa, dada las características o naturaleza de las aplicaciones informáticas, podrán los usuarios efectuar directamente su instalación.
5.3. Los usuarios en ningún caso podrán borrar o desinstalar las aplicaciones informáticas legalmente instaladas por la Administración de la Junta de Andalucía.
5.4. Los usuarios se limitarán a ejecutar las aplicaciones informáticas para las que estén autorizados, que les serán facilitadas por la Administración de la Junta de Andalucía.
5.5. Queda prohibido expresamente la instalación de aplicaciones informáticas sin la correspondiente licencia o no adecuándose a la legislación vigente.
5.6. Las aplicaciones informáticas están protegidas por la propiedad intelectual, por lo tanto, queda terminantemente prohibido el uso, reproducción, modificación, transformación, cesión o

comunicación sin la debida autorización, con finalidad externa a la propia de la Administración de la Junta de Andalucía.
5.7. Queda prohibida cualquier actuación que pueda tener consideración de provocadora o intimidatoria en el trabajo, de tal manera, que debe excluirse la instalación o visualización de salvapantallas, fotos, vídeos, comunicaciones u otros medios con contenidos ofensivos, violentos, amenazadores, obscenos o, en general, aquellos que agredan la dignidad de la persona.
5.8. Los usuarios están obligados a cumplir las medidas de seguridad diseñadas por la Administración de la Junta de Andalucía, así como las prevenciones que al efecto se establezcan.
Por tanto, no podrán desactivar los programas antivirus ni sus actualizaciones. Tampoco podrán introducir voluntariamente programas, virus, macros o cualquier otro dispositivo lógico o secuencia de caracteres, que causen o sean susceptibles de causar alteración o daño en los recursos informáticos de la Administración de la Junta de Andalucía o en los de terceros.
5.9. Los usuarios están obligados a utilizar exclusivamente los programas antivirus y sus respectivas actualizaciones u otros sistemas de seguridad, destinados a la prevención de la entrada en los Sistemas de Información de cualquier elemento destinado a alterar o dañar los recursos informáticos, que sean instalados por la Administración de la Junta de Andalucía.

6. Utilización de la información incorporada a los sistemas.
6.1. Toda la información albergada en los servidores de la Administración de la Junta de Andalucía, o que circule a través de su red mediante elementos de comunicación o transmisión, que sean de su propiedad o le hayan sido confiada, tiene carácter confidencial.
6.2. Los usuarios están obligados a proteger la información, evitando el envío no autorizado al exterior, incluyendo esta noción tanto el acceso como la visualización de la misma.
Una especial consideración de confidencialidad corresponde a ficheros o información que contenga datos de carácter personal.
6.3. El conocimiento por los usuarios de la información reseñada en el punto 6.1, no confiere derecho alguno en cuanto a posesión, titularidad o derecho de copia de la misma, por lo que su uso debe ser estrictamente oficial y profesional.
6.4. Los usuarios con acceso a información y datos deben usarlos únicamente para las operaciones para las que fueron generados e incorporados, sin destinarlos a otros fines o incurrir en actividades que puedan considerarse ilícitas o ilegales. Asimismo, sólo deben acceder a aquellos datos y recursos que precisen para el ejercicio de las funciones que les correspondan, y efectuar sólo los tratamientos que sean precisos para el cumplimiento de los fines del servicio al que estén adscritos. Para ello, se dispondrá de perfiles de acceso y una segmentación conveniente, tanto de los usuarios como de las necesidades de información.
6.5. Los usuarios están obligados a proteger la información y los datos a los que tienen acceso. Esta protección debe prevenir el empleo de operaciones que puedan producir una alteración indebida, inutilización o destrucción, robo o uso no autorizado, en definitiva, cualquier forma que pueda dañar los datos, aplicaciones informáticas y documentos electrónicos propios de la Administración de la Junta de Andalucía.
6.6. Los usuarios, conforme a las instrucciones que reciban, utilizarán los medios o programas de salvaguarda que les facilite la Administración de la Junta de Andalucía, con la finalidad de garantizar la integridad y seguridad de los equipos informáticos, de las aplicaciones informáticas y de la información que contengan. En cualquier caso, no intentarán descifrar claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervengan en los procesos telemáticos.
6.7. Los usuarios están obligados a notificar cualquier incidencia o anomalía en el uso de los medios informáticos que detecten: pérdida de información, de listados o de disquetes, acceso no autorizado, uso de su identificador de usuario o de su contraseña, introducción de virus, recuperación de datos, desaparición de soportes informáticos y, en general, toda situación que pueda comprometer el buen uso y funcionamiento de los sistemas de información.
6.8. Cualquier fichero que se introduzca en la red corporativa o en el puesto de trabajo del usuario a través de soporte automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a la propiedad intelectual, el control antivirus y la protección de datos de carácter personal.
6.9. En aquellos casos en que sea posible se evitará la ubicación de ficheros que contengan datos de carácter personal en los PC’s de usuarios.

6.10. Los usuarios sólo podrán crear ficheros temporales que contengan datos de carácter personal, cuando sean necesarios para el desempeño de sus funciones, en todo caso, deberán ser eliminados cuando hayan dejado de ser útiles para la finalidad para la que fueron creados.
6.11. Toda salida de información que contenga datos de carácter personal, sea en: soportes informáticos, correo electrónico, portátiles, etc., sólo podrá realizarse por personal autorizado formalmente por el responsable del fichero, siempre cumpliendo la normativa vigente que garantiza los niveles de protección. Existirá un registro donde quede anotado las salidas y entradas de estos soportes.
6.12. Los usuarios autorizados a manejar soportes que contengan datos de carácter personal deben guardarlos en lugar seguro, especialmente finalizada la jornada laboral. En todo caso, una vez concluida la finalidad de las tareas a las que estaban destinados estarán obligados a su devolución inmediata.
6.13. Si un usuario finaliza su relación funcionarial o laboral, con la Administración de la Junta de Andalucía o se traslada de puesto de trabajo, deberá dejar sin perjudicar todas las aplicaciones informáticas, ficheros, información, datos y documentos electrónicos que haya utilizado en su actividad profesional.
6.14. Finalizada la relación funcionarial o laboral del usuario con la Administración de la Junta de Andalucía, dejará de tener acceso a los equipos informáticos y a la información incorporada a los mismos, debiendo devolver aquellos que se encuentren en su posesión. Seguirá obligado a mantener la máxima reserva y confidencialidad, no sólo de la información y documentos, sino también de las claves, análisis y aplicaciones informáticas.
6.15. Se dará a conocer a los usuarios los Documentos de Seguridad e instrucciones que fijen las normas de seguridad físicas y lógicas, donde se recojan las funciones y obligaciones de aquellos que tengan acceso a datos de carácter personal y, en todo caso, las consecuencias que conllevan su incumplimiento.

7. Acceso a la información.
7.1. Todo usuario con acceso a un sistema de información dispondrá de una única autorización de acceso, personal e intransferible, compuesta al menos de identificador de usuario y contraseña. Estos permitirán una identificación individual, evitándose registros duplicados o múltiples.
7.2. Los usuarios deben custodiar convenientemente su identificador de usuario y/o contraseña, sin proceder a su revelación o puesta al alcance de terceros. Serán responsables de toda la actividad relacionada con el uso de su acceso personal autorizado.
7.3. Las contraseñas tendrán plazo de vigencia, los usuarios procederán, siguiendo las instrucciones del responsable del sistema, a cambiarlas antes de cumplirse el mismo. Si transcurrido dicho plazo no se hubiesen cambiado caducarán denegándose el acceso, de oficio serán modificada, comunicándose la nueva posteriormente al usuario. El plazo de vigencia en ningún caso podrá ser superiora los 9 meses.
7.4. Si los usuarios sospechan que su acceso autorizado (identificador de usuario y/o contraseña) está siendo utilizado por otra persona, deberá proceder inmediatamente al cambio de contraseña y notificar la correspondiente incidencia.
7.5. Los usuarios no deben intentar obtener otros derechos de acceso al suyo personal, ni utilizar ningún otro acceso autorizado que corresponda a otro usuario, aunque disponga de la autorización de éste, salvo en los supuestos permitidos por la Ley o conforme a las instrucciones que imparta la Administración de la Junta de Andalucía.

8. Acceso a las redes de comunicación.
8.1. La conexión de los usuarios a las redes de comunicación será facilitada por la Administración de la Junta de Andalucía.
8.2. Queda prohibido conectarse a la red corporativa de comunicaciones por otros medios distintos a los definidos y administrados por la Administración de la Junta de Andalucía.
8.3. Queda prohibido conectarse a la red corporativa de comunicaciones con cualquier equipo informático distinto a los instalados para tal fin por la Administración de la Junta de Andalucía. El personal externo que deba conectarse a los entornos corporativos desde sus equipos requerirá la autorización y, en su caso, la supervisión del responsable de los sistemas de información pertinente.
8.4. Los usuarios tienen prohibido intentar obtener otros derechos o acceso distintos a los que tienen asignados. Asimismo, no deben intentar distorsionar o falsear los registros «logs» de los sistemas de información.

9. Acceso a Internet.

9.1. El acceso a Internet por los usuarios se realizará únicamente empleando los medios y a través de la red establecida a estos efectos por la Administración de la Junta de Andalucía. Por lo que no está permitido su acceso llamando directamente a un proveedor de servicio de acceso y
usando un navegador, o con otras herramientas de internet conectándose mediante un módem.

9.2. Las conexiones a Internet que se produzcan a través de la red corporativa tendrán una finalidad profesional. En este sentido, cada usuario autorizado empleará estas conexiones exclusivamente para el ejercicio de las tareas y actividades que corresponden a las funciones de su puesto de trabajo.

9.3. No deberá accederse en ningún caso a direcciones de internet que tengan un contenido ofensivo o atentatorio de la dignidad humana. A estos efectos, la Administración de la Junta de Andalucía podrá restringir el acceso a determinados servidores de contenidos en internet.

9.4. Las autorizaciones de acceso a internet se concederán acordes con las funciones del puesto que desempeñe el usuario, produciéndose una segmentación de perfiles que habilite las conexiones.

9.5. La Administración de la Junta de Andalucía regulará y controlará los accesos a internet. Se podrá proceder a monitorizar las direcciones de acceso y el tiempo de conexión de los usuarios a internet, así como la limitación de su uso en razón de las funciones que ejerza, por motivos de seguridad o rendimiento de la red.

9.6. La Administración de la Junta de Andalucía registrará todos los accesos a servidores de la red, incluyendo al menos la información de: direcciones de páginas visitadas, fecha y hora, ficheros descargados, usuario y puesto desde el que se ha efectuado la conexión.

9.7. Queda terminantemente prohibida la instalación de proxys por los usuarios.

9.8. Las transferencias de datos desde o a internet se realizarán exclusivamente cuando lo exija el ejercicio de las funciones del puesto de trabajo. En todo caso, los usuarios deberán tener en cuenta, antes de utilizar la información proveniente de la red, si dicho uso es conforme a las normas que protegen la propiedad intelectual e industrial.

10. Correo electrónico.

10.1. La Administración de la Junta de Andalucía suministrará a cada usuario una dirección individual de correo electrónico, procediéndole a instalar y configurar una cuenta de correo. El acceso a dicha cuenta de correo se efectuará mediante una clave personal.

10.2. Los usuarios tienen prohibido terminantemente el uso en las redes de comunicación de otras cuentas de correo electrónico distintas a las facilitadas por la Administración de la Junta de Andalucía.

10.3. El uso por los usuarios del correo electrónico habilitado por la Administración de la Junta de Andalucía es estrictamente profesional, es decir, para el ejercicio de las funciones que corresponde al puesto de trabajo que desempeñe.

10.4. Los usuarios tienen prohibido expresamente el acceso a cuentas de correos que no le hayan sido asignadas. Para que un usuario distinto pueda acceder a una cuenta de correo será preciso que el titular de ésta lo autorice por escrito, salvo los supuestos de cuentas de correo asociadas a puestos singulares.

10.5. Los usuarios no pueden interceptar, leer, borrar, copiar o modificar el correo electrónico dirigido a otros usuarios.

10.6. Queda prohibido para todos los usuarios el uso abusivo del correo electrónico, utilizando mensajes con contenidos ofensivos o atentatorios a la dignidad humana. Asimismo, queda prohibido el envío deliberado de cualquier clase de programa o virus que puedan causar perjuicios en los sistemas de información de la Administración de la Junta de Andalucía o a terceros.

10.7. Los usuarios tienen prohibido el uso abusivo del sistema de listas de correos para el envío de mensajes de forma masiva o piramidal.

10.8. Con la finalización de la relación funcionarial o laboral se interrumpirá el acceso a la cuenta de correo del usuario.

11. Del personal con responsabilidades en los sistemas de información.

Se encontrarán exceptuados de aplicar las instrucciones precedentes que interfieran en su cometido aquellas personas adscritas a puestos de trabajo que tienen funciones de diseño, desarrollo, operación o administración de los sistemas de información y de las redes de comunicación. Sólo se entenderán autorizados para el ejercicio de tales funciones cuando

sigan estrictamente las directrices de los responsables de la Administración de la Junta de Andalucía.
Además, deberán tener especial consideración con:
11.1. No acceder a la información o datos aprovechando sus privilegios de administración. Sólo podrán acceder previa autorización del responsable del fichero para el ejercicio de las funciones que le corresponda.
11.2. Custodiar con especial cuidado identificadores y contraseñas que den acceso a los sistemas con privilegio de administrador.
11.3. Procurar que la información almacenada y tratada por los sistemas de información sea salvaguardada mediante copias de seguridad y para la recuperación de datos periódicamente, al menos con carácter semanal, salvo que en dicho período no se haya producido actualización de los datos.
11.4. Que los soportes informáticos que contengan datos de carácter personal estén convenientemente registrados en un inventario actualizado, donde figure el tipo de información que contienen y las personas autorizadas a su manejo. Que se cumpla escrupulosamente el control de acceso restringido a personal autorizado en los locales, edificios o recintos en que se encuentren los sistemas de almacenamiento y servidores con información confidencial o con datos de carácter personal.
11.5. Notificar cualquier violación de las normas de seguridad o de vulnerabilidad de los sistemas de información que detecten, no revelando en ningún caso a terceros estas debilidades, excepto a la persona autorizada que reciba en el encargo de realizar los trabajos para su corrección.

12. El uso de certificados digitales.
Se recomienda, para garantizar la validez y eficacia de la emisión y recepción de comunicaciones y documentos producidos telemáticamente, el uso de la firma electrónica.

13. La comprobación de los sistemas de información y de las redes de comunicación.
La Administración de la Junta de Andalucía, mediante los mecanismos formales y técnicos que considere oportunos, podrá comprobar, de forma periódica o cuando resulte conveniente por razones específicas de seguridad o del servicio, la correcta utilización de todos los sistemas de información y redes de comunicación.

14. Las exigencias de responsabilidades.
La Administración de la Junta de Andalucía cuando detectare en el uso de los medios informáticos actuaciones irregulares, ilícitas o ilegales, procederá al ejercicio de las acciones pertinentes para las exigencias de las responsabilidades legales que correspondan.

15. Sobre el conocimiento de las instrucciones.
Todos los usuarios de los sistemas de información y redes de comunicaciones que sean propiedad o estén bajo la supervisión de la Administración de la Junta de Andalucía están obligados al conocimiento y cumplimiento de las presentes instrucciones.