Circular 1/2014, de 18 de agosto, del director general del Servicio de Salud de las Islas Baleares, por la que se aprueba el Código de buenas prácticas del Servicio de Salud en el uso de los sistemas de información y en el tratamiento de los datos de carácter personal

1. Los sistemas de información son elementos básicos para lograr los objetivos fundamentales encomendados al Servicio de Salud, por lo que los usuarios deben usar estos recursos de manera que se preserven siempre las dimensiones de la seguridad sobre la información manejada y los servicios prestados: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

2. El uso de recursos tecnológicos para tratar la información tiene una finalidad doble para el Servicio de Salud:

   a) Facilitar y agilizar la asistencia sanitaria de atención primaria, de atención especializada y de urgencia, así como tramitar los procedimientos administrativos usando herramientas informáticas y aplicaciones de gestión.

   b) Proporcionar información completa, homogénea, actualizada y fiable a los usuarios.

3. El uso del equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización del sector público. Estos medios y recursos se ponen a disposición de los usuarios como instrumentos de trabajo para desempeñar su actividad profesional, razón por la cual compete al Servicio de Salud determinar las normas, las condiciones y las responsabilidades bajo las que deben usarse tales recursos tecnológicos.

4. La Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, determina que los datos personales —especialmente los relativos a la salud de la ciudadanía— requieren establecer medidas técnicas y organizativas que garanticen una seguridad adecuada, de tal manera que eviten la alteración, la pérdida y el tratamiento de dichos datos o el acceso no autorizado a ellos.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

5. Por otra parte, el Real decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, determina la política de seguridad que debe aplicarse en el uso de los medios electrónicos a los que se refiere la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

6. Estos requerimientos se refuerzan con la obligación de garantizar una protección adecuada de los datos clínicos, derivada de aplicar la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que establece diversas previsiones con la finalidad de proteger la confidencialidad y la intimidad relativas a la información relacionada con la salud de la ciudadanía.

7. En el ámbito autonómico, la Ley 5/2003, de 4 de abril, de salud de las Islas Baleares, establece los derechos y los deberes de la ciudadanía en el ámbito sanitario, entre ellos el derecho a la intimidad y a la confidencialidad de los datos que hagan referencia a la salud.

8. Toda esta normativa hace necesario incorporar al uso de las tecnologías de la información y de la comunicación las prácticas que permitan garantizar un entorno seguro para el tratamiento adecuado de la información y que optimicen el uso de los recursos disponibles en la prestación de los servicios sanitarios.

9. El Gobierno de las Islas Baleares —mediante la Dirección General de Innovación y Desarrollo Tecnológico de la Consejería de Economía y Competitividad—, por medio del Decreto 6/2013, de 2 de mayo, del presidente de las Islas Baleares reconoce la importancia del uso de las tecnologías de la información y de las comunicaciones para cubrir las necesidades de información en las diferentes actividades de la organización, y pone de manifiesto la necesidad de velar por la seguridad de la información y de los recursos tecnológicos.

10. En este sentido, con el objetivo de mantener unos niveles adecuados de protección de la información y de los recursos informáticos, el Servicio de Salud de las Islas Baleares ha desarrollado las pautas necesarias para mantener las medidas de seguridad que garanticen que se cumple la

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

normativa vigente y que se usan de manera adecuada y eficiente los recursos en la prestación de los servicios sanitarios.

11. La Circular 4/2009, de 28 de abril, del director general del Servicio de Salud, aprobó por primera vez el Código de buenas prácticas en el uso de los sistemas de información y el tratamiento de los datos de carácter personal del Servicio de Salud.

12. De acuerdo con el Real decreto 3/2010 y a causa de la necesaria gestión de los recursos tecnológicos de manera que proporcionen una protección adecuada de la información y de los servicios; de la proliferación del uso de los dispositivos personales para fines profesionales, y de la aparición y la evolución de los servicios de almacenamiento en la nube, se considera oportuno aprobar una actualización del Código de buenas prácticas y dejar sin efecto la Circular 4/2009.

13. Este Código de buenas prácticas detalla las medidas —orientadas a los usuarios— que forman parte de la política de seguridad del Servicio de Salud, el cumplimiento de las cuales se considera imprescindible. Mantener los niveles adecuados de seguridad de la información depende en gran medida del hecho de que todos los usuarios apliquen estos criterios al desempeñar sus funciones y también de su compromiso, en primer lugar, de custodiar la información (especialmente los datos de carácter personal) contra el acceso, el uso o la divulgación no autorizados, la pérdida o la destrucción, y, en segundo lugar, de proteger los recursos informáticos utilizados para el tratamiento de esos datos del uso no autorizado, de la alteración, de la destrucción, del mal uso y del robo.

Por todo lo que se ha expuesto, de acuerdo con el artículo 21 de la Ley 3/2003, de 26 de marzo, de régimen jurídico de la Administración de la Comunidad Autónoma de las Islas Baleares, dicto la siguiente

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

CIRCULAR

1. Objeto

Esta circular tiene por objeto establecer las directrices y las recomendaciones en el uso de los sistemas de información a fin de optimizar el uso de los recursos disponibles y mantener la seguridad, la confidencialidad, la disponibilidad y la integridad de los datos de carácter personal, todo ello sin perjuicio de cumplir la normativa vigente.

2. Ámbito de aplicación

2.1. Todos los usuarios —tanto los empleados públicos como los adscritos a empresas externas— que tengan acceso a los sistemas de información del Servicio de Salud de las Islas Baleares y/o a los datos que figuren bajo la titularidad de este tienen que conocer y aplicar los requisitos y las instrucciones de este Código de buenas prácticas.

2.2. El Código es aplicable a todos los recursos —equipamiento físico, equipamiento lógico, servicios e información— usados por los usuarios para desempeñar sus funciones.

2.3. Es necesario garantizar la seguridad de la información a lo largo de todas las fases de su ciclo de vida (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción) y la de los sistemas que la soportan (análisis, diseño, desarrollo, implantación, explotación, integración y mantenimiento).

3. Definiciones

1) *Activo*: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye información, datos, servicios, aplicaciones (*software*), equipos (*hardware*), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

2) *Autenticación*: procedimiento de comprobación de la identidad de un usuario.

3) *Autenticidad*: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

4) *Caracterización del puesto de trabajo*: definición de las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad y los requisitos que deben cumplir los usuarios en términos de confidencialidad.

5) *Código maligno (*malware*)*: tipo de *software* que tiene como objetivo infiltrarse o dañar un equipo informático o sistema de información sin el consentimiento de su propietario.

6) *Confidencialidad*: propiedad o característica que consiste en no poenr información a disposición de personas, entidades o procesos no autorizados ni revelársela.

7) *Correo basura*: mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades y que perjudican de alguna manera al receptor.

8) *Datos de carácter personal*: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo relativa a personas físicas identificadas o identificables.

9) *Datos de carácter personal relacionados con la salud*: informaciones relativas a la salud pasada, presente y futura —física o mental— de una persona. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

10) *Dato disociado*: dato que no permite identificar a la persona afectada o interesada.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

11) *Disponibilidad*: propiedad o característica de los activos que consiste en que las entidades o los procesos autorizados tienen acceso a aquellos cuando lo requieren.

12) *Identificación*: procedimiento de reconocimiento de la identidad de un usuario.

13) *Incidencia*: cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.

14) *Integridad*: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

15) *Persona identificable*: toda persona cuya identidad pueda determinarse directa o indirectamente por medio de cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considera identificable si la identificación requiere plazos o actividades desproporcionados.

16) *Procedimiento de disociación*: todo tratamiento de datos personales que permita obtener datos disociados.

17) *Servicio de atención a los usuarios*: servicio que presta soporte informático y gestiona las incidencias de los usuarios con relación a las aplicaciones y a las infraestructuras informáticas.

18) *Sistema de información*: conjunto de ficheros automatizados, programas, soportes y equipos usados para almacenar y tratar datos.

19) *Tratamiento de datos*: operaciones y procedimientos técnicos de carácter automatizado (o no) que permitan recoger, grabar, conservar, elaborar, modificar, consultar, utilizar, cancelar, bloquear o suprimir y ceder datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

20) *Trazabilidad*: propiedad o característica que consiste en que las actuaciones de una entidad pueden imputarse exclusivamente a esta.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

21) *Usuarios*: todos los empleados públicos que prestan servicio en el Servicio de Salud y el personal de empresas externas que desarrolle tareas de manera permanente u ocasional en cualquier órgano perteneciente o adscrito al Servicio de Salud.

4. Información a los usuarios

4.1. Esta circular se pondrá a disposición de todo el personal del Servicio de Salud por medio de su sede electrónica y en la intranet corporativa. Así mismo, se enviará a todos los usuarios un mensaje de correo electrónico con los enlaces a la normativa.

4.2. En los manuales de bienvenida de las gerencias territoriales debe incorporarse el Código de buenas prácticas a fin de que las personas que se incorporen lo consulten antes de usar los recursos del Servicio de Salud.

4.3. Los órganos de dirección y de gestión del Servicio de Salud, estructurados en Servicios Centrales y en gerencias territoriales, son los responsables de hacer llegar esta norma a las empresas externas a fin de que sus usuarios la conozcan y la cumplan.

5. Confidencialidad de la información

5.1. Como medida de protección de la información propia, confiada o tratada por el Servicio de Salud, los usuarios deben abstenerse de comunicar dicha información, divulgarla, distribuirla o ponerla en conocimiento o al alcance de terceras personas (externas o internas no autorizadas) por medio de soportes informáticos o por cualquier otro medio que no haya sido autorizado previamente.

5.2. Todo el personal del Servicio de Salud y el personal ajeno que, por razón de su actividad profesional, haya tenido acceso a información gestionada por el Servicio de Salud (datos personales, documentos, metodologías, claves, análisis, programas...) debe mantener una absoluta reserva sobre ella durante tiempo indefinido.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

5.3. Si se tiene acceso en cualquier tipo de soporte a información que no sea de libre difusión, debe entenderse que el acceso es estrictamente temporal, mientras dure la función encomendada, que conlleva la obligación indefinida de secreto o de reserva y que ello no otorga derecho alguno de posesión, titularidad o copia de esa información. Asimismo, es imprescindible devolver los soportes de información usados inmediatamente después de que hayan terminado las tareas que hayan originado su uso.

5.4. Los usuarios solo pueden acceder a la información para la cual tengan la autorización debida y explícita dependiendo de las funciones que desempeñen, de tal manera que en ningún caso pueden tener acceso a información que pertenezca a otros usuarios o grupos de usuarios para el cual no tengan autorización.

5.5. Los derechos de acceso a la información y a los sistemas de información que la tratan deben otorgarse siempre de conformidad con los principios del mínimo privilegio posible y de la necesidad de conocer.

6. Protección de datos de carácter personal

6.1. Los usuarios con acceso a datos personales o a sistemas de tratamiento de datos están obligados a cumplir todas las medidas de seguridad establecidas y los requisitos y las condiciones aplicables de acuerdo con las normas y los procedimientos vigentes y los controles de seguridad establecidos. Así mismo, tienen el deber de utilizar la información a la que tengan acceso solamente para los fines relacionados con el desempeño de sus competencias y exclusivamente para su trabajo y sus funciones. Dichos usuarios podrían tener que responder del hecho de incumplir estas obligaciones de conformidad con el régimen jurídico aplicable.

6.2. En las Islas Baleares, la protección de los datos personales está regulada por Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal; por el Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

Reglamento de desarrollo de dicha Ley orgánica, y por el Decreto 90/2006, de 20 de octubre, que regula el procedimiento de elaboración de disposiciones generales de creación, modificación y supresión de ficheros que contienen datos de carácter personal en el ámbito de la Administración de la Comunidad Autónoma de las Islas Baleares.

6.3. Sobre la base de la legislación establecida, se han desarrollado los criterios siguientes sobre las normas que deben cumplir los usuarios con acceso a datos personales:

a) Solamente pueden crearse ficheros que contengan datos personales por medio de una disposición de carácter general publicada en el *Boletín Oficial de las Islas Baleares*.

b) Los ficheros de carácter personal deben cumplir las condiciones de seguridad establecidas por la legislación vigente.

c) Es fundamental que los usuarios con acceso a datos de carácter personal guarden un estricto secreto profesional por tiempo indefinido sobre cualquier información a la que tengan acceso al desempeñar su trabajo. Ello implica que esta obligación sigue vigente incluso después de que se haya extinguido su relación con el Servicio de Salud.

d) Los usuarios tienen el compromiso de no tratar los datos de carácter personal a los que tengan acceso, ni cederlos, ni comunicarlos, ni utilizarlos en beneficio propio, ni revelarlos a terceras personas, y el compromiso de respetar siempre la privacidad y la confidencialidad de dichos datos.

e) Los usuarios deben conocer los principios básicos de la Ley orgánica 15/1999 relativos al tratamiento de datos de carácter personal requeridos para desempeñar sus funciones. A continuación se detallan algunas consideraciones esenciales sobre dichos principios:

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

1) Todos los usuarios que tengan acceso a datos de carácter personal deben conocer la finalidad de usarlos y sus obligaciones particulares relativas al tratamiento requerido en el desempeño de su actividad profesional.

2) Los datos de carácter personal deben ser exactos y puestos al día de manera que respondan con veracidad a la situación actual de la persona interesada.

3) Los usuarios que tengan acceso a ficheros con datos de carácter personal deben extremar las precauciones para evitar la difusión o el acceso no autorizado de estos y para no tratarlos sin la autorización previa correspondiente de la persona responsable de los ficheros. Las cesiones de datos deben contar con habilitación legal y deben llevarse a cabo de conformidad con las medidas de seguridad aplicables, aunque es preferible —siempre que sea posible— comunicar solamente datos disociados o anónimos.

4) Debe accederse a la información que contenga datos de carácter personal solamente por medio de los procedimientos habilitados a tal efecto por el Servicio de Salud.

5) Cualquier requerimiento nuevo para el tratamiento de datos de carácter personal que sea identificado —fuera de la actividad prevista— debe analizarse y autorizarse previamente.

6) Todos los usuarios deben colaborar para satisfacer el ejercicio de cualquiera de los derechos de acceso, rectificación, cancelación y oposición, cuyo ejercicio se reconoce a las personas interesadas, atendiéndolas correcta y adecuadamente e informándolas sobre cuál es el procedimiento que deben seguir.

f) Quien tenga necesidad de generar ficheros temporales debe asegurarse de los aspectos siguientes:

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

1) Garantizar que el fichero cumple las finalidades de tratamiento autorizadas.

2) Cumplir todas las medidas de seguridad previstas de acuerdo con el nivel de seguridad definido para cada fichero.

3) Ubicar los ficheros temporales en las unidades ofimáticas (carpetas) asignadas a los usuarios por el personal de informática para garantizar los controles técnicos preestablecidos, y evitar ubicarlos en ordenadores personales siempre que sea posible.

4) Eliminar o destruir convenientemente los ficheros cuando dejen de ser necesarios para la finalidad para la que hayan sido creados.

g) Todo tratamiento que deba hacerse fuera de los sistemas de información del Servicio de Salud tiene que ser autorizado previamente y ha de cumplir las medidas necesarias para proteger la información.

h) Cuando se envíen por primera vez datos personales —en formato electrónico o impresos en papel—, hay que validar el método de envío a fin de garantizar que se cumplen las medidas de seguridad requeridas por el nivel del fichero.

i) Los sistemas de información que gestionen datos de carácter personal identificados como "de nivel alto" deben generar un registro de accesos, de conformidad con los artículos 96 y 103 del Real decreto 1720/2007, a fin de supervisar y controlar el tratamiento y el uso que se hace de ellos.

j) Los usuarios autorizados a gestionar soportes con datos de carácter personal deben guardarlos en un lugar seguro cuando no los usen, especialmente fuera de la jornada laboral. Adicionalmente, deben elaborar y mantener un inventario de

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

los soportes que estén bajo su custodia. En caso de que se desechen o reutilicen los soportes, deben impedir que se pueda recuperar posteriormente la información almacenada.

k) Para tratar documentación que contenga datos de carácter personal es necesario observar las directrices siguientes:

1) En la medida de lo posible, hay que evitar generar ficheros impresos en papel a partir de datos informatizados, siempre que no sea estrictamente necesario.

2) Hay que poner un cuidado especial en no dejar documentos impresos con datos de carácter personal o confidenciales en la bandeja de salida de impresoras ni en los faxes, para evitar que estén al alcance de personas no autorizadas. De la misma manera, hay que evitar hacer fotocopias de dichos documentos; si se hacen, hay que controlar el uso que se les da y destruirlas oportunamente.

3) Los documentos deben guardarse en cajones o en armarios bajo llave en los periodos de ausencia del puesto de trabajo.

4) Las listas impresas que contengan datos con información personal no deben desecharse en los contenedores de papel para reciclar. Cada usuario debe revisar periódicamente los documentos que estén bajo su custodia y destruir los que sean obsoletos. La documentación impresa o en soporte óptico que contenga datos de carácter personal que tenga que desecharse debe eliminarse con máquinas destructoras de papel o mecanismos similares, o de alguna manera que evite que los datos es puedan recuperar.

l) Cualquier incidencia o anomalía que pueda afectar a la seguridad de los datos personales debe comunicarse al servicio de soporte correspondiente siguiendo el procedimiento de comunicación y gestión de incidencias.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

7. Uso de los recursos informáticos

7.1. Pautas generales:

a) El Servicio de Salud pone a disposición de los usuarios el acceso a determinados recursos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, que facilitan el desempeño de su trabajo. Estos recursos son propiedad del Servicio de Salud; como tal, deben utilizarse para las labores propias de los usuarios de acuerdo con las funciones asignadas. Con carácter general, los recursos informáticos y dispositivos de comunicaciones deben utilizarse para fines institucionales y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.

b) El Servicio de Salud es el responsable de determinar las normas, las condiciones y las responsabilidades oportunas para proteger los recursos informáticos. Los usuarios con acceso a estos son responsables de custodiarlos y de protegerlos ante las posibles amenazas (accesos no autorizados, uso indebido, errores u omisiones, robo, etc.).

c) Para no comprometer las medidas de seguridad establecidas por el Servicio de Salud, los usuarios deben evitar las acciones siguientes (salvo que dispongan de la autorización previa correspondiente):

1) Usar equipos o aplicaciones que no estén especificados directamente como parte del soporte lógico o del soporte físico estándar del Servicio de Salud. En ningún caso se puede modificar la configuración establecida de los recursos ni intercambiar componentes o periféricos (teclados, pantallas, ratones, etc.) entre ordenadores.

2) Extraer equipos de los locales o de las instalaciones del Servicio de Salud, salvo que esté autorizado previamente.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

3) Hacer conexiones a redes o a sistemas externos o a la red corporativa por medios que no sean los definidos y administrados por el personal informático competente. En este sentido, hay que evitar especialmente establecer conexiones adicionales de manera independiente. También hay que evitar usar redes inalámbricas ajenas, pues pueden utilizarse para capturar información sensible o comprometer la seguridad de los sistemas que se conecten a ellas.

4) Extraer o utilizar información confidencial o datos de carácter personal en entornos que no estén protegidos o configurados adecuadamente para evitar el acceso no autorizado. Para exportar dichos datos a otros entornos hay que garantizar el nivel de seguridad correspondiente antes de extraerlos.

5) Trasladar fuera de las instalaciones habituales de trabajo datos o informaciones —en formato digital, impresos en papel o en cualquier otro soporte— sin la autorización previa correspondiente.

6) Destruir, alterar, inutilizar o dañar de cualquier otra manera los recursos informáticos, los programas, los datos, los soportes y los documentos.

7) Intentar descifrar las claves, los sistemas o los algoritmos de cifrado y cualquier otro elemento de seguridad establecido.

8) Modificar o desactivar los mecanismos de seguridad implantados para proteger los recursos informáticos y los sistemas de información.

9) Acceder a información que no sea necesaria para desempeñar las funciones de cada persona.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

10) Dejar los recursos de tratamiento de información desatendidos sin las medidas de bloqueo adecuadas o mantener soportes con información sensible en lugares poco seguros.

11) Disponer de permisos de administrador de los equipos sin la autorización previa correspondiente.

d) El uso del ordenador, del programa navegador y del correo electrónico o de cualquier otro recurso para algún fin particular debe ser autorizado previamente.

e) Está prohibido expresamente utilizar los recursos informáticos para las finalidades siguientes:

1) Almacenar información con contenidos de carácter racista, xenófobo, pornográfico, sexual, de apología del terrorismo o que atente contra los derechos humanos, o que actúe en perjuicio de los derechos a la intimidad, al honor y a la imagen propia o contra la dignidad de las personas.

2) Instalar y/o usar programas o contenidos que atenten contra la legislación en materia de protección de la propiedad intelectual.

7.2. Uso de unidades ofimáticas

a) Con carácter general, la información almacenada de manera local en los ordenadores y equipos informáticos de los usuarios no será objeto de salvaguarda por medio de ningún procedimiento corporativo de copia de seguridad. El Servicio de Salud puede hacer copias de seguridad de todos los activos y sistemas de información almacenados de manera local cuando disponga del conjunto de herramientas, medios y recursos para la generación de dichas copias.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

b) El Servicio de Salud puede poner a disposición de los usuarios unidades ofimáticas —que consisten en espacio de disco en red asignado a cada usuario por el personal técnico del Servicio de Salud— para contener las salvaguardas periódicas de sus unidades locales. Tales unidades corporativas no deben utilizarse para fines privados, ya que constituyen una herramienta de trabajo, tienen una capacidad limitada y son compartidas por todos los usuarios, por lo que solo debe salvaguardarse la información que se considere estrictamente necesaria. En particular, hay que evitar almacenar en estas unidades —incluso con carácter provisional o temporal— contenidos de gran tamaño, como archivos multimedia (música, vídeos, imágenes...).

7.3. Uso y mantenimiento de programas informáticos

a) Hay que evitar usar, instalar o distribuir programas fuera de las recomendaciones y de los estándares aprobados por el Servicio de Salud, ya que pueden comprometer la seguridad de los sistemas de información.

b) Si es necesario instalar programas ajenos al estándar establecido, hay que pedir autorización a la persona responsable del servicio, aunque es necesaria la valoración previa del servicio de informática.

c) La instalación de programas informáticos debe ser siempre a cargo del servicio de informática correspondiente o debe ser monitorizada por este a fin de asegurar que se cumplen las medidas de seguridad requeridas y que se cuenta con las garantías de soporte oportunas. En ningún caso se pueden eliminar o deshabilitar las aplicaciones informáticas instaladas por el servicio de informática, especialmente las relacionadas con la seguridad.

d) La instalación y el uso de programas debe hacerse de acuerdo con las licencias de uso adquiridas y controladas por el Servicio de Salud, por lo que está prohibido instalar programas sin la

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

licencia correspondiente. Se prohíben la reproducción, la modificación, la transformación, la cesión, la comunicación y el uso fuera del ámbito del Servicio de Salud de las aplicaciones y de los programas informáticos instalados en los equipos que pertenecen a la organización. Tampoco está permitido hacer copias de los programas instalados en los ordenadores.

e) Todo usuario debe facilitar al servicio de atención al usuario el acceso a su equipo para labores de reparación, instalación o mantenimiento. Dicho acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que puedan encontrarse en el uso de los recursos informáticos y de comunicaciones, y terminará una vez que se haya completado el mantenimiento o se hayan resuelto los problemas.

f) Si el personal de soporte técnico detecta cualquier anomalía que indique que los recursos se utilizan de manera contraria a lo que establece este Código, informará de ello a la Subdirección de la Oficina de Tecnologías de la Información y la Comunicación (OTIC), que tomará las medidas correctoras oportunas.

g) Los equipos informáticos de la organización deben mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Hay que prestar especial atención a la actualización, la configuración y el funcionamiento correctos de los programas antivirus y cortafuegos.

7.4. Conexión de dispositivos personales y almacenamiento en la nube

a) No se puede conectar en la red informática de comunicaciones corporativa ningún dispositivo distinto de los configurados, habilitados y admitidos por el Servicio de Salud, salvo que se disponga de la autorización previa correspondiente.

b) Los dispositivos personales usados en el ámbito del Servicio de Salud que accedan a sus redes y aplicaciones pueden ser

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

sometidos a actividades de prevención y control por el Servicio de Salud, aunque se limitarán a las áreas, las aplicaciones y los contenedores de información corporativa de los dispositivos personales en cuestión.

c) El nivel de seguridad de los dispositivos personales debe ser el mismo que el de los dispositivos móviles corporativos empleados.

d) El almacenamiento en la nube consiste en la disposición de aplicaciones, plataformas o infraestructura que, a cargo de un proveedor o del propio Servicio de Salud, están accesibles por medio de Internet, independientemente de dónde estén alojados los sistemas de información, y de manera transparente para el usuario final.

e) Con carácter previo al uso de estos recursos externos, la Subdirección de la OTIC debe establecer las características del servicio prestado y las responsabilidades de las partes, detallando lo que se considera calidad mínima del servicio prestado y las consecuencias de incumplirlo.

f) No está permitido transmitir o alojar información sensible, confidencial, datos de carácter personal o información protegida propia del Servicio de Salud en servidores externos o soluciones de almacenamiento en la nube, salvo que se disponga de la autorización previa correspondiente. Debe comprobarse que no haya trabas legales para ello y verificar la suscripción de un contrato expreso entre el Servicio de Salud y la empresa responsable de la prestación del servicio, incluyendo los acuerdos de nivel de servicio que sean procedentes, el correspondiente acuerdo de confidencialidad, y siempre habiendo analizado previamente los riesgos asociados.

7.5. Control de códigos malignos y otros programas maliciosos

a) El código maligno es un tipo de *software* que tiene como objetivo infiltrarse en un equipo informático o sistema de

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

información o dañarlo sin el consentimiento de su propietario. La introducción de código maligno en los sistemas de información del Servicio de Salud puede originarse al visitar páginas web infectadas, al abrir mensajes de correo electrónico o al ejecutar un programa contaminado o un fichero infectado (procedente de un disco duro externo, una memoria USB, un CD-ROM, etc.). El usuario debe ser consciente de las amenazas que ello provoca; por tanto, es imprescindible que haga un uso responsable de los equipos para reducir este riesgo.

b) Todos los puestos de trabajo del Servicio de Salud deben tener instalados y activados los mecanismos adecuados para prevenir y detectar infecciones de programas maliciosos. Bajo ninguna circunstancia deben desactivarse esos mecanismos; no obstante, hay que tener en cuenta que no garantizan la protección contra las amenazas, por lo que de manera general hay que actuar con cautela y sentido común:

1) Ante la sospecha de una infección con un código maligno, virus, gusanos, etc., hay que comunicar la incidencia de acuerdo con el procedimiento de comunicación y gestión de incidencias correspondiente.

2) Hay que adoptar todas las precauciones posibles al ejecutar cualquier programa, incluso los procedentes de fuentes consideradas de confianza, dado que pueden haber sido suplantados.

3) Hay que evitar ejecutar archivos adjuntos recibidos por correo electrónico y visitar páginas web con contenidos de legalidad o moralidad dudosas, pues son una fuente habitual de infecciones.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

8. Medidas de seguridad

8.1. Medidas de seguridad de acceso físico

a) La información confidencial o con datos de carácter personal (en CD-ROM, en dispositivos de almacenamiento, en archivos visibles directamente en la pantalla del ordenador) debe custodiarse para evitar accesos no autorizados.

b) No debe mantenerse la información en sitios a la vista sin el control de la persona responsable en ese momento. En caso de ausencia, es necesario establecer mecanismos que impidan el acceso de personas no autorizadas a esa información, de acuerdo con las características del puesto de trabajo y del soporte en el que esté la información.

c) Adicionalmente, las pantallas deben orientarse de tal manera que se elimine en la medida de lo posible el ángulo de visión a las personas no autorizadas.

8.2. Medidas de seguridad de acceso lógico

a) El control de acceso a los sistemas de información está basado en el uso de identificadores de usuario y contraseñas ligadas a los perfiles de acceso. Estos perfiles han sido establecidos de acuerdo con las funciones que desempeña cada usuario.

b) El identificador de usuario y la contraseña correspondiente que se asignan al personal que los requiera son confidenciales, personales e intransferibles. Por tanto, es responsabilidad de la persona titular el uso que se haga de ellos.

c) Cada usuario debe velar por la confidencialidad de su contraseña; en ningún caso debe guardarla en archivos digitales ni escrita en papel o en cualquier otro tipo de soporte de manera legible o accesible. Tampoco puede comunicar a otra persona su identificador de usuario ni su contraseña, ni debe usar una sesión abierta bajo otra identidad.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

d) Si un usuario sospecha que su contraseña ha sido conocida de manera fortuita o fraudulenta por personas no autorizadas, debe modificarla y notificar la incidencia al servicio de soporte correspondiente.

e) Cada usuario debe cambiar su contraseña de acceso a los sistemas al menos una vez al año y siempre que se lo indique la persona encargada de la gestión de usuarios.

f) Si, en un momento dado, un usuario recibe una llamada telefónica o un mensaje de correo electrónico en el que se le solicita su nombre de usuario y/o su contraseña, nunca debe facilitar dichos datos y tiene que comunicar inmediatamente la incidencia al servicio de atención al usuario.

g) Cuando un usuario finalice su relación o vinculación con el Servicio de Salud, la persona directamente responsable del usuario debe comunicar esta nueva situación a la persona encargada de la gestión de usuarios para que dé de baja las cuentas y las autorizaciones que tenga. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por el Servicio de Salud estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tiene que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

8.3. Uso de otros mecanismos de identificación y autenticación

a) Todos los accesos a los sistemas que contengan información deben disponer de un mecanismo de identificación y autenticación que garantice la seguridad de acceso al sistema. Este mecanismo está basado normalmente en el uso de identificadores de usuario y contraseñas, aunque en otros casos puede basarse en otros mecanismos más sofisticados (como los certificados digitales, que aumentan el grado de confianza).

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

b) El avance en la aplicación de los algoritmos criptográficos y en la certificación digital permite aplicar informáticamente procedimientos que tradicionalmente se han aplicado manualmente, con lo que se establecen garantías equivalentes respecto a la autenticación de la identidad de los actores y a la confidencialidad, la integridad y el no repudio de la información tratada.

c) El uso de esos algoritmos requiere que el usuario use un certificado digital, cuya autenticidad e integridad están garantizadas por un tercero de confianza. En este caso, el usuario debe observar las pautas siguientes:

1) En el uso del servicio, el usuario debe aplicar las prácticas establecidas por el Servicio de Salud y por la entidad prestadora de servicios de certificación que sean necesarias para garantizar la validez de las transmisiones electrónicas emitidas y recibidas.

2) El usuario debe comunicar cualquier variación de los datos aportados para obtener el certificado a la entidad prestadora de servicios de certificación y/o registro.

3) El usuario debe salvaguardar sus claves privadas aplicando las pautas descritas en el apartado 8.2 de este Código y ha de proteger cualquier elemento (tarjeta o dispositivo criptográfico, archivo informático, programa, PIN, contraseña, etc.) que pueda ser necesario para acceder a esas claves.

4) El usuario debe comunicar inmediatamente cualquier incidencia que afecte a la seguridad de la clave privada o de los elementos y/o los códigos utilizados para acceder a ella, y debe hacerlo de acuerdo con los procedimientos establecidos por la entidad prestadora de servicios de certificación y/o registro.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

8.4. Puesto de trabajo despejado

a) Con carácter general, los puestos de trabajo deben estar despejados, sin más material encima de la mesa que el que se requiera para la actividad que se haga en cada momento.

b) En particular, cuando un usuario del Servicio de Salud con acceso a los sistemas de información abandone su puesto de trabajo debe guardar toda la información que esté tratando, de manera que no queden desatendidos memorias USB o soportes externos de información, listas o información visible en la pantalla del ordenador personal o documentación sobre el propio puesto de trabajo. El material de trabajo debe guardarse en un lugar cerrado (en un cajón o un armario bajo llave) o en un cuarto separado cerrado con llave, al menos fuera del horario de trabajo.

c) Se puede establecer un procedimiento para revisar que se cumple esta medida haciendo una inspección regularmente después del cierre, notificando los incumplimientos detectados y retirando el material olvidado en un lugar cerrado.

8.5. Bloqueo del puesto de trabajo

a) Todos los terminales, ordenadores personales y dispositivos móviles usados por los usuarios del Servicio de Salud con acceso a la información en el desempeño de sus funciones deben ser bloqueados convenientemente por el usuario antes de abandonar su puesto de trabajo, tanto momentáneamente como al final de la jornada laboral.

b) Asimismo, debe bloquear el puesto de trabajo al cabo de un tiempo de inactividad, establecido por la política de seguridad, que es parte de la configuración del equipo y no puede ser alterado por el usuario.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

9. Acceso por medio de redes

9.1. En el acceso y el uso de las redes implantadas en los diferentes centros del Servicio de Salud, todo usuario debe cumplir las normas de seguridad establecidas.

9.2. El acceso a las redes internas debe llevarse a cabo exclusivamente por los medios implantados corporativamente, por lo que no está permitido utilizar cualquier otro medio de conexión con redes externas sin la autorización previa correspondiente.

9.3. Para usar la red son necesarias las credenciales de acceso (generalmente un identificador y una contraseña), que se asignan solamente a los usuarios autorizados. La custodia de esas credenciales es responsabilidad del usuario autorizado, por lo que debe observar lo que disponen los apartados 8.2 y 8.3 de este Código.

9.4. Cualquier conexión remota que se vaya a habilitar —a petición de un usuario interno o de un proveedor externo— debe tener la autorización previa de la persona responsable correspondiente y la validación del servicio de informática, a fin de garantizar los niveles de seguridad requeridos.

10. Uso de Internet

10.1. Internet debe ser accesible exclusivamente a los usuarios que lo necesiten para desempeñar sus funciones, a quienes se proveerá de permisos de acceso.

10.2. En el uso de Internet, el usuario debe ser consciente de que al desempeñar sus funciones laborales está representando al Servicio de Salud; consiguientemente, se compromete a reflejar en su conducta la ética, la profesionalidad, la cortesía y la responsabilidad que se espera de los usuarios que están adscritos a este organismo.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

10.3. Debido a la necesidad de optimizar los recursos disponibles, el acceso a Internet debe responder a fines profesionales. El Servicio de Salud velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y de la productividad de los usuarios como desde el punto de vista de los riesgos de seguridad asociados al uso de Internet.

10.4. Sin perjuicio de lo que prevé el apartado 6.3.*d* con relación a las cesiones, hay que evitar enviar datos de carácter personal por medio de Internet. En cualquier caso, la transferencia solamente se puede efectuar usando los mecanismos que garanticen la ininteligibilidad y la integridad de los datos, y con la autorización previa correspondiente.

10.5. En general, la información transmitida por Internet no circula de manera cifrada. Sin embargo, en la transmisión de información sensible, confidencial o protegida es importante asegurar que sí lo esté. Una manera de asegurar la confidencialidad es comprobar, observando la barra de direcciones del navegador, si en la comunicación se utiliza el protocolo HTTPS ("protocolo seguro de transferencia de hipertexto") en vez del protocolo estándar HTTP ("protocolo de transferencia de hipertexto"). También debería aparecer un icono con forma de candado en alguno de los menús del navegador; haciendo clic en dicho icono se obtiene información sobre el certificado digital de identidad del sitio web visitado.

10.6. No deben usarse navegadores ni programas de correo electrónico —ni versiones de estos— que no estén previstos por los estándares en vigor. Tampoco se puede modificar la configuración de esos programas en los aspectos relacionados con la seguridad.

10.7. Hay que notificar al correspondiente servicio de atención al usuario cualquier anomalía detectada en el uso del acceso a Internet y cualquier sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

10.8. Se consideran como uso incorrecto del servicio los casos siguientes:

a) Acceder a sitios de Internet o distribuir mensajes con contenidos en que se incite o se promueva la pornografía o la segregación racial, sexual o religiosa, o con contenidos de violencia.

b) Descargar y transmitir indiscriminadamente imágenes, sonido y vídeos, ya que su tamaño satura el ancho de banda y disminuye la velocidad de transmisión, lo cual perjudica a otros usuarios. Se prohíbe expresamente usar utilidades de intercambio de información en Internet, como las redes de igual a igual (P2P, "*peer-to-peer*").

c) Distribuir virus o troyanos o llevar a cabo cualquier actividad a fin de acceder ilícitamente a otros sistemas de información con el objetivo de interceptar, dañar o manipular la información para obtener un beneficio personal, por diversión o para beneficiar o perjudicar a terceras personas.

d) Llevar a cabo por medio de Internet cualquier actividad ilegal o maliciosa que ocasione molestias o daños a segundas o a terceras personas dentro o fuera del Servicio de Salud.

e) Hacer un uso inadecuado de cualquier material multimedia con derechos de la propiedad intelectual.

f) Utilizar el acceso a Internet para usar sistemas de mensajería instantánea (Skype, Messenger, Hangout, etc.) y/o transferir archivos no relativos a las actividades profesionales del usuario (juegos, ficheros de sonido, fotos, vídeos o películas...).

g) Publicar en Internet información relacionada con el Servicio de Salud, salvo que se disponga de la autorización previa correspondiente. En este sentido, los usuarios se comprometen a garantizar la privacidad de los datos y de las contraseñas de acceso y evitar difundirlos.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

h) Llevar a cabo cualquier actividad de promoción de intereses personales.

10.9. Por motivos de seguridad y de rendimiento de la red del Servicio de Salud, los servicios informáticos pueden monitorizar y limitar el uso de Internet. El sistema que proporciona el servicio de navegación puede disponer de filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o códigos malignos. Igualmente, el sistema puede registrar y dejar traza de las páginas a las que se haya accedido y del tiempo de acceso y del volumen y el tamaño de los archivos descargados. El sistema permite establecer controles que posibiliten detectar y notificar usos prolongados e indebidos del servicio.

11. Uso del correo electrónico y de la agenda

11.1. El correo electrónico y la agenda proporcionados por el Servicio de Salud están destinados al uso profesional, ya que son herramientas de trabajo. Cualquier uso particular debe tener la autorización previa correspondiente y debe ser puntual y limitado en frecuencia y en duración. Se trata de un recurso compartido por todos los usuarios de la organización, por lo que un uso indebido repercute de manera directa en el servicio ofrecido a todos.

11.2. En ningún caso el uso autorizado para fines personales puede constituir una actividad comercial o con ánimo de lucro ni puede ser inapropiado u ofensivo. Se aconseja evitar también las actividades que exijan o aconsejen una privacidad especial, dadas las obligaciones del Servicio de Salud en cuanto a monitorización —según se desprende del apartado 14—, sin perjuicio del respeto estricto al derecho a la intimidad y al secreto de las comunicaciones.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

11.3. El servicio de correo electrónico corporativo solamente debe usarse a través de los medios y las herramientas tecnológicas autorizados debidamente por el servicio de informática correspondiente.

11.4. Todo usuario autorizado para usar el correo electrónico y la agenda es responsable del uso que haga de ellos. Debe decirse que dispone de una capacidad de almacenamiento limitada, por lo que debe eliminar los mensajes que no sea necesario mantener almacenados.

11.5. El correo electrónico es un medio de comunicación interpersonal, no un medio de difusión masiva e indiscriminada de información. Debe evitarse toda práctica que pueda poner en riesgo el funcionamiento y el buen uso del sistema.

11.6. Está expresamente prohibido leer, borrar, copiar o modificar mensajes de correo electrónico o archivos dirigidos a otros usuarios, y revelar a terceras personas el contenido de cualquier dato reservado o confidencial que sea propiedad del Servicio de Salud o de terceras personas, salvo que tal actuación se lleve a cabo para cumplir fines estrictamente profesionales, con el consentimiento previo de las personas afectadas.

11.7. En ningún caso las comunicaciones hechas en el desempeño de las tareas profesionales deben enviarse desde cuentas de correo electrónico personales ofrecidas por proveedores de Internet. Tampoco está permitido en ningún caso redirigir a cuentas particulares mensajes de correo electrónico de carácter profesional recibidos en la cuenta proporcionada por el Servicio de Salud.

11.8. Cuando se reenvíen correos electrónicos que hayan sido dirigidos a varios destinatarios, hay que evitar difundir las direcciones de correo electrónico de los destinatarios del mensaje original borrando esa información del mensaje reenviado, si es necesario.

11.9. Con carácter general, hay que evitar enviar información de carácter personal con datos de salud por medio del correo electrónico. Si es necesario hacer un envío de ese tipo, los datos deben ser cifradas.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

11.10. Antes de abrir un mensaje de correo electrónico, hay que intentar detectar si se trata de un mensaje de procedencia dudosa o desconocida analizando su cabecera. En caso de duda, hay que borrar los mensajes sospechosos sin abrirlos o bien consultar al soporte técnico.

11.11. Para evitar el correo masivo no solicitado —denominado "correo basura" o, en inglés, *spam*—, como regla general solamente hay que facilitar la dirección de correo electrónico a personas conocidas. No se puede introducir la dirección de correo electrónico en foros o páginas web no institucionales. Cuando se reciban correos electrónicos desconocidos o no solicitados no hay que contestarlos, ya que al hacerlo se confirma la dirección.

11.12. Adicionalmente, se consideran como uso inadecuado del servicio de correo electrónico los casos siguientes:

a) Propagar contenido de carácter racista, xenófobo, pornográfico, sexual, de apología del terrorismo o que atente contra los derechos humanos, o que actúe en perjuicio de los derechos a la intimidad, el honor y la imagen propia o contra la dignidad de las personas.

b) Difundir mensajes de correo electrónico sin identificar plenamente al remitente. Si la cuenta de correo es usada por grupos de usuarios, hay que identificar al autor.

c) Divulgar mensajes comerciales o propagandísticos sin la autorización previa correspondiente.

d) Hacer circular cartas encadenadas y participar en esquemas piramidales o en actividades similares.

e) Utilizar el servicio con el objetivo de degradar el Servicio de Salud.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

f) Enviar masivamente mensajes o información que consuman injustificadamente recursos tecnológicos.

g) Manipular la cabecera de los mensajes para intentar falsear u ocultar la identidad del remitente.

h) Instalar o emplear servidores o servicios de correo que no tengan la autorización previa correspondiente.

11.13. El sistema que proporciona el servicio de correo electrónico puede, de manera automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento del Código de buenas prácticas. Se puede insertar contenido adicional en los mensajes enviados para advertir a los receptores sobre los requisitos legales y de seguridad que deben cumplir con relación a dichos correos.

11.14. El uso de agendas telefónicas como herramienta de trabajo está sujeto al contenido y a los criterios de uso siguientes, ya que contienen información de carácter personal:

a) Los contenidos en las agendas corporativas solamente deben incluir la información siguiente:
1) nombre y apellidos
2) función o puesto de trabajo
3) direcciones postal o electrónica profesionales
4) números de teléfono y de fax profesionales

b) El uso de las agendas debe ser exclusivamente el correspondiente a los contactos requeridos con la persona interesada y solamente para los fines solicitados por esta.

12. Comunicación de incidencias de seguridad

12.1. El uso adecuado de los recursos informáticos evita que se produzcan incidentes que puedan ir en detrimento de la seguridad de la información, a la vez que garantiza un rendimiento óptimo.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

Por ello, cuando se detecten incidentes que puedan afectar a la seguridad de la información, es responsabilidad del Servicio de Salud llevar a cabo las actuaciones que se consideren convenientes y proporcionales para prevenir y/o corregir los riesgos identificados, por medio de la monitorización y el análisis de los recursos afectados para asegurar que se usan de la manera apropiada y para preservar la seguridad de los sistemas del Servicio de Salud.

12.2. Todo usuario debe informar de los incidentes que, a su juicio, puedan afectar a la seguridad de los activos del Servicio de Salud, mediante el servicio de soporte correspondiente. Debe indicar todos los detalles observados que le hayan llevado a la sospecha y prestar la colaboración necesaria para resolver la incidencia.

12.3. Asimismo, los usuarios deben colaborar para mantener actualizadas las aplicaciones, pues su colaboración es imprescindible para adaptar los sistemas a los requisitos de cada momento. Para ello, los usuarios deben comunicar por el cauce oportuno cualquier deficiencia que observen o cualquier mejora que consideren oportuna.

12.4. Cuando una incidencia y/o deficiencia pueda causar un impacto grave en el funcionamiento del servicio sanitario, el usuario —de acuerdo siempre con el servicio de soporte correspondiente— debe adoptar las medidas de urgencia oportunas. Debe informar en detalle sobre los hechos acontecidos y las medidas adoptadas para que se registren y evalúen con la finalidad de aplicar las acciones necesarias.

13. Finalización de la vinculación o relación con el Servicio de Salud

13.1. Cuando un usuario finaliza su relación o vinculación con el Servicio de Salud deja de tener acceso a los sistemas de información del Servicio de Salud y a los datos que contienen. Asimismo, tiene que devolver cualquier soporte que posea y que contenga datos a los que haya tenido acceso en el marco de su vinculación o relación con el Servicio de Salud.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

13.2. También debe ceder el control sobre cualquier fichero o documento relativo a su prestación profesional; en caso que haya creado ficheros o documentos de carácter no profesional, debe eliminarlos.

14. Monitorización y aplicación del Código

14.1. Por motivos legales, de seguridad y de calidad del servicio, y a fin de cumplir siempre los requisitos que al efecto establece la legislación vigente, de conformidad con el artículo 23 del Esquema Nacional de Seguridad, el Servicio de Salud llevará a cabo las acciones siguientes:

a) Revisará periódicamente el estado de los equipos, las aplicaciones instaladas, los dispositivos y las redes de comunicaciones que sean responsabilidad suya.

b) Monitorizará los accesos a la información contenida en sus sistemas.

c) Auditará la seguridad de las credenciales y de las aplicaciones.

d) Monitorizará los servicios de Internet y de correo electrónico y otras herramientas de colaboración.

14.2. El Servicio de Salud llevará a cabo esta actividad de monitorización sin utilizar sistemas o programas que puedan atentar contra los derechos constitucionales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, y mantendrá siempre la privacidad de la información manejada, salvo que sea necesario acceder a dicha información (salvaguardando siempre los derechos fundamentales de los usuarios) por un requerimiento legal o una investigación sobre un uso ilegítimo o ilegal; para vigilar y controlar el cumplimiento de obligaciones; para controlar los medios informáticos; para coordinar la continuidad laboral; para proteger el sistema

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

informático, y para prevenir responsabilidades frente a terceras personas.

14.3. Los sistemas en los que se detecte un uso inadecuado o que no se cumplen los requisitos mínimos de seguridad pueden ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de la inseguridad o de la degradación desaparezca. La Subdirección de la OTIC —con la colaboración de las restantes unidades del Servicio de Salud— velará para que se cumpla el Código de buenas prácticas e informará sobre los incumplimientos o las deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

15. Cumplimiento del Código

15.1. Todos los usuarios del Servicio de Salud deben cumplir el Código de buenas prácticas.

15.2. Adicionalmente, los requisitos y las previsiones descritos en el Código se complementan con el resto de la normativa vigente y con cualquier disposición legal de ámbito estatal o comunitario aplicable.

15.3. El incumplimiento de cualquiera de las pautas de comportamiento establecidas en el Código puede dar lugar a la responsabilidad disciplinaria correspondiente en aplicación de las normas reguladoras del régimen jurídico propio del usuario.

15.4. El uso de los recursos informáticos que el Servicio de Salud pone a disposición de los usuarios implica el conocimiento y la aceptación plena de las normas de uso, de las condiciones y de las advertencias legales que se especifican en el Código.

16. Difusión y publicación

Esta circular tiene que publicarse en la sede electrónica del Servicio de Salud y en otros medios que su órgano de dirección considere oportunos.

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605

17. Efectos

Queda sin efectos la Circular del director general del Servicio de Salud de las Islas Baleares 4/2009, de 28 de abril de 2009, por la que se aprueba el Código de buenas prácticas en el uso de los sistemas de información y el tratamiento de los datos de carácter personal del Servicio de Salud.

Palma, 18 de agosto de 2014
El director general
Miquel Tomàs Gelabert

C/ Reina Esclarmunda, 9. 07003 Palma
Tel.: 971 175 600. Fax: 971 175 605