I. COMUNIDAD DE MADRID

C) Otras Disposiciones

Consejería de Sanidad

12 *ORDEN 491/2013, de 27 de junio, por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica y de los sistemas de información de la Consejería de Sanidad de la Comunidad de Madrid.*

La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, consagra el derecho de los ciudadanos a comunicarse electrónicamente con la Administración Pública, asimismo, manifiesta la necesidad de una adecuada protección de la información y de los servicios que permitan usar los medios electrónicos con confianza. Con la intención de dar respuesta a esta necesidad se publicó el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) en el ámbito de la Administración Electrónica, que obliga a la Administración Pública a adoptar cuantas medidas de seguridad técnicas y organizativas sean precisas para hacer efectivas estas condiciones de seguridad.

El Real Decreto 3/2010, de 8 de enero, enuncia en sus artículos 4 a 10, los principios básicos que deben regir en materia de seguridad (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica y función diferenciada), para continuar señalando los requisitos mínimos que debe reunir la política de seguridad de la información, estableciendo la obligación que tienen todos los órganos superiores de la Administración Pública de disponer formalmente de su política de seguridad de la información, que se plasma en un documento, accesible y comprensible para todos los miembros que define lo que significa seguridad de la información en una organización determinada y que rige la forma en que una organización gestiona y protege la información y los servicios que considera críticos. Esta política, debe identificar a los responsables que velen por su cumplimiento y ser conocida por todos los miembros de la organización y en la cual, conforme se establece en el apartado 3.1 del anexo II, se precise al menos lo siguiente:

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

Además, la política de seguridad de la información debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el artículo 88 Real Decreto 1720/2007, de 21 de diciembre, en lo que corresponda.

El Real Decreto 3/2010, de 8 de enero, igualmente, se refiere al Centro Criptológico Nacional como organismo que, para dar cumplimiento a lo que establece el ENS, elaborará y difundirá guías de seguridad de las tecnologías de la información y las comunicaciones.

Por otro lado, pasados seis años desde la aprobación del Código de buenas prácticas para usuarios de sistemas informáticos de la Consejería de Sanidad y Consumo, se hace necesario una evolución del mismo, pasando a integrar sus principios básicos dentro de la política de seguridad de la información, debido, especialmente, a los cambios normativos que se han producido en estos años, como la entrada en vigor del 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, y el citado 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. Asimismo, la identificación de las obligaciones que debe cumplir la Consejería de Sanidad de la Comunidad de Madrid en seguridad de la información, ha llevado a elaborar el Decálogo de buenas prácticas para usuarios de sistemas de información de la Consejería de Sanidad, que se acompaña como anexo a esta política, con la intención de concienciar en esta materia al personal que la compone.

BOCM-20130718-12

En este marco competencial, mediante el Decreto 23/2012, de 27 de septiembre, del Presidente de la Comunidad de Madrid, por el que se establece el número y denominación de las Consejerías de la Comunidad de Madrid, se le atribuye a la Consejería de Sanidad las competencias que actualmente tiene atribuidas, esto es, la dirección y ejecución de la política del Gobierno de Madrid en materia de sanidad, ejerciendo las competencias que tiene atribuidas a estos efectos por el Estatuto de Autonomía, la Ley de Ordenación Sanitaria de la Comunidad de Madrid y demás normas que le sean de aplicación. Por otro lado, el Decreto 22/2008, de 3 de abril, del Consejo de Gobierno, por el que se establece la estructura orgánica de la Consejería de Sanidad y el Decreto 23/2008, de 3 de abril, del Consejo de Gobierno, por el que se establece la estructura orgánica del Servicio Madrileño de Salud, corresponde a la Dirección General de Sistemas de Información Sanitaria el establecimiento de medidas de seguridad en el sistema sanitario público de la Comunidad de Madrid, de acuerdo con la normativa vigente de los ficheros automatizados que contengan datos de carácter personal, y la realización de auditorías en el ámbito de la protección de datos de carácter personal.

En su virtud, de conformidad con lo establecido en el artículo 50.3 de la Ley 1/1983, de 13 de diciembre, de Gobierno y Administración de la Comunidad de Madrid,

DISPONGO

Artículo 1

Objeto y ámbito de aplicación

1. Constituye el objeto de la presente Orden la aprobación de la política de seguridad de la información (en adelante, la política), en el ámbito de la administración electrónica y de los sistemas de información de la Consejería de Sanidad de la Comunidad de Madrid, así como el establecimiento del marco organizativo y tecnológico de la misma.

2. La política, que se aprueba por esta Orden, será de especial aplicación a los sistemas de información previstos en la Ley 11/2007, de 22 de junio. Asimismo, deberá cumplirse, tanto por el personal destinado en los órganos y unidades dependientes de la Consejería de Sanidad, como por el personal que, aun no estando destinado en dichos órganos y unidades, tenga acceso a los sistemas de información.

Artículo 2

Marco normativo

Además de las disposiciones de esta Orden en materia de seguridad informática son de aplicación las siguientes normas:

a) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
b) Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
c) Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
d) 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.
e) 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.
f) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
g) 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.
h) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
i) Decreto 22/2008, de 3 de abril, del Consejo de Gobierno, por el que se establece la estructura orgánica de la Consejería de Sanidad.

BOCM-20130718-12

Artículo 3

Estructura organizativa

La estructura organizativa encargada de la gestión de la seguridad de la información en el ámbito de los sistemas de información y la administración electrónica de la Consejería de Sanidad, estará compuesta por los siguientes agentes:

a) Comité de seguridad de la información.
b) Responsable de seguridad.
c) Responsable del sistema.

Artículo 4

El comité de seguridad de la información

1. Se crea el comité de seguridad de la información (en adelante, el comité), al que le corresponde aplicar, en el ámbito de la Consejería de Sanidad, las previsiones contenidas en el ENS, y ejercerá las siguientes funciones:

a) La dirección y seguimiento de la aplicación de la legislación vigente, normas, estándares y buenas prácticas aplicables en materia de seguridad de las tecnologías de la información y las comunicaciones.
b) Definir, revisar y modificar tanto la política, como el "Decálogo de buenas prácticas para usuarios de sistemas de información de la Consejería de Sanidad", cuando hubiere cambios en las tecnologías de la información y las comunicaciones, o en la organización.
c) La aprobación del cuerpo normativo de seguridad que afecte transversalmente a toda la organización.
d) Impulsar nuevas líneas de trabajo en materia de seguridad de las tecnologías de la información y las comunicaciones, que conlleven la mejora continua del sistema de gestión de la seguridad de la información.
e) Gestionar, coordinar y supervisar la seguridad de la información a nivel de organización. En concreto, dirigir las acciones en materia de seguridad de la información de los proyectos cuyo fin sea generar acceso electrónico de los ciudadanos a los servicios de la Consejería de Sanidad.
f) Asumir las funciones del responsable de la información y del responsable del servicio, en los términos recogidos en el ENS y las Guías CCN-STIC del Centro Criptológico Nacional.
g) Informar regularmente del estado de la seguridad de la información a la dirección.

2. El comité estará compuesto por los siguientes miembros:

a) Presidente: Cargo que será ocupado por el titular del centro directivo competente en materia de asistencia sanitaria, o persona en quien delegue.
b) Vicepresidente: Cargo que será ocupado por el titular del órgano directivo competente en materia de sistemas de información sanitaria, adscrito a la Consejería de Sanidad o persona en quien delegue. Adoptará las funciones del presidente en ausencia de este.
c) Secretario: Cargo que será ocupado por la persona que ejerza la competencia en materia de seguridad de la información, del órgano adscrito a la Consejería de Sanidad. Actuará con voz pero sin voto. Serán funciones del secretario:
   i. Convocar las reuniones del comité.
   ii. Preparar los temas a tratar en las reuniones del comité, aportando información puntual para la toma de decisiones.
   iii. Elaborar el acta de las reuniones.
   iv. Ser responsable de la ejecución directa o delegada de las decisiones del comité.
d) Vocales: su designación será realizada por el presidente y serán:
   i. Los titulares de los departamentos del órgano directivo competente en materia de sistemas de información sanitaria.
   ii. Un representante por cada uno de los órganos directivos adscritos al centro directivo competente en materia de asistencia sanitaria.
   iii. Un representante propuesto por el centro directivo competente en materia de ordenación sanitaria.

BOCM-20130718-12

iv. Un representante de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid.
v. Asimismo, a las reuniones de la comisión podrán acudir, con voz pero sin voto, convocados por su presidente, aquellas personas que por razón de su actividad y conocimientos, tengan relación con los asuntos a tratar.

3. El comité se reunirá, previa convocatoria de su presidente y a iniciativa del mismo, como mínimo, una vez cada tres meses, y, con carácter extraordinario, cuando lo decida su presidente o lo soliciten la mayoría de sus miembros, y siempre que:

a) Aparezcan incidencias de seguridad graves que afecten a cualquier ámbito de competencia de la Consejería de Sanidad.
b) Surjan nuevas necesidades de seguridad que requiera la participación de los componentes del comité.

4. Todos los miembros serán convocados a las reuniones con la antelación necesaria. Las decisiones del comité se adoptarán por mayoría simple. El presidente gozará de derecho de veto.

5. El comité elaborará un reglamento de funcionamiento interno. En lo no previsto en el mismo, se regirá por las normas de funcionamiento previstas en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

6. Los hospitales, constituirán sus propios comités de seguridad de la información, sujetos a lo dispuesto en la política de la Consejería de Sanidad, siendo su obligación velar por la seguridad de la información y los datos de carácter personal de sus sistemas, para lo cual deberán adoptar cuantas medidas técnicas y organizativas sean necesarias.

Artículo 5

El responsable de seguridad

1. El responsable de seguridad será el titular del área o servicio responsable de la seguridad de sistemas de información, del órgano competente en materia de sistemas de información sanitaria.

2. Las funciones del responsable de seguridad se ejercerán con el apoyo de su equipo técnico.

3. Son funciones del responsable de seguridad:

a) Las funciones que le son propias como secretario del comité.
b) Promover la seguridad de la información manejada y de los servicios prestados por los sistemas de información, así como la formación y concienciación de los usuarios en la materia.
c) Llevar a cabo tareas de inspección mediante la realización de auditorías y controles periódicos, para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, por parte de las unidades y órganos que integran la Consejería de Sanidad.
d) Dirigir y coordinar la respuesta a los incidentes de seguridad, junto con otras unidades de la Consejería de Sanidad.
e) Elaborar informes periódicos del estado de la seguridad de la información en la Consejería de Sanidad, en colaboración con las unidades y centros que la componen, para el comité, que incluyan los incidentes más relevantes de cada período.

4. Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el comité, a propuesta del responsable de seguridad, podrá designar responsables de seguridad delegados, en el número que considere necesario, que tendrán dependencia funcional directa del responsable de seguridad y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

Artículo 6

Responsable del sistema

1. El responsable del sistema será el titular del área o servicio del órgano competente en materia de sistemas de información sanitaria, responsable de la explotación de los sistemas de información de la Consejería de Sanidad.

BOCM-20130718-12

2. Las funciones del responsable del sistema se ejercerán con el apoyo de su equipo técnico.

3. Son funciones del responsable del sistema, en relación con la política:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Definir la topología y sistema de gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Garantizar que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

4. Cuando por su complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el comité, a propuesta del responsable de sistema, podrá designar cuantos responsables de sistema delegados considere necesarios, que tendrán dependencia funcional directa del responsable de sistema, y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

Artículo 7

Gestión y coordinación de la seguridad de la información

1. La gestión de la seguridad se llevará a cabo de manera diferenciada por cada agente implicado.

2. La coordinación entre los diferentes agentes implicados deberá tener en cuenta que:

a) El responsable de seguridad informará al comité acerca de las siguientes cuestiones:

i. Las decisiones e incidentes en materia de seguridad que afecten a la información y al servicio de la Consejería de Sanidad, en particular, de lo relativo al riesgo residual y a las desviaciones de riesgo respecto de los márgenes aprobados como asumibles.

ii. Resumen consolidado de actuaciones en materia de seguridad y de incidentes relativos a seguridad de la información.

iii. Estado de la seguridad del sistema, en particular, del riesgo residual al que el sistema está expuesto.

b) El responsable del sistema informará al responsable de seguridad sobre:

i. Las incidencias relativas a la información y servicios que le competen.

ii. Actuaciones en materia de seguridad, en particular, en lo relativo a decisiones de arquitectura del sistema.

iii. Resumen consolidado de incidentes de seguridad.

iv. Resumen de la eficacia de las medidas de protección implantadas.

Artículo 8

Resolución de conflictos

En caso de conflicto en materia de seguridad de la información entre diferentes responsables, este será resuelto por el superior jerárquico de los mismos.

Artículo 9

Gestión de riesgos

1. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información sanitaria, conforme a los principios de la seguridad basada en los riesgos y reevaluación periódica, siendo el comité el encargado de que se realice el preceptivo análisis de riesgos y se proponga el tratamiento adecuado, calculando los riesgos residuales.

2. El responsable de seguridad es el responsable de que el análisis se realice en tiempo y forma, así como de identificar carencias y debilidades y ponerlas en conocimiento del comité.

3. El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionadas a los riesgos y estar justificadas, deberán revisarse y aprobarse cada año por el titular del órgano competente en materia de sistemas de información sanitaria, de acuerdo con un Plan de Adecuación al Esquema Nacional de Seguridad.

BOCM-20130718-12

4. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero, siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo, elaboradas por el Centro Criptológico Nacional.

Artículo 10

Datos de carácter personal

La Consejería de Sanidad trata datos de carácter personal, que se encuentran en los ficheros dados de alta en la agencia de protección de datos competente. Todos sus sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en los documentos de seguridad, los cuales se encuentran ubicados en las dependencias de cada responsable del fichero.

Artículo 11

Estructura documental y normativa

1. El cuerpo documental sobre seguridad de la información se desarrollará en cuatro niveles por ámbito de aplicación, nivel de detalle técnico y de obligado cumplimiento, de manera que cada documento de un determinado nivel de desarrollo se fundamente en los documentos de nivel superior. Dichos niveles de desarrollo documental son los siguientes:

a) Primer nivel. Política de seguridad de la información.
Está constituido por la presente Orden y es de obligado cumplimiento, al amparo de lo establecido por 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.

b) Segundo nivel. Directrices y recomendaciones de seguridad.
El cuerpo documental, que comprende las directrices y recomendaciones de seguridad de las tecnologías de la información y las comunicaciones (STIC) y las guías STIC, es de obligado cumplimiento, según lo establecido por 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, y se formalizará mediante aprobación del comité, mientras que las recomendaciones consistirán en buenas prácticas y consejos no vinculantes para mejorar las condiciones de seguridad.

c) Tercer nivel. Procedimientos e instrucciones técnicas.
Está constituido por el conjunto de procedimientos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. Son recomendaciones o informaciones relativas a temas concretos de seguridad basadas en instrucciones previas, que establecen las configuraciones mínimas de seguridad de los diferentes elementos de un sistema de información, recomendaciones de uso o de otro tipo. La responsabilidad de aprobación de estos procedimientos técnicos dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado. Se consideran incluidas en este nivel las guías CCN-STIC.

d) Cuarto nivel. Informes, registros y evidencias electrónicas.
Está constituido por los informes técnicos, que son documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o de una evaluación; registros de actividad o alertas de seguridad, que son documentos de carácter técnico que recogen amenazas y vulnerabilidades a sistemas de información.

2. El comité establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo documental con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la política.

Artículo 12

Obligaciones del personal

1. El personal que preste servicios en la Consejería de Sanidad tiene la obligación de conocer y cumplir esta política y demás normativa de seguridad derivada de ella, siendo responsabilidad del comité el que llegue a todos los usuarios.

BOCM-20130718-12

2. Asimismo, se encuentran obligados todos los usuarios de los sistemas de información de la Consejería de Sanidad a cumplir el "Decálogo de buenas prácticas para usuarios de sistemas de información de la Consejería de Sanidad", que figura como anexo de este documento.

Artículo 13

Formación y concienciación

1. Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación del personal que preste servicios en la Consejería de Sanidad, así como a la difusión entre los mismos de la política y de su desarrollo normativo, pudiendo, en algún caso, recabar la colaboración de entidades encargadas de coordinar las acciones de seguridad de la información de los organismos públicos.
2. A estos efectos, deberán incluirse actividades formativas en esta materia dentro de los Planes de Formación de la Consejería de Sanidad.

Artículo 14

Actualización permanente y revisiones periódicas de la política de seguridad

1. La presente Orden deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de administración electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.
2. Las propuestas de las sucesivas revisiones de la política se elaborarán por el comité.

DISPOSICIÓN ADICIONAL PRIMERA

Decálogo de buenas prácticas

El Decálogo de buenas prácticas para usuarios de sistemas de información de la Consejería de Sanidad se incluye, como Anexo, en la política.

Las consideraciones determinadas en el Decálogo tienen carácter de instrucción interna y se configuran, por tanto, como directrices y recomendaciones en materia de seguridad de la información.

DISPOSICIÓN ADICIONAL SEGUNDA

No incremento de gasto público

La aplicación de esta Orden no conllevará incremento de gasto público, atendiéndose el funcionamiento de toda la estructura orgánica contemplada en la misma, con los recursos humanos y materiales de que dispone la Consejería de Sanidad, sin que perciban retribución alguna por el desarrollo de las funciones y actividades contempladas en la presente norma.

DISPOSICIÓN ADICIONAL TERCERA

Habilitación de desarrollo

Se habilita al titular de la Dirección General de Sistemas de Información Sanitaria para dictar las disposiciones de desarrollo de esta Orden que sean precisas.

DISPOSICIÓN FINAL PRIMERA

Deber de colaboración en la implementación de la política de seguridad de la información

Todos los órganos y unidades de la Consejería de Sanidad prestarán su colaboración en las actuaciones de implementación de la política aprobada en esta Orden.

BOCM-20130718-12

DISPOSICIÓN FINAL SEGUNDA

Entrada en vigor

La presente Orden entrará en vigor al día siguiente al de su publicación en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID.

Dada en Madrid, a 27 de junio de 2013.

El Consejero de Sanidad,
JAVIER FERNÁNDEZ-LASQUETTY Y BLANC

BOCM-20130718-12

ANEXO

DECÁLOGO DE BUENAS PRÁCTICAS PARA USUARIOS DE SISTEMAS DE INFORMACIÓN DE LA CONSEJERÍA DE SANIDAD

1. Uso de los equipos informáticos.

1.1. Los equipos informáticos no deben ser utilizados para fines particulares.

1.2. No deben almacenarse en la memoria de los ordenadores documentos que contengan datos de carácter personal. En caso contrario, los usuarios serán responsables de la custodia y respaldo de toda la información que almacenen en los mismos.

1.3. No se podrán modificar los equipos informáticos y periféricos, así como su conexión a otros equipos ajenos a la CSCM, salvo que se obtenga autorización expresa de quien corresponda.

1.4. No se deberán sacar equipos fuera de las instalaciones, excepto que estuviera previamente autorizado por el responsable de seguridad designado conforme la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

1.5. Los usuarios comunicarán al responsable informático del centro, y/o al centro de soporte a usuarios, cualquier incidencia de funcionamiento o deficiencia de las aplicaciones informáticas que hubieran podido observar, así como cualquier mejora que se estime adecuada.

1.6. Cuando una incidencia y/o deficiencia pudiera causar un elevado impacto en el funcionamiento del servicio sanitario, los usuarios, de acuerdo siempre con el centro de soporte a usuarios, podrán adoptar las medidas de urgencia que se estimen oportunas. El detalle de los hechos acontecidos y de las medidas adoptadas se deberá poner en conocimiento de quien corresponda a fin de que éste tome las decisiones oportunas.

2. Internet.

2.1. La utilización del acceso a Internet debe responder a fines profesionales.

2.2. El uso de los sistemas de información tales como el acceso a Internet o el correo electrónico corporativo, podrá ser auditado en los términos que autorice la legislación vigente.

3. Tratamiento y uso de datos de carácter personal.

3.1. Los usuarios deben acceder, exclusivamente, a la información necesaria para el desarrollo de las funciones propias de su actividad y únicamente a la que esté autorizado.

3.2. En el acceso a ésta información los usuarios están obligados a cumplir todas las medidas de seguridad establecidas por la normativa en protección de datos, y demás requisitos aplicables conforme a las normas y procedimientos establecidos en la CSCM.

3.3. Todas las personas que intervengan en cualquier fase del tratamiento de datos de carácter personal están obligadas al secreto profesional respecto de los mismos.

3.4. Cuando un soporte informático (disco duro, USB, CD...), o documento, en formato electrónico o papel, contenga datos personales, y vaya a ser desechado, se deberán adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada o impresa en los mismos.

3.5. El personal que necesite extraer de la CSCM datos de carácter personal deberá solicitar la autorización pertinente del Responsable de Seguridad, conforme a la Ley Orgánica 15/1999, de 13 de diciembre, y aplicar las debidas medidas de seguridad para proteger esa información. Asimismo, el Responsable de Seguridad deberá llevar un registro actualizado de la salida de esta información.

3.6. Cualquier incidencia o anomalía que pudiera afectar a la seguridad de los datos personales deberá ser comunicada al responsable de seguridad del centro y al Área de Seguridad.

3.7. Los accesos a los sistemas de información podrán ser monitorizados y registrados para auditar el uso de los mismos, de conformidad con lo estipulado en el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre.

BOCM-20130718-12

4. Incidentes de seguridad de la información.

4.1. Cuando ocurra un incidente que afecte a la seguridad de la información, el usuario deberá reportar el detalle de los hechos acontecidos y de las medidas adoptadas a su superior jerárquico y/o al Área de Seguridad, a fin de que se tomen las decisiones oportunas.

4.2. Asimismo, el Responsable de Seguridad podrá, de oficio, conforme el artículo 6.3.c de la Política de Seguridad de la Información, y cuando razones de urgencia así lo justifiquen, proceder, de forma inmediata y directa, a realizar las acciones necesarias sobre el hardware o software de cualquier usuario (incluyendo la retirada de los mismos), reportando esta acción, en cuanto sea posible, a quien corresponda.

5. Uso de contraseñas.

5.1. Tanto las cuentas de usuario como las contraseñas son personales. En consecuencia, no se deberán facilitar a otros usuarios, salvo que se reciba autorización expresa del Responsable de Seguridad y/o responsable de informática, conforme la Ley Orgánica 15/1999, de 13 de diciembre.

5.2. Los usuarios deben ser cuidadosos y diligentes en la custodia y cuidado de las contraseñas y deben mantenerlas en secreto, debiendo informar en caso de pérdida o compromiso de la misma.

5.3. Los usuarios son los únicos autorizados para el uso de la cuenta, y deben ser conscientes de que son responsables de las acciones que se realicen con su identidad en los sistemas de información.

6. Uso de certificados digitales.

6.1. Los usuarios deberán hacerse responsables de salvaguardar sus claves privadas, aplicando las pautas descritas en el apartado 5.2 del presente Decálogo, y al de cualquier elemento (tarjeta o dispositivo criptográfico, archivo informático, programa “software”, etcétera) y/o código (PIN, contraseña, etcétera) que puedan ser necesarios para acceder a las mismas.

6.2. Los usuarios comunicarán a la oficina de registro del centro correspondiente, o a la Entidad Prestadora de Servicios de Certificación y/o registro, cualquier compromiso de su clave privada, o de los elementos y/o códigos utilizados para su acceso, a la mayor brevedad.

6.3. Los usuarios deberán respetar las garantías y requisitos suscritos por la CSCM y por la correspondiente Entidad Prestadora de Servicios de Certificación, así como la correspondiente Declaración de Prácticas de Certificación de la Autoridad de Certificación relevante, con respecto a la provisión de servicios técnicos, administrativos y de seguridad necesarios para garantizar la validez de las transmisiones electrónicas emitidas y recibidas.

7. Correo de la CSCM.

7.1. El servicio de correo electrónico de la CSCM es de uso obligatorio y únicamente se utilizará por aquellos usuarios a los que se les haya dotado de cuenta de correo para uso profesional, debiendo observarse el deber de diligencia en la utilización del mismo.

7.2. Deberá minimizarse el uso del correo de la CSCM con fines distintos a los laborales.

7.3. Con carácter general, está prohibido el envío de datos de salud fuera de la red de la CSCM mediante correo electrónico. En caso de ser necesario tal envío, los datos deberán ser cifrados. En cualquier caso, debe observarse lo descrito en el apartado 2.7 del presente Decálogo.

7.4. Para evitar el correo masivo no solicitado, también denominado “spam”, como regla general, solo se debe dar nuestra dirección de correo electrónico a personas y/o entidades conocidas. No se debe introducir la dirección de correo electrónico en foros o páginas Web no institucionales. Cuando se reciban correos electrónicos desconocidos o no solicitados no se deben contestar, ya que al hacerlo se reconfirma la dirección.

7.5. En el caso de recibir correos electrónicos cuyo remitente y/o contenido sea dudoso, deberá ponerse en contacto con el centro de soporte de usuarios para que se analice su posible malignidad, conforme el apartado 8 del presente Decálogo.

BOCM-20130718-12

8. Virus informáticos y otro tipo de "malware".

8.1. Todos los puestos de la CSCM deben disponer de mecanismos adecuados para el control de "software" malicioso (virus, gusanos, etcétera), y han de permanecer activados. No está permitida la desactivación de dichos mecanismos.

8.2. Ante la sospecha de una infección por virus, gusanos, etcétera, se deberá comunicar la incidencia al centro de soporte de usuarios.

9. "Software".

9.1. Debido a la naturaleza dinámica y cambiante de los requisitos que han de satisfacer, las aplicaciones informáticas han de mantenerse siempre actualizadas, para lo cual resulta imprescindible la colaboración de todos y cada uno de los usuarios.

9.2. Para preservar el buen funcionamiento de los sistemas de información se prohibe la instalación de "software" o programas no corporativos en los ordenadores. Si fuera necesaria su instalación, deberá solicitarse al responsable correspondiente para que lo gestione. Igualmente, no se podrán realizar copias del "software" instalado en los ordenadores.

9.3. Los servicios de soporte correspondientes, así como el Área de Seguridad, quedan facultados para que de forma directa o remota actúen sobre este "software" no permitido.

9.4. Los usuarios no podrán modificar el "software" instalado a nivel corporativo, que en ningún caso deberá ser desactivado.

10. Mesas limpias y bloqueo del ordenador.

10.1. Cuando los usuarios se ausenten del puesto de trabajo o dejen desatendido el ordenador deberán activar el sistema de bloqueo del que disponga su equipo (salvapantalla protegida por contraseña, bloqueo del terminal, etcétera) con el fin de que se no visualicen datos en la pantalla, así como evitar que se acceda al equipo o aplicaciones por terceros no autorizados.

10.2. Del mismo modo todos los documentos en papel que contengan datos de carácter personal deberán ser custodiados en todo momento, mientras estén siendo usados, por la persona a cargo, evitando el acceso por personas no autorizadas. Una vez que se haya terminado de trabajar con dichos documentos estos deberán guardarse bajo llave o utilizando cualquier otro mecanismo que garantice su custodia e impida el acceso a los mismos.

El incumplimiento de cualquiera de las pautas de comportamiento contenidas en el presente Decálogo de buenas prácticas podrá dar lugar a la correspondiente responsabilidad disciplinaria, si a ello hubiere lugar, en aplicación de las normas reguladoras del régimen jurídico disciplinario propio del usuario.

(03/23.504/13)

BOCM-20130718-12