OFICINA DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁMBITO SANITARIO

Ramos Mayorga, M
Asesoría Jurídica Consejería de Sanidad y Gerencia Regional de Salud
Comunidad de Castilla y León

Rodriguez Lorca, A.
Asesoría Jurídica Consejería de Sanidad y Gerencia Regional de Salud
Comunidad de Castilla y León

RESUMEN

La Tecnología de la Información y las Comunicaciones constituyen a día de hoy una herramienta imprescindible para la prestación eficiente en los servicios públicos cobrando una importancia fundamental en los Servicios de Salud.

Señala la Agencia Española de Protección de Datos que en órganos, organismos o entes de gran tamaño en que exista un único delegado de protección de datos, éste debe estar respaldado por una unidad administrativa específicamente dedicada a la protección de datos, por ello, ante la insuficiencia de medios personales, la Gerencia Regional de Salud ha promovido la creación de una OFICINA DE SEGURIDAD DE LA INFORMACION en el ámbito sanitario de la Comunidad de Castilla y León.

Se expondrá el planteamiento para su implantación atendiendo a la solución de las dificultades que se pudieran encontrar, a su contenido y funcionamiento y controles futuros.

PALABRAS CLAVE

Seguridad, información, delegado, protección de datos, sistemas, procesos, riesgos, prevención.

1. INTRODUCCIÓN: LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidas la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros. Incumbe a todos los ámbitos de nuestro

entorno, ya sean gobiernos, entidades militares, instituciones financieras, hospitales y empresas públicas y privadas que estén en posesión de información confidencial sobre sus empleados, clientes, productos o su situación financiera.

La entrada en vigor de la nueva Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos y garantía de los derechos digitales, y el cumplimiento del 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 modificado por el Real Decreto 951/2015, multiplican las exigencias de seguridad en los datos de carácter personal y de la información.

Los términos seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información. Sin embargo, no son exactamente lo mismo existiendo algunas sutiles diferencias. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

Es importante señalar que, el tratamiento de la seguridad de la información va a estar basado en la tecnología y si su contenido es confidencial tendrá un alto valor; la información puede ser divulgada, mal utilizada, ser robada, borrada o saboteada, en cuyo caso su disponibilidad se va a ver afectada, lo que la coloca en una situación de riesgo, exigiendo la implementación de distintas estrategias.

Atendiendo a las posibilidades estratégicas que ofrece tener acceso a cierta información, podemos distinguir:

- Por una parte, la seguridad de la información comprende diversos aspectos, entre los que podemos citar, la disponibilidad, la comunicación, la identificación de problemas, el análisis de riesgos, la integridad y la confidencialidad. Su objeto son los sistemas en sus vertientes de acceso, uso, divulgación, interrupción o destrucción no autorizada de información.

- Por otra parte, la seguridad de la información lleva consigo la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

El Servicio de Salud de Castilla y León (en adelante Sacyl) acomete la tarea de asegurar la información con las exigencias previstas en la normativa actual a través de una Oficina de Seguridad de la Información.

Los objetivos de este centro serán gestionar y proteger los datos de salud y los sistemas relacionados con la seguridad de las tecnologías de la información.

Para la creación de la misma se prevé una inversión de más de 3 millones de euros.

2. PLANTEAMIENTO

La insuficiencia de medios propios, tanto personales, como materiales que puedan cubrir las necesidades actualmente existentes en materia de seguridad determina la necesidad de promover un procedimiento de licitación para su implementación.

Las exigencias de seguridad en los datos de carácter personal y de la información se multiplican con la entrada en vigor de la nueva Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos y garantía de los derechos digitales y para el cumplimiento del 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 modificado por el Real Decreto 951/2015, de 23 de octubre.

El Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante ENS) tiene como finalidad la creación de condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. También se persigue además de la seguridad individual de cada sistema y en base a la imbricación entre los diferentes sistemas de información de las Administraciones una protección global con independencia de que cada organismo sea responsable de su propio perímetro.

El objetivo que se persigue es el de proporcionar el servicio de soporte especializado en seguridad de la información y protección de datos personales

de los usuarios del sistema sanitario para el aseguramiento de los aspectos de confidencialidad, integridad y disponibilidad.

Por tanto la OSI pretende configurarse como un todo homogéneo dentro de la propio servicio de salud y constituir el instrumento que coordine de manera unitaria la prevención, detección y en su caso la respuesta a posibles amenazas y riesgos para la seguridad de los datos de todos los centros de la Gerencia Regional de Salud, lo que abarca aproximadamente 20.000 puestos informáticos en más de 1500 centros integrados en la red privada sanitaria de Castilla y León.

3. OBJETIVOS DE LA OFICINA DE SEGURIDAD DE LA INFORMACIÓN

Las competencias de este órgano se extenderán tanto a los servicios centrales del Sacyl como a las diferentes organizaciones territoriales que forman parte de la organización del Sistema Regional de Salud.

Dentro de las funciones atribuidas a esta OSI podemos encontrar:

- Asesoramiento técnico y apoyo al desarrollo de políticas, normas y procedimientos en materia de seguridad de la información.

- Asesoramiento técnico multidisciplinar en materia de seguridad y protección de datos en consonancia con la legislación vigente.

- Apoyo a los centros en materia de seguridad, ofrecido como un servicio, manteniendo siempre éstos un grado de autonomía suficiente para la implantación de las medidas de seguridad.

- Integración en el ciclo de vida de los proyectos de la DGITI.

- Alerta temprana y prevención de riesgos y su respuesta protocolizada.

- Alimentar y gestionar la Web de la Oficina de Seguridad del Sistema sanitario de Castilla y León.

- Mantener actualizada las prácticas y documentos exigidos por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el R.D. 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica.

- Apoyo en la adaptación al Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y, en su caso, la Ley Orgánica de Protección de Datos Personales.

- Asesoramiento en la definición de estrategias y estructuras adecuadas que garanticen el cumplimiento de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

4. CONFLICTOS DE COMPETENCIA CON OTROS ÓRGANOS DE LA ADMINISTRACIÓN

La OSI se concibe como respaldo a la figura del Delegado de Protección de Datos de la Gerencia Regional de Salud (DPD), siguiendo las indicaciones de la AEPD.

4.1 Delegado de Protección de Datos

La regulación que hace el RGPD tanto de la posición como de las funciones de los DPD es válida tanto para responsables y encargados privados como para autoridades y organismos públicos. Sin embargo, hay algún aspecto en que existen disposiciones diferenciadas para el sector público y, en todo caso, el perfil del DPD puede presentar particularidades en las organizaciones públicas, como cuál será su lugar en la organización.

Señala la Agencia Española de Protección de Datos (AEPD) que en órganos, organismos o entes de gran tamaño en que exista un único DPD lo habitual será que desempeñe sus funciones a tiempo completo, en entidades de menor tamaño será posible que el DPD compagine sus funciones con otras.

El DPD actúa como asesor y supervisor interno, por lo que ese puesto no puede ser ocupado por personas que, a la vez, desarrollen tareas que impliquen decisiones sobre la existencia de tratamientos de datos o sobre el modo en que van a ser tratados los datos (p.ej.: responsables de ITC, o responsables de seguridad de la información).

El RGPD ofrece la posibilidad de que se contraten externamente las funciones de DPD. Esta opción puede ser utilizada en determinados casos, como podría ser el de pequeños municipios que se beneficien de un servicio que ofrezca una diputación provincial

o una comunidad autónoma o, incluso, que donde ese servicio no exista puedan optar por los servicios de entidades privadas especializadas.

4.2 Solución a los conflictos de competencia que pudieran presentarse en el ámbito de la Gerencia Regional de Salud

Al iniciarse el expediente de contratación se atribuyeron a la Oficina una serie de actuaciones que originaban una colisión con las funciones atribuidas normativamente no sólo al DPD, sino también con la Asesoría Jurídica de la Consejería de Sanidad.

El conflicto con la Asesoría Jurídica surgió en un primer momento al encomendarse a la Oficina el asesoramiento la aplicación de normativa en materia de seguridad. La solución pasó por disociar las tareas de asesoramiento, encomendando a la OSI las consultas desde el punto de vista técnico-normativo.

En cuanto a la colisión de funciones con el DPD tras la revisión pormenorizada de las mismas y determinación de las que correspondían en exclusiva al DPD en el Pliego de Prescripciones Técnicas, se describieron cada uno de los perfiles personales que iban a ser necesarios para la ejecución del contrato, correspondiendo al DPD de la Gerencia Regional de Salud la coordinación de los distintos aspectos a desarrollar con carácter general, siendo necesaria su previa aprobación en determinados asuntos.

5. CONTENIDO DEL SERVICIO DE OFICINA DE SEGURIDAD DE LA INFORMACIÓN

En el marco del contrato, por parte de la GRS se designará la figura del Responsable del Servicio, quien, junto al DPD de la Gerencia Regional de Salud, dirigirá y controlará su correcta ejecución. Ellos serán quienes interaccionen mediante la celebración de reuniones ordinarias de seguimiento con carácter periódico y reuniones extraordinarias cuando la situación lo requiera.

Este servicio está orientado al desarrollo de actividades de asesoría y consultoría para la adecuación a la legislación y normativa relacionada con el cumplimiento del ENS.

1. Entre las actividades de asesoría, consultoría y apoyo podemos relacionar:

- Asesoramiento técnico y consultoría legal y normativa en materia de tecnologías de la información y comunicaciones y seguridad informática.

- Soporte a la DGITI en la interlocución con los agentes implicados en temas de seguridad de la información: AEPD, CCN[1], fuerzas de seguridad, juzgados, etc.

- La coordinación, dinamización y asesoramiento técnico y legal a los comités y comisiones de trabajo en materia de seguridad definidos por la GRS.

- Asesoramiento técnico en la elaboración y actualización de políticas, normas, procedimientos e instrucciones en materia de seguridad (política de contraseñas, acceso remoto, uso del correo electrónico, gestión de la documentación en formato papel, funciones y obligaciones del personal con acceso a datos personales, etc.) de acuerdo con la legislación, normativa estándares y códigos de buenas prácticas.

- Asesoramiento técnico en los procedimientos de contratación de la GRS que puedan afectar a la disponibilidad, accesibilidad, confidencialidad e integridad de los datos personales de la organización, garantizando el debido respeto de las medidas de seguridad.

- Asesoramiento técnico y apoyo en el uso y custodia de certificados digitales y servicios de firma electrónica, servicios electrónicos al ciudadano y manejo seguro de documentación digital.

- Asesoramiento técnico en la gestión y utilización de herramientas Web 2.0: redes sociales, plataformas educativas, aulas virtuales, encuestas en línea, agregadores de noticias, entre otras.

- Apoyo al DPD en la elaboración de los análisis de riesgos y evaluaciones de impacto en materia de protección de datos, los cuales se llevarán a cabo apoyados en la herramienta ASSI-RGPD[2] del Ministerio de Trabajo, Migraciones y Seguridad Social.

2. Más en detalle, en cumplimiento del RD 3/2010, de 8 de enero, por el que se regula el

1 Centro Criptológico Nacional.

2 Auditoría de Seguridad de los Sistemas de Información-Reglamento General de Protección de Datos

Esquema Nacional de Seguridad en el Ámbito de la Administración Electrónica se realizarán labores de coordinación y seguimiento del plan de adecuación al ENS, entre ellas:

- Proponer las medidas y recomendaciones necesarias para que los Sistemas de Información, cumplan con la Política de Seguridad de la Información de la Junta de Castilla y León.

- Mantener actualizada la categorización de los Sistemas de Información existentes y la identificación y categorización de los de nueva creación, de acuerdo con las reglas y pautas marcadas en el Anexo I del ENS.

- Elaborar y actualizar periódicamente los análisis de riesgos de los diferentes sistemas de información, los cuales se llevarán a cabo a través de la herramienta PILAR[3] del CNN [4] y mediante la metodología Magerit[5].

  Será objeto del contrato la instalación, configuración y administración de la citada herramienta para lo cual la GRS dotará y pondrá a disposición del adjudicatario en sus CPD corporativos la infraestructura IT que sea necesaria cuyo dimensionamiento deberá indicarse en la oferta.

- Mantener actualizada (de manera formal y detallada) la declaración de aplicabilidad en los sistemas de información del sistema sanitario de Castilla y León de las medidas de seguridad comprendidas en el Anexo II del ENS.

- Establecer las recomendaciones que se consideren convenientes, para que, dentro del proceso de mejora continua, los sistemas cumplan los objetivos del ENS y se consiga un sistema de gestión de la seguridad de la información que se ajuste a los requisitos exigidos.

- Establecer las recomendaciones en el plan de mejora de la seguridad, que detallará los proyectos y actuaciones destinadas a subsanar las deficiencias detectadas.

  La OSI, gestionará y prestará apoyo en la implantación de las medidas recogidas en el plan de mejora de la seguridad.

- Las auditorias de cumplimiento requeridas de conformidad con lo indicado en el art.34 del RD 3/2010.

6. DESARROLLO DE LAS ACTIVIDADES A REALIZAR POR LA OSI

6.1 Plan de comunicación y plan de concienciación

Se elaborará una estrategia de comunicación y concienciación para el propio personal de la Gerencia Regional de Salud, tanto sanitario como no sanitario. Dentro de la estrategia es fundamental dar a conocer la OSI entre dicho personal para lo cual se definirá una identidad mediante el diseño de un logo.

Tendrá acceso por tanto al portal de Salud de Castilla y León para mantener actualizado el espacio web de la OSI publicando las políticas y normas aplicables para el conocimiento de los usuarios, creará un boletín informativo de seguridad.

En cuanto al Plan de Concienciación, este servicio se realizará siempre en apoyo del DPD y bajo su supervisión y autorización.

6.2 Gestión de incidentes de seguridad

Para el cumplimiento del artículo 35 del RD 3/2010 que establece la obligación de evaluar regularmente el estado de seguridad de los sistemas de las apps, la OSI será la encargada de cumplimentar la información a través de la llamada herramienta INES[6].

Se encargará de llevar a cabo la gestión de los incidentes de seguridad, para ello utilizará la herramienta LUCÍA[7] y PILAR, ambas desarrolladas por el Centro Criptográfico Nacional y que están a disposición de las administraciones para el análisis de riesgos y la gestión de incidentes de seguridad para ello debe realizar la instalación, configuración y administración de las mismas.

3 Procedimiento Informático y Lógico de Análisis de Riesgos.

4 Centro Criptológico Nacional.

5 MAGERIT es la metodología de análisis y gestión de riesgos que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno.

6 Informe Nacional del Estado de Seguridad.

7 Listado Unificado de Coordinación de Incidentes y Amenazas.

También deberá aportar las herramientas informáticas necesarias para el cumplimiento del ENS (análisis de riesgos, herramientas para evaluar el grado de cumplimiento y cuadro de mando.)

6.3 Gestión documental

Mediante la herramienta INES se dará cumplimiento a la obligación de evaluar regularmente el estado de seguridad de los sistemas de las apps, siendo el encargado de cumplimentar la información a través de la herramienta.

6.4 Auditoría

Este servicio tiene como objetivo velar por un adecuado grado de madurez de la seguridad de los sistemas de información que asegure la continuidad del servicio contratado sin ningún tipo de riesgos o brechas.

Se trata de una evaluación de carácter interno para evaluar las medidas de seguridad en la implantación de los sistemas de información y servicios que hagan uso de las tecnologías de la información y las comunicaciones.

En concreto:

- Se realizará la auditoría de cumplimiento normativo tanto en materia de seguridad de la información como en materia de protección de datos.

- Control interno de cada uno de los centros en materia de seguridad.

- Auditorías de seguridad física y medioambiental.

6.5 Análisis del Software y Hardware

Asumirá la comprobación de niveles de seguridad de los sistemas de la información, aplicaciones informáticas, hardware.

7. DIMENSIONAMIENTO DE RECURSOS HUMANOS

Para la prestación regular de este servicio se demanda desde el comienzo del contrato la constitución de los siguientes equipos de trabajo:

- Un equipo de trabajo permanente, con dedicación exclusiva y a tiempo completo que estará compuesto por un mínimo de técnicos los cuales deberán ajustarse a perfiles profesionales estrictamente delimitados debido a la necesaria especialización de acuerdo con las tareas a desarrollar.

- Un equipo que preste las asistencias técnicas con dedicación parcial/temporal en el desempeño de trabajos muy específicos y delimitados. Los trabajos con cargo al servicio de asistencia técnica deberán ser previamente conocidos y aprobados por parte del Responsable del Servicio de la GRS y se establecerán en función del perfil: elaboración de informes, auditorías, análisis de riesgos, etc.

El Responsable del Servicio verificará que la capacitación del personal dedicado a dichos trabajos cumple con los requisitos de capacitación que correspondan a ese perfil de acuerdo a lo ofertado.

8. FUTURO DE LA OFICINA DE SEGURIDAD DE LA INFORMACIÓN

Cuestión importante es asegurar la pervivencia de la OSI más allá del presente contrato, ya que la seguridad de la información no puede quebrar cuando, en cumplimiento de la normativa vigente en materia de contratos haya que acudir a licitar el servicio nuevamente.

Se controla, por tanto, que el impacto de una posible trasferencia del servicio a un nuevo adjudicatario sea mínima. De este modo se va a exigir al adjudicatario que esté prestando el servicio:

- Cooperar con el nuevo contratista seleccionado por la GRS en todas las actividades que, relacionadas con la implantación efectiva de los servicios por parte del nuevo proveedor, requieran su participación, aportando, para ello, todo el personal y material que resulte necesario y garantizando, en todo momento, la continuidad en la prestación del servicio sin que éste sufra ninguna interrupción como consecuencia del cambio.

- Transferir información. El adjudicatario proporcionará a la GRS toda la información generada y gestionada por el adjudicatario, incluyendo el código fuente de desarrollos software y parametrización de sistemas, contraseñas, etc. que se hayan realizado al amparo de este contrato. Toda

la información se entregará en formato accesible y susceptible de evolucionar progresivamente en el tiempo adaptándose a los nuevos requerimientos que puedan existir.

9. CONCLUSIONES

La mayoría de los sistemas de la información y telecomunicaciones que dan soporte tecnológico al sistema sanitario de Castilla y León se encuentra centralizado o está en proceso de homogeneización por parte de la Dirección General de Infraestructuras y Tecnologías de la Información (en adelante DGITI).

El objetivo de la Oficina de Seguridad de la Información (en adelante, OSI) es proporcionar el servicio de soporte especializado en seguridad de la información y protección de datos personales con el fin de facilitar el aseguramiento de los aspectos de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de los mismos, de acuerdo con los requerimientos legales y buenas prácticas, constituyéndose en referente para todos los ámbitos de seguridad de la información, tanto técnicos como jurídicos, de todos los centros dependientes de la Gerencia Regional de Salud de Castilla y León.

La OSI se constituye, por tanto, con una doble función:

- Instrumento de prevención, detección, respuesta a amenazas y riesgos de seguridad.

- Órgano responsable de la coordinación e implantación de políticas y medidas de seguridad de la organización.

Va a prestar a los diferentes centros dependientes de la Gerencia Regional de Salud, una serie de servicios tanto reactivos, como preventivos, con el objeto de impulsar y dar soporte a la implantación de las medidas de seguridad por parte de dichos centros.

10. BIBLIOGRAFÍA: REGULACIÓN / HABILITACIÓN NORMATIVA

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

- Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos y garantía de los derechos digitales.

- 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.

- Real Decreto 951/2015, de 23 de octubre de modificación del 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.

- Ley 8/2011, de 28 de abril por la que se establecen medidas para la protección de las infraestructuras críticas.