ESQUEMA NACIONAL DE SEGURIDAD

POLÍTICA DE SEGURIDAD

CONTROL DE CAMBIOS			
Versión	Identificación del cambio	Apartado	Fecha
1.0	Generación del documento		02/06/2016

ÍNDICE

Capítulo I. Política de Seguridad de la Información del Centro Nacional de investigaciones oncológicas.

Artículo 1. Objeto y ámbito de aplicación.

Artículo 2. Misión.

Artículo 3. Legislación y normativa de referencia.

Artículo 4. Principios de la seguridad de la información.

Artículo 5. Alcance.

Capitulo II. Organización de la Seguridad de la Información.

Artículo 6. Comité de gestión de la seguridad de la información.

Artículo 7. Roles.

Artículo 8. Resolución de conflictos.

Artículo 9. Obligaciones del personal.

Capitulo III. Asesoramiento especializado en materia de seguridad.

Artículo 10. Asesoramiento especializado.

Artículo 11. Cooperación entre organismos y otras Administraciones Públicas.

Artículo 12. Revisión independiente de la seguridad de la información.

Capitulo IV. Protección de datos, formación y gestión.

Artículo 13. Tratamiento de los datos de carácter personal.

Artículo 14. Formación y concienciación.

Artículo 15. Análisis y gestión de riesgos de los sistemas de información.

Capítulo V. Estructura Normativa.

Artículo 16. Estructura de la documentación de seguridad.

Artículo 17. Primer nivel: Política de seguridad.

Artículo 18. Segundo Nivel: Normativa de uso de medio y códigos de conducta en relación a la Tecnología de la Información.

Artículo 19. Tercer Nivel: Procedimientos técnicos de seguridad.

Artículo 20. Cuarto Nivel: Informes, registros y evidencias electrónicas.

Artículo 21. Otra documentación.

Disposición final primera. Publicidad de la política de seguridad.

Disposición final segunda. Entrada en vigor.

Disposición final tercera. Derogación.

CAPÍTULO I

Política de Seguridad de la Información del Centro Nacional de Investigaciones Oncológicas

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, señala entre sus fines la creación de unas condiciones de confianza en el uso de los medios electrónicos. Se establece para ello las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal garantizando la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. Estos fines han sido desarrollados por 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. Asimismo, la información tratada en los sistemas electrónicos a los que se refiere el ENS estará protegida teniendo en cuenta los criterios establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

El ENS, por su parte, establece el marco regulatorio de la 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. La Política de Seguridad debe generarse conforme con los requisitos que figuran en el ENS que establece que todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de una Política de Seguridad de la Información aprobada por el órgano superior competente.

En virtud de lo expuesto, la Política de Seguridad de la Información del Centro Nacional de Investigaciones Oncológicas se regirá por las siguientes normas:

Artículo 1. Objeto y ámbito de aplicación.

1. Constituye el objeto de la presente Resolución la aprobación de la Política de Seguridad de la Información, en adelante Política de Seguridad, del Centro Nacional de Investigaciones Oncológicas (en adelante CNIO), y el establecimiento de un marco organizativo y tecnológico de la misma.
2. Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.
3. Debe ser conocida y cumplida por todo el personal del CNIO, independientemente del puesto, cargo y responsabilidad dentro del mismo.

Artículo 2. Misión.

1. Corresponden al CNIO las competencias y funciones establecidas por los estatutos del propio organismo, así como aquellas que derivaran de su relación con el resto de administraciones públicas del estado o los ciudadanos.

Artículo 3. Legislación y normativa de referencia.

1. Serán base del cumplimiento normativo para la generación de la presente política de seguridad, las siguientes normas:

   - Ley 11/2007, de 22 de junio, de Acceso Electrónico de los ciudadanos a los Servicios Públicos.

   - 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.

   - 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 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

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

   - 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.

   - Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común.

   - Ley 59/2003, de 19 de diciembre, de firma electrónica.

   - Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

   - Otras normativas internas.

Artículo 4. Principios de la Seguridad de la Información.

1. Los principios que conforman la Política de Seguridad de la Información son los siguientes:

   – La información que posee y trata CNIO tiene un valor muy importante para el propio organismo así como para los ciudadanos y otros organismos públicos, por lo que es primordial protegerla.

- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola con la confidencialidad e integridad debida.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información del CNIO deben atender a la necesidad de protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada, tal y como regula el propio ENS.
- La información relativa a las personas y ciudadanos que trate el CNIO pertenece a ellos y no a la Administración conforme a la normativa en protección de datos de carácter personal del que se da debido cumplimiento.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos, según los preceptos marcados por el ENS y otras normas en vigor que le fueran de aplicación.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad, así como las guías CCN-STIC de la serie 800 elaboradas por el Centro Criptológico Nacional adscrito al Centro Nacional de Inteligencia.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

Artículo 5. Alcance.

1. Debido a la misión de la entidad, la organización desestima la aplicación de la presente política de seguridad sobre todo el conjunto del sistema de información.

   En base a ello, la organización aplicará la presente política sobre el grueso de los sistemas TIC que gestiona de manera centralizada a través del Servicio de Tecnologías de la Información y las Comunicaciones. Será de aplicación específicamente sobre todos aquellos sistemas que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de

deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

2. De forma concreta la presente política de seguridad en relación con el cumplimiento del ENS es aplicable sobre los siguientes servicios y los sistemas TIC que los conforman:

   – Servicio de Biotecnología.

   – Análisis clínico.

   – Formación y doctorado.

   – Eventos científicos organizados por el organismo.

3. Adicionalmente y aun entendiéndose que otros servicios del centro no se encuentran directamente en el alcance estipulado por el Esquema Nacional de Seguridad, debido a su importancia en la funcionalidad del centro, se acuerda extender el alcance de la Política de Seguridad y el cumplimiento del ENS a otros servicios del centro necesarios para el cumplimiento de los objetivos fundamentales del mismo tal y como se detallan en sus estatutos.

CAPÍTULO II

Organización de la Seguridad de la Información

Artículo 6. Comité de Gestión de la Seguridad de la Información.

1. Las funciones asignadas al Comité de Gestión indicadas en el RD 3/2010 las asume un equipo coordinado, compuesto por los diferentes roles definidos en el ENS.

   - La Comisión de Seguridad tendrá informado al Equipo de Gobierno.

   - Las funciones de la Comisión de Seguridad en relación al ENS son:

     - Divulgación de la política y normativa de seguridad de la Organización.

     - Aprobación de la normativa de seguridad de la Organización.

     - Revisión anual de la política de seguridad.

     - Desarrollo del procedimiento de designación de roles.

Artículo 7. Roles.

1. Adicionalmente al comité cada responsable en relación al cumplimiento del ENS, tendrá definidas sus propias tareas.

2. Responsable de la información y servicios.

Serán tareas a llevar a cabo por el Responsable de Información y Servicio en relación al Esquema Nacional de Seguridad las siguientes:

- Identificar, valorar y aprobar la información de ciudadanos o de otras administraciones públicas que fueran tratada por el Centro Nacional de Investigaciones Oncológicas.
- Identificar, valorar y aprobar los servicios tecnológicos prestados a ciudadanos o a otras administraciones públicas por el Centro Nacional de Investigaciones Oncológicas.
- Será conocedor del estado de la seguridad de la información tratada, así como de los servicios prestados.
- Comunicará al gobierno del organismo la necesidad de suspender un servicio por aquellas violaciones de la seguridad que afectaran a la información manejada o al propio servicio.

El rol del Responsable de la información y servicios recae sobre el Director Técnico del CNIO.

3. Responsable de Seguridad

Serán tareas a llevar a cabo por el Responsable de Seguridad en relación al Esquema Nacional de Seguridad las siguientes:

- Asesorar a los responsables correspondientes, en las tareas de identificación de la información y servicios, así como en la evaluación de los niveles de seguridad requeridos para la información y el servicio.
- Realizar la categorización del sistema en el Centro Nacional de Investigaciones Oncológicas.
- Elaborar la política de seguridad.
- Realizar el análisis de riesgos sobre los sistemas de Información según determina las normas de seguridad anexas al Esquema Nacional de Seguridad.
- Elaborar el documento de aplicabilidad del Esquema Nacional de Seguridad.
- Establecer las medidas de seguridad en función del nivel de seguridad resultante.
- Elaborar los documentos con los procedimientos operacionales de gestión de la seguridad, así como la normativa de uso de medios que será aprobada por la dirección.
- Revisar la puesta en marcha de los procedimientos operaciones de gestión de la seguridad, así como su evaluación en el ciclo de vida de los sistemas de la información.

- Elaborar los planes de mejora de la seguridad.

El rol del Responsable de Seguridad recae sobre el Responsable de Sistemas de Información del CNIO.

4. Responsables del Sistema IT.

Serán tareas a llevar a cabo por el Responsable del Sistema en relación al Esquema Nacional de Seguridad las siguientes:

- La implementación de las medidas de seguridad de índole técnicas que hubiera estipulado como necesarias el Responsable de Seguridad.
- La puesta en marcha de los planes de continuidad de servicio, asesorado por el Responsable de Seguridad.

El rol del Responsable del Sistema recae sobre el Responsable de SAP del CNIO.

5. Administrador de la Seguridad del Sistema

Serán tareas a llevar a cabo por el Administrador de la Seguridad del Sistema las siguientes:

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- La aprobación de los cambios en la configuración vigente del Sistema de Información.
- El asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- El asegurar que son aplicados los procedimientos aprobados, para manejar el sistema de información.
- El supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- La monitorización del estado de seguridad del sistema, proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica que se hubieran implementado.

El Administrador de Servicios de Red e infraestructura del CNIO será el Administrador de la Seguridad del Sistema.

Artículo 8. Resolución de conflictos.

1. En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad.

Artículo 9. Obligaciones del Personal.

1. Todo el personal del CNIO, así como el que preste servicios al Organismo relacionados con los sistemas de información, tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas y lo procedimientos derivados de la misma. Se encontrarán entre ellas las relativas a la protección de datos de carácter personal, debiendo el Responsable de Seguridad disponer de los mecanismos necesarios para que la información llegue a todos.
2. El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

CAPÍTULO III

Asesoramiento especializado en materia de seguridad

Artículo 10. Asesoramiento especializado.

1. El Responsable de Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en CNIO con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

Artículo 11. Cooperación entre organismos y otras Administraciones Públicas.

1. A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, CNIO podrá mantener contactos periódicos con organismos y entidades especializadas en temas de seguridad.

Artículo 12. Revisión independiente de la Seguridad de la Información.

1. El Comité de Seguridad propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la Política de Seguridad con el fin de garantizar que las prácticas en el CNIO reflejan adecuadamente sus disposiciones.

CAPÍTULO IV

Protección de datos, formación y gestión

Artículo 13. Tratamiento de los datos de carácter personal.

1. Para el tratamiento de datos de carácter personal en los sistema de información se seguirá en todo momento lo desarrollado en el documento de seguridad y su documentación asociada conforme a lo exigido en el Título VIII de las medidas de seguridad en el tratamiento de datos de carácter personal 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.

Artículo 14. Formación y concienciación.

1. El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal del CNIO y a todas las actividades de acuerdo al principio de seguridad integral recogido en el artículo 5 del ENS. A estos efectos, el CNIO, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.
2. El responsable de seguridad aprobará una Política de formación y concienciación en el tratamiento seguro de la información con los siguientes objetivos:
    a) Formación sobre la protección de la información de datos de carácter personal, orientada a los responsables de los ficheros y hacia los usuarios con privilegios sobre los datos.
    b) Formación sobre los procedimientos desarrollados.

Artículo 15. Análisis y gestión de riesgos de los sistemas de información.

1. CNIO asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigentes bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad en análisis y gestión de riesgos.
2. Con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en seguridad, el responsable de seguridad acordará la realización de un análisis de riesgos cuyas conclusiones se plasmarán en actuaciones para tratar y mitigar el riesgo, e incluso replantear la seguridad de los sistemas en caso necesario.
3. Se contemplará la realización adicional de un análisis de riesgos de los sistemas de información cuando:
    a) Se modifiquen los servicios que almacenan o tratan la información.

b) Se modifiquen los servicios prestados.

c) Ocurran incidentes graves de seguridad.

d) Se reporten vulnerabilidades graves que afecten a los sistemas de la información de la Organización.

4. Las conclusiones de los análisis de riesgos serán revisadas por el Responsable de Seguridad y éste las comunicará al Comité de Seguridad.

CAPÍTULO V

Estructura normativa

Artículo 16. Estructura de la documentación de seguridad.

1. La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

   a) Primer nivel: Política de Seguridad de la Información.

   b) Segundo nivel: Normativa de uso de medios y códigos de conducta en relación a la Tecnología de la Información

   c) Tercer nivel: Procedimientos Técnicos de Seguridad.

   d) Cuarto nivel: Informes, registros y evidencias electrónicas.

Artículo 17. Primer nivel: Política de Seguridad.

1. Documento de obligado cumplimiento por todo el personal, interno y externo, recogido en el presente documento y aprobada por la Dirección Gerencia del CNIO.

Artículo 18. Segundo Nivel: Normativa de uso de medios y códigos de conducta en relación a la Tecnología de la Información.

1. De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente.

2. La responsabilidad de aprobación de los documentos redactados en este nivel será competencia de la Dirección Gerencia del CNIO.

Artículo 19. Tercer Nivel: Procedimientos Técnicos de Seguridad.

1. Documentos 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.

2. La responsabilidad de aprobación de estos procedimientos técnicos es del Responsable de Seguridad.

Artículo 20. Cuarto Nivel: Informes, registros y evidencias electrónicas.

1. Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida de los sistemas de la información.
2. La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información en su ámbito de actuación.

Artículo 21. Otra documentación.

1. Se podrá seguir en todo momento los procedimientos STIC, las normas STIC, las instrucciones técnicas STIC, así como las guías CCN-STIC de las series 800.

Disposición final primera. Publicidad de la Política de Seguridad.

La presente Resolución se publicará, en la plataforma web del Centro Nacional de Investigaciones Oncológicas.

Disposición final segunda. Entrada en vigor.

La Política de Seguridad será de aplicación a partir del día siguiente al de su aprobación por la Dirección Gerencia del Centro Nacional de Investigaciones Oncológicas.

Disposición final tercera. Derogación.

La presente Política de Seguridad que se aprueba deroga las anteriores políticas de seguridad que existieran en el Centro Nacional de Investigaciones Oncológicas.