POLÍTICA

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

COD. PO-12
Edición 05.2

Elaborado por:	Revisada esta edición por:	Aprobada esta edición por:
Juan Ramón Martín Huertas RSI-ASCS Firmado digitalmente por: MARTIN HUERTAS JUAN RAMON - [redacted] Motivo: Política de Seguridad ASCS Localización: Málaga Fecha y hora: 04.03.2020 11:11:25 Fecha 04/03/2020	Comité de Seguridad Fecha: 03/03/2020	Mª. Luisa Lorenzo Nogueira Directora Gerente Firmado digitalmente por: LORENZO NOGUEIRAS MARIA LUISA - [redacted] Motivo: Política de Seguridad ASCS Localización: Málaga Fecha y hora: 04.03.2020 11:13:47 Fecha:04/03/2020

Control de cambios:

15/10/2012 – Primera edición
16/09/2013 – Suprimida marca de agua "pendiente publicación Boja"
29/09/2014 – Segunda edición. Adaptado a Organización seguridad.
17/05/2016 – Edición 03. Revisión responsable ASCS y Comité Seguridad. Cambiado Logotipo.
10/07/2018 – Edición 04 Cambios legislativos varios (ley 11, RGPD, etc.)
27/07/2019 – Edición 05. Cambios legislativos varios (ISO/IEC 27002, RD 951/2015, etc.) e inclusión de responsables (Sistemas, Servicio e Información).
08/08/2019 - Aprobada Comité de Seguridad
12/02/2020 - Añadido art.7 Resolución conflictos. Posicionamiento y otros.
03/03/2020 – Actualizado posicionamiento, objetivo y logo Agencia.

ÍNDICE

Índice de contenido

1. OBJETIVO....4
2. ÁMBITO DE APLICACIÓN....5
3. LEYES Y REGLAMENTOS....6
4. RESPONSABILIDADES....7
5. DESCRIPCIÓN....8
6. APROBACIÓN Y ENTRADA EN VIGOR....14
7. ANEXOS....15
Anexo I. Requisitos mínimos....15
8Anexo II. Referencias legislativas....18

1. OBJETIVO.

La seguridad en los sistemas de información es un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos sobre los que gravita mediante la formación, concienciación e información continua, la responsabilidad de la calidad y continuidad de los servicios prestados al ciudadano, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural. (art.4 ENS).

Nuestra política de seguridad de los sistemas de información (PSSI) se entiende como **el conjunto de normas, reglas y prácticas, que regulan el modo en que los bienes que contienen información sensible son gestionados, protegidos y distribuidos dentro de nuestra organización**. La PSSI afecta, por tanto, a la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de estos bienes y de su uso.

Más allá que atender un simple imperativo legal se pretende alcanzar un marco que garantice la continuidad y la calidad del servicio que ésta presta a los ciudadanos, atendiendo especialmente a los aspectos soportados por las tecnologías de la información y que nace de la compresión de la seguridad como un proceso integral técnico, humano y organizativo.

La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarcan políticas, prácticas, procedimientos, estructuras organizativas y funciones. Para la correcta implementación y cumplimiento de la presente Política de Seguridad es necesario aplicar los siguientes requisitos de seguridad de obligado cumplimiento tal como se describe en el anexo I de este documento.

La Consejería de Salud de la Junta de Andalucía, y por ende todos sus organismos, asumen el compromiso de controlar sus riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigentes bajo un proceso de mejora continua mediante la implementación en espiral de un Sistema de Gestión de Seguridad de la Información (SGSI), ajustado a los marcos metodológicos vigentes (MAGERIT, Metodología de Análisis y Gestión de Riesgos para la Seguridad de los Sistemas de Información del Ministerio para las Administraciones Públicas; ISO/IEC 27001 y 27002) con el fin de estudiar y actuar sobre el nivel de exposición de los sistemas de información e infraestructuras de la organización, adoptando una perspectiva de estudio de riesgos (art. 6 ENS), y abordando los aspectos de seguridad necesarios para la protección y funcionamiento de estos sistemas.

Las medidas de seguridad se contienen en el conjunto de políticas, normas y procedimientos de seguridad de la Agencia Sanitaria Costa del Sol, entre ellas las contenidas en el **Documento de Seguridad del RGPD**, que afecta al tratamiento de datos personales, siendo todas ellas de obligado cumplimiento para el personal con acceso a los sistemas de información, tanto automatizados como no automatizados, y que efectúen o no tratamientos.

2. ÁMBITO DE APLICACIÓN.

La política será de aplicación a:

1. La Agencia Publica Empresarial Sanitaria Costa del Sol, tanto en sus servicios centrales como periféricos.

2. Todos los trabajadores de la (ASCS).

3. Toda persona que, no estando adscrita a la ASCS, tenga acceso a la información gestionada por la ASCS o a los sistemas de información de la misma.

3. LEYES Y REGLAMENTOS.

La PSSI se fundamenta en las siguientes normas de rango legal y reglamentario:

- **Reglamento General de Protección de Datos de la Unión Europea**, por la que se hace necesario adoptar medidas organizativas y técnicas que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información, garantizando la restricción de utilización, la prevención de alteraciones y la protección a procesos informáticos, con el fin último de que en el tratamiento de datos personales se protejan las libertades públicas y los derechos fundamentales de las personas físicas, especialmente su honor e intimidad personal y familiar (Considerandos 1 a 4 y Art. 1).
- Ley Orgánica 3/2018, de 5 de diciembre, de **Protección de Datos Personales y garantía de los derechos digitales** (LOPDgdd).
- Real Decreto 3/2010, de 8 de enero, que regula el **Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica** cuya finalidad es la creación de las 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, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- 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.
- Decreto 1/2011, de 11 de enero, por el que se establece la **Política de Seguridad de las tecnologías de la información y comunicaciones (TIC) en la Administración de la Junta de Andalucía** y en particular lo indicado en el apartado 2 del artículo 1 en su capítulo I, donde se dice que cada entidad incluida en el ámbito de aplicación del Decreto desarrollará y aprobará formalmente el documento de política de seguridad TIC para la misma.
- Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.
- Resolución de 27 de septiembre 2004, de la Secretaría General para la Administración Pública, por la que se establece el **manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía**.

4. RESPONSABILIDADES.

Todos los profesionales sanitarios y no sanitarios tienen el deber de cumplir las especificaciones de esta política en materia de seguridad de sistemas de información.

Será responsabilidad de la Dirección la tutela y correcta aplicación de la Política, así como del cumplimiento de los procedimientos asociados a la misma.

Todas las personas empleadas que presten servicios en la ACS o en sus entidades vinculadas o dependientes tienen la obligación de conocer y cumplir la política de seguridad de la información y las normas de seguridad derivadas, siendo responsabilidad del Comité de Seguridad TIC establecer mecanismos adecuados para que la información llegue a las personas afectadas.

Todas las personas empleadas que se incorporen a la ASCS o a sus entidades vinculadas o dependientes, o vayan a tener acceso a datos personales tratados por esta, o a algunos de sus sistemas de información, deberán ser informadas de la política de seguridad de la información y la normativa de seguridad derivada. Dicha información será proporcionada por la persona de la que dependa jerárquicamente la persona recién incorporada o a través de los medios que se articulen en función de la vinculación por la que tenga acceso a dichos datos.

Las personas empleadas públicas al servicio de la Administración de la Junta de Andalucía comprendidas dentro del ámbito de esta política deberán cumplir, además, con las instrucciones y normas que regulen el comportamiento de las personas empleadas públicas en el uso de los sistemas informáticos y redes de comunicaciones de esta.

Cualquier persona que actúe bajo la autoridad del Responsable o Encargado de un Tratamiento de datos personales en el ámbito de aplicación de esta política y tenga acceso a datos personales, solo tratará dichos datos respetando las instrucciones del Responsable del Tratamiento, salvo que esté obligada a ello en virtud del ordenamiento jurídico comunitario, nacional o autonómico.

5. DESCRIPCIÓN.

Artículo 1.- Todas las personas que prestan sus servicios en los distintos centros de la ASCS deberán cumplir las directrices, normas y procedimientos que se establecen en esta Política y que el cumplimiento de ésta pudiera generar, en el Documento de Seguridad de la ASCS, así como en la normativa vigente en materia de seguridad y protección de datos, en concreto el Reglamento General de Protección de Datos de la Unión Europea, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el Real Decreto 3/2010 que regula el Esquema Nacional de Seguridad y el Decreto 1/2011, por el que se establece la Política de Seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Sin perjuicio de las directrices establecidas en el marco normativo de seguridad TIC de la administración de la Junta de Andalucía.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad. (art.4 ENS) desplegándose los programas de formación específicos que se estimen necesarios según la evolución de los riesgos, amenazas y marco normativo.

Artículo 2.- Se consideran instrumentos básicos para el desarrollo de la presente Política de Seguridad a los siguientes:

- **Documento de Seguridad** con el ordenamiento normativo de obligado cumplimiento en cuanto a medidas de seguridad.
- Sistema de aseguramiento de la calidad (SAC) como vértice del trinomio Funcionalidad-Calidad-Seguridad, siendo esta última un elemento más de las funcionalidades a exigir a los sistemas.

Artículo 3.- Todas las medidas en materia de seguridad contempladas en el Esquema Nacional de Seguridad al caso, serán aplicadas y de obligado cumplimiento para toda la organización. En particular se tomarán:

- Medidas de Protección de las instalaciones e infraestructuras, para lo cual se proveerán los recursos necesarios a tal efecto (art. 17 ENS).
- Medidas orientadas a garantizar la continuidad del servicio mediante el fomento de la realización de estudios y análisis de impacto y la confección y mantenimiento de un plan de continuidad.
- Gestión de personal, fundamentada en la profesionalización (art. 15 ENS), junto con la formación e información de naturaleza iterativa y atendiendo siempre el "estado del arte" en los aspectos de seguridad en IT.
- Protección de activos, que permiten la existencia de servicios y atención al ciudadano.
- Protección de la información, según marca el RGP.
- Protección de las aplicaciones, teniendo especial atención al desarrollo, a la aceptación y puesta en servicio.
- Generación y actualización de la documentación existente en materia de seguridad.
- Todas aquellas que, a propuesta del **Comité de Seguridad** y/o el **Delegado de Protección de Datos** se estime oportuno.

Todas estas actuaciones, así como cualquier otra medida en este ámbito, deberán de ser enmarcadas en un conjunto programático o línea de actuación, evitándose el carácter puntual de las mismas y permitiéndose así, su supervisión, control, métrica y análisis de impacto en los aspectos de funcionalidad y continuidad del servicio.

Asimismo, se realizarán de forma periódica análisis y gestión de riesgos de seguridad, que garanticen que las medidas adoptadas para mitigar o suprimir los riesgos sean proporcionales a los riesgos de seguridad.

Artículo 4.- Todas las personas que prestan sus servicios en los distintos centros de la Agencia deberán:

- Conocer y cumplir las obligaciones relativas al uso correcto de los recursos informáticos y documentales, **recogidas en la Resolución de 27 de septiembre de 2004 de la Secretaría General para la Administración Pública** (Manual del Empleado Público), así como en las demás normas sobre esta materia.
- Conocer los tratamientos con datos de carácter personal declarados por la Agencia en su registro de Actividades de Tratamiento y que se relacionen con las funciones a desarrollar en su puesto de trabajo. Además, deberán cumplir cuantas medidas sean adoptadas por los titulares de los Órganos responsables de dichos tratamientos, tanto en lo relativo a la seguridad de los datos como en lo referente al cumplimiento de aquellas otras medidas dirigidas a hacer efectivas las garantías, derechos y obligaciones contemplados en la normativa de protección de datos vigente.
- Asumir el deber de colaboración con la Organización en el interés de que no se produzcan alteraciones o violaciones de estas reglas y da cuenta inmediatamente de todas las incidencias de que tenga conocimiento al inmediato superior. El incumplimiento de esta Orden podrá dar lugar a la exigencia de responsabilidad disciplinaria conforme a los procedimientos legales y demás normas aplicables.

Artículo 5.- Esta Política de seguridad se difundirá, por los titulares de los órganos directivos, entre todo el personal que preste sus servicios en la ASCS.

Artículo 6.- La organización de la seguridad en la ASCS será la siguiente:

- **Comité de Seguridad de la Información que es el máximo órgano al que compete la Seguridad de la Información en la ASCS. Este Comité dirige y controla los procesos relacionados con la seguridad. Y tiene como funciones:**

  1. Su principal función y responsabilidad es la de establecer objetivos y estrategias relacionados con la seguridad de la información.
  2. Debe periódicamente revisar el estado general de la seguridad de la información.
  3. Revisar y monitorizar los incidentes de seguridad de la información.
  4. Revisar y aprobar los proyectos de seguridad de la información.
  5. Aprobar las modificaciones o nuevas políticas de seguridad de la información.
  6. Realizar otras actividades de alto nivel relacionadas con la seguridad de la información.

  El comité de seguridad de la información debe estar conformado por miembros de alto nivel de los departamentos y Áreas de la ASCS, y queda reflejado en el documento de Organización de la seguridad en la ASCS.

- **El Responsable del Tratamiento es la Agencia Sanitaria Costa del Sol (representada en la persona de su Director Gerente), definido como el órgano administrativo que tiene atribuida la competencia a la que sirva instrumentalmente los datos contenidos en el fichero y los tratamientos que con ellos se realicen. Como tal responsable de tratamiento, ostenta las siguientes funciones:**

    1. Decidir sobre la finalidad, uso y contenido de los ficheros y los tratamientos a realizar.
    2. Nombrar uno o varios Responsables de Seguridad encargados de coordinar y controlar las medidas de seguridad definidas en el Documento de Seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al Responsable del Tratamiento.
    3. Seleccionar un encargado con garantías (art. 28).
    4. Garantizar principios relativos al tratamiento (art. 5).
    5. Establecer la legitimidad del tratamiento (art. 6).
    6. Obtener un consentimiento válido (arts 7 i ss).
    7. Transparencia en la recogida de datos (arts. 12 i ss).
    8. Garantizar los derechos de los interesados (arts 15 i ss).
    9. Medidas de seguridad (art. 24 i 32).
    10. Privacidad desde el diseño y por defecto (art. 25).
    11. Registro de actividades de tratamientos (art. 30).
    12. Notificar incidencias de seguridad (art. 33 i 34).
    13. Evaluación de impacto de protección de datos (art. 35).
    14. Consulta previa a la Agencia de Protección de Datos (art. 36).
    15. Nombramiento del Delegado en Protección de Datos (arts. 37 i ss).
    16. Control de transferencias internacionales de datos (art. 46).

    La persona en quien recaerá la figura del Responsable del Tratamiento queda reflejada en el documento de Organización de la seguridad en la ASCS

- **Delegado de Protección de Datos (DPD/DPO) de la Información que asuma las tareas y responsabilidades que conlleva este rol:**

    1. Informar, asesorar y sensibilizar al responsable de la empresa y a sus trabajadores de las obligaciones que deben cumplir, en particular en relación a las medidas técnicas y organizativas de seguridad respecto de los datos personales que tratan de sus clientes, trabajadores… y documentarlo.
    2. Supervisar la implementación y aplicación de las políticas de la empresa en materia de protección de datos personales, incluida la asignación de responsabilidades, la formación de los trabajadores y las auditorías correspondientes.
    3. Supervisar la implementación y aplicación de la normativa, en particular por lo que hace referencia a los requisitos relativos a la protección de datos desde el diseño, es decir, la protección de datos por defecto y la seguridad de los datos.
    4. Atender las peticiones de información de los interesados y las solicitudes presentadas en el ejercicio de sus derechos de conformidad con la legislación de protección de datos.

5. Velar por la conservación de la documentación que contenga datos personales.
6. Supervisar la documentación, notificación y comunicación de las violaciones de datos personales de conformidad con la normativa.
7. Supervisar la realización de la evaluación de impacto relativa a la protección de datos por parte de la empresa y la presentación de solicitudes de autorización o consultas previas, si fueran necesarias de conformidad con el reglamento.
8. Supervisar la respuesta a las solicitudes de la Agencia Española de Protección de Datos y cooperar con la misma a solicitud de esta o a iniciativa propia.
9. Actuar como punto de contacto para la Agencia Española de Protección de Datos (autoridad de control) sobre las cuestiones relacionadas con el tratamiento y consultar con la misma, si procede, a iniciativa propia.
10. Comprobar la conformidad del tratamiento cuando sea necesario realizar una consulta previa a la Agencia Española de Protección de Datos.

La persona en quien recaerá la figura del Responsable de Protección de Datos queda reflejada en el documento de Organización de la seguridad en la ASCS.

- **Responsable de los Servicios y de la Información que asuma las tareas y responsabilidades que conlleva este rol:**

  El responsable de la Información (propietario de la información), en lo relativo al ENS, es la figura que determinará y aprobará los niveles de seguridad del servicio y de la información dentro del marco establecido en el anexo I del RD 3/2010, por el que se regula el Esquema Nacional de Seguridad, siendo posible la presentación de una propuesta previa por parte del Comité de Seguridad.

  La persona en quien recaerá la figura de Responsable de Información queda reflejada en el documento de Organización de la seguridad en la ASCS y, de acuerdo con la guía de seguridad CCN-STIC-801, deberá tener la responsabilidad última del uso que se haga de la información y, por tanto, de su protección. Es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

  Las personas en quienes recaerán la figura del Responsable del Servicio y de la Información, coinciden con los Responsables Funcionales RGPD, y quedan reflejadas en el documento de Organización de la seguridad en la ASCS.

- **Responsable Funcional RGPD velará por el cumplimiento de sus funciones y obligaciones en su concreto ámbito de actuación. En términos generales, las funciones y obligaciones de los responsables funcionales RGPD vienen designadas y heredadas de las funciones del Responsable del Tratamiento y por tanto son:**

  1. Velar por el cumplimiento de las normas de seguridad comprendidas en el **Documento de Seguridad** en el tratamiento de los datos
  2. Conceder o denegar a los trabajadores de su área o unidad la autorización de acceso a los sistemas de información.
  3. Notificar al **Comité de Seguridad** cualquier modificación que se produzca en la estructura de datos de los sistemas de información.
  4. Adoptar medidas oportunas para que todo el personal de su unidad orgánica conozca las normas de seguridad que afecten el desarrollo de sus funciones y las consecuencias en que pueden incurrir en caso de incumplimiento.
  5. Designar a los trabajadores autorizados para realizar los tratamientos.
  6. Informar respecto a las demandas de cesión de datos a terceras personas.

7. Describir la estructura de datos de los ficheros y tratamientos con los mismos que sean de su responsabilidad.
8. Velar por el cumplimiento de las obligaciones derivadas de los principios de información y consentimiento de RGPD y asumir el control de estas obligaciones en todos los sistemas de recogida de datos personales de los tratamientos de su responsabilidad.

Las personas en quienes recaerán las figuras de los Responsables Funcionales RGPD quedan reflejadas en el documento de Organización de la seguridad en la ASCS.

- **Responsable de Seguridad (Organizativa, TIC) de la Información que asuma las tareas y responsabilidades que conlleva este rol:**
  1. Proporcionar soporte, asesorar e informar al Comité de Seguridad de la ASCS, así como de ejecutar las decisiones y acuerdos adoptados por este.
  2. Diseñar y ejecutar los programas de actuación propios de la ASCS, incluyendo, entre otros, planes directores de seguridad, proyectos de desarrollo normativo, auditorías de cumplimiento y planes de adecuación legal.
  3. Definir, implantar y mantener los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como la realización y mantenimiento de los análisis de riesgos de la ASCS.
  4. Definir y ejecutar los programas formativos y de concienciación relacionadas con buenas prácticas de seguridad de la información en el ámbito de la ASCS.
  5. Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio.
  6. Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad de la información.
  7. Dar las directivas para controlar el acceso a los sistemas de información y la modificación de privilegios.
  8. Identificar qué Leyes, Normativas o Reglamentos pueden tener incidencia, en términos de seguridad de la información, con el fin de evaluar su impacto y proponer las medidas que resulten de aplicación
  9. Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes.
  10. Recibir capacitación en el tema de seguridad de la información.
  11. Realizar estudios de penetración y pruebas de seguridad en todos los ambientes (Desarrollo, Pruebas, Producción y Contingencia).
  12. Prestar apoyo en tareas de seguridad de la información para la organización al Delegado de Protección de Datos.
  13. Es Responsable de Seguridad, en los términos establecidas en 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.

La persona en quien recaerá la figura del Responsable de Seguridad queda reflejada en el documento de Organización de la seguridad en la ASCS.

- **Responsable del Sistema y Seguridad Fisica, cuyas tareas y responsabilidades en lo relativo al ENS son**:
  1. Gestionar el Sistema durante todo su ciclo de vida, desde la especificación, la instalación, hasta el seguimiento de su funcionamiento.
  2. Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.

3. Implantar y controlar las medidas específicas de seguridad del Sistema.
4. Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
5. Suspender el manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.
6. Identificación de necesidades de seguridad física. Conseguir la elaboración de un presupuesto anual de inversiones y actuaciones en seguridad física. Supervisar la instalación y el mantenimiento posterior de los elementos y servicios destinados a la seguridad física. Analizar los incidentes de seguridad física que se puedan haber producido y establecer actuaciones para dar respuesta a los mismos.

La persona en quien recaerá la figura del Responsable del Sistema y Seguridad Fisica queda reflejada en el documento de Organización de la seguridad en la ASCS.

Artículo 7.- Resolución de conflictos.

1. Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura organizativa de la política de seguridad de la información serán resueltos por el superior jerárquico común, que podrá elevar consulta previa al Comité de Seguridad TIC. En caso de conflicto prevalecerán las decisiones del Comité de Seguridad TIC.
2. En los conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad de la información y las personas responsables definidas en la normativa de protección de datos de carácter personal prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

6. APROBACIÓN Y ENTRADA EN VIGOR.

Texto aprobado el día 04 de marzo de 2020 por el Comité de Seguridad de la ASCS. Y rubricado por la Dirección Gerencia y Responsable de Seguridad de la Información.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

7. ANEXOS.

Anexo I. Requisitos mínimos

Para la correcta implementación y cumplimiento de la presente Política de Seguridad es necesario aplicar una serie de requisitos de obligado cumplimiento:

1.1 La seguridad en la Organización

La seguridad debe comprometer a todos los miembros de la ASCS, sin excepción.

En el artículo 6 del apartado 6 (Descripción) del presente documento, se especifica la Organización de la seguridad con la definición de la estructura organizativa.

Asimismo, la implementación de dicha organización está en el marco normativo cubierto por el establecimiento de un sistema de Gestión de la Seguridad, basado en el ENS.

1.2 Análisis y Gestión de riesgos

Los servicios e infraestructuras bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.

La descripción de la metodología y evaluación del riesgo están desarrollados en "Metodología de análisis y gestión de riesgos".

El análisis de riesgos se realizará igualmente cuando se vaya a iniciar o a modificar un tratamiento de datos de carácter personal, en línea a lo establecido en el Reglamento General de Protección de Datos. En estos casos se contemplarán en el alcance del análisis todos aquellos activos que intervengan en el tratamiento, considerando tanto activos relacionados con los sistemas de información, como humanos, locales o terceros.

A raíz de los resultados obtenidos en los mencionados análisis de riesgos se determinarán las medidas necesarias para proteger dichos datos.

1.3 Gestión de personal

En el punto 10.4 Caracterización del puesto de trabajo de la Política de Seguridad del Personal se detalla la obligatoriedad de conocimiento y concienciación en materia de seguridad según sus responsabilidades. Los recursos necesarios para la implementación del sistema de seguridad, así como aquellos que lleven a cabo su operación, mantenimiento, supervisión, o tenga relación con el sistema se establece en los planes estratégicos de la ASCS, y son aprobados por el Comité de Dirección a propuesta del Comité de Seguridad de la Información.

La selección de personal se lleva a cabo, aplicando estos criterios por parte del Responsable de Formación y Selección del Área de Profesionales de la ASCS.

Periódicamente se realizarán evaluaciones de desempeño y seguimiento del personal vía DPPO[1].

1.4 Profesionalidad

En el punto 10.1 de la Política de Seguridad del Personal se detallan los objetivos de las acciones de formación y concienciación y en el 10.3 se detallan las funciones y responsabilidades del personal.

Con periodicidad bianual se diseña un plan de formación específico en el que se tiene en cuenta las necesidades de profesionalización del sistema de seguridad.

1 Dirección Participativa Por Objetivos.

1.5 Autorización y control de Acceso

El acceso a los sistemas de información estará restringido y limitado a aquellos usuarios o procesos que lo necesiten para el desarrollo de su actividad y estén previamente autorizados.

El acceso a la información seguirá el principio de "necesidad de conocer", de forma que los privilegios otorgados a cada entidad sean los mínimos imprescindibles para el desarrollo de su actividad.

La identificación de los usuarios será tal que se pueda conocer en todo momento quién recibe derechos de accesos y quién ha realizado alguna actividad, por lo que los identificadores deberán ser personales, no compartidos, e intransferibles.

Los lugares con acceso restringido igualmente deben estar controlados y previamente autorizados por los responsables asignados.

1.6 Protección de las instalaciones

Los sistemas de información deberán estar ubicados en zonas protegidas, con acceso restringido, habilitado únicamente al personal autorizado. Tal y como se indica en el documento Políticas de Seguridad de la Información apartados 8 y 9 (Políticas de Seguridad física), en el punto 8.3 se definen los responsables y responsabilidades.

1.7 Adquisición de productos

Para el proceso de adquisición de nuevos productos, sistemas o servicios se establecen protocolos de análisis de riesgos con proveedores y se mantienen actualizados los listados de proveedores habituales. Las adquisiciones deben ser autorizadas por los responsables del área implicada y el Área de Suministros a través de informes favorables del proveedor, en caso de requerirse.

1.8 Seguridad por Defecto

Los sistemas y aplicaciones se diseñarán y construirán bajo el principio de seguridad por defecto, de tal forma que:

- El sistema ofrecerá la funcionalidad mínima necesaria, y ninguna adicional. Cualquier función que no sea de interés o innecesaria será deshabilitada o no implementada.
- La operación y explotación de los sistemas estará limitada a aquellas personas o ubicaciones que se autoricen, quedando prohibidas para el resto.
- El uso del sistema ha de ser seguro, de tal forma que el uso inseguro requiera intención por parte del usuario.

La seguridad estará presente desde la concepción de un sistema o aplicación y permanecerá presente durante todo su ciclo de vida.

En la concepción de un nuevo sistema o aplicación, o modificación sustancial de un sistema o aplicación existentes, se contará siempre, y desde el inicio, con la participación del Responsable de Seguridad de la Información

1.9 Integridad y actualización del sistema

Se deberán seguir en todo momento las informaciones acerca de las vulnerabilidades que afectan a los sistemas de información.

Se seguirán las recomendaciones de los fabricantes de equipos y software en cuanto a actualizaciones de seguridad, que deberán ser analizadas en cuanto a su idoneidad y conveniencia, y aplicadas en caso positivo con la menor dilación.

1.10 Protección de la Información Almacenada y en Tránsito

Se deberán proteger los entornos que contienen información almacenada y en tránsito entre entornos inseguros. En este sentido se deberán proteger convenientemente los equipos portátiles que puedan contener información, así como los soportes extraíbles (lápices de memoria, discos duros extraíbles, etc.)

1.11 Prevención ante otros sistemas de información interconectados

Se desplegarán las protecciones necesarias para proteger el perímetro de la red corporativa de ASCS, de forma que se neutralicen las posibles intrusiones procedentes del exterior, ya sea iniciadas malintencionadamente por terceros o como consecuencia de la interconexión con sistemas de terceros.

1.12 Registro de Actividad

Los sistemas y aplicaciones generarán los registros de actividad necesarios para conocer la actividad en los sistemas, de forma que se pueda determinar en todo momento qué persona actúa, sobre qué datos, con qué operaciones y sus privilegios de acceso.

1.13 Gestión de Incidentes de Seguridad

ASCS definirá e implantará procedimientos de gestión de incidentes de seguridad que aseguren la correcta gestión y respuesta efectiva que permita anular o minimizar el impacto del incidente en la información, los servicios, los empleados, los usuarios y, en general, en la actividad de ASCS.

El procedimiento de gestión y respuesta a incidentes de seguridad contemplará la comunicación y notificación de los incidentes a los organismos receptores de dicha información, de acuerdo con la legalidad vigente.

1.14 Continuidad de Negocio

Para asegurar la disponibilidad de los servicios y sistemas de información, ASCS diseñará e implantará Planes de Continuidad de Servicio que eviten las interrupciones de las actividades de la ASCS y garanticen, ante una contingencia, la reanudación de los servicios y sistemas de información a los niveles adecuados de operatividad.

1.15 Gestión de la Seguridad y Mejora Continua

Se deberá establecer un Sistema de Gestión de la Seguridad que permita conocer en cada momento el estado de la seguridad, mediante la definición y medida de indicadores, y permita tomas las decisiones informadas pertinentes para cumplir los requisitos de seguridad establecidos.

Se establecerá un proceso de mejora continua mediante el análisis de la situación, la implantación de nuevas medidas de seguridad, la mejora de las existentes y la aportación de mejoras sugeridas por el Comité de Seguridad de la Información y por toda la ASCS en su conjunto.

8Anexo II. Referencias legislativas

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.

Artículo 11. Requisitos mínimos de seguridad.
1. Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente. √

Anexo II Sección 3.1
La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, 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 para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación. √
d. La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, 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. √

La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Reglamento General de Protección de Datos de la Unión Europea, en lo que corresponda. √

GUÍA DE SEGURIDAD (CCN-STIC-804) ESQUEMA NACIONAL DE SEGURIDAD. GUÍA DE IMPLANTACIÓN (BORRADOR) 2.1.1. [ORG.1] POLÍTICA DE SEGURIDAD
La guía CCN-STIC 805 trata esta sección en detalle.

GUÍA CCN-STIC 805 – POLÍTICA DE SEGURIDAD ISO/IEC 27002:2013:

- 5.1 Política de seguridad de la información
- 6.1.3 Asignación de responsabilidades relativas a la seguridad de la información
- 15.1.1 Identificación de legislación aplicable
- NIST Special Publication 800-12 Chapter 5 – Computer Security Policy
- Criterios de Seguridad:
- Capítulo 3 – Política de seguridad
- Capítulo 4 – Organización y planificación de la seguridad
- RD 1720: artículos 89.1 y 95.1
- Se considerará evidencia suficiente del cumplimiento de esta medida
- existe el documento, firmado por la Dirección.
- el documento cubre los puntos arriba citados.
- existe un procedimiento de revisión y firma regular.

La presente Política será revisada, y modificado su contenido si procediese, en caso de que se produzca algún cambio en cualquiera de los aspectos anteriormente mencionados y de forma rutinaria una vez al año a contar desde la fecha de su aprobación.

En caso de que se necesite modificar el presente texto, el Responsable de Seguridad será el encargado de gestionar la generación una nueva versión actualizada y de su aprobación por el órgano superior competente.

Esta política sera difundida a través de la organización, publicándose en la intranet y otros medios de difusión disponibles en la ASCS.