RESOLUCIÓN POR LA QUE SE APRUEBA LA REVISIÓN DE LA PS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL INSTITUTO DE ESTADÍSTICA Y CARTOGRAFÍA DE ANDALUCÍA

PREÁMBULO

La actividad del Instituto de Estadística y Cartografía de Andalucía (en adelante IECA o Instituto) se ha venido simultaneando con el desarrollo de una Política de Seguridad y con un marco organizativo de la misma aprobados por sucesivas resoluciones de la Dirección de esta Agencia, la última de ellas el 21 de julio del 2022.

El IECA cumple, a fecha de hoy, las disposiciones contempladas en la normativa que regula la protección derivada del secreto estadístico, establecida en la Ley 4/1989, de 12 de diciembre, de Estadística de la Comunidad Autónoma de Andalucía, y la normativa reguladora de la protección de datos de carácter personal, establecida en el Reglamento General de Protección de Datos (en adelante RGPD) y en la Ley Orgánica de Protección de Datos y Garantía de los derechos Digitales (en adelante LOPDGDD).

Asimismo cumple con lo previsto en el Esquema Nacional de Seguridad, regulado en el Real Decreto 311/2022, de 3 de mayo, en el ámbito de la Administración Electrónica, y la recogida en el Decreto 1/2011, de 11 de enero, por el que se establece la Política de Seguridad TIC en la Administración de la Junta de Andalucía y su modificación por el Decreto 70/2017, de 6 de junio y Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

En la implementación de esta política el IECA siempre ha considerado que la seguridad de los activos TIC está íntimamente relacionada con otros aspectos de la misma, que por sí solos también son muy importantes para la organización. Así la protección de la información y los servicios en procedimientos y soportes no automatizados y una adecuada seguridad física de su sede son dimensiones de la seguridad que tienen un tratamiento conjunto, para proporcionar seguridad y protección integral a toda la actividad de la organización. Por estas razones el ámbito de las actuaciones de los perfiles de seguridad actuales incluye los datos sometidos a secreto estadístico, los datos de carácter personal, los activos sometidos al Esquema Nacional de Seguridad, resto de activos TIC y, en general, toda la información y servicios prestados por el IECA.

Así el presente documento se enmarca en un entorno normativo y de recomendaciones en materia de seguridad de la información procedente de diversos entes reguladores, que abarcando distintas facetas de la seguridad, dan lugar a cierta complejidad y, al mismo tiempo, riqueza de matices que deben ser integrados en una política conjunta. En este sentido la organización integra, en esta Política de Seguridad, las diferentes funciones y figuras previstas en la legislación comentada, en aras de una mayor homogeneidad y eficiencia.

También se ha tenido en cuenta, a la hora de asignar funciones y responsabilidades a los distintos órganos de este Instituto, las limitaciones de su estructura orgánica. Así se le asignaron al Consejo de Dirección las funciones encomendadas al Comité de Seguridad, los distintos roles de responsabilidad ejecutiva se

concentraron en la Dirección y el resto en los distintos órganos de gestión que ya venían ejerciendo funciones asimiladas.

Pero la Política de Seguridad debe ser una estrategia viva, permanentemente revisada y sobre todo, es interés del IECA que cale e implique a toda la organización, y que su desarrollo se organice en niveles o ámbitos de actuación que abarque desde lo puramente normativo, hasta lo más procedimental o de apoyo.
La aparición de nueva normativa en materia de seguridad también obliga a la adecuación de la Política de Seguridad, como se establece en la Orden de 4 de abril de 2022 de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades, por la que se modifica la de 12 de julio de 2019, de la Consejería de Economía, Conocimiento, Empresas y Universidad, por la que se establece la Política de Seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería y de sus entidades adscritas, entre las que se encuentra el IECA.

Y por último, la experiencia adquirida en materia de seguridad a lo largo de los años determinan que en el seno del Comité de Seguridad Interior y Seguridad TIC se considere la necesidad de proponer a la Dirección del mismo la revisión de la Política de Seguridad.

La normativa en materia de protección de datos de carácter personal, así como el Esquema Nacional de Seguridad, establecen las figuras de los Responsables de la Información y su Tratamiento y los Responsables del Servicio. En línea con lo expuesto anteriormente, ahora se asignan estos perfiles respectivamente en las personas titulares de las Áreas de Gestión y Secretaria General, y Servicios por ser los que determinan los fines de la información tratada, los recursos y los requisitos para su seguridad, dejando a la persona que ostenta la Dirección del IECA como responsable última de la seguridad interior y de las tecnologías de la información y comunicaciones en el IECA.

También se concretan y detallan las funciones del Responsable de Seguridad TIC y del Delegado de Protección de Datos, proporcionándoles un papel de coordinación y supervisión en el ámbito de activos TIC y de protección de datos de carácter personal respectivamente. Y en un ámbito más global, el Responsable de Seguridad Interior y los Responsables de seguridad del tratamiento no automatizado de los datos de carácter personal.

Asimismo, el Esquema Nacional de Seguridad establece la existencia del Responsable del Sistema, figura con responsabilidad en el desarrollo, despliegue y explotación de los sistemas de información, que ya es asumida por la persona titular del Gabinete Estratégico del servicio de Analítica y Gobierno del Dato de la Agencia Digital de Andalucía que presta su servicios en el IECA. También se incluye una nueva figura, la de Administración de seguridad, que con funciones más operativas dará apoyo al Responsable del Sistema.

En su virtud, y en ejercicio de las competencias que me confiere el artículo 31.3 e) y i) de la Ley 4/1989, de 12 de diciembre, de Estadística de la Comunidad Autónoma de Andalucía, en relación con el artículo 57.2 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, y a propuesta del Comité de Seguridad adoptada en la sesión celebrada en fecha 19 de junio de 2024

RESUELVO

PRIMERO.- Aprobar la revisión de la Política de Seguridad TIC del IECA, cuyo texto consolidado se adjunta a la presente Resolución como Anexo I, adaptado al RGPD, a la LOPDGDD, al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, al Decreto 1/2011, de 11 de enero y su modificación por el Decreto 70/2017, de 6 de junio y Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía, por el que se establece la Política de Seguridad de las tecnologías de la información y las comunicaciones en la Administración de la Junta de Andalucía, y a la Orden de 4 de abril de 2022 de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades, por la que se modifica la de 12 de julio de 2019, de la Consejería de Economía, Conocimiento, Empresas y Universidad, por la que se establece la Política de Seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería y de sus entidades adscritas.

SEGUNDO.- Aprobar el Organigrama de Seguridad del IECA de Andalucía, que se adjunta a la presente Resolución como Anexo II.

TERCERO.- Derogar la anterior Política de Seguridad TIC del Instituto, aprobada mediante Resolución de 19 de diciembre de 2023 del IECA.

CUARTO.- Ordenar la publicación de los documentos relacionados en los apartados PRIMERO y SEGUNDO en la intranet y el portal público de este Instituto, para general conocimiento del personal que presta servicios en el mismo.

El Director del Instituto de Estadística y Cartografía de Andalucía

ANEXO I

DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES DEL INSTITUTO DE ESTADÍSTICA Y CARTOGRAFÍA DE ANDALUCÍA

ÍNDICE

Sumario

SIGLAS

RSEG	–	Responsable de seguridad TIC
RSIS	–	Responsable del sistema
RIT	–	Responsable de la información y de su tratamiento
RSERV	–	Responsable del servicio
RSEGINT	–	Responsable de seguridad interior
RFNA	–	Responsable de ficheros no automatizados
DPD	–	Delegado de protección de datos personales
PS	–	Política de seguridad
CS	–	Comité de seguridad
ENS	–	Esquema Nacional de Seguridad
RGPD	–	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
LOPDGDD	–	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

1. OBJETO

Este documento tiene como objeto establecer la PS interior y seguridad TIC en el IECA, que se ha de aplicar para asegurar las instalaciones, el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos, que gestione el Instituto en el ejercicio de sus competencias. Integrará las políticas de seguridad interior, de seguridad TIC y de protección de datos, y es de obligado cumplimiento, de conformidad con lo dispuesto en la legislación vigente.

Con esta PS se pretende, en definitiva, dirigir y dar soporte a su gestión mediante el establecimiento de una estructura organizativa en la que se apoyará su gobierno, así como de unas directrices básicas de acuerdo a los requisitos propios que le son inherentes y a la regulación aplicable, constituyéndose en el marco dentro del que se definirá el conjunto de procedimientos y prácticas que determinen el modo en que los activos deberán ser gestionados y distribuidos en una situación de protección.

El desarrollo de la PS se realizará en tres niveles:

- Nivel 1.- Consiste en la revisión y aprobación de la PS, que culmina con esta resolución.
- Nivel 2.- En el que la PS se concrete en un conjunto de normativas de seguridad, aprobadas por el CS, que desarrollen la PS del IECA. En ellas se determinarán las funciones, obligaciones y buenas prácticas para todos los usuarios de las instalaciones y con acceso a cualquier activo TIC, y especialmente a los que posibiliten el acceso a datos de carácter personal.
- Nivel 3.- En el que se establezcan y concreten los procedimientos, procesos instrucciones, manuales y guías técnicas, que serán aprobadas por los correspondientes Responsables de Seguridad, de cómo se debe realizar cada tarea de desarrollo de la política y ejecución de las normativas y aplicación de los procedimientos.

2. MARCO NORMATIVO

En cuanto al marco regulador se asume lo que en cada momento se defina en esta materia, en virtud de la disposición adicional primera del Decreto 1/2011, de 11 de enero, por la Consejería competente en materia de coordinación y ejecución de las políticas de seguridad TIC, a propuesta del CS TIC de la Junta de Andalucía, así como por la normativa de protección de datos de carácter personal y del secreto estadístico. Todo ello, sin perjuicio de cualquier otra normativa aplicable al IECA, en virtud de su naturaleza legal y de sus competencias. Se consideran de aplicación directa en el ámbito de la administración electrónica y la ciberseguridad las siguientes:

- Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS 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 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 (Reglamento general de protección de datos)
- Ley 4/1989, de 12 de diciembre, de Estadística de la Comunidad Autónoma de Andalucía
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Reglamento Europeo de Firma Electrónica (eIDAS). Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Decreto 1/2011, de 11 de enero y su modificación por el Decreto 70/2017, de 6 de junio, por el que se establece la PS de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.
- Decreto 171/2020, de 13 de octubre, por el que se establece la PS Interior en la Administración de la Junta de Andalucía.Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.
- Orden de 4 de abril de 2022, por la que se modifica la de 12 de julio de 2019, de la Consejería de Economía, Conocimiento, Empresas y Universidad, por la que se establece la PS de las tecnologías de la información y comunicaciones en el ámbito de la Consejería y de sus entidades adscritas.
- Orden de 22 de julio de 2022, por la que se modifica la Orden de la Consejería de Hacienda, Industria y Energía, de 21 de octubre de 2019, por la que se establece la política de seguridad de la información de la Consejería.

Otras normativas de aplicación serán identificadas mediante el Procedimiento de legislación aplicable.

3. MISIÓN

El IECA, creado por la Ley 4/1989, de 12 de diciembre, es una agencia administrativa con personalidad jurídica pública diferenciada, plena capacidad jurídica y de obrar, patrimonio y tesorería propios, así como con autonomía de gestión para el cumplimiento de sus fines, según el Decreto 372/2009, de 17 de

noviembre, por el que se regula la organización y funcionamiento del Sistema Estadístico de Andalucía, modificado por el Decreto 151/2017, de 26 de septiembre.
De forma general corresponde al IECA la generación y difusión de servicios y productos estadísticos y cartográficos propios, así como la coordinación de las actuaciones, en este ámbito, del resto de las entidades que componen el Sistema Estadístico y Cartográfico de Andalucía.
Para el desarrollo de las actividades que le competen, en el Instituto se recopila información que se organiza en sistemas, se gestiona a través de servicios y se distribuye, una vez agregada, en forma de productos estadísticos y cartográficos.

4. ÁMBITO DE APLICACIÓN

Lo establecido en la PS es de aplicación a todos aquellos aspectos y dimensiones de la actividad del Instituto, de forma que se pueda garantizar sus instalaciones, la integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad de la información, de su tratamiento y de los servicios prestados, por lo que implica a todas sus áreas y unidades.
Todas las personas que prestan sus servicios en el IECA, así como las que se relacionan con el mismo por razón de su actividad, deberán cumplir las directrices, normas y procedimientos que se establecen en este documento o que se generen a raíz de su desarrollo.

5. PRINCIPIOS Y DIRECTRICES

Los principios que deben contemplarse a la hora de garantizar la seguridad so la prevención, la detección, la respuesta y la conservación, de forma que las amenazas existentes no se materialicen o, en caso de que ocurra, no afecten gravemente a la información que maneja o los servicios que se prestan.

5.1 Prevención

Se debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad de cualquier tipo. Para ello deberán implementarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de un análisis de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los responsables de la seguridad interior, la información y los servicios deben:

- Autorizar la entrada en operación de los sistemas.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

5.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respecto a la información, gestionada por sistemas y servicios, es imprescindible una detección rápida de los incidentes que puedan producir brechas de seguridad, y que ponga en riesgo los derechos y libertades de las personas a las que correspondan los datos.

5.3 Respuesta

Se deben:

- Establecer mecanismos de contención para responder rápida y eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

5.4 Conservación

Para garantizar la integridad y confidencialidad de la información y la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC y actividades de recuperación.
11.4 5.5.

5.5 Otros principios generales

A considerar, aparte de los ya relacionados:

- El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniendo su confidencialidad e íntegridad.
- 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 tienen acceso a la información del IECA deben 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.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- 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 ENS, así como las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del 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 RGPD, la LOPDGDD y.la Ley 4/1989, de 12 de diciembre, de Estadística de Andalucía.

6. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad del Instituto se establece mediante la identificación de las diferentes actividades y de sus actores, de la asignación de las correspondientes responsabilidades, en materia de gestión de la seguridad, de la implantación de una estructura que las soporte y de la determinación e implementación de una serie de medidas acordes con la categoría de los datos, sistemas y servicios, que el organismo precisa para el desarrollo de su actividad.

Esta PS se organizará en el IECA tal y como se detalla en el Anexo II y estará integrada por:

- Persona que ostenta la Dirección del IECA
- Comité de Seguridad Interior y Seguridad TIC
- Responsables de la información y de su tratamiento
- Responsables del servicio
- Responsable de seguridad TIC
- Responsable del sistema
- Persona Delegada de protección de datos de carácter personal (DPD)
- Responsables de seguridad de los ficheros no automatizados
- Responsable de seguridad Interior
- Responsabilidad individual

6.1 Persona que ostenta la Dirección del IECA

A la persona titular de la Dirección del IECA le corresponde la dirección, control y supervisión de todas las actividades del organismo (artículo 31.2 de la Ley 4/1989, de 12 de diciembre), por tanto, a nivel de gobierno, es:

- Responsable en el desarrollo de las competencias de seguridad de la entidad.
- Responsable de la implantación del ENS.
- Responsable de garantizar el cumplimiento de las normas relativas a seguridad interior.
- Responsable de la aprobación de la PS y de las medidas propuestas por el CS.
- Nombrar a los responsables y definir sus responsabilidades en gestión de la seguridad TIC
- Aprobar los objetivos, iniciativas y planes estratégicos para la seguridad interior, incluido el Plan de Seguridad Interior.
- Adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Responder a las solicitudes de ejercicio de derechos.
- Responsable de que se realicen controles y de promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de protección de datos.
- Ejecutar los planes de acción e iniciativas que garanticen la implantación de la PS en el IECA.

6.2 Comité de Seguridad Interior y Seguridad TIC

El 26 de abril de 2013 se creó el CS del IECA de conformidad con lo previsto en el artículo 10 del Decreto 1/2011, de 11 de enero y del Decreto 70/2017, de 6 de junio, que lo modifica, así como por el resto de normativa aplicable, Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía y la normativa de protección de

datos de carácter personal. Dicho CS adoptó el cambio de su propia denominación por el de CS Interior y Seguridad TIC, así como la coordinación e integración de ambas actividades, en cumplimiento del Decreto 171/2020, de 13 de octubre y la Orden de 4 de abril de 2022, por la que se modifica la de 12 de julio de 2019, de la Consejería de Economía, Conocimiento, Empresas y Universidad, por la que se establece la PS TIC en el ámbito de la Consejería y de sus entidades adscritas.

El CS Interior y TIC estará constituido por:

- La presidencia le corresponde a la persona titular de la Dirección, que en caso de vacante, ausencia, enfermedad y, en general, cuando concurra una causa justificada, podrá ser sustituida por la persona titular de la Secretaría General.
- Las vocalías les corresponden a las personas titulares de las distintas Áreas de Gestión, la Secretaría General del IECA y la persona RSEG TIC
- La persona titular del servicio competente en materia de seguridad interior, la persona que ejerce de DPD y la persona RSIS, que se incorporan de forma permanente, con voz y sin voto.
- La Secretaría del Comité, que será asumida por la persona titular de la Secretaría General que será suplida, en caso de necesidad, por quien designe la Presidencia.

Podrá convocarse a las personas que ejercen las jefaturas de servicios cuando lo considere la Presidencia, así como a las personas que estime necesarias en función de la materia a tratar.

El CS Interior y Seguridad TIC deberá reunirse al menos semestralmente, y de forma extraordinaria, cuando la Presidencia lo estime conveniente.

La composición del CS Interior y Seguridad TIC, teniendo en cuenta a sus suplentes, deberá tener una representación equilibrada entre hombres y mujeres, conforme a lo establecido en los artículos 3.3 y 11.2 de la Ley 12/2007, de 26 de noviembre. No podrán participar en el mismo aquellas personas que hayan sido condenadas por razón de violencia de género o sobre las que haya recaído sanción por resolución firme en vía administrativa o sentencia judicial firme por razón de discriminación en prácticas laborales.

Son funciones del CS Interior y Seguridad TIC las siguientes:

- Definición y seguimiento de los objetivos, iniciativas y planes estratégicos para la seguridad interior, incluido el Plan de Seguridad Interior.
- Facilitar los recursos necesarios para una adecuada ejecución de la PS.
- Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en el ámbito de la Seguridad TIC.
- Establecimiento de directrices comunes y supervisión del cumplimiento de la normativa de seguridad interior.
- Aprobar la promoción de la educación, el entrenamiento y la concienciación sobre las medidas relativas a la seguridad interior entre el personal.

- Análisis y adopción de decisiones en la respuesta a incidentes susceptibles de generar una crisis de seguridad interior.
- Aprobar las normativas de seguridad TIC que se definan para dar cumplimiento y desarrollo a la PS.

- Resolver discrepancias y problemas que pudieran surgir en la gestión de la seguridad.
- Aceptar los riesgos residuales.
- Aprobar el plan de tratamiento de riesgos.
- Aprobar las normativas de seguridad de obligado cumplimiento.

6.3 Responsables de la información y de su tratamiento

Las personas titulares de las Áreas de Gestión y de la Secretaría General son responsables, a nivel ejecutivo, de toda la información, que tengan capacidad para decidir sobre su finalidad, contenido y uso, así como de su tratamiento, de acuerdo con lo establecido en el ENS y en el RGPD respectivamente.

Entre sus funciones están:

- Determinar los requisitos de seguridad de la información y su tratamiento.
- Autorizar las normas relativas al secreto estadístico y de las de protección de datos de carácter personal.
- Valoración de las consecuencias de una brecha de seguridad relativa a datos personales.
- Garantizar la observancia de los principios relativos al tratamiento incluidos en la política, normativa y procedimientos concernientes a la protección de datos personales.
- Garantizar, en coordinación con el DPD, el adecuado mantenimiento del RAT.
- Realizar controles y promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de protección de datos.

Las personas titulares de las Áreas de Gestión y de la Secretaría General podrán delegar funciones y operativas que consideren oportunas en las personas que ostentan las jefaturas de servicio, debiendo estar esta delegación de funciones debidamente acreditada en un documento firmados tanto por la persona titular del Área de Gestión o de la Secretaria General como por la persona que ostente la jefatura de servicio correspondiente.

6.4 Responsable del servicio

La persona titular de cada jefatura de servicio es responsable, a nivel ejecutivo, de:

- Redacción de pliegos técnicos para servicios.
- Promover la formación y concienciación en materia de Seguridad TIC a todo el personal. Ejecutada por el Servicio de Estudios.
- Determinar los requisitos de seguridad de los servicios.
- Ejecutar, en coordinación con el DPD, el adecuado mantenimiento del RAT.

- Adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Valorar las consecuencias de un incidente de seguridad en los servicios.

6.5 Responsable de seguridad TIC

A nivel de supervisión será la persona titular del Área de Infraestructuras de Información, tanto de la seguridad de la información como del cumplimiento de lo establecido en el artículo 11 del ENS, ejerciendo las siguientes funciones:

- Desarrollo de las competencias de seguridad de la entidad.
- Implantación del ENS.
- Política de seguridad y medidas propuestas por el CS.
- Responsable de que se faciliten los recursos necesarios para una adecuada ejecución de la PS TIC y no TIC.
- Responsable de los procedimientos de seguridad TIC que se definan para dar cumplimiento y desarrollo a la PS.
- Formalizar y aprobar la Declaración de Aplicabilidad de las medidas del Anexo II del ENS
- Responsable de que se realicen los planes de acción e iniciativas que garanticen la implantación de la PS en el IECA .
- Normativas de seguridad TIC que se definan para dar cumplimiento y desarrollo a la PS.
- Verificar que todas las acciones llevadas a cabo en materia de seguridad TIC se encuentren enmarcadas en la PS.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del IECA en materia de Seguridad TIC.
- Responsable de que se promueva la formación y concienciación en materia de Seguridad TIC a todo el personal.
- Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la Seguridad, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad interior y seguridad TIC en el IECA.
- Responsable de que se valoren y evalúen los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad interior y la seguridad TIC en el IECA.
- Difundir entre el personal las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.
- Análisis de riesgos y las salvaguardas a implantar. Trasladar al Comité los riesgos residuales calculados.
- Elaborar Plan de Tratamiento de Riesgos.
- Realizar controles y promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad y protección de datos.
- Responsable de la coordinación técnica en materia de seguridad TIC.
- Responsable del desarrollo y seguimiento de programas de formación y concienciación.

- Informar del estado de la seguridad TIC y de los incidentes al CS.
- Supervisar el cumplimiento de la PS de la información de la Organización, así como de sus normas y procedimientos derivados.
- Responsable de determinar las medidas de seguridad, adecuadas y eficaces, para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
- Presentar al CS las normativas de obligado cumplimiento.
- Aprobar los procedimientos de alcance general y técnico.
- Supervisar la documentación de cuarto nivel (informes, registros y evidencias electrónicas) de obligado cumplimiento.
- Autorizar la recuperación de datos tratados.

6.6 Responsable del sistema

Esta responsabilidad recaerá en la persona titular del Gabinete Estratégico del servicio de Analítica y Gobierno del Dato de la Agencia Digital de Andalucía que presta su servicios en el IECA y, a nivel operativo, ejercerá las funciones descritas para esta figura en el ámbito del ENS. Le corresponden, entre otras:

- Garantizar el cumplimiento de las normas relativas al secreto estadístico y de las de protección de datos de carácter personal.
- Facilita los recursos necesarios para una adecuada ejecución de la PS TIC.
- Planes de acción e iniciativas que garanticen la implantación de la PS en el IECA .
- Redacción de pliegos técnicos en materia TIC.
- Procedimientos de seguridad TIC que se definan para dar cumplimiento y desarrollo a la PS.
- Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad TIC.
- Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad interior y la seguridad TIC en el IECA.
- Adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Difundir entre el personal las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.
- Coordinación técnica en materia de seguridad TIC.
- Desarrollo y seguimiento de programas de formación y concienciación.
- Implantar las medidas de seguridad según los requisitos de seguridad de la organización, siguiendo en todo momento lo exigido en el Anexo II del ENS.
- Desarrollar los procedimientos de alcance general y técnico.
- Desarrollar la documentación de cuarto nivel (informes, registros y evidencias electrónicas) de obligado cumplimiento.
- Desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida.

6.7 Persona delegada de protección de datos de carácter personal

Será nombrada por la persona titular de la Presidencia del CS, a propuesta del mismo. De acuerdo con el RGPD, tendrá funciones de informar y supervisar:

- Determinar cuándo hay que realizar las evaluaciones de impacto sobre tratamientos de datos personales.
- Garantizar la observancia de los principios relativos al tratamiento incluidos en la política, normativa y procedimientos concernientes a la protección de datos personales.
- Responder a las solicitudes de ejercicio de derechos.
- Asesorar al Responsable de tratamiento, al de seguridad TIC y de Interior y al Comité en materia de datos personales.
- Cooperar con la autoridad de control en materia de protección de datos de carácter personal.
- Garantizar el adecuado mantenimiento del RAT.

Además será consultado en las siguientes materias:

- Implantación del ENS.
- Cumplimiento de las normas relativas al secreto estadístico y de las de protección de datos de carácter personal.
- Cumplimiento de las normas relativas a seguridad interior.
- Política de seguridad y medidas propuestas por el CS.
- Normativas de seguridad TIC que se definan para dar cumplimiento y desarrollo a la PS.
- Resolver discrepancias y problemas que pudieran surgir en la gestión de la seguridad.
- Determinar los requisitos de seguridad de la información y su tratamiento.
- Valoración de las consecuencias de una brecha de seguridad relativa a datos personales.
- Adopción de las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Difusión entre el personal las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.
- Valorar las consecuencias de un incidente de seguridad en los servicios.
- Análisis de riesgos y las salvaguardas a implantar. Trasladar al Comité los riesgos residuales calculados.
- Elaboración del Plan de Tratamiento de Riesgos.
- Controles y auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad.
- Estado de la seguridad TIC y de los incidentes al CS.
- Normativas de seguridad relativas a datos personales de obligado cumplimiento.
- Procedimientos de alcance general y técnico, relativos a datos personales.

La persona delegada de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del mismo.

6.8 Responsables de seguridad de los ficheros no automatizados

Las personas titulares de los distintos servicios del Instituto serán responsables de seguridad de los ficheros no automatizados, que se encuentren dentro de su ámbito competencial, por lo que les corresponden, como a cualquier otro sistema de información, la protección de la información que contienen, y específicamente si es de carácter personal; así como la adecuada gestión de los soportes de forma que además de ser protegidos puedan ser también conservados y consultados, cuando sea preciso.

Para ello se asegurarán:

- Del cumplimiento de la normativa de archivo y documentación sobre conservación de documentos.
- De que solo sean accesibles al personal y para los asuntos que corresponda.
- Que la seguridad en el acceso sea proporcional a la criticidad (nivel de protección) de la información que contienen.

6.9 Responsable de seguridad interior

En caso de que se considere necesario por la Consejería a la que el IECA se adscribe, en virtud del volumen o singularidad de los activos de esta agencia, la responsabilidad de seguridad interior del IECA será ejercida por la persona titular de la Secretaría General. Asimismo corresponderá a la citada Consejería determinar las condiciones y requisitos mínimos que deben contener el Plan de Seguridad Interior, pudiendo corresponderle en este caso si así se determina las siguientes funciones:

- Garantizar la seguridad del entorno y sistemas auxiliares de los activos TIC y de la información, tales como vigilancia y control de accesos al edificio, suministro eléctrico, sistemas de detección y contra incendios, refrigeración del centro de proceso de datos y salas técnicas, protección frente a inundaciones y, en general, cualquier amenaza física.
- Adoptar las medidas de seguridad que le competan dentro de las dispuestas por el CS Interior y Seguridad TIC, informando de su implantación, eficacia e incidentes.
- Las labores de soporte, asesoramiento e información al CS, así como la ejecución de sus decisiones y acuerdos en materia de seguridad interior. Propuesta de un Plan de Seguridad Interior para el IECA.
- Proponer las adaptaciones necesarias, a su ámbito, del modelo general de seguridad interior, incluso valores, tablas y métricas adecuadas al conjunto de los activos en su ámbito.
- El desarrollo, el mantenimiento y la supervisión del marco regulador de la seguridad interior en el IECA.

- La generación y supervisión de criterios y directrices para la gestión de la seguridad interior en el ámbito del IECA.
- La recogida sistemática de información y la supervisión del estado de las principales variables de seguridad interior en el ámbito del IECA.
- El asesoramiento técnico y la auditoría del sistema de seguridad interior en el ámbito del IECA.
- Velar por la coherencia de la aplicación del modelo de seguridad interior en el ámbito del Instituto, mantenerlo actualizado e impulsar su implantación.
- Gestionar para el ámbito del IECA, la relación con la Unidad de Seguridad Interior de la Consejería.
- Definir los criterios de protección de activos especialmente sensibles a riesgos que conciernen a la seguridad interior conforme a las especificidades del ámbito del IECA.
- Desarrollar para el ámbito del IECA, planes de contingencia en respuesta a incidentes de seguridad interior, incluso situaciones de crisis.
- Asegurar en el ámbito del IECA, el funcionamiento de los mecanismos previstos para recopilar, recibir, analizar y procesar la información relevante para la seguridad interior, destinados a generar inteligencia al respecto.
- Promover y coordinar la cooperación con las autoridades del sector correspondiente al ámbito material del IECA en materia de inteligencia para la seguridad.
- Informar sobre incidentes de seguridad interior en el IECA que se consideren relevantes.
- Asegurar en su nivel el correcto funcionamiento en la cadena de comunicación y escalado de incidentes de seguridad interior.
- Proponer a la aprobación del CS Interior y Seguridad TIC el Plan de Seguridad Interior del IECA.
- Cuantas otras le sean encomendadas, en relación con la seguridad interior, por el CS Interior y Seguridad TIC.
- Promoción de la educación, el entrenamiento y la concienciación sobre las medidas relativas a la seguridad interior entre el personal.
- Planes de acción e iniciativas que garanticen la implantación de la PS en el IECA .
- Redacción de pliegos técnicos en materia de seguridad interior.

6.10 Responsabilidad individual

La seguridad en el Instituto no es solo una tarea de los que tienen asignadas responsabilidades para su organización, sino que es un objetivo común que debe ser compartido por todas las personas que desarrollan su actividad en el mismo. También las personas que se vayan incorporando a la organización tendrán que ser informadas, formadas y concienciadas del cumplimiento de la PS y de la importancia que tiene para la organización.

7. ASESORAMIENTO ESPECIALIZADO EN MATERIA DE SEGURIDAD

7.1 Asesoramiento especializado

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

7.2 Cooperación entre organismos y otras Administraciones Públicas

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

7.3 Revisión independiente de la Seguridad de la Información y de su tratamiento

El CS propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la PS con el fin de garantizar que las prácticas en el IECA reflejan adecuadamente sus disposiciones.

8. CONCIENCIACIÓN Y FORMACIÓN

Todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema de información están afectados por la seguridad, debiéndose prestar la máxima atención a la concienciación y formación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que la ignorancia o falta de conocimiento no constituya un riesgo de seguridad.

Todo el personal de este Instituto tiene la obligación de conocer esta PS de la Información y las medidas de seguridad necesarias para el desarrollo de su actividad laboral, reflejadas en el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía (Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía) y en toda la

información que se genere, según se establece en el preámbulo de esta resolución. Asimismo, están sometidos al cumplimiento de la normativa indicada en el apartado 2 de este documento.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida que la necesiten para realizar su trabajo.
A instancias del RSEG, el CS debe promover la disponibilidad de los medios necesarios para asegurar el cumplimiento de lo indicado en los párrafos anteriores.

9. GESTIÓN DE RIESGOS

El IECA realizará una gestión de la seguridad basada en el análisis de los riesgos y el control del riesgo residual, evaluando las posibles amenazas que se puedan generar.

Los riesgos se minimizarán hasta niveles aceptables, mediante el despliegue de las correspondientes medidas de seguridad, que se actualizarán de forma periódica para responder a nuevas amenazas, y que irán orientadas a conseguir un equilibrio entre la criticidad de los datos y de su tratamiento, los riesgos a los que están expuestos y los recursos que precisa la implantación de las medidas.

El diseño de cualquier tratamiento, sistema o servicio se realizará siempre considerando el riesgo que pueda suponer para los mismos. De la misma forma la reevaluación del riesgo será inherente a cualquier modificación que se opere sobre sistemas, tratamientos o servicios.

De esta manera dará cumplimiento a la legislación y normas internas vigente bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad.

Para ello, con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en materia de seguridad, el RSEG se responsabilizará de que se realicen, con periodicidad al menos anual, análisis de riesgos cuyos resultados se plasmen en actuaciones para tratar y mitigar el riesgo, o incluso, replantear la seguridad de los sistemas, en caso necesario.

Se realizará un análisis de riesgos:

- Antes de realizar un tratamiento o la implantación de un nuevo sistema o servicio.
- Regularmente, una vez al año.
- Cuando haya cambios en los tratamientos, sistemas o servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- Cuando ocurra un incidente de seguridad grave.
- Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

Las conclusiones de los análisis de riesgos serán elevadas al CS.

10. ESTRUCTURA NORMATIVA

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:

- Primer nivel: PS de la Información.
- Segundo nivel: Normativas de Seguridad.
- Tercer nivel: Procedimientos de Seguridad.
- Cuarto nivel: Informes, registros y evidencias electrónicas.

10.1 Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, del IECA, recogido en el presente documento y aprobado mediante esta Resolución. Estará disponible para todoa la ciudadanía.

10.2 Segundo Nivel: Normativas de Seguridad

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente.
La responsabilidad de aprobación de los documentos redactados en este nivel será competencia de la persona titular de la Secretaría General a propuesta del CS. Disponibles para personal interno del IECA.

10.3 Tercer Nivel: Procedimientos de Seguridad

Documentos 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.
La responsabilidad de aprobación de estos procedimientos es del RSEG, a propuesta del RSIS y con el visto bueno del CS. Los procedimientos de alcance general estarán disponibles para todo el personal que preste sus servicios en el IECA. Los de alcance técnico solo para personal técnico que preste sus servicios en el IECA.

10.4 Cuarto Nivel: Informes, registros y evidencias electrónicas

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 del sistema de información.

La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información en su ámbito. Disponibles solo para personal técnico que preste sus servicios en el IECA.

10.5 Otra documentación

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

11. DATOS DE CARÁCTER PERSONAL Y SECRETO ESTADÍSTICO

Todos los activos de información que contengan datos de carácter personal o se encuentren sometidos a secreto estadístico, tanto si su tratamiento es automatizado como si no, se ajustarán a los niveles de seguridad requeridos por la normativa y los primeros serán recogidos en el Registro de Actividades de Tratamiento, en su caso.

La SG tiene la responsabilidad de mantener el Registro de Agentes Estadísticos de Andalucía, que de acuerdo con el Decreto 345/2011, de 22 de noviembre, por el que se regula la organización y el funcionamiento del Registro General de Agentes Estadísticos de Andalucía, tiene la finalidad de garantizar los derechos fundamentales reconocidos en el artículo 18.1 de la Constitución, como instrumento necesario para conocer a todas aquellas personas que, por razón de su actividad, pudieran tener acceso a la información protegida por el deber del secreto estadístico.

12. TERCERAS PARTES

Cuando se presten servicios a otros organismos o se maneje información procedente de estos se les hará participes de esta PS y los procedimientos de seguridad que sean oportunos, estableciéndose canales para la comunicación y coordinación y para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o se les ceda información, se les comunicarán las obligaciones o procedimientos de seguridad que deban cumplir en relación a dichos servicios o información. Dichas terceras partes quedarán sujetas, en todo caso, a las obligaciones establecidas en la normativa correspondiente.

13. REVISIÓN DE LA POLÍTICA DE SEGURIDAD

La PS debe responder a una estrategia permanentemente actualizada, tanto por los flujos de información que genera la actividad de este organismo como por la evolución de la tecnología que, al mismo tiempo que propicia una más eficiente gestión de los riesgos sobre los activos, da lugar a nuevas vulnerabilidades.

La revisión de esta PS será misión del CS Interior y Seguridad TIC, que propondrá las modificaciones que se consideren oportunas en función de las necesidades.

Se deberá revisar la presente Política como mínimo una vez cada dos años.

La PS será aprobada por la Dirección del IECA y difundida para que la conozcan todas las partes afectadas.

ANEXO II
ORGANIGRAMA DE SEGURIDAD INTERIOR Y SEGURIDAD TIC DEL IECA