Proyecto de decreto por el que se aprueba la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de las Illes Balears

El artículo 29 del Estatuto de Autonomía encomienda a los poderes públicos impulsar el acceso a las nuevas tecnologías, a la plena integración en la sociedad de la información y a la incorporación de los procesos de innovación.

Son estos poderes públicos los responsables de generar la confianza de los ciudadanos y ciudadanas en el uso de los medios tecnológicos en sus relaciones con las administraciones de las Illes Balears. Para conseguir esta confianza, los medios tecnológicos utilizados deben ser seguros.

Con dicho objetivo, el Decreto 97/2006, de 24 de noviembre, creó dentro del ámbito de la Administración de la Comunidad Autónoma de las Illes Balears la Comisión Directora y la Comisión Técnica de la Seguridad de la Información encargadas de garantizar, dentro de sus respectivas funciones, la seguridad de los sistemas de información.

Posteriormente, la Ley 4/2011, de 31 de marzo, de la buena administración y del buen Gobierno de las Illes Balears reconoce el derecho de los ciudadanos y las ciudadanas a realizar trámites y recibir información por medios electrónicos como un principio informador de la buena administración y dedica el artículo 7 a los medios electrónicos, informáticos y telemáticos.

La consolidación del derecho de la ciudadanía a relacionarse con las administraciones por medios electrónicos la establece la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público con la implantación definitiva del uso de las tecnologías de la información y de las comunicaciones dentro de las administraciones públicas, tanto para mejorar la eficiencia en la gestión como para favorecer las relaciones de colaboración y cooperación entre ellas.

Ambas leyes, junto con el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, determinan el marco jurídico para el funcionamiento electrónico de la Administración. En este contexto, la digitalización de la actuación administrativa como forma habitual de relación con la ciudadanía y entre las administraciones demanda una exigencia de fiabilidad a fin de que la ciudadanía pueda realizar sus trámites administrativos de manera segura. La confianza en los sistemas de información debe

extenderse a las garantías sobre las comunicaciones, el tratamiento y el almacenaje de la información.

Asimismo, la Ley 39/2015, de 1 de octubre, entre los derechos de las personas en sus relaciones con las administraciones públicas previstas en el artículo 13, incluye lo relativo a la protección de los datos personales y, en particular, a la seguridad de los datos que figuran en los ficheros, sistemas y aplicaciones de las administraciones públicas.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece en el artículo 156 que el Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos, y lo incorpora como parte esencial en la configuración del archivo electrónico de los documentos regulado en el artículo 46 y en el régimen de relaciones electrónicas y transferencias de tecnología entre las administraciones públicas, tal como establece el artículo 158.

El Real Decreto 311/2022, de 3 de mayo, regula el Esquema Nacional de Seguridad como conjunto de principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades que, de acuerdo con el artículo 2 de la Ley 40/2015, de 1 de octubre, integran el sector público con el objetivo de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionan en el ejercicio de sus competencias.

En este marco, las tecnologías de la información y las comunicaciones constituyen un instrumento estratégico y necesario de digitalización de la Administración de la Comunidad Autónoma de las Illes Balears y su sector público autonómico. Por lo tanto, es imprescindible que los sistemas de información y comunicaciones se administren con diligencia y cuenten con las medidas adecuadas para protegerse de cualquier amenaza con potencial para incidir en la confidencialidad, la integridad y la disponibilidad de la información y de los servicios.

El apartado 1 del artículo 12 del Real Decreto 311/2022 antes citado, define la política de seguridad de la información como el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. Y en el apartado 2 de este mismo artículo 12 exige que cada administración pública disponga de una política de seguridad aprobada formalmente por el órgano competente. En cuanto a los entes del sector público instrumental, el citado artículo prevé que se puedan incluir en el ámbito de la política de seguridad que apruebe la

Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de autoorganización.

La Administración de la Comunidad Autónoma de las Islas Baleares cumple dicho mandato con la aprobación de este decreto. La política de seguridad que se aprueba es el instrumento que debe servir de apoyo a la Administración para conseguir sus objetivos en la utilización segura de los sistemas de información y comunicaciones, defenderse de las amenazas, garantizar la continuidad de los sistemas de la información, minimizar los riesgos de daño y asegurar el cumplimiento eficiente de sus objetivos. A tal fin, el decreto determina las medidas de seguridad de naturaleza organizativa, física y lógica para proteger cada sistema de información en el ámbito de la Administración de la Comunidad Autónoma, dado que la seguridad, entendida como proceso integral y de mejora continua, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones. Por ello, la política de seguridad se aplica en el ámbito de la Administración autonómica y de los entes del sector público que no tengan aprobada una propia y se adhieran a esta, y a todos los activos de la información de los que sean titulares o gestores.

La política de seguridad de la Administración de la Comunidad Autónoma constituye el marco de referencia orientado a facilitar la gestión, la administración y la implementación de los mecanismos y procedimientos de seguridad establecidos en el Esquema Nacional de Seguridad. Establece los pilares del cuerpo normativo de seguridad de esta Administración y la estructura organizativa que debe velar por su cumplimiento, e identifica los deberes que tienen los distintos responsables que se integran en esta estructura.

También, en la configuración de la política de seguridad que aprueba este Decreto se han tenido en consideración las guías del Centro Criptológico Nacional (CNN), especialmente las guías CCN-STIC-801 y CCN-STIC-805, las cuales orientan a las administraciones públicas no solo a tener modelos de políticas de la seguridad de la información, sino también a determinar las responsabilidades y funciones de los distintos órganos de la gestión de la seguridad de la información, entre los que está el establecimiento de un comité a muy alto nivel, dado que la seguridad de la información es un proceso que puede implicar distintos ámbitos fuera de los exclusivamente tecnológicos como, por ejemplo, el operativo, el presupuestario, el legal o el de relaciones con las fuerzas de seguridad. Adicionalmente, y teniendo en cuenta la posibilidad no despreciable de que en algún momento, a pesar de las protecciones que se vayan desarrollando, ocurran incidentes de seguridad que pueden

llegar a ser graves o críticos, el decreto crea unos órganos de crisis con unas funciones acordes con la guía del CCN -CERT BP/ 20 de buenas prácticas en la gestión de cibercrisis.

A su vez, el Real Decreto 311/2022, de 3 de mayo, determina que la política de seguridad debe ser coherente con lo establecido en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas respecto del tratamiento de datos personales y la normativa vigente en esta materia, la cual tiene carácter prevalente con relación a la protección de datos de carácter personal en caso de discrepancia.

En la elaboración de este decreto se han observado los principios de buena regulación del artículo 49 de la Ley 1/2019, de 31 de enero, del Gobierno de las Illes Balears. En concreto, se adecua a los principios de necesidad y eficacia, dado que con la aprobación de la Política de Seguridad de la Información la Administración de la Comunidad Autónoma se dotará de un marco de protección en el uso de los sistemas de la información dentro de su ámbito y su regulación, que adopta la forma y el rango de decreto, es la idónea para alcanzar los objetivos que se quieren conseguir. Asimismo, se adecua al principio de proporcionalidad porque incluye el contenido imprescindible que exige el Esquema Nacional de Seguridad con el fin de alcanzar los objetivos perseguidos. De acuerdo con el principio de eficiencia, la norma no conlleva cargas administrativas innecesarias o accesorias. Se ha garantizado la transparencia en la tramitación de la norma y se ha asegurado la participación de las personas interesadas. Igualmente, se ajusta al principio de seguridad jurídica, dado que establece reglas claras con la finalidad de garantizar la mejor protección de los sistemas de la información y es coherente con el resto del ordenamiento jurídico, así como con los principios de calidad y simplificación en la medida en que en la elaboración de este decreto se ha seguido el procedimiento establecido legalmente, con respeto a los principios de buena regulación y se ajusta a las directrices que son de aplicación en relación con la forma y estructura de los textos normativos.

Por todo ello, a propuesta del consejero de Economía, Hacienda e Innovación, de acuerdo/oído el Consejo Consultivo de las Illes Balears y habiéndolo considerado el Consejo de Gobierno de las Illes Balears en la sesión de ...

DECRETO

CAPÍTULO I

Disposiciones generales

Artículo 1
Objeto

1. Este decreto tiene por objeto aprobar la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de las Illes Balears (en adelante, PSI-CAIB), así como su marco organizativo y de gestión.

Artículo 2
Ámbito de aplicación

1. Este decreto se aplica a la Administración de la Comunidad Autónoma de las Islas Baleares.

2. Los entes del sector público autonómico aprobarán su política de seguridad propia, que debe ser coherente con la PSI-CAIB y debe respetar los principios fundamentales establecidos en el artículo 4 de este Decreto.

No obstante, se podrán adscribir a la PSI-CAIB, cuando así lo determinen los órganos competentes de los entes en el ejercicio de las potestades de organización. En este supuesto, el secretario del órgano competente del ente debe enviar el certificado del acuerdo de adhesión adoptado al secretario de la Comisión Directora de la Seguridad de la Información.

3. La PSI-CAIB se aplica a los activos de tecnologías de la información y de las comunicaciones de los que la Administración autonómica es titular o tiene encomendada su gestión.

4. A efectos de este decreto, se remite a las definiciones de activo y de sistema de información establecidas en el anexo IV del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, Esquema Nacional de Seguridad).

Artículo 3
Misión

1. La Administración de la Comunidad Autónoma de las Illes Balears tiene como misión servir con objetividad los intereses generales y actuar de acuerdo con los principios constitucionales de eficacia, jerarquía, descentralización, desconcentración y

coordinación para conseguir los objetivos que establecen las leyes y el ordenamiento jurídico.

2. Los objetivos en materia de seguridad que la Administración de la Comunidad Autónoma pretende garantizar con la PSI-CAIB son:

- Garantizar la confidencialidad, integridad y autenticidad de la información y la continuidad en la prestación de los servicios.

- Implementar medidas de seguridad en función del riesgo.

- Formar y concienciar a todos los niveles de la Administración autonómica respecto de la seguridad de la información a fin de que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que pueden correr.

- Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en ejercicio de sus funciones.

- Desplegar y controlar la seguridad física para que los activos de la información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.

- Establecer la seguridad en la gestión de las comunicaciones mediante los procedimientos necesarios para conseguir que la información que se transmita por las redes de comunicaciones esté debidamente protegida.

- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de la información, garantizando su seguridad por defecto.

- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios y mantener el control en la adquisición e incorporación de nuevos componentes del sistema.

- Gestionar los incidentes de seguridad para su correcta detección, contención, mitigación y resolución, adoptando las medidas necesarias para evitar que se vuelvan a reproducir.

- Proteger la información personal adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.

- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

Artículo 4
Principios fundamentales

1. Los principios son directrices fundamentales de seguridad que deben tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información.

2. La PSI-CAIB debe desarrollarse, con carácter general, de acuerdo con los siguientes principios:

a. Seguridad como proceso integral: la seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos. La seguridad de la información debe considerarse como parte de la operativa habitual y se aplicará desde el diseño inicial de los sistemas de información, proporcionará las funcionalidades mínimas requeridas y hará que el uso ordinario del sistema sea sencillo y seguro, de manera que una utilización insegura requiera un acto consciente por parte del usuario. Además, las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañados de los correspondientes procedimientos de control, y deberá conocerse en todo momento el estado de seguridad de los sistemas en relación con las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que les afecten, y deberá reaccionarse con diligencia para gestionar el riesgo en vista del estado de seguridad.

b. Gestión de la seguridad basada en los riesgos: el análisis y gestión de riesgos es parte esencial del proceso de seguridad y constituye una actividad continua y actualizada. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que

establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, entre el impacto y la probabilidad de los riesgos a los que estén expuestos y entre la eficacia y el coste de las medidas de seguridad.

c. Prevención, detección, respuesta y conservación: se deben contemplar acciones relativas a los aspectos de prevención, detección y respuesta, con el fin de minimizar las vulnerabilidades y conseguir que las amenazas no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

d. Existencia de líneas de defensa: el sistema de información debe disponer de una estrategia de protección constituida por múltiples capas de seguridad, constituidas, a su vez, por medidas de naturaleza organizativa, física y lógica.

e. Vigilancia continua y reevaluación periódica: las medidas de seguridad deben reevaluarse y actualizarse periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La evaluación permanente del estado de seguridad servirá para medir la evolución del sistema de gestión de seguridad de la información, así como para detectar vulnerabilidades, deficiencias de configuración y actividades o comportamientos anómalos y responder de manera oportuna. La seguridad de la información será atendida, revisada y auditada por personal cualificado, diferenciado, dedicado e instruido en todas las fases del ciclo de vida de los sistemas de información.

f. Responsabilidad diferenciada: en los sistemas de información se debe diferenciar al responsable de la información, al responsable del servicio, al responsable de seguridad y el responsable del sistema. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de estos sistemas de información.

g. Principio de proporcionalidad: la implantación de las medidas que mitiguen los riesgos de seguridad de los activos de tecnologías de la información y de las comunicaciones debe hacerse bajo un enfoque de proporcionalidad, tanto respecto de los costes económicos y operativos, como respecto de los riesgos y gravedad de la información y de los servicios afectados.

h. Principio de concienciación y formación: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones con respecto al

tratamiento seguro de la información. Igualmente, se fomentará la formación específica en materia de seguridad de tecnologías de la información y de las comunicaciones de todas aquellas personas que gestionan y administran sistemas de información y de las comunicaciones.

Artículo 5
Marco normativo

1. El marco normativo en el que se desarrollan las actividades de la Administración de la Comunidad Autónoma de las Islas Baleares en el ámbito de la seguridad de la información es el siguiente:

a) 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).

b) Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

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

d) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

e) Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

f) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

g) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

h) Ley 4/2011, de 31 de marzo, de la buena administración y del buen gobierno de las Illes Balears.

i) Ley 3/2003, de 26 de marzo, de Régimen Jurídico de la Administración de la Comunidad Autónoma de las Illes Balears.

j) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

k) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

l) Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

m) 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.

n) Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.

o) Decreto 24/2022, de 11 de julio, de la Comisión Superior de Sistemas de Información en Tecnología y Comunicaciones.

p) Decreto 113/2010, de 5 de noviembre, de acceso electrónico a los servicios públicos de la Administración de la Comunidad Autónoma de las Illes Balears.

q) Decreto 107/2006, de 15 de diciembre, de regulación del uso de la firma electrónica en el ámbito de la Administración de la Comunidad Autónoma de las Illes Balears.

r) Decreto 10/2025, de 14 de julio, de la presidenta de las Illes Balears, por el que se establecen las competencias y la estructura orgánica básica de las consejerías de la Administración de la Comunidad Autónoma de las Illes Balears.

s) El resto de normativa que complemente, desarrolle o sustituya las anteriores y que se encuentren dentro del ámbito de aplicación de la PSI-CAIB.

2. Igualmente, forman parte del marco regulador de la PSI-CAIB todas las normas a que hace referencia el Capítulo III.

CAPÍTULO II
Estructura organizativa

Artículo 6
Organización de la seguridad de la información

1. La preservación de la seguridad es un objetivo común de todo el personal, órganos y unidades de la Administración de la Comunidad Autónoma de las Illes Balears.

2. La estructura organizativa de gestión de la seguridad de la información de la Administración de la Comunidad Autónoma está compuesta por:

a) Comisión Directora de la Seguridad de la Información.

b) Comisión Técnica de la Seguridad de la Información.

c) Responsables de la información.

d) Responsables del servicio.

e) Responsables de seguridad.

f) Responsables del sistema.

g) Administradores de la seguridad del sistema.

Artículo 7
Comisión Directora de la Seguridad de la Información

1. La Comisión Directora de la Seguridad de la Información es el órgano colegiado encargado de dar el impulso organizativo y normativo necesario en materia de seguridad de la información. La Comisión se adscribe a la Consejería de Economía, Hacienda e Innovación, a través de la Dirección General de Estrategia Digital y Desarrollo Tecnológico.

2. Esta Comisión tendrá la siguiente composición:

a. La presidencia,ocupada por el consejero de Economía, Hacienda e Innovación.

b. La vicepresidencia, ocupada por el director general de Estrategia Digital y Desarrollo Tecnológico.

c. Vocales:

- El secretario general de la Consejería de Presidencia, Coordinación de la Acción de Gobierno y Cooperación Local.

- El director general de Función Pública .

- El director general de Emergencias e Interior.

- El director de la Dirección de la Abogacía de la Comunidad Autónoma.

- El interventor general de la Comunidad Autónoma.

d. La secretaría, ocupada por el jefe del Departamento de Ciberseguridad y Telecomunicaciones.

3. Podrán asistir, con voz pero sin voto, los órganos directivos de la consejería o del ente del sector público autonómico promotor de la propuesta en materia de seguridad de la información que, en su caso, deba formar parte del orden del día de la sesión.

4. El presidente, por iniciativa propia o a propuesta de cualquiera de sus miembros, podrá convocar, con voz pero sin voto, a los órganos directivos diferentes del promotor, cuando se traten asuntos que afecten a sus competencias.

5. La Comisión podrá nombrar a los asesores que considere oportunos, con carácter permanente o puntual, los cuales podrán ser invitados a asistir a las sesiones, con voz pero sin voto.

6. El vicepresidente sustituirá al presidente en caso de vacante, ausencia, enfermedad o cualquier otra causa justificada.

7. En casos de vacante, de ausencia, enfermedad y, en general, cuando se dé alguna causa justificada, el vicepresidente y los vocales podrán designar a otras personas para que asistan a las sesiones con plenas facultades para ejercer las funciones propias de estos miembros. La designación se podrá hacer entre personas funcionarias con dependencia orgánica del vicepresidente o del vocal de que se trate en cada caso, con rango mínimo de jefe de servicio, o entre las personas titulares de los órganos directivos de la consejería de que se trate.

8. En caso de vacante, ausencia, enfermedad o cualquier otro impedimento justificado del secretario, lo suplirá la persona que determine el presidente de la Comisión.

9. Se atribuyen a esta Comisión las siguientes funciones:

a. Aprobar la propuesta de la política de seguridad de la información y sus modificaciones, y elevarla al consejero de Economía, Hacienda e Innovación para que impulse su tramitación.

b. Velar por el cumplimiento de la PSI-CAIB, impulsar su desarrollo y cumplimiento normativo, así como difundirla.

c. Elaborar la estrategia de evolución de la organización respecto a la seguridad de la información.

d. Recibir el informe consolidado del estado de seguridad de la Administración de la Comunidad Autónoma que elabore la Comisión Técnica de Seguridad de la Información.

e. Resolver, en última instancia, los conflictos de responsabilidad en los términos establecidos en el artículo 18.

f. Proveer los recursos y medios necesarios para asegurar la concienciación y formación en materia de seguridad de la información de todo el personal afectado por este decreto.

g. Promover la mejora continua del sistema de gestión de la seguridad de la información.

h. Implementar las medidas organizativas de seguridad de acuerdo con los planes de mejora.

10. La Comisión Directora de la Seguridad de la Información podrá encomendar a la Comisión Técnica de la Seguridad de la Información las tareas necesarias para el mejor ejercicio de sus funciones.

11. La Comisión se reunirá de manera ordinaria una vez al año y, de manera extraordinaria, a petición motivada de cualquier miembro.

12. La Comisión se rige por lo establecido en este decreto y por lo dispuesto en los artículos 15 a 18 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y el capítulo V del título I de la Ley 3/2003, de 26 de marzo, de Régimen Jurídico de la Administración de la Comunidad Autónoma de las Illes Balears.

Artículo 8
Comisión Técnica de la Seguridad de la Información

1. La Comisión Técnica de la Seguridad de la Información es el órgano colegiado encargado de coordinar e impulsar los aspectos técnicos en materia de seguridad de la información. La Comisión se adscribe a la Consejería de Economía, Hacienda e Innovación, a través de la Dirección General de Estrategia Digital y Desarrollo Tecnológico.

2. Esta Comisión tendrá la siguiente composición:

a. La presidencia, ocupada por el director general de Estrategia Digital y Desarrollo Tecnológico.

b. La vicepresidencia, ocupada por el jefe del Departamento de Ciberseguridad y Telecomunicaciones.

c. Vocales:

- El director general de Innovación y Transformación Digital.
- El jefe del Departamento de Desarrollo Tecnológico.
- El jefe del Departamento de Infraestructuras Tecnológicas y Plataformas Corporativas
- El jefe del Departamento de la Oficina de Administración Digital.
- El jefe del Servicio Jurídico de Administración Digital.

d. La secretaría, ocupada por el jefe del Servicio de Ciberseguridad.

3. El Delegado de Protección de Datos de la Administración de la Comunidad de las Illes Balears asistirá con voz pero sin voto cuando se traten cuestiones relativas a la protección de datos de carácter personal.

4. Podrán asistir, con voz pero sin voto, los órganos directivos de la consejería o del ente del sector público autonómico promotor de la propuesta en materia de seguridad de la información que, en su caso, deba formar parte del orden del día de la sesión.

5. El presidente, por iniciativa propia o a propuesta de cualquiera de sus miembros, podrá convocar, con voz pero sin voto, a los órganos directivos diferentes del promotor, cuando se traten asuntos que afecten a sus competencias.

6. La Comisión podrá nombrar a los asesores que considere oportunos, con carácter permanente o puntual, y los podrá invitar a asistir a las sesiones, con voz pero sin voto.

7. El vicepresidente sustituirá al presidente en caso de vacante, ausencia, enfermedad o cualquier otra causa justificada.

8. En casos de vacante, ausencia, enfermedad y, en general, cuando se dé alguna causa justificada, el vicepresidente y los vocales podrá designar a otras personas para

que asistan a las sesiones con plenas facultades para ejercer las funciones propias de estos miembros. La designación se podrá hacer entre personas funcionarias con dependencia orgánica del vicepresidente o del vocal de que se trate en cada caso, con rango mínimo de jefe de sección.

9. En caso de ausencia o cualquier otro impedimento justificado del secretario, lo suplirá la persona que determine el presidente de la Comisión.

10. Se atribuyen a esta Comisión las siguientes funciones:

a. Elevar la propuesta de la política de seguridad de la información de la Administración de la Comunidad Autónoma de las Illes Balears a la Comisión Directora de la Seguridad de la Información, revisarla anualmente y proponer sus modificaciones.

b. Revisar, si procede, las propuestas de las políticas de seguridad de la información de los entes del sector público autonómico e informar a la Comisión Directora de Seguridad de la Información.

c. Proponer las normas de segundo nivel de acuerdo con el artículo 13.

d. Proponer a la Comisión Directora de la Seguridad de la Información las medidas organizativas a implementar de acuerdo con los planes de mejora de la seguridad de la información.

e. Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

f. Realizar las tareas de apoyo encomendadas por la Comisión Directora de la Seguridad de la Información de acuerdo con el apartado 10 del artículo 7.

g. Elaborar el informe consolidado del estado de seguridad de la información de la Administración de la Comunidad Autónoma con base en los informes de los responsables de seguridad, y elevarlo a la Comisión Directora de Seguridad de la Información.

h. Velar para que la creación y utilización de servicios horizontales permitan la reducción de duplicidades y tengan un funcionamiento homogéneo en los sistemas de información.

i. Monitorizar los principales riesgos residuales asumidos por los responsables del servicio y responsables de la información y recomendar posibles actuaciones.

j. Promover auditorías periódicas y/o autoevaluaciones que permitan verificar el cumplimiento de las obligaciones de la Administración de la Comunidad Autónoma en materia de seguridad de la información.

k. Resolver los conflictos de responsabilidad en los términos establecidos en el artículo 18.

l. Aprobar los planes de mejora y de continuidad de la seguridad.

11. La Comisión se reunirá de manera ordinaria cada tres meses y, de manera extraordinaria, a petición motivada de cualquier miembro.

12. Los acuerdos se adoptarán por mayoría de votos. En caso de empate, el presidente tiene voto de calidad.

13. La Comisión se rige por lo establecido en este decreto y por lo dispuesto en los artículos 15 a 18 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y el capítulo V del título I de la Ley 3/2003, de 26 de marzo, de Régimen Jurídico de la Administración de la Comunidad Autónoma de las Illes Balears.

Artículo 9
Responsables de la información

1. El responsable de la información es la persona que determina los requisitos de seguridad de la información.

2. Esta responsabilidad recae en los órganos directivos de las consejerías respecto de la información tratada en el ámbito de sus competencias.

3. Son funciones de los responsables de la información:

a. Aprobar los niveles de seguridad de la información, valorando los impactos de los incidentes que afecten a la seguridad de la información en cada una de las dimensiones de seguridad que establece el Esquema Nacional de Seguridad. Para esta aprobación pueden obtener una propuesta del responsable de la seguridad y, si procede, del responsable del sistema.

b. Asignar los recursos económicos y humanos necesarios para llevar a cabo los análisis de riesgos y sus controles compensatorios.

c. Aceptar, junto con los responsables del servicio, los riesgos residuales calculados en el análisis de riesgos y realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta última tarea.

d. Proponer al responsable de seguridad la suspensión del tratamiento de la información o la prestación del servicio correspondiente si se aprecian deficiencias graves de seguridad.

e. Aprobar las normas de tercer nivel de acuerdo con el artículo 16.

f. Ejercer cualquier otra función prevista por la normativa de seguridad.

Artículo 9
Responsables del servicio

1. El responsable del servicio es la persona que determina los requisitos de seguridad de los servicios prestados.

2. Esta responsabilidad recae en los órganos directivos de las consejerías que gestionen los procedimientos o trámites del servicio prestado dentro del ámbito de sus competencias.

3. Son funciones de los responsables del servicio:

a) Aprobar los niveles de seguridad del servicio prestado, valorando los impactos de los incidentes que afecten a la seguridad de la información en cada una de las dimensiones de seguridad que establece el Esquema Nacional de Seguridad. Para su aprobación pueden obtener una propuesta del responsable de la seguridad y, si procede, del responsable del sistema.

b) Asignar los recursos económicos y humanos necesarios para llevar a cabo los análisis de riesgos y sus controles compensatorios.

c) Aceptar, junto con los responsables de la información, los riesgos residuales calculados en el análisis de riesgos y realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta última tarea.

d) Proponer al responsable de seguridad la suspensión de tratamiento de la prestación del servicio si se aprecian deficiencias graves de seguridad.

e) Aprobar las normas de tercer nivel de acuerdo con el artículo 16.

f) Ejercer cualquier otra función prevista por la normativa de seguridad.

Artículo 10
Responsables de seguridad

1. El responsable de seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisa la implantación de medidas necesarias para garantizar que se satisfacen los requisitos e informa sobre estos aspectos.

2. El responsable de cada servicio nombrará al responsable de seguridad. Cuando la gestión de la seguridad de un sistema de información la asuma por razón de competencia la Dirección General de Estrategia Digital y Desarrollo Tecnológico, el responsable de seguridad será el jefe del Departamento de Ciberseguridad y Telecomunicaciones de esta Dirección General, que podrá delegar esta función en los jefes de servicio adscritos a este Departamento.

3. El cargo de responsable de seguridad es incompatible con los cargos de responsable del sistema, del servicio y de la información. En todo caso, no podrá haber dependencia jerárquica entre el responsable de seguridad y el responsable del sistema. Esta restricción no es aplicable a los sistemas de información cuyo objeto principal sea la prestación de servicios de seguridad de la información.

4. Son funciones del responsable de seguridad:

a) Velar por la aplicación de la seguridad en todos los sistemas de información durante todo su ciclo de vida.

b) Velar por el cumplimiento del cuerpo normativo definido en el artículo 13.

c) Colaborar en la elaboración de las normas de segundo y tercer nivel definidas en el artículo 13.

d) Aprobar las normas de tercer nivel de acuerdo con el artículo 13.

e) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

f) Mantener la documentación de seguridad organizada y actualizada, y gestionar los mecanismos para acceder, junto con el responsable del sistema.

g) Proponer les actividades de concienciación y formación en materia de seguridad.

h) Coordinar y hacer el seguimiento de la adecuación al Esquema Nacional de Seguridad.

i) Supervisar el funcionamiento las medidas de seguridad de la información, sean de carácter tecnológico u organizativo, y realizar controles para comprobar su efectividad.

j) Realizar auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y analizar los informes de auditoría, elaborando las conclusiones, que se presentarán al responsable del sistema para que adopte las medidas correctoras adecuadas.

k) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes y elevarlos a la Comisión Técnica de Seguridad de la Información.

l) Determinar la categoría del sistema de información según el procedimiento descrito en el Esquema Nacional de Seguridad y las medidas de seguridad que deben aplicarse.

m) Realizar los análisis de riesgos y hacer el seguimiento del proceso de gestión del riesgo.

n) Aprobar la declaración de aplicabilidad, que comprenderá la relación de medidas de seguridad seleccionadas para un sistema de información.

o) Elaborar los planes de mejora de la seguridad y los planes de continuidad, junto con el responsable del sistema.

p) Aprobar, con carácter previo a la implantación, los cambios que impliquen un riesgo de nivel alto en la seguridad del sistema.

q) Ordenar la suspensión del tratamiento de la información o de la prestación del servicio correspondiente si se aprecian deficiencias graves de seguridad, e informar a los responsables de la información, del servicio y del sistema.

r) Ejercer cualquier otra función prevista por la normativa de seguridad.

Artículo 11
Responsable del sistema

1. El responsable del sistema es el encargado de desarrollar la forma concreta de implementar la seguridad en el sistema y de supervisar su operación diaria. Podrá delegar esta última tarea en los administradores de seguridad.

2. El responsable de cada servicio nombrará un responsable de sistema. En el caso de que la gestión de la seguridad de un sistema de información la asuma, por razón de competencia, la Dirección General de Estrategia Digital y Desarrollo Tecnológico, el responsable del sistema será el jefe del Departamento de Infraestructuras Tecnológicas y Plataformas Corporativas, que podrá delegar en los jefes de servicio adscritos a este Departamento. En el supuesto de que la explotación y mantenimiento del sistema informático esté externalizado, el contrato recogerá la obligación del cumplimiento de las funciones propias del responsable del sistema.

3. Son funciones propias del responsable del sistema:

a) Operar y mantener el sistema durante todo su ciclo de vida y responsabilizarse de sus especificaciones, de la instalación y de la verificación de su correcto funcionamiento.

b) Definir la tipología y la política de gestión del sistema, y establecer los criterios de uso y los servicios de que dispone.

c) Comprobar que las medidas específicas de seguridad se integran adecuadamente dentro del marco general de seguridad.

d) Suspender el uso de la información o de la prestación de un determinado servicio si le informan de deficiencias graves de seguridad que puedan afectar a la satisfacción de los requisitos que se hayan establecido e informar inmediatamente a los responsables de la seguridad, del servicio y de la información.

e) Proponer las normas de tercer nivel de acuerdo con el artículo 13.

f) Elaborar los planes de mejora de la seguridad y los planes de continuidad, junto con el responsable de la seguridad.

g) Mantener la documentación de seguridad organizada y actualizada y gestionar los mecanismos para acceder, junto con el responsable de seguridad.

h) Cualquier otra función en el ámbito de la seguridad de sistemas de información que le sea encomendada a través de la normativa de seguridad.

Artículo 12
Administradores de la seguridad del sistema

1. Los administradores de la seguridad del sistema, designados por el responsable de seguridad o por el responsable del sistema, tienen las siguientes funciones dentro de su ámbito de responsabilidad:

a) Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información.

b) Gestionar, configurar y actualizar el *hardware* y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.

c) Gestionar las autorizaciones concedidas a los usuarios del sistema y monitorizar la actividad desarrollada en el sistema para comprobar que se ajusta a lo autorizado.

d) Aplicar los procedimientos de seguridad de la información.

e) Asegurar que se cumplen estrictamente los controles de seguridad establecidos.

f) Asegurar que se aplican los procedimientos aprobados para manejar el sistema de información.

g) Supervisar las instalaciones de hardware y software, así como sus modificaciones y mejoras, con el fin de asegurar que la seguridad no se encuentra comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

h) Monitorizar el estado de la seguridad de los sistemas obtenido a través de las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

i) Informar a los responsables de la seguridad y a los responsables del sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

j) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

k) Mantener la documentación de seguridad organizada y actualizada, y gestionar los mecanismos para acceder, junto con el responsable de seguridad.

l) Cualquier otra función que dentro de su ámbito de actuación le encomiende el responsable de seguridad o del sistema.

CAPÍTULO III

Cuerpo normativo de seguridad de la información

Artículo 13
Estructura del cuerpo normativo

1. El cuerpo normativo de seguridad de la información es de obligado cumplimiento y debe basarse en los principios fundamentales del artículo 4.

2. El cuerpo normativo de seguridad de la Información estará a disposición de todas las personas que necesiten conocerlo, en particular de aquellas que utilicen, operen o administren los sistemas de información y comunicaciones.

3. El cuerpo normativo de seguridad de la información se estructura en los cuatro niveles siguientes relacionados jerárquicamente, de manera que cada norma esté fundamentada en las normas de nivel superior:

a) Primer nivel normativo: está constituido por la PSI-CAIB y la normativa de carácter general sobre la seguridad de la información.

b) Segundo nivel normativo: está constituido principalmente por las normas y directrices de seguridad generales que, de acuerdo con la PSI-CAIB, determinan qué se puede hacer y qué no desde el punto de vista de la seguridad, sin entrar en detalles de implementación ni tecnológicos. En todo caso, los documentos describirán, como mínimo, las medidas técnicas y organizativas necesarias para asegurar el control de acceso a los sistemas de información, controlando y limitando las autorizaciones y el acceso a sus funciones.

La documentación de este segundo nivel la aprobará el director general de Estrategia Digital y Desarrollo Tecnológico, a propuesta de la Comisión Técnica de Seguridad de la Información.

c) Tercer nivel normativo: está constituido por los documentos en que se formalizan los procedimientos técnicos, incluyendo detalles de implementación y tecnológicos, y que explican cómo se deben llevar a cabo determinadas tareas con respeto a los principios de seguridad, así como a los procesos internos que se establezcan. En concreto, los documentos determinarán cómo llevar a cabo las tareas habituales, quién debe realizar cada tarea, cómo identificar y reportar comportamientos anómalos y la forma en que se debe tratar la información en función del nivel de seguridad que requiere.

La documentación de este nivel la aprobarán, según el ámbito de competencia, los responsables de seguridad, o los responsables de la información o de los servicios. Se podrá aplicar a un ámbito organizativo específico o a un sistema de información determinado.

d) Cuarto nivel normativo: está constituido por documentación de carácter formativo, como guías o recomendaciones, con la finalidad de orientar a los usuarios en la aplicación correcta de las medidas de seguridad, en especial proporcionando razonamientos donde no existen procedimientos precisos.

La documentación de este nivel la aprobarán, según el ámbito de competencia, los responsables de seguridad, o los responsables de la información o de los servicios. Se podrá aplicar a un ámbito organizativo específico o a un sistema de información determinado.

CAPÍTULO IV

Protección de datos de carácter personal

Artículo 14
Medidas de protección de datos de carácter personal

1. La seguridad de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, constituye uno de los principios que deben regir su tratamiento.

2. Cuando un sistema de información trate datos de carácter personal, también le será de aplicación la normativa en materia de protección de datos personales.

3. En estos supuestos, el responsable o el encargado del tratamiento, con el asesoramiento del delegado de protección de datos, deberá realizar el análisis de riesgos o, en su caso, la evaluación del impacto relativo a la protección de datos, tal y como establecen los artículos 24 y 35 del Reglamento 2016/679 del Parlamento

Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre.

4. En el caso de que el análisis de riesgos o del impacto a que se refiere el apartado anterior determine medidas de seguridad agravadas respecto de las previstas en el Esquema Nacional de Seguridad, aquellas serán las que deberán implementarse con carácter prevalente en la protección de datos de carácter personal.

CAPÍTULO V

Gestión de la seguridad

Artículo 15
Gestión de riesgos

1. La gestión de riesgos se realizará de manera continua sobre los sistemas de información, de acuerdo con los principios de gestión de la seguridad basada en los riesgos, de vigilancia continua y reevaluación periódica definidos en el artículo 4.

2. El proceso de gestión de riesgos comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deben ser proporcionales a los riesgos y deben estar justificadas.

3. Las fases de la gestión de riesgos mencionadas en el apartado anterior se realizarán de acuerdo con los anexos I y II del Esquema Nacional de Seguridad.

4. Los responsables del servicio o los responsables de la información son los encargados de solicitar el análisis de riesgos preceptivo.

5. Los responsables de seguridad, una vez que los responsables de la información y del servicio hayan calificado la información y hayan determinado el nivel de seguridad del sistema, realizarán los análisis de riesgos con la colaboración de estos responsables, y elaborarán la declaración de aplicabilidad y el conjunto de medidas para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y del servicio respectivo. El análisis de los riesgos identificará los riesgos residuales, con base en los cuales determinarán el tratamiento adecuado y lo comunicarán a los responsables de la información y del servicio.

6. Los análisis de riesgos, así como su tratamiento, deberán realizarse también cuando se detecten incidentes de seguridad o se identifiquen cambios organizativos, metodológicos, legales o tecnológicos que puedan suponer un incremento del riesgo al que se encuentran expuestos los sistemas de información.

7. Cuando del análisis de riesgos realizado resulte probable que el tratamiento suponga un riesgo significativo para los derechos y las libertades de las personas, conforme al artículo 35 del Reglamento (UE) 2016/679 los responsables del tratamiento, con el asesoramiento del delegado de protección de datos, realizarán previamente una evaluación de impacto de las operaciones de tratamiento en la protección de los datos personales.

Artículo 16
Gestión de incidentes

1. La Dirección General de Estrategia Digital y Desarrollo Tecnológico implantará los mecanismos apropiados para identificar correctamente, registrar y resolver los incidentes de seguridad de los sistemas de información de la Administración de la Comunidad Autónoma.

2. Esta Dirección General deberá notificar los incidentes de seguridad al Centro Criptológico Nacional (CCN-CERT) a través de la herramienta desarrollada para este fin.

3. Todos los responsables de seguridad de los sistemas de información incluidos en el ámbito de aplicación de la PSI-CAIB notificarán de forma inmediata los incidentes de seguridad a la Dirección General de Estrategia Digital y Desarrollo Tecnológico con una propuesta de categorización del incidente según las guías CCN-CERT de gestión de incidentes de la seguridad. La citada Dirección General, con carácter urgente, convocará al comité de crisis pertinente de acuerdo con el artículo 17.

Artículo 17
Comités de crisis

1. Los comités de crisis son los órganos encargados de gestionar, tomar decisiones, y coordinar las acciones necesarias para hacer frente a los incidentes de seguridad en los sistemas de información que se hayan calificado como crisis.

2. Los comités deberán determinar si se está ante una crisis o no, su nivel, las medidas a tomar y el reparto de responsabilidades. Asimismo, llevarán a cabo la gestión adecuada de los grupos de interés y la gestión de la comunicación tanto durante las crisis como posteriormente, durante la recuperación.

3. El Comité Operativo de Crisis estará formado por los miembros de la Comisión Técnica de la Seguridad de la Información. El Comité Superior de Crisis estará formado por los miembros de la Comisión Directora de Seguridad de la Información.

4. El Comité Operativo actuará ante los incidentes de seguridad calificados con un impacto bajo, medio y alto. En estos casos no será necesaria la declaración de crisis.

5. El Comité Superior actuará ante los incidentes de seguridad calificados con un impacto crítico y muy alto, en coordinación permanente con el Comité Operativo, y debe declarar la crisis. El presidente del Comité Superior informará permanentemente a la Presidencia del Gobierno de las Islas Baleares sobre el estado del incidente y su evolución.

6. La coordinación entre los dos comités se realizará a través del jefe del Departamento de Ciberseguridad y Telecomunicaciones y el jefe del Servicio de Ciberseguridad.

Artículo 18
Resolución de conflictos

1. En caso de conflicto entre los diferentes responsables que componen la estructura organizativa definida para la gestión de la seguridad de la información, deberán atenderse las siguientes reglas:

   a. Si los responsables en conflicto tienen un superior jerárquico común de nivel directivo, este resolverá el conflicto. En el caso de que no exista un superior jerárquico común o este sea el director general de Estrategia Digital y Desarrollo Tecnológico, resolverá la Comisión Técnica de la Seguridad de la Información.

   b. En los casos en que la Comisión Técnica de la Seguridad de la Información resuelva el conflicto, cualquiera de las partes en conflicto, a través de su órgano directivo, podrá apelar a la Comisión Directora de la Seguridad de la Información para que resuelva el conflicto en última instancia.

2. En cualquier caso, mientras no se pueda aplicar el mecanismo de resolución de conflictos descrito, prevalecerá la decisión del responsable de seguridad que garantice un nivel de protección de la información y de los servicios más alto.

Artículo 19
Obligaciones de cumplimiento de la política de seguridad

1. La PSI-CAIB y el cuerpo normativo de desarrollo es de obligado cumplimiento para todos los órganos superiores, órganos directivos y el personal de la Administración de la Comunidad Autónoma de las Illes Balears; así como para el personal de otros organismos o entidades que hayan sido autorizados para acceder a los sistemas de información de la Administración autonómica, con independencia del destino, adscripción o relación.

2. Todas las personas a quienes les sea de aplicación la PSI-CAIB tienen el deber de informar al responsable de seguridad correspondiente de cualquier riesgo significativo para la seguridad de los sistemas de información protegidos y de las violaciones de seguridad de las que tengan conocimiento, de acuerdo con los procedimientos establecidos.

3. El incumplimiento de la normativa de seguridad podrá conllevar la exigencia de las responsabilidades administrativas y legales correspondientes.

Artículo 20
Terceras partes

1. Cuando la Administración de la Comunidad Autónoma utilice servicios o trate información de otras entidades, se las hará partícipes de la PSI-CAIB y se establecerán mecanismos de información y coordinación de los respectivos responsables de seguridad.

2. Cuando la Administración de la Comunidad Autónoma preste servicios o ceda información a terceros, se les hará partícipes de la PSI-CAIB y de la normativa de seguridad que afecta a estos servicios e información. En este caso, los terceros quedarán sujetos a las obligaciones establecidas en esta normativa, sin perjuicio de poder desarrollar sus propios procedimientos operativos para satisfacerla.

Artículo 21
Revisión de la Política de Seguridad de la Información

La Comisión Técnica de Seguridad de la Información de la Comunidad Autónoma de las Illes Balears revisará la PSI-CAIB a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que mantenga su idoneidad, adecuación y eficacia.

Disposición adicional primera
Dotación presupuestaria

La aplicación de las previsiones contenidas en este decreto no supone ningún incremento del gasto público, dado que se atenderá con los medios materiales y humanos de que dispone la Administración autonómica, por lo que no se requiere ninguna dotación presupuestaria.

Disposición adicional segunda
Adaptación de políticas de seguridad existentes

Los entes del sector público instrumental de la Administración de la Comunidad Autónoma de las Illes Balears que dispongan de una política de seguridad de la información propia a la entrada en vigor de este decreto, deberán revisarla y adaptarla, si procede, para mantener la coherencia con la Política de Seguridad de la Información de la Administración autonómica y el respeto a los principios que en ella se recogen.

Disposición adicional tercera
Referencias a los cargos

1. En este decreto se utiliza la forma no marcada en cuanto al género, que coincide formalmente con la masculina, en todas las referencias a órganos, cargos y funciones, de manera que deben entenderse referidas al masculino o al femenino según la identidad de género de la persona titular de quien se trate.

2. Las referencias contenidas en este decreto a los cargos que se mencionan a continuación se interpretarán de la siguiente manera:

a) Las referencias al director general de Estrategia Digital y Desarrollo Tecnológico se hacen como órgano competente sobre los sistemas de información, recursos tecnológicos y servicios informáticos y telemáticos de la Administración de la Comunidad Autónoma; con funciones de encargo del tratamiento de los datos personales en relación con estos sistemas, recursos y servicios, y competente sobre la seguridad de la información de los recursos tecnológicos.

En el momento en que la Agencia Balear de Digitalización, Ciberseguridad y Telecomunicaciones asuma las competencias mencionadas en el párrafo anterior, las referencias al director general de Estrategia Digital y Desarrollo Tecnológico se entenderán realizadas al gerente de la Agencia.

b) Las referencias al director general de Función Pública se hacen como órgano competente en materia de ordenación y gestión del personal al servicio de la Administración de la Comunidad Autónoma de las Illes Balears.

c) Las referencias al director general de Emergencias e Interior se hacen como órgano competente en materia de emergencias, seguridad de las sedes de la Administración autonómica y coordinación de policías locales.

d) Las referencias al director general de Innovación y Transformación Digital se entienden como órgano competente en la promoción de la cultura de la ciberseguridad en la sociedad de las Illes Balears, incluyendo ciudadanos, administraciones y empresas.

e) Las referencias al secretario general de la Consejería de Presidencia, Coordinación de la Acción de Gobierno y Cooperación Local se entienden como consejería competente en materia de coordinación interdepartamental entre los órganos de consejerías diversas y de coordinación de las materias de carácter transversal.

f) Las referencias al consejero de Economía, Hacienda e Innovación se entienden como titular de la consejería de adscripción de la Dirección General de Estrategia Digital y Desarrollo Tecnológico.

Disposición adicional cuarta
Constitución de la Comisión Directora de la Seguridad de Información y de la Comisión Técnica de Seguridad de la Información

La sesión constitutiva de la Comisión Directora de la Seguridad de la Información y de la Comisión Técnica de la Seguridad de la Información deberá llevarse a cabo en el plazo de cuatro meses desde la entrada en vigor de este decreto.

Disposición adicional quinta
Definiciones

Los términos o expresiones utilizadas en este decreto tienen el significado indicado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Disposición derogatoria única
Normas que se derogan

Quedan derogadas todas las disposiciones de rango igual o inferior que se opongan, contradigan o sean incompatibles con lo que dispone este decreto y, en particular:

El Decreto 97/2006, de 24 de noviembre, por el que se crean y regulan las comisiones para la mejora continua de la seguridad de la información en la Administración de la Comunidad Autónoma de las Illes Balears.

Disposición final primera
Modificación del Decreto 24/2022, de 11 de julio, de la Comisión Superior de Sistemas de Información en Tecnologías y Comunicaciones

El apartado 2 del artículo 6 del Decreto 24/2022, de 11 de julio, de la Comisión Superior de Sistemas de Información en Tecnologías y Comunicaciones queda modificado de la siguiente manera:

«2. Corresponde a la Comisión Superior de Sistemas de Información en Tecnología y Comunicaciones emitir el informe previo y preceptivo sobre los pliegos de prescripciones técnicas para los contratos en materia de sistemas de información de cuantía superior a quinientos mil euros y, al director general de Estrategia Digital y Desarrollo Tecnológico, cuando no se supere este importe, en ambos casos, previa consulta a los jefes de departamento adscritos a esta Dirección General.»

Disposición final segunda
Desarrollo

Se faculta al consejero de Economía, Hacienda e Innovación para dictar las disposiciones necesarias para desarrollar este Decreto.

Disposición final tercera
Entrada en vigor

Este decreto entrará en vigor el día siguiente de su publicación en el *Boletín Oficial de las Illes Balears.*