Sección III. Otras disposiciones y actos administrativos

ADMINISTRACIÓN DE LA COMUNIDAD AUTÓNOMA
CONSEJERÍA DE ECONOMÍA, HACIENDA E INNOVACIÓN

374 ***Acuerdo del Consejo Rector del Instituto de Estadística de las Illes Balears por el que se aprueba la política de seguridad de la información del Instituto***

De acuerdo con el artículo 30.32 del Estatuto de Autonomía de las Illes Balears, la Comunidad Autónoma tiene competencia exclusiva en las estadísticas de interés para la comunidad autónoma y en la organización y gestión de un sistema estadístico propio.

La Ley 3/2002, de 17 de mayo, de Estadística de las Illes Balears, creó, mediante el artículo 32, el Instituto de Estadística de las Illes Balears (IBESTAT), como organismo autónomo adscrito a la consejería competente en materia de economía. Las funciones del Instituto se recogen en el artículo 34 de la mencionada Ley 3/2002, que suponen asumir la planificación, la normalización, la coordinación y la gestión del sistema estadístico de las Illes Balears, así como llevar a cabo las actividades estadísticas que se le encomienden en los programas anuales de estadística, y promover la difusión de las estadísticas relativas a la comunidad autónoma de las Illes Balears.

Por otra parte, el artículo 13 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establece los derechos de las personas en sus relaciones con las administraciones públicas; concretamente en la letra *h)* establece el derecho a la seguridad y la confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha ampliado el ámbito de aplicación del Esquema Nacional de Seguridad (ENS) a todo el sector público, y establece en su artículo 3, relativo a los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y la seguridad de las soluciones y los sistemas adoptados por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por estos medios, y señala el ENS como instrumento fundamental para alcanzar estos objetivos en el artículo 156.

El IBESTAT depende de los sistemas basados en las tecnologías de la información y la comunicación (TIC) para conseguir sus objetivos. Estos sistemas deben administrarse con diligencia, y se deben tomar las medidas adecuadas para protegerlos contra daños accidentales o deliberados que puedan afectar a la disponibilidad, trazabilidad, autenticidad, integridad o confidencialidad de la información tratada o de los servicios prestados. El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continua de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los diferentes departamentos deben garantizar que la seguridad de las TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde la concepción hasta la retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en los pliegos de licitación para proyectos de TIC. La información y los servicios prestados están sometidos a amenazas y riesgos provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, de 3 de mayo, determina la política de seguridad a aplicar en la utilización de los medios electrónicos. El ENS está constituido por los principios básicos y los requisitos mínimos para una adecuada protección de la información. La adecuación ordenada al ENS requiere el tratamiento de las siguientes cuestiones:

a) Preparar y aprobar la política de seguridad, incluyendo la definición de roles y la asignación de responsabilidades.
b) Categorizar los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados.
c) Llevar a cabo el análisis de riesgos, incluyendo la valoración de las medidas de seguridad existentes.
d) Preparar y aprobar la declaración de aplicabilidad de las medidas del anexo II del ENS.
e) Elaborar un plan de adecuación para mejorar la seguridad, en base a las insuficiencias detectadas, que debe incluir plazos estimados de ejecución.
f) Implantar, operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente.
g) Auditar la seguridad.
h) Informar sobre el estado de la seguridad.

De acuerdo con el artículo 12 del citado Real Decreto 311/2022, cada administración pública debe disponer de una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 del citado Real Decreto dispondrá de una política de seguridad formalmente aprobada por el órgano

https://intranet.caib.es/eboibfront//eboibfront/pdf/es/2025/9/1180811

competente.

La Comisión Directora de Seguridad de la Información de la Comunidad Autónoma de las Illes Balears emitió el informe correspondiente sobre el borrador de la política de seguridad del IBESTAT en la sesión del 28 de octubre de 2024, de acuerdo con 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.

Por todo ello, el Consejo Rector en la sesión del día 17 de diciembre de 2024 adopta el siguiente

Acuerdo

Primero. Aprobar la política de seguridad de la información del Instituto de Estadística de las Illes Balears, que se incorpora como anexo a este Acuerdo.

Segundo. Disponer que este Acuerdo, junto con el anexo, se publique en el *Boletín Oficial de las Illes Balears y en* el portal web del IBESTAT.

Tercero. Establecer que este Acuerdo produzca efectos desde la fecha de su publicación en el *Boletín Oficial de las Illes Balears*.

Palma, en la fecha de la firma electrónica *(14 de enero de 2025)*

La secretaria suplente del Consejo Rector del IBESTAT
Laura Alomar Llorente

ANEXO
Política de seguridad de la información del Instituto de Estadística de las Illes Balears

1. Objeto

1.1. Constituye el objeto de esta Resolución fijar la política de seguridad de la información (PSI) en el ámbito del Instituto de Estadística de las Illes Balears (IBESTAT), así como establecer el marco organizativo, operacional y tecnológico de esta entidad.

1.2. La política de seguridad de la información identifica responsabilidades y establece principios y directrices para alcanzar una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las tecnologías de la información y la comunicación (TIC).

1.3. La política de seguridad de la información es el instrumento en el que se apoya el IBESTAT para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones. La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones, y debe comprenderse no como un producto, sino como un proceso continuo de adaptación y mejora, que debe ser controlado, gestionado y monitorizado con la implantación de la cultura de la seguridad en el IBESTAT.

2. Ámbito de aplicación

2.1. La PSI es de obligado cumplimiento para todas las personas responsables del IBESTAT tanto en el campo de la gestión como en el técnico; también es de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la misma información que gestione cada área, con independencia de cuál sea el destino, la adscripción o la relación con el área.

2.2. Esta política es de aplicación y de obligado cumplimiento para todas las áreas y servicios del IBESTAT y también afecta a todos los recursos y procesos incluidos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, ya sean internos o externos, vinculados a la entidad a través de contratos o acuerdos con terceros.

2.3. Esta política debe aplicarse a los sistemas de información del IBESTAT que están relacionados con la prestación de servicios por medios electrónicos a la ciudadanía, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del alcance del Esquema Nacional de Seguridad (ENS).

https://intranet.caib.es/eboibfront//eboibfront/pdf/es/2025/9/1180811

3. Misión

El IBESTAT es el órgano central de estadística de la Comunidad Autónoma de las Illes Balears, creado por la Ley 3/2002, de 17 de mayo, de Estadística de las Illes Balears. Entre las funciones que determinan su misión destacan las siguientes:

a) Llevar a cabo las actividades estadísticas que le asignen los planes y los programas estadísticos aprobados por el Gobierno de las Illes Balears, con independencia técnica y profesional, atendiendo al hecho insular y otras desagregaciones territoriales, y cumpliendo los principios establecidos en el Código de buenas prácticas de las estadísticas europeas.

b) Coordinar la actividad estadística autonómica como responsable de la promoción, gestión y coordinación del Sistema Estadístico de las Illes Balears (SESTIB). En este sentido, confecciona la propuesta de planes y programas estadísticos que aprobará el Gobierno de las Illes Balears.

c) Establecer todos los elementos técnicos necesarios para desarrollar el artículo 30.32 del Estatuto de Autonomía referente a la competencia exclusiva en materia estadística de interés de la comunidad autónoma, de acuerdo con la citada Ley de estadística autonómica y demás normativa estadística que pueda afectarle.

4. Objetivos

4.1. Son objetivos generales del IBESTAT los siguientes:

a) Establecer un marco de gestión de la seguridad de la información adecuado al Real Decreto 311/2022, reconociendo así como activos estratégicos la información y los sistemas que la soportan.

b) Establecer las bases sobre las que el personal del IBESTAT y la ciudadanía pueden acceder a los servicios en un entorno de gestión seguro, anticipándose a sus necesidades y preservando sus derechos.

c) Proteger la información de un amplio abanico de amenazas, con el fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el cumplimiento eficiente de los objetivos del IBESTAT.

d) Garantizar el adecuado funcionamiento de las actividades de control, monitorización y mantenimiento de las infraestructuras e instalaciones generales, necesarias para la adecuada prestación de servicios, así como de la información derivada de dicho funcionamiento.

4.2. Son objetivos específicos del IBESTAT los siguientes:

a) Contribuir desde la gestión de la seguridad de la información al cumplimiento de la misión y los objetivos establecidos para el IBESTAT.

b) Disponer de las medidas de control necesarias para cumplir los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo que se refiere a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.

c) Asegurar el acceso, la integridad, la confidencialidad, la disponibilidad, la autenticidad y la trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

d) Proteger los recursos de información del IBESTAT y la tecnología utilizada para procesarlos contra amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, la integridad, la disponibilidad, la legalidad y la fiabilidad de la información.

5. Revisión de la política de seguridad de la información

5.1. El Comité para la Gestión y la Coordinación de la Seguridad de la Información (en adelante, Comité) tiene que proponer, revisar y difundir la PSI, con el apoyo de la persona responsable de seguridad, que debe velar activamente por conservarla, actualizarla y difundirla entre todas las partes afectadas.

5.2. La política de seguridad de la información debe revisarse una vez al año y siempre que existan cambios relevantes en la organización, con el fin de asegurar que se adecua a la estrategia y las necesidades de la organización.

5.3. En caso de conflictos o diferentes interpretaciones de esta política, la dirección del IBESTAT es el órgano competente para resolverlos.

https://intranet.caib.es/eboibfront//eboibfront/pdf/es/2025/9/1180811

6. Marco normativo

Se toma como referencia básica en materia de seguridad de la información la normativa relacionada con el Código del derecho de la ciberseguridad establecido por el Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática, en la que se detalla toda la normativa aplicable, entre las cuales se encuentran las siguientes normativas, enunciadas a título informativo no limitativo:

— Reglamento (UE) núm. 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 se refiere 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 Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
— Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
— Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público.
— Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información.
— Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
— 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.
— 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.
— Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
— Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
— Real Decreto Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
— Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
— Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.
— Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma 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.
— 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.
— 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.
— Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas por la que se aprueba la Instrucción técnica de seguridad del informe del estado de la seguridad.
— Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas por la que se aprueba la Instrucción técnica de seguridad de conformidad con el Esquema Nacional de Seguridad.
— Resolución de 27 de marzo de 2018 de la Secretaría de Estado de Función Pública por la que se aprueba la Instrucción técnica de seguridad de la auditoría de la seguridad de los sistemas de información.
— Resolución de 13 de abril de 2018 de la Secretaría de Estado de Función Pública por la que se aprueba la Instrucción técnica de seguridad de notificación de incidentes de seguridad.
— Ley 3/2002, de 17 de mayo, de Estadística de las Illes Balears.
— Ley 7/2010, de 21 de julio, del Sector Público Instrumental de la Comunidad Autónoma de las Illes Balears.
— Decreto 128/2007, de 5 de octubre, de Organización y Funcionamiento del Instituto de Estadística de las Illes Balears.
— Decreto 8/2021, de 9 de febrero, sobre la transparencia y derecho de acceso a la información pública.
— Decreto 31/2023, de 22 de mayo, por el que se establece la organización administrativa en materia de transparencia y se desarrolla el ejercicio del derecho de acceso a la información pública en la Administración de la Comunidad Autónoma de las Illes Balears y en su sector público instrumental.

7. Principios básicos en materia de seguridad de la información

El IBESTAT, para conseguir el cumplimiento de las previsiones recogidas en el Real Decreto 311/2022, debe implementar las medidas de seguridad proporcionales a la naturaleza de la información y los servicios que deben protegerse y teniendo en cuenta la categoría de los sistemas afectados.

Por ello, deben tenerse en cuenta los principios básicos desglosados en el capítulo 2 del Real Decreto 311/2022:

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en los riesgos.

https://intranet.caib.es/eboibfront//eboibfront/pdf/es/2025/9/1180811

c) Prevención, detección, respuesta y conservación.
d) Existencia de líneas de defensa.
e) Vigilancia continua.
f) Reevaluación periódica.
g) Diferenciación de responsabilidades.

8. Estructura de la documentación de seguridad

8.1. Sin perjuicio del marco normativo previsto en el punto 6 de este anexo, el cuerpo jurídico específico de la PSI de este organismo autónomo que sea de obligado cumplimiento debe desarrollarse en tres niveles, según el ámbito de aplicación y el detalle técnico. Estos niveles son los siguientes:

a) Primer nivel: marco común y directrices básicas de la política de seguridad de la información en el ámbito de la administración electrónica de la Comunidad Autónoma de las Illes Balears. Constituyen este primer nivel el Acuerdo del Consejo Rector del Instituto de Estadística de las Illes Balears por el que se aprueba la política de seguridad de información del Instituto y las disposiciones, directrices y normas de seguridad generales en el ámbito de aplicación de la PSI que define el punto 6 de este anexo.
b) Segundo nivel: instrucciones operativas de seguridad de la información e instrucciones de las TIC. Estas instrucciones dan respuesta, sin entrar en detalles de implementación ni tecnológicos, a lo que se puede hacer y a lo que no en relación con un determinado tema desde el punto de vista de la seguridad, qué se considera un uso apropiado o inapropiado, o qué consecuencias se derivan del incumplimiento, entre otros aspectos. Los documentos relativos a este segundo nivel serán elaborados por el Comité y aprobados por el titular de la dirección del IBESTAT, a propuesta de la persona responsable de seguridad.
c) Tercer nivel: instrucciones técnicas de seguridad de las tecnologías de la información y la comunicación (STIC). Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a la forma en que se puede llevar a cabo una determinada tarea, respetando los principios de seguridad de la organización y los procesos internos establecidos. Los documentos relativos a este tercer nivel serán elaborados por el Comité y aprobados por el titular de la dirección del IBESTAT, a propuesta de la persona responsable de seguridad.

8.2. Además de los documentos mencionados en el apartado anterior, la documentación de seguridad del sistema puede disponer, bajo el criterio de la persona responsable de seguridad, de otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros o evidencias electrónicas, entre otros aspectos.

9. Desarrollo de la política de seguridad de la información

Esta política de seguridad de la información debe desarrollarse mediante una normativa de seguridad que trate aspectos específicos. La normativa de seguridad debe estar a disposición de todos los miembros de la organización que necesiten conocerla, en particular para quienes utilicen, operen o administren los sistemas de información y las comunicaciones.

Las normas y los procedimientos deben prever, al menos, los siguientes aspectos:

a) Protección de datos de carácter personal: deben implantarse medidas técnicas y organizativas que permitan cumplir los requisitos normativos en esta materia.
b) Gestión de activos de información: los activos de información se deben inventariar, categorizar y asociar a un responsable.
c) Seguridad ligada a los recursos humanos: la seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios, por lo que deben implantarse los mecanismos que permitan a los usuarios conocer sus responsabilidades y cómo cumplirlas.
d) Seguridad física: las instalaciones del IBESTAT deben mantener una seguridad física correcta para evitar los accesos no autorizados, así como cualquier otro tipo de daño o interferencia externa.
e) Seguridad lógica: se deben establecer medidas organizativas y técnicas para controlar los accesos, proteger frente a códigos nocivos, asegurar las comunicaciones, realizar copias de seguridad, etc.
f) Gestión de incidentes de seguridad: deben establecerse responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los acontecimientos en materia de seguridad.

10. Gestión y acceso a la documentación del sistema

10.1. El IBESTAT desarrolla la política de gestión y conservación de los documentos electrónicos que se implementa mediante normas internas, procedimientos e instrucciones técnicas.

10.2. Debe disponerse de un sistema para gestionar la elaboración, la aprobación, la conservación, la estructura y el acceso, entre otros, de los documentos del sistema de gestión de la seguridad aplicado sobre los sistemas de información.

https://intranet.caib.es/eboibfront//eboibfront/pdf/es/2025/9/1180811

11. Organización de la gestión de la PSI

11.1. La organización de la seguridad queda establecida mediante la identificación y la definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte.

11.2. Todas y cada una de las personas usuarias de los sistemas de información del IBESTAT son responsables de la seguridad de los activos de información, por lo que tienen que hacer siempre un uso correcto, de acuerdo con sus atribuciones profesionales.

11.3. Para responder mejor a incidentes de seguridad, el IBESTAT debe mantener relaciones de cooperación en materia de seguridad con las autoridades competentes, los proveedores de servicios informáticos o de comunicación, así como con organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

11.4. La estructura organizativa para gestionar la seguridad de la información en el ámbito descrito en esta PSI del IBESTAT está integrada por los siguientes órganos y agentes:

a) Comité para la Gestión y la Coordinación de la Seguridad de la Información.
b) Responsable de la información.
c) Responsable del servicio.
d) Responsable de seguridad.
e) Responsable del sistema.

12. Comité para la Gestión y la Coordinación de la Seguridad de la Información

12.1. Se crea el Comité para la Gestión y la Coordinación de la Seguridad de la Información como una comisión de trabajo integrada en el IBESTAT, y está constituido por los siguientes miembros:

a) Presidencia: la persona responsable de la dirección del IBESTAT.
b) Secretaría: una persona del IBESTAT, con vínculo funcionarial, designada por la presidencia, que actúa con voz y sin voto.
c) Vocalías: las personas titulares de los servicios del IBESTAT; la persona o el órgano designado delegado de protección de datos, que actúa con independencia y no puede participar en las decisiones relativas a los fines y medios del tratamiento, y la persona ocupe el puesto de trabajo de jefe o jefa de la Sección I de la especialidad de informática del IBESTAT.

12.2. El Comité se regirá por lo dispuesto en la Ley 40/2015 para los órganos colegiados en lo que concierne al régimen de funcionamiento en todo aquello que no esté previsto en este anexo.

12.3. El Comité debe reunirse cada año con carácter ordinario y con carácter extraordinario a propuesta de la presidencia. No se percibirán indemnizaciones en concepto de asistencia a las reuniones del Comité.

12.4. Puede acordarse la constitución de grupos de trabajo para analizar, elaborar y ejecutar trabajos o actividades específicas, dentro del ámbito de sus funciones. El Comité debe conocer en las sesiones del pleno los resultados de las actuaciones de los grupos de trabajo.

12.5. Corresponden al Comité las siguientes funciones:

a) Elaborar los borradores de modificación y actualización de la PSI.
b) Analizar los riesgos e impulsar su evaluación.
c) Revisar el informe anual de análisis de riesgos realizado por la persona responsable de seguridad.
d) Impulsar la actualización de los criterios y directrices sobre seguridad de la información.
e) Impulsar medidas para mejorar y reforzar los sistemas de seguridad y control.
f) Impulsar la difusión y el cumplimiento de la PSI, y promover actividades de concienciación y formación en materia de seguridad para el personal del IBESTAT.
g) Elaborar los borradores de directrices y normas de seguridad generales del IBESTAT, que deben cumplir el marco normativo de este anexo.
h) Elaborar la normativa de seguridad de segundo y tercer nivel.
i) Coordinar las decisiones y actuaciones de la persona responsable de seguridad, y asesorar para resolver los posibles conflictos bajo el criterio de garantizar la seguridad de las infraestructuras tecnológicas compartidas.
j) Impulsar los proyectos para adecuarlos al cumplimiento del Esquema Nacional de Seguridad.
k) Compartir experiencias de éxito en materia de seguridad entre los miembros del Comité para velar por el cumplimiento de la PSI y la normativa que la desarrolla.
l) Coordinar todas las actividades relacionadas con la seguridad de los sistemas de información.
m) Velar para que la seguridad de la información sea parte del proceso de planificación del IBESTAT.

https://intranet.caib.es/eboibfront//eboibfront/pdf/es/2025/9/1180811

n) Cualquier otra actuación en materia de seguridad de la información que no corresponda específicamente a otro agente.

13. Responsable de la información

13.1. Las funciones de la persona responsable de la información establecida en la normativa regulada en el Esquema Nacional de Seguridad corresponden a la dirección del IBESTAT.

13.2. Dentro de su ámbito de actuación, debe determinar los requisitos de la información tratada, establecer las necesidades de seguridad de la información y realizar las valoraciones del impacto que tendría un incidente que afectase a su seguridad; además, tiene la potestad de modificar el nivel de seguridad requerido.

13.3. Para desarrollar estas funciones, debe contar con la colaboración de las personas gestoras titulares de las unidades a su cargo con rango de servicio o equivalente.

14. Responsable del servicio

14.1. La tarea de responsable del servicio corresponde a los jefes de servicio para áreas de gestión de las que son titulares, tal y como establece la normativa que regula el Esquema Nacional de Seguridad. Concretamente los servicios afectados son los siguientes:

— Producción Estadística
— Difusión Estadística
— Coordinación y Planificación Estadística

14.2. Dentro de su ámbito de actuación, determina los requisitos de seguridad de los servicios prestados.

15. Responsable de seguridad

15.1. Las funciones de la persona responsable de seguridad corresponden a la dirección del IBESTAT.

15.2. Determina las decisiones para satisfacer los requisitos de seguridad de la información y servicios, supervisa la implantación de las medidas necesarias para garantizar la consecución de los requisitos e informa sobre estas cuestiones.

15.3. El ámbito de actuación del responsable de seguridad debe limitarse única y exclusivamente a los sistemas de información y a los servicios de tecnología de la información y la comunicación que sean competencia y responsabilidad directa del IBESTAT.

15.4. Coordina de forma continuada el desarrollo de la seguridad de la información en el ámbito de aplicación de este anexo, además de ejercer las siguientes funciones específicas:

a) Promover la seguridad de la información utilizada y de los servicios electrónicos de los sistemas de información.
b) Mantener la documentación de seguridad actualizada y organizada en los sistemas de conocimiento corporativos y gestionar los mecanismos para acceder a ellos.
c) Proponer al Comité la normativa de seguridad de segundo y tercer nivel.
e) Promover las actividades de concienciación e información en materia de seguridad en su ámbito de responsabilidad.
f) Llevar a cabo la coordinación y seguimiento de la implantación de los proyectos de adecuación al Esquema Nacional de Seguridad.
g) Elaborar, con los responsables de los servicios, los preceptivos análisis de riesgo, seleccionar las salvaguardas a implantar, revisar el proceso de gestión del riesgo y elevar un informe anual al Comité.
h) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, analizar los informes de auditoría y elaborar las conclusiones que deben presentarse a las personas responsables del servicio para que, junto con la persona responsable de la información, adopten las medidas correctoras adecuadas.
i) Coordinar el proceso de gestión de la seguridad.
j) Firmar la declaración de aplicabilidad, que comprende la aplicación de medidas de seguridad seleccionadas por un sistema conforme al artículo 28 del Real Decreto 311/2022.
k) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes de cada período.
l) Determinar la categoría de seguridad de los sistemas de información, según el procedimiento descrito en el anexo 1 del Real Decreto 311/2022, y las medidas de seguridad que deben aplicarse de acuerdo con el anexo 2 de este Real Decreto.
m) Determinar la categoría de seguridad de acuerdo con las valoraciones que realicen los responsables de la información y del servicio conforme al anexo 1 del Real Decreto 311/2022.

15.5. Para ejercer sus funciones, debe contar con el apoyo del Comité.

15.6. Dado que el responsable de seguridad recae sobre la dirección del IBESTAT, se tomarán medidas compensatorias, consistentes en realizar auditorías periódicas de seguridad o bien documentar y justificar las decisiones tomadas por el Comité para la Gestión y la

https://intranet.caib.es/eboibfront//eboibfront/pdf/es/2025/9/1180811

Coordinación de la Seguridad de la Información.

16. Responsable del sistema

16.1. Es responsable del sistema la persona titular del Servicio de Asistencia Técnica y Computacional del IBESTAT, dado que es la unidad administrativa que ejerce las competencias en materia de gestión de sistemas de información.

16.2. Las funciones de la persona responsable del sistema son las siguientes:

a) Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, siguiendo las indicaciones de la persona responsable de seguridad.
b) Aprobar todas las modificaciones substanciales de cualquier elemento del sistema.
c) Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informada de deficiencias graves de seguridad previo informe de la persona responsable de esta información o servicio y de la persona responsable de seguridad. En caso de no llegar a un acuerdo en este sentido, debe atenerse el régimen de resolución de conflictos previsto en el punto 20 de este anexo.

17. Obligaciones del personal

17.1. Toda persona que preste servicios en el IBESTAT tiene la obligación de conocer y cumplir la PSI y la normativa de seguridad derivada, siendo responsabilidad del Comité disponer de los medios necesarios para que la información esté disponible para las personas afectadas y comunicar esta disponibilidad.

17.2. Todas las personas que empleen o tengan acceso a los sistemas tecnológicos o de información tienen las siguientes obligaciones:

a) Conocer y respetar la PSI, así como las normas de seguridad y los procedimientos de seguridad que la desplieguen y que le afecten.
b) Asistir a las acciones de concienciación en materia de seguridad de la información que se lleven a cabo.
c) Emplear los servicios y los sistemas de información, así como la información que contengan y a la que tengan acceso, con una finalidad profesional de acuerdo con las tareas encomendadas en función del puesto de trabajo y las finalidades y propósitos que motivaron la concesión del acceso.
d) Velar por la confidencialidad de la información a la que tengan acceso según su clasificación y características.
e) Notificar actuaciones o hechos que puedan suponer una incidencia de seguridad o evidencien una debilidad que pueda implicar incidentes posteriores.
f) Colaborar en la resolución de incidentes de seguridad y en la realización de acciones preventivas cuando sea necesaria su participación.
g) No llevar a cabo acciones intencionadas que perjudiquen a la seguridad de los sistemas tecnológicos o de información, ni a la información que contienen.

17.3. El incumplimiento de estas obligaciones podrá sancionarse de conformidad con la normativa disciplinaria correspondiente.

17.4. En caso de personas vinculadas a entidades externas, el uso de sistemas tecnológicos o de información debe limitarse a las tareas o actividades circunscritos a los términos del contrato o acuerdo que regula la relación entre esta entidad y el IBESTAT.

18. Terceras partes

18.1. Cuando se presten servicios a otros organismos o se ceda información a terceros:

a) Se les hará participar de la PSI y de las normas de seguridad o procedimientos de seguridad relacionados con el servicio o la información afectados.
b) Se establecerán canales de información y coordinación entre las personas responsables de gestión de la seguridad de la información respectivas y establecerán procedimientos de seguridad para reaccionar ante los incidentes que puedan llevarse a cabo.

18.2. Cuando se empleen servicios o se maneje información de otros organismos o entidades, se procurarán canales de información y coordinación en materia de seguridad de la información.

18.3. En los contratos de implantación, mantenimiento o gestión de sistemas o aplicaciones informáticas, de prestación de servicios tecnológicos, así como en el caso de contratos de prestación de servicios de otro tipo que implique el uso de servicios, aplicaciones o sistemas informáticos internos, se tendrán en cuenta las medidas y consideraciones de seguridad de la información que sean de aplicación, según la legislación vigente en la materia. También deben tenerse en cuenta las medidas y las consideraciones de seguridad de la información que resulten de aplicación legal, en caso de acuerdo de cesión de sistemas, aplicaciones o acceso a servicios de otros organismos o entidades.

https://intranet.caib.es/eboibfront//eboibfront/pdf/es/2025/9/1180811

18.4. Cuando alguna parte no pueda satisfacer algún aspecto de la PSI, se requerirá al Comité un informe sobre los riesgos en que puede incurrirse y la forma de tratarlos. A la vista de este informe, y antes de que se haga efectiva la prestación, uso, acceso o gestión de que se trate, las personas responsables de la información o de los servicios afectados decidirán sobre la aceptación del riesgo residual.

18.5. En todo caso, se dará cumplimiento tanto a la normativa del Esquema Nacional de Seguridad como a la normativa en materia de protección de datos personales. Es de especial aplicación el Esquema Nacional de Seguridad a los sistemas de información de las entidades del sector privado, incluida la obligación de disponer de la política de seguridad, cuando, de acuerdo con la normativa aplicable, y en virtud de una relación contractual, presten servicios o provean soluciones al IBESTAT para que éste pueda ejercer sus competencias y potestades administrativas, de conformidad con el artículo 2.3 del Real Decreto 311/2022.

19. Gestión de riesgos

19.1. La gestión de riesgos es un factor esencial para gestionar correctamente la seguridad de la información, y debe llevarse a cabo de forma continuada sobre los sistemas de información, de acuerdo con los principios de gestión de la seguridad basada en los riesgos del artículo 7 y la reevaluación periódica del artículo 10 del Real Decreto 311/2022.

19.2. La persona responsable de seguridad es la encargada del análisis del riesgo de los sistemas de información gestionados por el IBESTAT y de seleccionar las medidas a implantar. El informe del análisis de riesgos con las medidas contenidas en el mismo debe ser analizado y revisado por el Comité.

19.3. Las personas responsables de la información y del servicio son las responsables de los riesgos sobre la información y sobre los servicios respectivamente y, por tanto, de aceptar los riesgos residuales calculados en el análisis y de realizar su seguimiento y control.

19.4. El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad que deben aplicarse, que deben ser proporcionadas a los riesgos y estar justificadas, debe revisarse cada año.

19.5. En el caso de riesgos que se deriven del tratamiento de datos personales, la persona responsable del tratamiento, asesorada por la persona delegada de protección de datos, debe llevar a cabo un análisis de riesgos y, en los supuestos previstos en la normativa de protección de datos, una evaluación de impacto en la protección de datos. En todo caso, estas medidas prevalecerán en caso de resultar agravadas respecto de las previstas en el Real Decreto 311/2022.

20. Resolución de conflictos

20.1. En caso de conflicto entre las personas responsables de la estructura organizativa de la PSI, éste será resuelto por la persona superior jerárquicamente. En su defecto, será resuelto por la persona titular de la dirección del IBESTAT, una vez oído el Comité.

20.2. En caso de conflicto entre las personas responsables que componen la estructura organizativa de la PSI y las definidas en la normativa de protección de datos de carácter personal, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de datos de carácter personal según determine la persona responsable del tratamiento.

21. Auditoría

21.1. Los sistemas de información propios del IBESTAT serán objeto de una auditoría ordinaria interna o externa que verifique el cumplimiento de los requerimientos del Esquema Nacional de Seguridad. Con carácter extraordinario se realizará esta auditoría siempre que se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad requeridas.

21.2. Los informes de auditoría deben permanecer a disposición del Comité.

22. Formación y concienciación

22.1. El IBESTAT debe desarrollar actividades formativas específicas orientadas a concienciar y formar al personal de este organismo autónomo, así como difundir la PSI y desplegarla normativamente.

22.2. El Comité y la persona responsable de seguridad deben encargarse de promover las actividades de formación y concienciación en materia de seguridad.

https://intranet.caib.es/eboibfront//eboibfront/pdf/es/2025/9/1180811