POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INFORMACION DEL DOCUMENTO

Título del documento	**PO-01 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**
Tipo de documento	Política de Seguridad
Descripción	La Política de Seguridad de la Información es un documento de alto nivel que define lo que significa 'seguridad de la información' en una organización. El documento debe estar accesible por todos los miembros de la organización
Nivel de seguridad recomendado	Publica
Propietario del documento	La Agencia Tributaria de las Illes Balears (ATIB)

Registro de versiones		
Descripción	**Versión**	**Fecha**
Versión inicial del documento	1.0	27/02/2024
Corrección de Marco Legislativo	1.1	08/05/2024
Se Anexa punto 6.5 resolución de conflictos	1.1	08/05/2024
Se Anexa apartado 10. Gestión documental	1.1	08/05/2024
Se ajusta el apartado 7. Datos de Carácter Personal	1.1	08/05/2024
Se han adaptados los apartados que no se ajustaban en su totalidad a la organización y su estructura organizacional	1.2	16/05/2024
Se han corregido error en las responsabilidades en el apartado 6	1.2	17/05/2024

Tabla de contenido

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día **21 de Mayo de 2024** en sesión del comité de Seguridad de la Información de La Agencia Tributaria de les Illes Balears (ATIB).

Esta “Política de Seguridad de la Información”, en adelante Política, será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

La Agencia Tributaria de les Illes Balears (ATIB) depende en gran medida de los sistemas de Tecnologías de Información y Comunicaciones (TIC) para alcanzar sus objetivos operativos. Dada esta dependencia crítica, es imperativo administrar estos sistemas con la máxima diligencia, implementando medidas efectivas para salvaguardarlos contra posibles daños, tanto accidentales como intencionados, que pudieran comprometer la disponibilidad, integridad, autenticidad, trazabilidad y confidencialidad de la información manejada y los servicios proporcionados.

El propósito fundamental de la política de seguridad de la información es asegurar la calidad de la información y la continuidad sin interrupciones en la prestación de servicios. Esto se logra a través de una combinación de enfoques preventivos, supervisión constante de las actividades diarias y una respuesta ágil ante cualquier incidente que pueda surgir.

Dada la naturaleza dinámica y en constante evolución de las amenazas a los sistemas TIC, es esencial adoptar una estrategia proactiva que se adapte a los cambios en el entorno de seguridad. Esto implica la implementación de medidas mínimas de seguridad establecidas por el Esquema Nacional de Seguridad, así como la vigilancia continua de los niveles de servicio, el análisis de vulnerabilidades reportadas y la preparación de planes de respuesta a incidentes eficaces para garantizar la continuidad de los servicios.

Cada departamento dentro de la organización debe asegurarse de que la seguridad de las TIC sea una consideración integral en todas las etapas del ciclo de vida de los sistemas, desde su concepción y desarrollo hasta su retirada. Los requisitos de seguridad y las necesidades financieras deben ser identificados y abordados en todas las fases de planificación, adquisición y operación de proyectos relacionados con las TIC.

Es fundamental que los departamentos estén preparados para prevenir, detectar, responder y recuperarse de incidentes de seguridad, conforme a lo establecido en el Artículo 7 del Esquema Nacional de Seguridad. Esto garantizará la capacidad de la ATIB para mantener la integridad y la continuidad de sus operaciones en un entorno cada vez más desafiante en términos de seguridad de la información.

2.1. Prevención

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

Para garantizar el cumplimiento de la política, los departamentos deben:

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

2.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 8 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. Respuesta

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE.

Esta Política se aplicará a los sistemas de información de La Agencia Tributaria de les Illes Balears, que están relacionados con el ejercicio de derechos y 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).

Todos los empleados públicos y cargos de La Agencia Tributaria de les Illes Balears, así como el personal de terceros relacionados con éste, que se encuentren afectados por el alcance del ENS, tienen la obligación de conocer y cumplir esta “Política de Seguridad de la Información” y la normativa de seguridad, siendo responsabilidad del comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

4. MISIÓN

Describir los objetivos de servicio del organismo.

La Agencia Tributaria de les Illes Balears (ATIB), para la gestión de sus intereses y de las funciones y competencias que tiene encomendadas, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y expectativas de la población y de todos los grupos de interés.

La Agencia Tributaria de les Illes Balears (ATIB), desea potenciar el uso de las nuevas tecnologías tanto internamente como en sus relaciones con la ciudadanía.

Los principales objetivos que se persiguen son, entre otros, los siguientes:

- Mejorar la calidad de los servicios públicos
- Fomentar la relación electrónica de la ciudadanía con la entidad, creando la confianza necesaria entre ciudadano y la agencia en esa relación.
- Reducir los tiempos de tramitación.
- Reducir las cargas administrativas.
- Hacer transparente la actividad de la Agencia Tributaria.
- Fomentar la participación y colaboración.

5. MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades y competencias La Agencia Tributaria de les Illes Balears (ATIB), en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por la siguiente legislación:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de 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 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la 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 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 Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (enlace a https://www.boe.es/doue/2014/257/L00073-00114.pdf), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (reglamento eIDAS).
- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2013, de 27 de diciembre, de Impulso de la factura electrónica y creación del Registro electrónico de facturas en el sector público.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (archivo).
- 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.
- 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 9/2014, de 9 de mayo, General de Telecomunicaciones (Vigente en los apartados señalados en la Disposición Derogatoria Única de la Ley 11/2022, de 28 de junio).
- 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.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones (según plazos entrada en vigor de Disposición de esta Ley).
- También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica La Agencia Tributaria de les Illes Balears (ATIB), derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política.

El mantenimiento del marco normativo será responsabilidad La Agencia Tributaria de les Illes Balears (ATIB), y se mantendrá en un Anexo a este documento. Incluido el perfil de cumplimiento específico y las instrucciones técnicas de

seguridad de obligado cumplimiento, publicadas por parte del Centro Criptológico Nacional (CCN) tal y como se establece en el “Artículo 30. Perfil de cumplimiento específico”.

Así mismo, La Agencia Tributaria de les Illes Balears (ATIB), también será responsable de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. Comités: Funciones y Responsabilidades.

El Comité de Seguridad de la Información coordina la seguridad de la información. Procurará estar formado por representantes de las áreas afectadas por el ENS (se detalla en el Documento de PR-01 Organización de la seguridad).

La Comisión de Seguridad TIC reportará a la Dirección de ATIB y tendrá las siguientes funciones:

- Establecer los mecanismos de cooperación y coordinación con las diversas áreas de La Agencia Tributaria de les Illes Balears en materia de seguridad de la información.
- Establecer los mecanismos de cooperación y coordinación con las diversas áreas de La Agencia Tributaria de les Illes Balears en materia de seguridad de la información.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua de la gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Dirección en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por el órgano municipal competente.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En

particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

El Comité de Seguridad TIC estará formado por:

- **Responsable de Seguridad:** Rodríguez Zambrano Ivohe
- **Responsable de Sistemas**: Pedrona Comas Serra
- **Responsable de Información:** Justo Alberto Roibal Hernández
- **Responsable de Servicios:** Rafael Estelrich Planas
- **DPD:** Larisa Harabor

Aquí aparecen cargos corporativos y designaciones de departamentos dentro del organismo cuando proceda.

6.2. Roles: Funciones y Responsabilidades.

El ENS se rige por el Real Decreto 311/2022 y establece 4 roles en 2 niveles según su artículo 11. Los cuales también están detallados en la Guía 801 del Centro Criptológico Nacional.

	ROLES	
NIVEL DE GOBIERNO	RESPONSABLE DE INFORMACIÓN Determinar los niveles de seguridad de la información	RESPONSABLE DE SERVICIO Determinar los niveles de seguridad de los servicios
NIVEL OPERATIVO	RESPONSABLE DE LA SEGURIDAD Atiende la seguridad de la información	RESPONSABLE DEL SISTEMA Explotación de la Tecnología

A nivel de Gobierno podemos encontrar:

El responsable de la información: Determina los requisitos de seguridad de la información tratada según los parámetros del anexo I del ENS. Puede tratarse de una persona o de un órgano colegiado.

El responsable de servicio: Determina los requisitos de seguridad de los servicios prestados según los parámetros del anexo I del ENS. Puede tratarse de una persona física singular o de un órgano colegiado, formando parte de lo que se denomina Comité de Seguridad de la Información.

Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

A nivel Operativo podemos encontrar:

El responsable de Seguridad (o CISO): Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por el responsable de la información y de los servicios. Deberá ser una persona física jerárquicamente independiente del responsable del sistema. En caso de servicios externalizados, la responsabilidad última la tiene siempre la entidad.

Funciones:

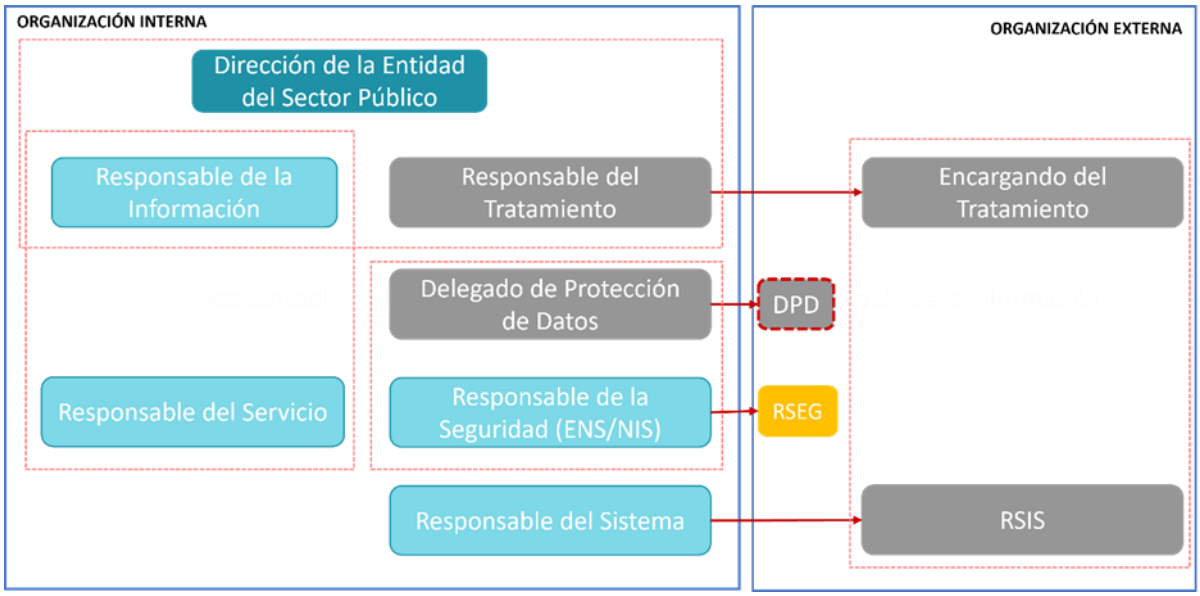
- Elaborar Planes con Medidas para gestionar los riesgos detectados.
- Supervisar y desarrollar las políticas de seguridad, normativas y procedimientos, su efectividad… Haciendo controles periódicos.
- Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad.
- Promover y formar sobre “buenas prácticas” de la organización en materia de ciberseguridad
- Remitir a la autoridad competente las notificaciones de incidencias con efectos adversos.
- Recibir, interpretar y supervisar la aplicación de instrucciones y guías de la autoridad competente
- Recopilar y suministrar información o documentación a la autoridad competente.

El responsable de sistema: Se encarga de la operación del Sistema de información atendiendo a las medidas de seguridad determinadas por el responsable de la seguridad. Su responsabilidad puede estar situada dentro de la organización o estar compartimentada. Los informes de autoevaluación y los informes de auditoría serán analizados por el responsable de la seguridad competente, que evaluará las conclusiones del responsable del Sistema para que adopte las medidas correctivas adecuadas.

Funciones:

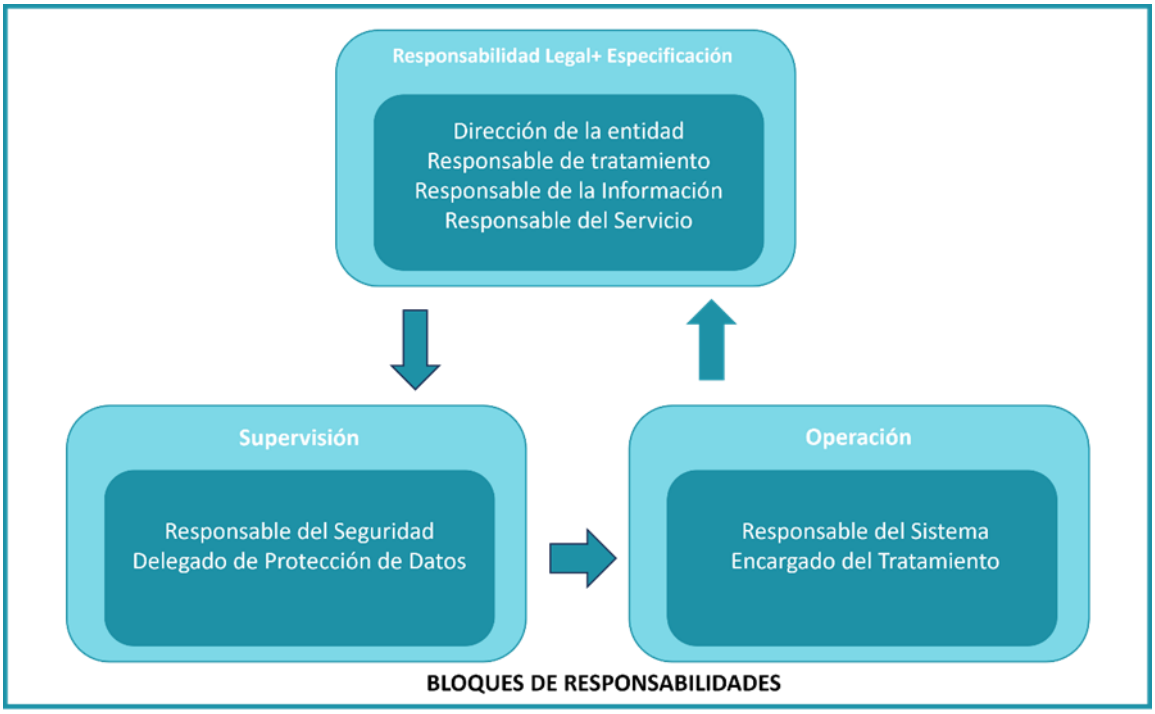
- Desarrollar, operar y mantener el sistema.
- Definir la tipología y política de Gestión del Sistema
- La conexión/desconexión de equipos/usuarios
- Aprobar los cambios operativos que afecten al sistema
- Decidir las medidas de seguridad que aplicarán los proveedores de componentes.
- Implantar controlar e integrar medidas específicas de seguridad.
- La configuración autorizada y aprobación de modificaciones sustanciales del hardware y software.
- Mantener actualizado el Análisis de Riesgos en el sistema
- Determinar la Categoría del Sistema (proceso en Anexo I ENS) y las medidas de seguridad que deben aplicarse (Anexo II ENS)

- Elaborar y aprobar la documentación del sistema y determinar las responsabilidades de los involucrados en el mantenimiento, explotación, implantación y supervisión del sistema.
- Ha de investigar Incidentes de Seguridad y comunicarlo a quien corresponda si procede
- Establecer Planes de Contingencia o Emergencia y llevar a cabo ejercicios calendarizados.
- Acordar el uso de determinada información o prestación de servicio si hay vulnerabilidades graves en el sistema, decisión acordada con el responsable de Seguridad previamente.



En **el Artículo 11 del Real Decreto 311/2022**, por el que se regula el Esquema Nacional de Seguridad, también establece que:

- "En los sistemas de información se **diferenciará el responsable de la información, el responsable del servicio, el responsable de la 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 los sistemas de información**."
- "La política de seguridad de la información detalla las **atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos**".



El Marco Operacional Real Decreto 311/2022 comenta la importancia de la "Segregación de Funciones y tareas" donde encontramos **los requisitos que han de cumplirse**.

En concreto, describe "El sistema de control de accesos se organiza de forma que se exija la concurrencia de 2 o más personas para realizar tareas críticas…". Lo que implica que:

- Las capacidades **de desarrollo y operación no recaerán en la misma persona**.
- Las **personas que autorizan y controlan el uso de la información** serán distintas.
- La misma persona **no aunará funciones de configuración y mantenimiento** del sistema.
- La misma **persona no puede aunar funciones de auditoría o supervisión con cualquier otra función**.

Una vez establecidos los roles a distintas personas del organismo, y tras diferenciar bien las funciones y responsabilidades de cada una de ellas, se dispondrá del Comité de Seguridad de la Información.

6.3. Procedimiento de Designación

El responsable de Seguridad de la Información será nombrado por <órgano que nombra> y propuesto para del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo con la Ley 11/2007 designará al responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

6.4. Política de Seguridad de la Información.

Será misión del Comité de Seguridad TIC **la revisión anual** de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta. La Política será aprobada por La Agencia Tributaria de les Illes Balears y difundida para que la conozcan todas las partes afectadas.

6.5. Resolución de Conflictos

El Comité de Seguridad de la Información, se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

7. DATOS DE CARÁCTER PERSONAL

La Agencia Tributaria de les Illes Balears (ATIB) solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido.

La Agencia Tributaria de les Illes Balears (ATIB) realiza tratamientos en los que hace uso de datos de carácter personal sometidos a lo dispuesto por 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 en lo que respecta al tratamiento de datos personales y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Política de Protección de Datos:

La Agencia Tributaria de les Illes Balears (ATIB) se compromete a garantizar la protección de los datos personales conforme a lo establecido por el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Todos los tratamientos de datos realizados por ATIB cumplirán con los principios de licitud, lealtad y transparencia en el tratamiento de datos personales, así como con el principio de minimización de datos, asegurando que únicamente se recaben los datos estrictamente necesarios para la finalidad del tratamiento. Asimismo, se adoptarán las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales, evitando su alteración, pérdida, tratamiento o acceso no autorizado. El Delegado de Protección de Datos de la Agencia Tributaria de les Illes Balears (ATIB) supervisará el cumplimiento de estas políticas y normativas en materia de protección de datos. *Véase el documento* **(SGPD_02 - POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES)**

Las políticas de seguridad aplicables a los tratamientos se rigen por las medidas de seguridad implantadas de acuerdo con el Anexo II (Medidas de seguridad) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Además, se dispone de un RAT (Registro de Actividades del Tratamiento) donde se indexan los distintos tratamientos de datos afectados por la normativa.

Todos los sistemas de información de la Agencia Tributaria de les Illes Balears (ATIB) se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal. El Delegado de protección de Datos de la Agencia Tributaria de les Illes Balears (ATIB) velará por el cumplimiento del RGPD y de la LOPDGDD.

Se puede consultar el Registro de Actividades de Tratamiento en los siguientes enlaces: Agència Tributària de les Illes Balears - A.T.I.B. 759 (atib.es)

8. GESTION DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de esta, para su aprobación por parte de la Dirección de La Agencia Tributaria de les Illes Balears (ATIB).

10. DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA, GESTIÓN Y ACCESO.

Todos los documentos que formen parte del sistema de gestión incluirán una reseña indicando quién los ha revisado y quién los ha aprobado. Preferiblemente, los documentos deberán ser revisados por el Responsable de Seguridad y aprobados por el Comité de Seguridad.

El sistema colaborativo que albergue toda la documentación de seguridad deberá permitir la gestión de versiones de los documentos, así como el seguimiento de las actividades realizadas en dicha documentación.

11. OBLIGACIONES DEL PERSONAL

Todos los miembros de La Agencia Tributaria de les Illes Balears, tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de La Agencia Tributaria de les Illes Balears atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la agencia, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12. TERCERAS PARTES

Cuando La Agencia Tributaria de les Illes Balears, preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando La Agencia Tributaria de les Illes Balears utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.