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
Adecuación guía CCN_805	2.0	30/12/2025

Tabla de contenido

1. APROBACIÓN Y ENTRADA EN VIGOR/EFECTIVIDAD

Texto aprobado el día **08 de enero de 2026** 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.

Las modificaciones de la presente Política que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Seguridad de la Información, que deberá revisarla anualmente.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por la persona u órgano con las debidas competencias, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.

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. PRINCIPIOS RECTORES DE LA POLÍTICA

- Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente
- Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.

- Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, danto una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.
- Existencia de líneas de defensa, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.
- Vigilancia continua y reevaluación periódica: la entidad implementa medios la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- Diferenciación de responsabilidades, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

4. 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.

5. MISIÓN

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.

6. MARCO NORMATIVO

La Agencia Tributaria de les Illes Balears (ATIB) desarrolla sus actividades en el ámbito de la administración electrónica y de la seguridad de la información de conformidad con el marco normativo vigente que resulte de aplicación en cada momento, incluyendo, entre otros, la normativa en materia de procedimiento administrativo, régimen jurídico del sector público, protección de datos personales, seguridad nacional, servicios electrónicos de confianza y, de forma específica, el Esquema Nacional de Seguridad (ENS).

Con el fin de garantizar la vigencia, actualización y control del cumplimiento normativo, el detalle del marco legislativo y reglamentario aplicable no se recoge de forma exhaustiva en la presente Política, sino que se mantiene actualizado en el Procedimiento y Registro de Legislación Aplicable, donde se identifican:

- Las normas legales y reglamentarias de aplicación.
- Las Instrucciones Técnicas de Seguridad (ITS) de obligado cumplimiento.
- El perfil de cumplimiento específico establecido conforme al artículo 30 del Real Decreto 311/2022.
- Las guías y recomendaciones del Centro Criptológico Nacional (CCN) que resulten aplicables para reforzar el cumplimiento del ENS.

Dicho procedimiento y registro constituyen el repositorio oficial de referencia normativa, siendo objeto de revisión periódica para incorporar modificaciones legislativas, nuevas disposiciones o actualizaciones relevantes, sin que ello implique la necesidad de modificar ni volver a aprobar la presente Política de Seguridad de la Información.

La responsabilidad del mantenimiento, revisión y actualización del marco normativo aplicable corresponde a la Agencia Tributaria de les Illes Balears (ATIB), de acuerdo con los roles y responsabilidades definidos en el Sistema de Gestión de la Seguridad de la Información y en cumplimiento de los principios establecidos por el Esquema Nacional de Seguridad.

7. ORGANIZACIÓN DE LA SEGURIDAD

7.1. 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:** Externalizado según licitación
- **Responsable de Sistemas**: Responsable del Departamento de Informática
- **Responsable de Información:** Director ATIB.
- **Responsable de Servicios:** Responsable Área de Auditoría
- **DPD:** Externalizado según licitación

7.2. 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:

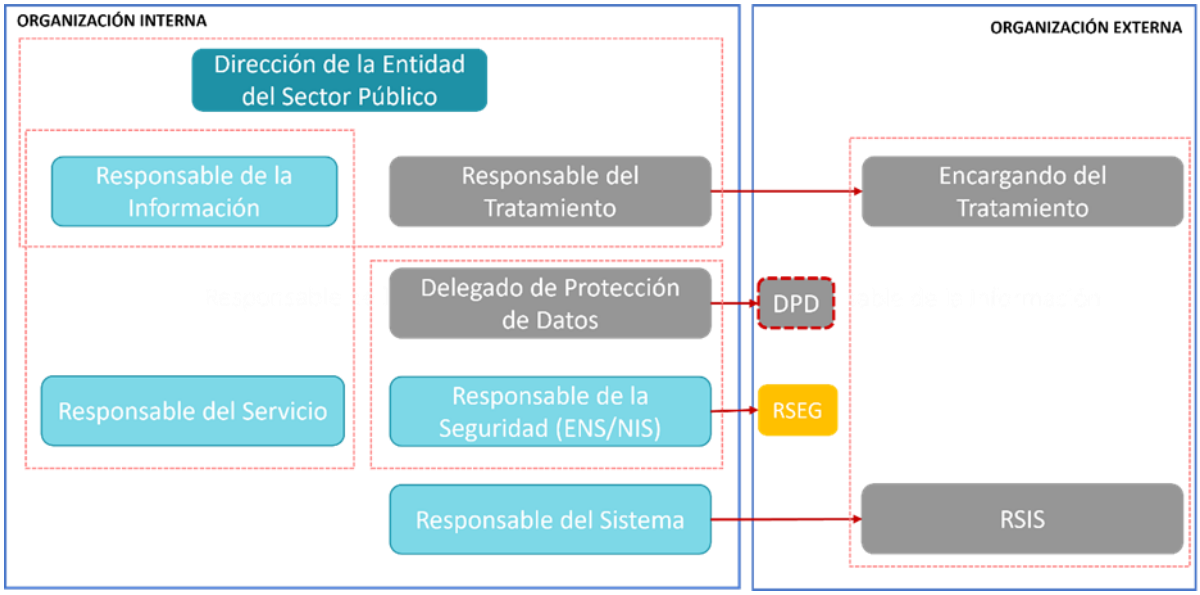
- Elaborar Planes con Medidas para gestionar los riesgos detectados.
- Supervisar y desarrollar las políticas de seguridad, normativas y procedimientos, su efectividad… Haciendo controles periódicos.
- Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad.
- Promover y formar 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:

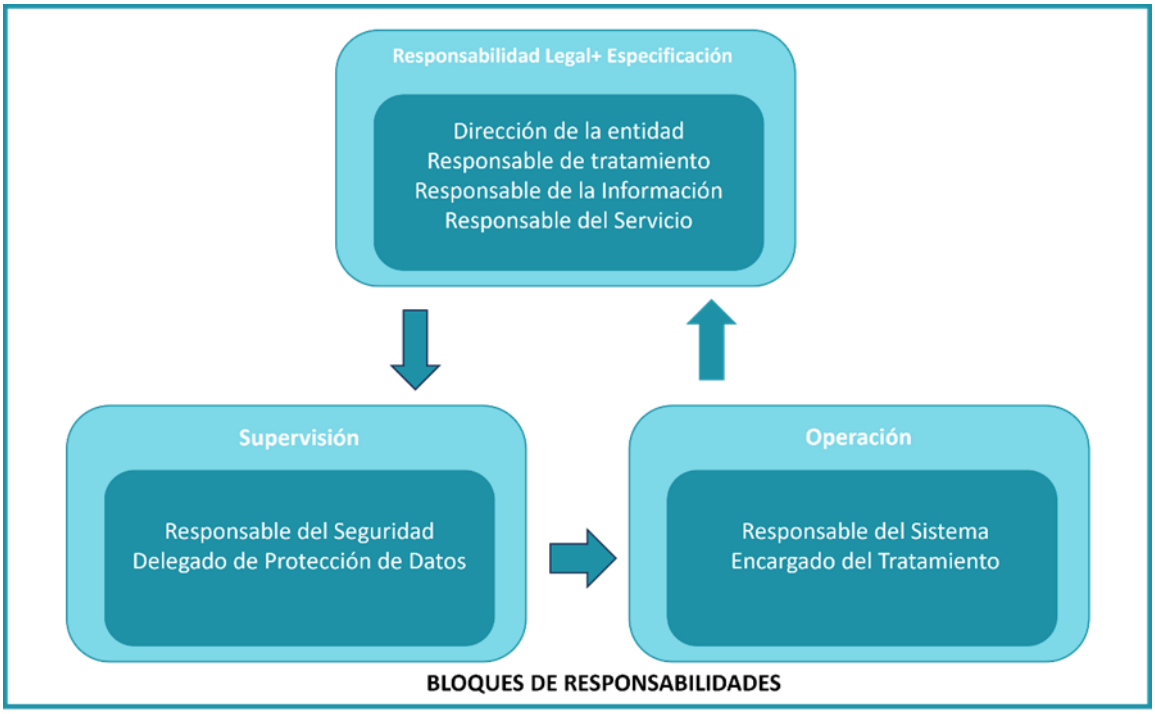
- Desarrollar, operar y mantener el sistema.
- Definir la tipología y política de Gestión del Sistema
- La conexión/desconexión de equipos/usuarios
- Aprobar los cambios operativos que afecten al sistema
- Decidir las medidas de seguridad que aplicarán los proveedores de componentes.
- Implantar controlar 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.

7.3. Procedimiento de Designación

Los miembros del Comité de Seguridad de la Información serán desinados por Dirección de ATIB.

El responsable de Seguridad de la Información será nombrado y propuesto por el Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El responsable de la Información será designado a propuesta del Comité de Seguridad.

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.

7.4. 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.

7.5. 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.

8. 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)

9. 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
- Cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

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.

Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del Delegado de Protección de Datos, además se coordinarán los planes del tratamiento del riesgo.

10. 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).

Esta Política se desarrollará por medio de normativa de seguridad que aborde aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de ATIB que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible por diversos medios a disposición de los usuarios en los repositorios internos de la agencia.

11. 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.

12. 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.

13. TERCERAS PARTES /PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES

Cuando ATIB preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando ATIB 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, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

En la adquisición de derechos de uso de activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las Guía de desarrollo.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que la <entidad> pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe 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 del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable

de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

14. GESTIÓN DE INCIDENTES DE SEGURIDAD

ATIB dispone de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.