



AJUNTAMENT *de*
RIBA-ROJA DE TÚRIA

POLÍTICA DE SEGURIDAD

USO PÚBLICO

Contenido

1.	INTRODUCCIÓN	3
2.	MISIÓN DEL AYUNTAMIENTO	3
3.	ALCANCE.....	3
4.	MARCO NORMATIVO	4
5.	CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS DE SEGURIDAD	4
6.	MODELO DE GOBERNANZA	7
6.1.	Roles o perfiles de seguridad	7
6.2.	Comité de Seguridad de la Información	8
6.3.	Responsabilidades asociadas al Esquema Nacional de Seguridad	8
6.4.	Funciones del Comité de Seguridad de la Información	9
6.5.	Procedimientos de designación	10
6.6.	Resolución de conflictos	10
7.	TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL.....	10
8.	USO SEGURO Y ÉTICO DE TECNOLOGÍAS EMERGENTES (IA)	11
9.	DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.....	11
10.	TERCERAS PARTES	11
11.	OBLIGACIONES DEL PERSONAL	12
12.	GESTIÓN DE INCIDENTES DE SEGURIDAD.....	12
13.	ANEXO I - MARCO NORMATIVO	13



Control del documento

ID Documento:	POL_Política de Seguridad_V1.0
Revisado por:	FGN
Aprobado por:	Pleno Municipal

Control de versiones

Fecha Publicación	Versión	Autor	Descripción
03/2026	V.1.0	Área de Organización, Sistemas de Información y Comunicaciones	Versión inicial del Documento

Texto aprobado el día 9 de marzo de 2026 por el Pleno del Ayuntamiento Riba-roja de Túria.

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

1. INTRODUCCIÓN

El Ayuntamiento Riba-roja de Túria, en adelante “**Ayuntamiento**” depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos, ejercer sus competencias y prestar los servicios que tiene atribuidos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la confidencialidad, integridad, autenticidad y trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y la valoración de su coste deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

2. MISIÓN DEL AYUNTAMIENTO

El Ayuntamiento, para la gestión de sus intereses y de las funciones y competencias que tiene atribuidas en diferentes normas o convenios, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población. Para ello pone a disposición de esta la realización de trámites online con el objetivo de impulsar la tramitación electrónica de los procedimientos administrativos, la mejora en la prestación de los servicios y la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la mejora de la eficacia y eficiencia de la acción pública.

Se desea potenciar por otro lado el uso de las nuevas tecnologías en el Ayuntamiento y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son: fomentar la relación electrónica de la ciudadanía con el Ayuntamiento, crear la confianza necesaria entre ciudadano y Ayuntamiento en esta relación.

3. ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento, que están relacionados con el ejercicio de derechos por medios electrónicos, 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 ámbito de aplicación del Esquema Nacional de Seguridad (ENS).

4. MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades y competencias del Ayuntamiento, 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 toda relacionada en el Anexo I de este mismo documento.

5. CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS DE SEGURIDAD

El Ayuntamiento, para lograr el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS, que recoge los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

La seguridad como un proceso integral y mínimo privilegio

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La aplicación del ENS al Ayuntamiento, estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

- El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
- Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Vigilancia continua, reevaluación periódica e integridad, actualización del sistema y mejora continua del proceso de seguridad

La vigilancia continua por parte del Ayuntamiento, permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información

Gestión de personal y profesionalidad

Todo el personal, propio o ajeno relacionado con los sistemas de información del Ayuntamiento, dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Incidentes de seguridad, prevención, detección, reacción y recuperación

El Ayuntamiento, dispone de procedimientos de gestión de incidentes de seguridad acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados

El Ayuntamiento, ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema del Ayuntamiento se conecta a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Diferenciación de responsabilidades, organización e implantación del proceso de seguridad

El Ayuntamiento, ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de “MODELO DE GOBERNANZA” del presente documento.

Autorización y control de los accesos

El Ayuntamiento, ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Protección de las instalaciones

El Ayuntamiento, ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad el Ayuntamiento Riba-roja de Túria, tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

Protección de la información almacenada y en tránsito y continuidad de la actividad

El Ayuntamiento, prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Registro de actividad y detección de código dañino

El Ayuntamiento, con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, el Ayuntamiento podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Infraestructuras y servicios comunes

El Ayuntamiento, tendrá en cuenta que la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto.

Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras

El Ayuntamiento, tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para Entidades Locales que sean de aplicación.

6. MODELO DE GOBERNANZA

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información en el Ayuntamiento Riba-roja de Túria, designará roles de seguridad y constituirá un Comité de Seguridad de la información.

6.1. Roles o perfiles de seguridad

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Responsable de Información: Alcaldía
- Responsable de los Servicios: Secretaría
- Responsable de Seguridad: Técnico Superior en Informática

- Responsable del Sistema: Técnico Medido en Informática
- DPD: Perfil externalizado

6.2. Comité de Seguridad de la Información

Se ha constituido un Comité de Seguridad de la Información, como **s**, y está formado por los siguientes miembros:

- Presidente/a: Alcalde-Presidente.
- Secretario/a: Secretaria General
- Vocales:
 - Responsable de Información.
 - Responsable de Servicios.
 - Responsable de Seguridad.
 - Responsable del Sistema.
- Delegado de Protección de datos (DPD): con funciones de asesoramiento y supervisión en materia de protección de datos

Los responsables de la Información y de los Servicios serán convocados en función de los asuntos a tratar.

Asimismo, y con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

Los miembros del Comité serán renovados cada cuatro años o con ocasión de vacante.

6.3. Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS:

Funciones del Responsable de la Información y de los Servicios

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto del Esquema Nacional de Seguridad.
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.

Funciones del Responsable de Seguridad

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.

Funciones del Responsable del Sistema

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al Responsable de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

6.4. Funciones del Comité de Seguridad de la Información

Las funciones propias de un Comité de Seguridad de la Información son las siguientes:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
 - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
 - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando 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 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.
 - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.

- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

6.5. Procedimientos de designación

La designación de los Responsables identificados en esta Política ha sido realizada por el pleno del Ayuntamiento, y comunicada a las partes afectadas.

Los cambios de adscripción del personal entre áreas departamentales se formalizarán mediante Resolución de Alcaldía. Toda resolución que afecte a funciones, responsabilidades o dependencia orgánica activará, de forma inmediata, la revisión y actualización de los perfiles de acceso, autorizaciones y segregación de funciones en los sistemas de información, conforme a esta Política y a la Normativa de Seguridad que la desarrolla.

Los roles de seguridad serán revisados cada cuatro años en el caso de que exista una vacante, la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

6.6. Resolución de conflictos

Si hubiera conflicto entre los responsables, será resuelto por el Comité de Seguridad de la Información.

7. TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

El Ayuntamiento, trata datos de carácter personal, según se describe en el Registro de Actividades del Tratamiento.

Se evaluarán los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado

El análisis de riesgos será reevaluado de forma periódica, contando con el asesoramiento y supervisión que realice el Delegado de Protección de Datos, y, en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizar, en su caso, una evaluación de impacto. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales

8. USO SEGURO Y ÉTICO DE TECNOLOGÍAS EMERGENTES (IA)

El Ayuntamiento reconoce el avance y creciente presencia de tecnologías emergentes, como la inteligencia artificial (IA), la automatización avanzada, el aprendizaje automático, o el análisis masivo de datos, que podrían ser aplicadas en el futuro a distintos procesos internos o servicios ofrecidos.

En caso de considerar su incorporación, se velará que dichas tecnologías sean evaluadas previamente desde el punto de vista de la seguridad, la protección de datos personales, la trazabilidad de las decisiones automatizadas y los principios éticos y jurídicos aplicables.

Cualquier uso o prueba de tecnologías emergentes deberá estar sujeto a análisis de riesgos, revisión de cumplimiento normativo (incluyendo el ENS, el RGPD y su normativa de desarrollo), y supervisión técnica y organizativa.

Hasta que exista una regulación o directriz específica a nivel interno, el uso de estas tecnologías no se considerará aprobado salvo expresa autorización por parte del Comité de Seguridad de la Información u órgano competente designado.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información se complementará con documentos más precisos que ayuden a implementar lo propuesto, de acuerdo con lo recomendado en la guía CCN-STIC 821 del Centro Criptológico Nacional “Normas de seguridad en el ENS”:

- Normas de seguridad (security standards): uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.
- Procedimientos de seguridad (security procedures): afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.
- Guías de seguridad (security guides): tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos

La normativa de seguridad estará disponible por diversos medios a disposición de los usuarios en la red corporativa municipal. Para su organización se han definido las directrices para la organización, gestión y acceso.

La revisión anual de la presente Política corresponde al Comité de Seguridad de la Información proponiendo en caso de que sea necesario mejoras de la misma, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

10. TERCERAS PARTES

Cuando el Ayuntamiento 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 el Ayuntamiento 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 atañe 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 el Ayuntamiento 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, sumiendo 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.

11. OBLIGACIONES DEL PERSONAL

Todos los miembros del Ayuntamiento tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad del Ayuntamiento a través del Comité de Seguridad y del área de personal de disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de entidad atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de entidad, 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. GESTIÓN DE INCIDENTES DE SEGURIDAD

El Ayuntamiento dispondrá 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 Ayuntamiento 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.

13. ANEXO I - MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades y competencias del Ayuntamiento, 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 toda relacionada en el Anexo I de este documento.

La base normativa que afecta al desarrollo de las actividades y competencias del Ayuntamiento, 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.
- 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.
- 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) N.º 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).
- Política de firma electrónica del Ayuntamiento Riba-roja de Túria.
- Reglamento por el que se establece la Sede Electrónica del Ayuntamiento Riba-roja de Túria,

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento, derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política, entre otras.

El mantenimiento del marco normativo será responsabilidad del Ayuntamiento, incluido las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el Real Decreto.

Así mismo, el Ayuntamiento, 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.