Expediente nº:	**4308/2024**
Registro de entrada nº:	**-**
Procedimiento:	**Expedientes de seguridad y autorizaciones a sistemas**
Asunto:	**Aprobación de la Política de Seguridad de la Información y creación del Comité de Seguridad**
Unidad Orgánica:	**Informática**

ESTEFANÍA CONTRERAS SALMERÓN, SECRETARIA DEL AYUNTAMIENTO DE MOTRIL.

CERTIFICO: Que el Pleno de la Corporación, en su sesión del día 14 de mayo de 2024, adoptó, entre otros, el siguiente acuerdo:

15. Informática.
Numero: 4308/2024.

APROBACIÓN DE LA POLÍTICA DE SEGURIDAD DEL AYUNTAMIENTO DE MOTRIL CONFORME AL ESQUEMA NACIONAL DE SEGURIDAD.

Se da cuenta de la propuesta que suscribe, D. Nicolás J. Navarro Díaz, concejal de Economía, Hacienda, Desarrollo del Litoral, Proyectos Estratégicos y Nuevas Tecnologías, cuyo texto dice:

“El artículo 1 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, establece que este está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Según lo establecido en su artículo 2, el Esquema Nacional de Seguridad es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.

Adicionalmente, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, han definido un escenario donde los medios electrónicos adquieren un especial protagonismo como elemento ineludible de la gestión interna, además de facilitador de las relaciones entre la ciudadanía y la propia administración, y entre diferentes administraciones.

Por un lado, la Ley 39/2015, de 1 de octubre, establece en su artículo 13 el derecho a la protección de datos de carácter personal y, en particular, a la seguridad y

confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Por otro lado, la Ley 40/2015, de 1 de octubre, establece en su artículo 3 que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

Como se establece en su exposición de motivos, la actualización del ENS, a través del RD 311/2022, de 3 de mayo, obedece al objetivo de alinearlo con el marco normativo y el contexto estratégico existente, siempre con la intención de garantizar la seguridad en la prestación de los servicios administrativos, donde la utilización de medios electrónicos, además de obligatoria, ocupa cada vez una posición más estratégica; y garantizando, en todo caso, la protección de los datos personales.

En el sentido anterior, la Estrategia Nacional de Ciberseguridad del año 2019, constituida por un total de 5 objetivos estratégicos, tiene como primer objetivo la seguridad y resiliencia de las redes, donde la existencia de nuevos vectores de ataque, amenazas y la existencia de nuevos sistemas y mecanismos de respuesta, refuerzan la necesidad de adaptarnos a esta nueva realidad.

Considerando lo expuesto, queda de manifiesto la necesidad de articular aquellas actuaciones que conduzcan a establecer los mecanismos técnicos y organizativos que garanticen la disponibilidad de los sistemas municipales y la protección de los datos e información sobre los que nuestra organización presta sus servicios a la ciudadanía e interopera con otras administraciones.

En la línea anterior, el RD 311/2022, de 3 de mayo, establece en su artículo 12 que cada Administración Pública contará con una Política de Seguridad de la Información aprobada por el órgano competente.

Del mismo modo, también en su artículo 12, el RD 311/2022, de 3 de mayo, establece que la Política de Seguridad deberá definir la estructura y composición del Comité o Comités para la gestión y coordinación de la seguridad, así como su ámbito de responsabilidad y relación con otros elementos de la organización.

Toda esta tramitación, como se desprende, tiene como fin último garantizar que las organizaciones- en nuestro caso, el Ayuntamiento de Motril-, prestan sus servicios en base a una serie de requisitos fundamentales que garantizan, en cada caso, el acceso, la confidencialidad, integridad, trazabilidad, autenticidad, disponibilidad, y conservación de los datos, la información y los servicios prestados.

La aprobación de la Política de Seguridad de la Información y la Creación del Comité constituyen las bases para articular, controlar y medir todas aquellas actuaciones relacionadas con la seguridad- ya sean de índole organizativa o técnica- que permitirán garantizar la prestación de servicios seguros y confiables, y por tanto, mejorar la calidad de la relación con la ciudadanía en base a medios electrónicos.

Por todo ello, se eleva al Pleno de la Corporación la siguiente propuesta de **ACUERDO**:

PRIMERO: Aprobar la POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE MOTRIL, en los siguientes términos:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE MOTRIL

APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información (en adelante, Política de Seguridad) entrará en vigor el día posterior a la fecha de su aprobación, y tendrá vigencia hasta que sea reemplazada por una nueva política.

OBJETO

El Ayuntamiento de Motril hace uso de las tecnologías de la información y comunicación para prestar sus servicios. El desarrollo de las infraestructuras tecnológicas posibilita el tratamiento de grandes volúmenes de datos e información, en base a sistemas integrados e interoperables que están sujetos a riesgos y amenazas de muy diversa índole: ataques lógicos, errores humanos, desastres naturales, fallos organizativos… Los datos y la información- como entidades fundamentales sobre la que operan las infraestructuras tecnológicas- se erigen como un valor estratégico de importancia capital dentro de nuestra organización, posibilitando la extracción de conocimiento y, por tanto, facilitando la toma de decisiones que contribuyan a prestar nuestras funciones de manera más eficaz y eficiente.

El RD 311/2022, de 3 de mayo, tiene por objeto regular el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. El ENS establece los requisitos mínimos que debe satisfacer el Ayuntamiento con la finalidad de proteger adecuadamente los activos e información de la organización, así como los servicios prestados por nuestra entidad, garantizando el acceso, confidencialidad, integridad, trazabilidad, autenticidad, disponibilidad y conservación de los datos, información y servicios en base a los cuales se ejercen las competencias municipales, por medios electrónicos. En concreto, el Real Decreto 311/2022, de 3 de mayo, establece en su artículo 12 y en la medida org.1 del Anexo II que “las Administraciones Públicas deberán disponer formalmente de una Política de Seguridad, que será aprobada por el titular del órgano superior competente”. La política, además, deberá integrar las siguientes cuestiones:

- Objetivos o misión de la organización.

- Marco regulatorio en el que se desarrollarán las actividades.

- Los roles o funciones de seguridad, junto con sus responsabilidades y el procedimiento para su designación y renovación.

- La estructura del comité o comités para para la organización y gestión de la seguridad.

- Las directrices para la estructuración de la documentación de la seguridad del sistema.

Con la intención de dar cumplimiento al ENS y garantizar que los servicios prestados a través de medios electrónicos alcanzan los niveles de seguridad establecidos por la normativa, el Ayuntamiento desarrolla y aprueba esta Política de Seguridad de la Información, que constituirá el marco de referencia para delimitar la definición, gestión, administración e implementación de las políticas y mecanismos establecidos por el Esquema Nacional de Seguridad.

MISION

El Ayuntamiento de Motril, en virtud de las competencias que tiene legalmente atribuidas, promueve actividades y proyectos, y presta servicios, que tienen como objetivo contribuir a satisfacer las necesidades y aspiraciones de la población del municipio; facilitar la interacción y participación de la ciudadanía en los asuntos públicos, y contribuir a simplificar la interacción de las personas con el Ayuntamiento ante cualquier necesidad de aquellos en la que este pudiera ser partícipe.

Para satisfacer lo anterior, el Ayuntamiento de Motril, en el empeño por cumplir los intereses, funciones y competencias encomendadas, pone a disposición de la ciudadanía los servicios públicos y actividades necesarias para satisfacer las aspiraciones e intereses del municipio y sus ciudadanos. Para potenciar su misión pública, el Ayuntamiento hace uso de las correspondientes tecnologías- sede electrónica y otras herramientas e infraestructuras de índole tecnológica- y promueve la utilización de estas herramientas entre la ciudadanía.

Estos sistemas pretenden garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, y reaccionando a los incidentes que puedan ocurrir. Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

Documento firmado electrónicamente (RD 203/2021). Verificable mediante **CSV: 15250142442565553772** en sede.motril.es/validacion

1. Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos personales y a la prestación de servicios a través de medios electrónicos.

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

3. Proteger los recursos de información de la entidad y la tecnología utilizada para su procesamiento frente a amenazas, internas o externas, deliberadas o accidentales.

4. Proporcionar confianza a los ciudadanos protegiendo su información durante todo su ciclo de vida.

5. Facilitar la mejora continua de los procesos de seguridad, procedimientos, productos y servicios.

6. Garantizar la continuidad de la entidad estableciendo proyectos de contingencia en los servicios críticos y manteniendo en todo momento la seguridad.

7. Concienciar, formar y motivar al personal municipal sobre la importancia de la seguridad en el entorno del trabajo.

ALCANCE

La presente Política de Seguridad tiene aplicación a todas las áreas, servicios y empleados del Ayuntamiento de Motril, cualquiera que sea su clasificación jerárquica. Igualmente, aplica a todos los sistemas de la información e infraestructuras de la información comunicación utilizadas para la realización de las funciones propias del Ayuntamiento.

Con esta Política de Seguridad de la Información, el Ayuntamiento de Motril muestra su compromiso por establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de acuerdo a los principios recogidos en el artículo 5 del Real Decreto 311/2022. Esto es:

- Entender la seguridad como un proceso integral.
- Gestionar la seguridad basándonos en los riesgos.
- Monitorizar y vigilar continuamente los eventos de seguridad para garantizar la prevención, detección, respuesta y conservación de la información.
- Establecer defensas

Documento firmado electrónicamente (RD 203/2021). Verificable mediante **CSV: 15250142442565553772** en sede.motril.es/validacion

- Evaluar el estado de la seguridad periódicamente
- Realizar una diferenciación clara de las responsabilidades

MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades y competencias del Ayuntamiento de Motril, 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 regulada, principalmente, 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.
- 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).

- Toda normativa orientada a regular la administración electrónica y los medios e infraestructuras sobre los que se prestan servicios a la ciudadanía.

También forman parte del marco normativo las restantes normas europeas, estatales y autonómicas orientadas a la Administración Electrónica y que pudieran afectar a la prestación del servicio del Ayuntamiento de Motril, a la seguridad de la información y los servicios que ésta maneja, así como a la protección de datos de carácter personal.

El mantenimiento de todo este marco normativo será responsabilidad del órgano competente del Ayuntamiento de Motril y se mantendrá de forma Anexa en los medios y/o soportes que determine el Comité de Seguridad. También se incluirán 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). De igual manera, el Responsable de la Seguridad comprobará que se han identificados las guías de seguridad del CCN que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

PRINCIPIOS BÁSICOS Y REQUISITOS MÍNIMOS DE SEGURIDAD

Con la intención de dar cumplimiento al ENS y garantizar que los servicios prestados a través de medios electrónicos alcanzan los niveles de seguridad establecidos por la normativa, el Ayuntamiento de Motril desarrolla y aprueba esta Política de Seguridad de la Información, aplicando las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad en lo referente a los siguientes ámbitos y principios.

Organización e implantación del proceso de seguridad

En su artículo 12, el ENS establece que la seguridad deberá comprometer a todos los miembros de la organización. La Política de Seguridad, según detalla el Anexo II del ENS, en su sección 3.1, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

De igual modo, la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Los requerimientos de la seguridad de la información se atenderán durante todo el ciclo de vida de los activos, desde su planificación hasta su retirada.

Análisis y gestión de los riesgos

El proceso de seguridad estará basado en una evaluación y análisis continuo de los riesgos. Se analizarán los riesgos de todas las actuaciones implicadas en el proceso de seguridad, estableciéndose las medidas de seguridad correspondientes que permitan minimizar los riesgos hasta niveles aceptables. Se contemplarán medidas de prevención, detección y corrección para evitar amenazas y que estas, si se producen, no afecten gravemente a la información y servicios prestados.

Gestión de personal y profesionalidad

Se definirá un programa de concienciación orientado a todos los empleados municipales y miembros de la corporación del Ayuntamiento de Motril, en particular a los de nueva incorporación.

Autorización y control de los accesos

En todo momento, el Ayuntamiento de Motril, controla el acceso a sus sistemas de información, limitándolos a los mínimos estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones

El Ayuntamiento de Motril controla el acceso físico a sus instalaciones, 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

La adquisición de productos garantizará en todo momento que estos dispongan de la correspondiente certificación en materia de seguridad, salvo en aquellos casos en que los riesgos potenciales que podrían asumirse no justifiquen una exigencia desproporcionada, a juicio del responsable de Seguridad.

Mínimo privilegio

En todo momento se asigna a los usuarios el mínimo nivel de permisos necesario para la realización de sus funciones laborales.

Integridad y actualización del sistema

El Ayuntamiento de Motril ha implementado sistemas de evaluación periódica de la seguridad, basados en sistemas propios e integrados con terceros (Centro Criptológico Nacional) que permiten monitorizar y recibir alertas relacionadas con vulnerabilidades potencialmente explotables de sus sistemas de información.

Estos sistemas permiten atender y reaccionar con anticipación a la materialización de un incidente mayor.

La incorporación de nuevos elementos en el sistema (bien la red de comunicaciones, bien demás equipamiento tecnológico) requerirá la correspondiente autorización por parte del Responsable del Sistema.

Protección de la información almacenada y en tránsito

El Ayuntamiento de Motril implementa medidas orientadas a garantizar la continuidad de las operaciones que se basan en información en tránsito (residente en móviles, portátiles, tablets…).

Por otro lado, el Ayuntamiento, igualmente, dispone de procedimientos e infraestructuras que garantizan la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de sus competencias.

Prevención ante otros sistemas de información interconectados

El Ayuntamiento de Motril ha implementado un sistema de protección basado en múltiples capas de defensa. Este sistema está conformado por múltiples capas de seguridad, dispuestas de forma que, cuando una de las capas falla, permite:

1) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
2) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
3) Minimizar el impacto final sobre el mismo.

Las líneas de defensa se complementarán por medidas de naturaleza organizativa, física y lógica.

Registro de la actividad y detección de código dañino

El Ayuntamiento de Motril implementa registros de la actividad de los usuarios que retienen la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto de la presente política de seguridad, 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.

Incidentes de seguridad

Se desarrollarán políticas y procedimientos encaminados a evitar incidentes relacionados con la seguridad. La seguridad del sistema deberá contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o a los servicios que se prestan.

Las medidas de prevención deberán eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se resuelvan lo antes posible. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios e infraestructuras de trabajo, garantizando la continuidad del sistema.

Mejora continua del proceso de seguridad

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para

adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

ORGANIZACIÓN DE SEGURIDAD

Para gestionar y coordinar proactivamente la seguridad de la información se constituye como órgano de gestión el **COMITÉ DE SEGURIDAD DE LA INFORMACIÓN.**

Este Comité estará constituido por los siguientes cargos:

A. RESPONSABLE DE LA INFORMACIÓN

Determinará los requisitos de la información tratada, es decir, le corresponde la potestad de determinar los niveles de seguridad de la información.

Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección, siendo el responsable último de cualquier error o negligencia que pudiera que tenga como consecuencia un incidente de confidencialidad, integridad o seguridad.

Así mismo informará sobre el estado de la seguridad en el área de los sistemas de la información y comunicación. Podrá convocar las reuniones, remitir información y comunicados a los miembros de la comisión.

B. RESPONSABLE DE SERVICIO

Determinará los requisitos de los servicios prestados.

Será la persona o personas responsables de la explotación de las distintas áreas de la entidad estableciendo requisitos, fines y medios para la realización de dichas tareas. Determinará los requisitos de seguridad de los servicios prestados. Esto incluye la responsabilidad de determinar los niveles de seguridad de los servicios y para ello, podrá recabar asesoramiento del Responsable de Seguridad y del Responsable del Sistema.

Incluirá las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control. Tendrá, además, la misión de valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios, teniendo en consideración la repercusión en la capacidad del Ayuntamiento para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

Además, tendrá la obligación de vigilar el cumplimiento de las normas de seguridad dentro de su área e informar al **Responsable de la Información** del cumplimiento de la normativa de seguridad aprobada por el Comité de Seguridad.

Documento firmado electrónicamente (RD 203/2021). Verificable mediante **CSV: 15250142442565553772** en sede.motril.es/validacion

C. RESPONSABLE DE LA SEGURIDAD

Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

Es la persona designada por el máximo órgano de gobierno para la supervisión del sistema de seguridad de la información y será el encargado de determinar las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.

Las dos funciones esenciales del Responsable de la Seguridad son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en esta Política de Seguridad de la Información de la organización.

- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Si el sistema de información, dado su complejidad, distribución, separación física o número de usuarios así lo requiriera, el Ayuntamiento podrá designar **Responsables de Seguridad Delegados**, en los que se podrá delegar funciones, pero nunca responsabilidades. Estos Responsables de Seguridad Delegados tendrán dependencia directa del Responsable de Seguridad.

Entre las funciones que se le atribuyen al Responsable de Seguridad, se encuentran las siguientes:

- Coordinará y controlará las medidas definidas en el Registro de Actividades del Tratamiento y en general se encargará del cumplimiento de las medidas de seguridad que detalla el informe de evaluación de impacto en la protección de datos.
- Reportará directamente al Comité de Seguridad de la Información.
- Podrá actuar, en caso de que así se determinara, como Secretario del Comité de Seguridad de la Información.
- Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y realizará la categorización del Sistema.
- Realizará el Análisis de Riesgos.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.

Documento firmado electrónicamente (RD 203/2021). Verificable mediante **CSV: 15250142442565553772** en sede.motril.es/validacion

- Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Coordinará la elaboración de la Documentación de Seguridad del Sistema.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política de Seguridad de la Información, para su aprobación por parte de los Órganos de Gobierno municipales.
- Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.
- Elaborará los Procedimientos Operativos de Seguridad de la Información.
- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Analizará y propondrá salvaguardas que prevengan incidentes similares en caso de que estos se hubieran producido.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.
- Elaborará los Planes de Continuidad de Sistemas que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.
- Aprobará las directrices propuestas por el Responsable de Sistema para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
- Determinará la categoría de seguridad del sistema en función de la valoración del impacto que tendría un incidente de seguridad que afectase a la información o a los servicios.

El Responsable de Seguridad deberá ser distinto del Responsable del Sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades.

En el caso de externalización del servicio de Responsable de Seguridad, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la

información tratada y el servicio prestado.

RESPONSABLE DEL SISTEMA

Se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

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 (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados. Sus funciones, de manera concreta, son las siguientes:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- 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 de seguridad se integren adecuadamente en el marco general de seguridad.
- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
- Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
- Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

Si el sistema de información, dado su complejidad, distribución, separación física o número de usuarios requiriera personal adicional para el desempeño de estas funciones, el Ayuntamiento podrá designar **Responsables del Sistema**

Delegados, en los que se podrá delegar funciones, pero nunca responsabilidades. Estos Responsables del Sistema Delegados tendrán dependencia directa del Responsable del Sistema.

ADMINISTRADOR DE SEGURIDAD

Sus funciones más significativas serían las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad (POS).
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- 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 del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

El Administrador de Seguridad puede depender del Responsable del Sistema o del Responsable de la Seguridad, pero no de ambos al mismo tiempo. Esta figura será opcional en función de las necesidades de la propia organización. En caso de ausencia, dichas funciones las asumirá el Responsable del Sistema.

SECRETARIO DEL COMITÉ

Levantará acta de las reuniones. Dicha función, en caso de no ser nombrada persona alguna para el ejercicio de esta función, la asumirá el Responsable de Seguridad.

DELEGADO DE PROTECCIÓN DE DATOS

Velará y asesorará para proteger el cumplimiento de los derechos de los interesados en materia de protección de datos.

Documento firmado electrónicamente (RD 203/2021). Verificable mediante **CSV: 15250142442565553772** en sede.motril.es/validacion

NOMBRAMIENTO DE LOS MIEMBROS DEL COMITÉ:

Los miembros de este Comité serán nombrados por Decreto de Alcaldía y posteriormente se informará al Pleno, contemplando medidas transitorias con objeto de garantizar el cumplimiento de la seguridad. Además, las futuras resoluciones de nombramientos de responsables de áreas, responsables de entidad vinculada o cambios en la distribución de funciones de área y entidades deberán contemplar expresamente el nombramiento como miembro en este comité de seguridad de la información.

Los miembros del Comité, así como los roles de seguridad serán revisados cada cuatro años o con ocasión de vacante.

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. En caso de que el Comité no tuviera capacidad o autoridad para la resolución de determinados conflictos, lo elevará al órgano jerárquico superior para su resolución.

FUNCIONES DEL COMITÉ DE SEGURIDAD

Sus funciones son las siguientes:

- Responsabilidades derivadas del tratamiento de datos personales.
- Atender las inquietudes de la Corporación y de las diferentes áreas.
- Informar regularmente del estado de la seguridad de la información al órgano superior de gobierno.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución del Ayuntamiento de Motril en lo que respecta a la 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 propio Comité de Seguridad antes de su aprobación final en pleno.
- Aprobar la normativa de seguridad de la información.
- Evaluar los riesgos de manera periódica para establecer las adecuadas medidas de seguridad necesarias atendiendo a los resultados.
- 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 por el Ayuntamiento y recomendar posibles actuaciones respecto de ellos.

Documento firmado electrónicamente (RD 203/2021). Verificable mediante **CSV: 15250142442565553772** en sede.motril.es/validacion

- 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 auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- 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.
- Establecer medidas adecuadas para la formación, información y concienciación de todo el personal en materia de seguridad de la información y protección de datos de carácter personal.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- En caso de ocurrencia de incidentes de seguridad de la información, aprobará el Plan de Mejora de la Seguridad.

El Comité de Seguridad de la Información no es un comité técnico, pero recabará regularmente del personal técnico propio o externo la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría externa.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

GESTIÓN DE LA DOCUMENTACIÓN

El Comité de Seguridad de la Información aprobará la creación de un sistema de gestión de la seguridad que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad; y que estará o podrá estar basado en el desarrollo de nuevas normativas procedimientos o políticas auxiliares

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.

La información de normativas y procedimientos, así como de otras posibles políticas se pondrá a disposición del personal que trabaja en la entidad (empleados y proveedores), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del ENS.

La información documentada será clasificada en: pública o publicable, interna, confidencial y secreta, dando el uso adecuado de acuerdo a dicha clasificación y según el criterio que se establezca en la normativa de clasificación de la información.

FUNCIONES Y OBLIGACIONES

Todo el personal municipal que tenga algún tipo de relación con el uso, la gestión, mantenimiento y explotación de la información y de los servicios prestados sobre ella, tiene la obligación de conocer la Política de Seguridad de la Información y cumplirla. El Comité de Seguridad dispondrá los medios para que esta Política llegue a los interesados.

Todo el personal anterior deberá asistir a sesiones de concienciación en materia de seguridad, las cuales se establecerán en el plan de formación y concienciación anual.

Las personas con responsabilidad en el uso, la gestión, mantenimiento o explotación de los servicios soportados por TICs, 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.

FORMACION Y CONCIENCIACIÓN

El Ayuntamiento de Motril establecerá los mecanismos necesarios, atendiendo a las propuestas del Comité de Seguridad, para que todo el personal disponga de la información, formación y concienciación apropiada para gestionar la información conforme a esta Política de Seguridad y su normativa, tanto en materia de privacidad como de seguridad. En este sentido, al menos una vez al año, se realizará la correspondiente sesión de formación y concienciación en materia de seguridad, en base al correspondiente Plan de Formación y Concienciación anual que será definido.

Documento firmado electrónicamente (RD 203/2021). Verificable mediante **CSV: 15250142442565553772** en sede.motril.es/validacion

El Comité establecerá mecanismos adecuados de difusión de la información y registrará todas las acciones formativas de las que se disponga.

GESTIÓN DEL RIESGO

El Ayuntamiento de Motril realizará periódicamente- y cada vez que los sistemas de la información sufran una alteración significativa- un análisis de riesgos, siguiendo las directrices expuestas por el ENS en su artículo 6, de modo que se puedan anticipar los riesgos existentes. Este Análisis de Riesgos y sus conclusiones han de ser analizadas por el Comité de Seguridad y establecer las salvaguardas adecuadas para que el nivel de riesgo sea aceptable.

Para que esto se materialice, el Comité desarrollará un procedimiento de análisis de riesgos y evaluación de impacto potencial que ha de establecer claramente los valores de riesgo aceptables, los criterios de aceptación de riesgo residual, la periodicidad del análisis y cuándo se realizará de modo excepcional.

El análisis de riesgos que realice el Ayuntamiento de Motril atenderá igualmente y de manera concreta a aquellos que se deriven del tratamiento de los datos personales en el desempeño de sus funciones.

Se utilizará MAGERIT como metodología base para la realización del análisis de riesgos. La periodicidad del análisis se concreta de la siguiente forma:

- Una vez al año.
- Cuando haya cambios significativos en las infraestructuras tecnológicas.
- Cuando haya cambios en los servicios esenciales prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se identifiquen amenazas severas o vulnerabilidades graves que no se contrarresten por las medidas de protección vigentes.

De acuerdo a la metodología MAGERIT, el nivel de riesgo deberá estar situado por debajo de ALTO para poder ser considerado como aceptable (el riesgo residual máximo debe ser MEDIO). Valores de riesgo por encima de MEDIO deben ser aceptados explícitamente por el Comité de Seguridad, previa justificación de la conveniencia de su aceptación.

Si el nivel de riesgo residual es ALTO, deberá establecerse el correspondiente Plan de Actuación para rebajar dicho nivel a valores aceptables.

PROTECCIÓN DE DATOS PERSONALES

El Ayuntamiento de Motril únicamente recogerá datos personales 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. De igual modo, adoptará las medidas técnicas y organizativas pertinentes para el cumplimiento de la

Documento firmado electrónicamente (RD 203/2021). Verificable mediante **CSV: 15250142442565553772** en sede.motril.es/validacion

legislación en materia de protección de datos.

Estas medidas, tal y como se indica en la disposición adicional primera de la Ley 3/2018 de 5 de diciembre, sobre Protección de Datos y Garantía de Derechos Digitales, se corresponderán con las descritas en el Esquema Nacional de Seguridad, que estarán definidas en las políticas, normativas y procedimientos que correspondan.

Los principios que aplicará el Ayuntamiento durante el tratamiento de datos personales serán aquellos recogidos por el reglamento General de Protección de Datos:

- Principio de *licitud, transparencia y lealtad*: los datos deberán ser tratados de manera lícita, leal y transparente para el interesado.

- Principio de *limitación de la finalidad*: implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.

- Principio de *minimización de datos*: el Ayuntamiento de Motril solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

- Principio de *exactitud*: los datos deben ser exactos y, si fuera preciso, actualizados, debiendo adoptarse por parte del Ayuntamiento todas las medidas razonables para que se rectifiquen o supriman los datos inexactos en relación a los fines que se persiguen.

- Principio de *limitación del plazo de conservación*: solo pueden tratarse los datos adecuados, pertinentes y necesarios para una finalidad, la conservación de esos datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados.

- Principio de *integridad y confidencialidad*: obligación de actuar proactivamente con el objetivo de proteger los datos que manejan frente a cualquier riesgo que

amenace su seguridad.

- Principio de *responsabilidad proactiva*: implica aplicar por parte del Ayuntamiento las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el RGPD.

TERCERAS PARTES

Cuando el Ayuntamiento de Motril preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. El Comité de Seguridad establecerá canales para reporte y coordinación de los respectivos Comités de Seguridad y establecerá procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Motril preste servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de las normativas de seguridad existentes que atañan a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se solicitará un informe del Responsable de Seguridad que precisará 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.

APROBACIÓN Y REVISIÓN DE ESTA POLÍTICA DE SEGURIDAD

La presente política de seguridad ha de ser un documento que refleje fielmente el compromiso del Ayuntamiento de Motril y entidades vinculadas con la seguridad de la información. Por lo tanto, esta política podrá ser modificada a propuesta del Comité de Seguridad para adaptarse a cambios en el entorno legislativo, técnico u organizativo. Tanto la aprobación inicial de esta política como la revisión futura de la misma, se realizará por el órgano superior competente de la entidad tras propuesta del comité de seguridad de la información.

Esta política se revisará- al menos- con una periodicidad anual por el Comité de seguridad, o bien, cuando se produzca una modificación notable de las

Documento firmado electrónicamente (RD 203/2021). Verificable mediante **CSV: 15250142442565553772** en sede.motril.es/validacion

infraestructuras tecnológicas, los servicios prestados o las circunstancias así lo requieran.

SEGUNDO: Publicar en la Sede Electrónica Municipal el documento de *Política de Seguridad de la Información del Ayuntamiento de Motril."*

Visto el dictamen de la Comisión Informativa de Cuentas, Economía e Interior y de Seguimiento de la Gestión Municipal, el Pleno, con los votos favorables de los veinticuatro concejales presentes en la Sala, miembros de los grupos del PP (11), PSOE (5), PMAS (4), AxSI (2) e IU-Verdes EQUO (2), ACUERDA, por unanimidad, aprobar en sus propios términos la propuesta anteriormente transcrita.

Y para que conste, extiendo la presente a resultas de la aprobación del acta correspondiente, de conformidad con lo establecido en el art. 206 del ROFRJ de las Entidades Locales, aprobado por RD 2568/1986, con el visto bueno de la Sra. Alcaldesa Presidenta, en Motril, a la fecha indicada en la firma electrónica.

Visto bueno

Firmado electrónicamente
27 de mayo de 2024 - 9:10:40
LUISA MARIA GARCIA CHAMORRO
Alcaldesa Presidenta

Firmado electrónicamente
27 de mayo de 2024 - 9:09:13
Estefanía Contreras Salmerón
Secretaria