PO.ENS-01

POLÍTICA DE SEGURIDAD

Ayuntamiento de Jimena
Enero 2022

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	PO.ENS-01	DOCUMENTO:	POLÍTICA DE SEGURIDAD

REVISIÓN NÚMERO:	1.0	FECHA DE ENTRADA EN VIGOR:	

ES ORIGINAL:	☒	ES COPIA CONTROLADA:	☐	ES COPIA NO CONTROLADA:	☐

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
TIC4YOU		
FECHA:	FECHA:	FECHA:
Diciembre 2021		
FIRMA:	FIRMA:	FIRMA:

CONTROL DE CAMBIOS:

REVISIÓN Nº:	FECHA:	APARTADO MODIFICADO:	CAUSA DEL CAMBIO:	ENTRADA EN VIGOR:

DOCUMENTACIÓN OBSOLETA:	☐	FECHA:	

CLASIFICACIÓN DE LA INFORMACIÓN:

SEGURIDAD

PÚBLICA:	☐	PUBLICABLE	☐	USO INTERNO	☒	CONFIDENCIAL:	☐	SECRETA:	☐

PRIVACIDAD

NO IP	☐	IP A	☒	IP B	☐	IP C	☐

Confidencialidad Acerca de este documento

Ayuntamiento de Jimena

Plaza de la Constitución, 1
23530 Jimena, Jaén
ESPAÑA
www.jimena.es

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 17 de enero de 2021 por Decreto de Alcaldía, nº 2022-0025.

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

2. OBJETO

Los ciudadanos confían en que los servicios disponibles por medios electrónicos se presten en unas condiciones de seguridad equivalentes a las que se encuentran cuando se acercan personalmente a las oficinas de la Administración. Además, buena parte de la información contenida en los sistemas de información de las AA.PP. y los servicios que prestan constituyen activos nacionales estratégicos. La información y los servicios prestados están sometidos a amenazas y riesgos provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.

Por lo anteriormente expuesto, el Ayuntamiento de Jimena aprueba la siguiente Política de Seguridad y debe aplicar las medidas mínimas de seguridad exigidas por el ENS, 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.

Las diferentes áreas y servicios deben cerciorarse de que la seguridad de la información es una parte vital de los servicios públicos prestados por el Ayuntamiento de Jimena, y ha de custodiar dicha información en todo su ciclo de vida (recogida, transporte, tratamiento, almacenamiento y destrucción). Las áreas y servicios deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, garantizando así la continuidad en la prestación de los servicios con una calidad y seguridad adecuada.

3. ALCANCE

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

4. OBJETIVOS

El Ayuntamiento tiene como objetivo principal asegurar la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios, junto con la tecnología y los activos de información de la entidad, según el documento de aplicabilidad.

Los objetivos genéricos que el ayuntamiento ha establecido para cumplir a lo largo del tiempo son:

- Proporcionar confianza a los ciudadanos protegiendo su información durante todo su ciclo de vida.
- Facilitar la mejora continua de los procesos de seguridad, procedimientos, productos y servicios.
- Cumplir los requisitos legales que le son de aplicación (explícitos e implícitos) relacionados con seguridad de la información.
- Garantizar la continuidad de la entidad estableciendo proyectos de contingencia en los servicios críticos y manteniendo en todo momento la seguridad.
- Garantizar que se provean los recursos necesarios para garantizar la seguridad, así como asignar funciones y responsabilidades al personal encargado de mantener el sistema.
- Concienciar, formar y motivar al personal sobre la importancia de la seguridad en el entorno del trabajo.

5. MARCO NORMATIVO

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, establecía principios y derechos relativos a la seguridad en relación con el derecho de los ciudadanos a comunicarse con las AA.PP. a través de medios electrónicos; y su artículo 42 crea el Esquema Nacional de Seguridad.

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos. El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado por las AA.PP. para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestione en el ejercicio de sus competencias.

El Esquema Nacional de Interoperabilidad (ENI), regulado por el Real Decreto 4/2010, de 8 enero, establece el conjunto de criterios y recomendaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad. Las normas técnicas complementarias de interoperabilidad desarrollan ciertos aspectos técnicos.

Las Leyes 39/2015 y 40/2015 regulan el Procedimiento Administrativo Común y el Régimen Jurídico de las Administraciones. Dentro de estas leyes se hace referencia expresa al ENS como sistema de gestión segura de la información para las administraciones y al ENI como referencia en la interoperabilidad de las administraciones.

Así mismo, la Ley Orgánica 3/2018, de 5 de Diciembre, de Protección de Datos y garantía de los derechos digitales, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, además de garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

El Reglamento (UE) 2016/679, de 27 de abril de 2016, de Tratamiento de Datos de Carácter Personal y Libre Circulación de Datos establece la obligación de disponer medidas técnicas y organizativas para garantizar la confidencialidad, disponibilidad e integridad de la información. Así mismo dispone que dichas medidas han de ser proactivas y el responsable del tratamiento ha de ser capaz de demostrar que se siguen esas medidas y demostrar su aplicación.

La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión en la que se establecen las obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información; establecer requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales.

El Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información que asegura la alineación del derecho español con el marco armonizado europeo conforme a la Directiva 2016/1148 (Directiva NIS).

Con este Real Decreto se pretende concretar algunas de las principales obligaciones y procedimientos a utilizar a fin de asegurar una óptima gestión de riesgos de seguridad en redes y sistemas de información en sectores críticos así como para asegurar una adecuada coordinación entre los distintos actores implicados en este tipo de situaciones de riesgo. Para ello, se han establecido una serie de obligaciones organizativas y de actuación para los operadores sujetos a este régimen, como son la definición de medidas técnicas y organizativas para la adecuada gestión de los riesgos de ciberseguridad, designación de un responsable de seguridad, notificación y gestión de incidentes de seguridad.

6. ORGANIZACIÓN DE SEGURIDAD

Para gestionar y coordinar proactivamente la seguridad de la información se crea la figura del Responsable de Seguridad de Sistemas de Información Municipal, cuyas funciones serán responsabilizarse del cumplimiento de lo exigido en este documento, para garantizar la seguridad de los sistemas de información y de la disponibilidad y continuidad de los servicios prestados, mediante el cumplimiento de las medidas de seguridad, así como promover la concienciación y formación en materia de seguridad de los sistemas de información dentro de su ámbito de responsabilidad.

Secretaría: tendrá la obligación de supervisar que los procedimientos aprobados por el Responsable de Seguridad de Sistemas de Información Municipal se ajusten a derecho y asesorar en esta materia. Además, levantará acta de las reuniones.

Delegado de protección de datos: velará y asesorará para proteger el cumplimiento de los derechos de los interesados en materia de protección de datos.

Serán nombrados por Decreto de Alcaldía una vez aprobado en Pleno este documento, contemplando medidas transitorias con objeto de garantizar el cumplimiento de la seguridad.

6.1 FUNCIONES DEL RESPONSABLE DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN MUNICIPAL

Sus funciones son:

- Responsabilidades derivadas del tratamiento de datos de carácter personal.
- Atender las inquietudes de la Corporación y de las diferentes áreas.
- Informar regularmente del estado de la seguridad de la información si lo estiman conveniente a la Comisión encargada o en su defecto, al Pleno.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución del Ayuntamiento de Jimena 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.
- 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.
- 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 del ayuntamiento. 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.
- En caso de ocurrencia de incidentes de seguridad de la información aprobará el Plan de Mejora de la Seguridad.

El Responsable de Seguridad de Sistemas de Información Municipal recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. Se podrá asesorar 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.

6.2 GESTIÓN DE LA DOCUMENTACIÓN

Se deberá comunicar la información documentada relativa a los controles de seguridad al 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.

7. CONCIENCIACIÓN

El Ayuntamiento de Jimena establecerá los mecanismos necesarios, atendiendo a las propuestas del Responsable de Seguridad de los Sistemas de Información Municipal, para que todo el personal disponga de la información, formación y concienciación apropiada para gestionar de acuerdo a esta Política de Seguridad y su normativa interna derivada, la información tanto en materia de privacidad como de seguridad.

El Responsable establecerá mecanismos adecuados de difusión de la información y registrará todas las acciones formativas que se dispongan en este sentido.

8. GESTIÓN DEL RIESGO

El Ayuntamiento de Jimena 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 riesgo y sus conclusiones han de ser analizadas por el Responsable de Seguridad de los Sistemas de Información Municipal y establecer las salvaguardas adecuadas para que el nivel de riesgo sea aceptable.

Para que esto se plasme el Responsable 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.

9. PROTECCIÓN DE DATOS PERSONALES

Se aplicarán a los datos personales que sean objeto de tratamiento por parte del Ayuntamiento y sus entidades vinculadas o dependientes, las medidas de seguridad determinadas en las diferentes normativas y/o procedimientos que corresponden y las que se definen en el Esquema Nacional de Seguridad, de

conformidad con lo descrito en la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos y garantía de derechos digitales.

10. REVISIÓN DE ESTA POLÍTICA DE SEGURIDAD

La presente política de seguridad ha de ser un documento que refleje fielmente el compromiso del Ayuntamiento de Jimena y entidades vinculadas con la seguridad de la información. Por lo tanto, esta política podrá ser modificada a propuesta del Responsable de Seguridad de Sistemas de Información Municipal para adaptarse a cambios en el entorno legislativo, técnico u organizativo.