



**Excmo. Ayuntamiento  
de Cazorla**

PO.ENS-01

## **POLÍTICA DE SEGURIDAD**

Ayuntamiento de  
Cazorla  
Junio 2023


TIC  YOU  
[www.tic4you.com](http://www.tic4you.com)

## CONTROL DE DOCUMENTACIÓN:

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

REVISIÓN NÚMERO:	1.0	FECHA DE ENTRADA EN VIGOR:	
------------------	-----	----------------------------	--

ES ORIGINAL:	<input checked="" type="checkbox"/>	ES COPIA CONTROLADA:	<input type="checkbox"/>	ES COPIA NO CONTROLADA:	<input type="checkbox"/>
--------------	-------------------------------------	----------------------	--------------------------	-------------------------	--------------------------

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
TIC4YOU	Comité de Seguridad	Pleno Municipal
FECHA:	FECHA:	FECHA:
Enero 2023		
FIRMA:	FIRMA:	FIRMA:
		

## CONTROL DE CAMBIOS:

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

DOCUMENTACIÓN OBSOLETA:	<input type="checkbox"/>	FECHA:	
-------------------------	--------------------------	--------	--

## CLASIFICACIÓN DE LA INFORMACIÓN:

### SEGURIDAD

PÚBLICA:	<input type="checkbox"/>	PUBLICABLE	<input type="checkbox"/>	USO INTERNO	<input checked="" type="checkbox"/>	CONFIDENCIAL:	<input type="checkbox"/>	SECRETA:	<input type="checkbox"/>
----------	--------------------------	------------	--------------------------	-------------	-------------------------------------	---------------	--------------------------	----------	--------------------------

### PRIVACIDAD

NO IP	<input type="checkbox"/>	IP A	<input checked="" type="checkbox"/>	IP B	<input type="checkbox"/>	IP C	<input type="checkbox"/>
-------	--------------------------	------	-------------------------------------	------	--------------------------	------	--------------------------


## Confidencialidad Acerca de este documento

---


AVISO: Este documento está protegido por la legislación referente a propiedad intelectual e industrial y por tratados internacionales. La utilización permitida de esta documentación queda limitada exclusivamente en relación con el Ayuntamiento de Cazorla, y todo uso no autorizado será perseguido de acuerdo con la legislación aplicable. Se prohíbe su copia, modificación, reproducción o distribución sin permiso del titular.

### Ayuntamiento de Cazorla

Plaza Francisco Martínez, 1  
23470 Cazorla, Jaén  
ESPAÑA  
[www.cazorla.es](http://www.cazorla.es)

	<b>PO.ENS-01 POLÍTICA</b>	
	<b>POLÍTICA DE SEGURIDAD</b>	Junio 2023
		Edición: 1.0

<b>1. APROBACIÓN Y ENTRADA EN VIGOR</b>	<b>5</b>
<b>2. OBJETO</b>	<b>5</b>
<b>3. ALCANCE</b>	<b>5</b>
<b>4. MISIÓN Y OBJETIVOS</b>	<b>6</b>
<b>5. MARCO NORMATIVO</b>	<b>6</b>
<b>6. ORGANIZACIÓN DE SEGURIDAD</b>	<b>8</b>
6.1 FUNCIONES DEL COMITÉ DE SEGURIDAD	11
6.2 GESTIÓN DE LA DOCUMENTACIÓN	12
<b>7. CONCIENCIACIÓN</b>	<b>13</b>
<b>8. GESTIÓN DEL RIESGO</b>	<b>13</b>
<b>9. PROTECCIÓN DE DATOS PERSONALES</b>	<b>13</b>
<b>10. APROBACIÓN Y REVISIÓN DE ESTA POLÍTICA DE SEGURIDAD</b>	<b>13</b>

	<b>PO.ENS-01 POLÍTICA</b>	
	<b>POLÍTICA DE SEGURIDAD</b>	Junio 2023
		Edición: 1.0

## 1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día <<día>> de <<mes>> de <<año>> por <<órgano que la aprueba>>.

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


El Ayuntamiento de Cazorla (en adelante Ayuntamiento) considera la información un activo esencial para el cumplimiento adecuado de sus funciones. 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.

En su empeño por garantizar que los servicios disponibles a través de medios electrónicos a los ciudadanos se presten en unas condiciones de seguridad equivalentes a las que se encuentran cuando se acercan personalmente a las oficinas de la Administración, el Ayuntamiento desarrolla y aprueba esta Política de Seguridad de la Información, aplicando las medidas mínimas de seguridad exigidas por el ENS en lo referente a:

- A. Organización e implantación del proceso de seguridad.
- B. Análisis y gestión de los riesgos.
- C. Gestión de personal.
- D. Profesionalidad.
- E. Autorización y control de los accesos.
- F. Protección de las instalaciones.
- G. Adquisición de productos de seguridad y contratación de servicios de seguridad.
- H. Mínimo privilegio.
- I. Integridad y actualización del sistema.
- J. Protección de la información almacenada y en tránsito.
- K. Prevención ante otros sistemas de información interconectados.
- L. Registro de la actividad y detección de código dañino.
- M. Incidentes de seguridad.
- N. Continuidad de la actividad.
- O. Mejora continua del proceso de seguridad.

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, 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.

Esta Política de Seguridad asegura un compromiso manifiesto de las máximas autoridades de la entidad para la difusión, consolidación y cumplimiento de la presente Política.

	<b>PO.ENS-01 POLÍTICA</b>	
	<b>POLÍTICA DE SEGURIDAD</b>	Junio 2023
		Edición: 1.0

### 3. ALCANCE

La presente Política de Seguridad tiene aplicación a todas las áreas, servicios, empleados internos y externos del Ayuntamiento de Cazorla, 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.

Con esta política de seguridad de la información, la organización 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. .
- Establecer defensas
- Evaluar el estado de la seguridad periódicamente
- Realizar una diferenciación clara de las responsabilidades

### 4. MISIÓN Y OBJETIVOS

El Ayuntamiento de Cazorla, 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 tecnologías apropiadas y pone en valor la relación electrónica con los ciudadanos, creando la confianza necesaria basada en un sistema de seguridad de la información integral y que alcanza a toda la institución.

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

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.

	<b>PO.ENS-01 POLÍTICA</b>	
	<b>POLÍTICA DE SEGURIDAD</b>	Junio 2023
		Edición: 1.0

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

## 5. MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades y competencias del Ayuntamiento de Cazorla, 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.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad, con vigencia hasta mayo de 2024.
- 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). 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).

También forman parte del marco normativo las restantes normas estatales y autonómicas orientadas a la Administración Electrónica y que pudieran afectar a la prestación del servicio del Ayuntamiento de Cazorla, 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 Cazorla 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). Así mismo, el Responsable de la Seguridad asegurará 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.

## 6. 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

	<b>PO.ENS-01 POLÍTICA</b>	
	<b>POLÍTICA DE SEGURIDAD</b>	Junio 2023
		Edición: 1.0

Determinará los requisitos de la información tratada.

Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. Asesorará y tendrá potestad para determinar técnicamente los requisitos de la información y de los servicios en materia de seguridad. Tendrá la potestad, igualmente, de determinar los niveles de seguridad de la información.

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, tendrán 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.

#### 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:

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




	<b>PO.ENS-01 POLÍTICA</b>	
	<b>POLÍTICA DE SEGURIDAD</b>	Junio 2023
		Edición: 1.0

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 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.
- 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 los Responsables de Sistemas 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 la 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

	<b>PO.ENS-01 POLÍTICA</b>	
	<b>POLÍTICA DE SEGURIDAD</b>	Junio 2023
		Edición: 1.0

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.

#### d. 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:


- a. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- b. Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- c. Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- d. 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.
- e. Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
- f. Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- g. Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
- h. 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.

#### e. ADMINISTRADOR DE SEGURIDAD

Sus funciones más significativas serían las siguientes:

- a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

	<b>PO.ENS-01 POLÍTICA</b>	
	<b>POLÍTICA DE SEGURIDAD</b>	Junio 2023
		Edición: 1.0

- b. 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.
- c. 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.
- d. La aplicación de los Procedimientos Operativos de Seguridad (POS).
- e. Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- f. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- g. 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.
- h. 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.
- i. Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- j. 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.

#### f. SECRETARÍA

Tendrá la obligación de supervisar que los procedimientos aprobados por el Comité se ajusten a derecho, así como de asesorar al Comité en esta materia. Además, levantará acta de las reuniones. Dicha función, en caso de no ser nombrada persona alguna para el ejercicio de esta tarea, la asumirá el Responsable de Seguridad.

#### g. DELEGADO DE PROTECCIÓN DE DATOS

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


#### NOMBRAMIENTO

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.

### **6.1 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 Cazorla en lo que respecta a la seguridad de la información.

	<b>PO.ENS-01 POLÍTICA</b>	
	<b>POLÍTICA DE SEGURIDAD</b>	Junio 2023
		Edición: 1.0


- 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.
- 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.
- 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.

## 7. GESTIÓN DE LA DOCUMENTACIÓN

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

	<b>PO.ENS-01 POLÍTICA</b>	
	<b>POLÍTICA DE SEGURIDAD</b>	Junio 2023
		Edición: 1.0

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.

## 8. CONCIENCIACIÓN

El Ayuntamiento de Cazorla 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 de acuerdo a esta Política de Seguridad y su normativa interna derivada la información, tanto en materia de privacidad como de seguridad.

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

## 9. GESTIÓN DEL RIESGO

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

## 10. PROTECCIÓN DE DATOS PERSONALES

El Ayuntamiento de Cazorla 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 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 estará definidas en las políticas, normativas y procedimientos que correspondan.

	<b>PO.ENS-01 POLÍTICA</b>	
	<b>POLÍTICA DE SEGURIDAD</b>	Junio 2023
		Edición: 1.0

## 11. TERCERAS PARTES

Cuando el Ayuntamiento de Cazorla preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento de Cazorla utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que atañe 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 requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

## 10. 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 Cazorla 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 cuando las circunstancias así lo requieran.