AJUNTAMENT DE VALÈNCIA | capi casal

València Sostenible

PO-01
Política de seguridad de la información

Contenido

1 APROBACIÓN Y ENTRADA EN VIGOR 3
2 INTRODUCCIÓN 3
3 ALCANCE 3
4 MISIÓN 3
5 PRINCIPIOS RECTORES DE LA POLÍTICA 5
6 MARCO LEGISLATIVO 5
7 ORGANIZACIÓN DE LA SEGURIDAD 5
7.1 COMITÉS: FUNCIONES Y RESPONSABILIDADES 5
7.2 ROLES: FUNCIONES Y RESPONSABILIDADES 7
7.2.1 Funciones del Responsable de la Información y de los Servicios 7
7.2.2 Funciones del Responsable de Seguridad 7
7.2.3 Funciones del Responsable del Sistema 7
7.3 PROCEDIMIENTOS DE DESIGNACIÓN 8
7.4 RESOLUCIÓN DE CONFLICTOS 8
8 TRATAMIENTO DE DATOS PERSONALES EN LA ENTIDAD 8
9 GESTIÓN DE RIESGOS 9
10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 9
11 OBLIGACIONES DEL PERSONAL 9
12 TERCERAS PARTES /PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES 10
13 GESTIÓN DE INCIDENTES DE SEGURIDAD 11
14 APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR/EFECTIVIDAD 11

1 APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 6 de octubre de 2026 por el Comité de Seguridad de la Información del Organismo Autónomo Municipal "València Sostenible".

Esta Política se Seguridad de la Información está vigente desde la fecha de aprobación (o publicación para las entidades que sea obligatoria su publicación oficial) y hasta que sea reemplazada por una nueva Política.

2 INTRODUCCIÓN

El Organismo Autónomo Municipal "València Sostenible" depende de los sistemas de información para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o la disponibilidad de los servicios prestados.

El objetivo último de la seguridad de la información es garantizar que la entidad pueda cumplir con sus objetivos, desarrollar sus funciones o competencias y prestar los servicios para la cual se ha sido constituida 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.

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

El Organismo Autónomo Municipal "València Sostenible" debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

3 ALCANCE

Esta política se aplica a todos los sistemas de información del Organismo Autónomo Municipal "València Sostenible" a las personas que conforman la organización y a los prestadores de servicios o proveedores de soluciones TIC del Organismo Autónomo Municipal "València Sostenible".

4 MISIÓN

El Organismo Autónomo Municipal "València Sostenible" se constituye como una entidad de derecho público de carácter municipal, encaminada a impulsar la eficiencia energética, adaptación urbana, el aprovechamiento de nuestros recursos y la conservación de nuestro patrimonio natural.

Sus principales ámbitos de actuación incluyen:

- Eficiencia energética.
- Educación y cultura energética.
- Adaptación urbana.
- Alimentación saludable.
- Protección, promoción y gestión de espacios naturales, alimentarios y de biodiversidad urbana.

Todo ello respetando las competencias y ámbitos de gestión de los servicios y delegaciones municipales existentes.

Los objetivos en materia de seguridad que el Organismo Autónomo Municipal "València Sostenible" pretende garantizar con la presente Política serán:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes del Organismo Autónomo Municipal "València Sostenible" respecto a la seguridad de la información. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmita a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

5 PRINCIPIOS RECTORES DE LA POLÍTICA

Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente

Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.

Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, danto una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.

Existencia de líneas de defensa, la estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.

Vigilancia continua y reevaluación periódica: la entidad implementa medios la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.

Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.

Diferenciación de responsabilidades, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

6 MARCO LEGISLATIVO

El marco legislativo que afectan a esta Política se ha establecido y se mantiene actualizado en el registro VS-REG-01-Registro de Normas Jurídicas del Marco Legal y Regulatorio.

Con periodicidad mínima anual, y con la ayuda externa de la consultora externa correspondiente, el departamento jurídico de la entidad revisará el registro.

7 ORGANIZACIÓN DE LA SEGURIDAD

7.1 COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad de la Información estará formado por:

Función en el comité	Cargo en la entidad
Presidente/a	Director/a del OAM València Sostenible
Secretario/a	Responsable de Seguridad
Vocal	Responsable del Sistema
Vocal	Coordinador/a área de comunicación
Vocal	Administración

El Secretario/a del Comité de Seguridad de la Información tendrá como funciones convocar y documentar las reuniones del Comité, redactando y custodiando las actas y acuerdos adoptados.

El Comité de Seguridad de la Información tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
    - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
    - Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
    - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
    - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.

- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

7.2 ROLES: FUNCIONES Y RESPONSABILIDADES

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

7.2.1 Funciones del Responsable de la Información y de los Servicios

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

7.2.2 Funciones del Responsable de Seguridad

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

7.2.3 Funciones del Responsable del Sistema

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al Responsable de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.

- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
  - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
  - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
  - Aprobar los cambios en la configuración vigente del Sistema de Información.
  - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
  - Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
  - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
  - Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

7.3 PROCEDIMIENTOS DE DESIGNACIÓN

Los miembros del Comité de Seguridad de la Información así como los roles establecidos en la presente política serán designados por correo electrónico.

Los nombramientos podrán ser revisados cada dos años, pudiendo realizarse antes cuando el puesto quede vacante o por un incumplimiento reiterado de sus funciones, previo apercibimiento. El Organismo Autónomo Municipal “València Sostenible” debe disponer de un mecanismo que permita la sustitución de los responsables designados en caso de ausencias de larga duración o aquellas de menor duración pero que puedan provocar ineficiencias en las funciones de cada uno de ellos que afecten al sistema.

7.4 RESOLUCIÓN DE CONFLICTOS

En el caso de conflictos entre los diferentes responsables, el Comité de Seguridad de la Información podrá dirimir las discrepancias.

8 TRATAMIENTO DE DATOS PERSONALES EN LA ENTIDAD

El Organismo Autónomo Municipal “València Sostenible” trata datos de carácter personal, según se describe en el Registro de Actividades del Tratamiento. El Organismo Autónomo Municipal “València Sostenible” deberá evaluar los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado

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

protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales.

9 GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año.
- cuando se produzcan cambios en la información manejada.
- cuando se produzcan cambios en los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.
- cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

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

10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se desarrollará por medio de una normativa de seguridad de la información que aborde aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros del Organismo Autónomo Municipal “València Sostenible” que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible por diversos medios a disposición de los usuarios en el Drive.

Se elaborarán además procedimientos, guías, manuales y registros para desarrollar con mayor precisión las distintas actividades vinculadas a la gestión de usuarios, el control de accesos, la administración de sistemas y aplicaciones, la protección de la información, la gestión de incidentes de seguridad, la realización de copias de seguridad y el cumplimiento de las medidas previstas en el Esquema Nacional de Seguridad.

11 OBLIGACIONES DEL PERSONAL

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

Todos los miembros del Organismo Autónomo Municipal “València Sostenible” atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se

establecerá un programa de concienciación continua para atender a todos los miembros del Organismo Autónomo Municipal "València Sostenible", en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12 TERCERAS PARTES /PRESTADORES DE SERVICIOS / PROVEEDORES DE SOLUCIONES

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

Cuando el Organismo Autónomo Municipal "València Sostenible" utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

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

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

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado/a de Protección de Datos emitir su parecer.

13 GESTIÓN DE INCIDENTES DE SEGURIDAD

El Organismo Autónomo Municipal "València Sostenible" dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

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

14 APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR/EFECTIVIDAD

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

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

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

Control del documento

Versión	Fecha	Responsable	Control de cambios
1.0	06/10/2026	Sonia Gómez Escobés	Redacción inicial

Autor:	Revisado por:	Aprobado por:
Responsable de Seguridad	Comité de Seguridad de la Información	Presidencia

Clasificación:
Público