JOSEFA MARTINEZ CABALLERO (1 de 1)
TÉCNICO ADMINISTRACIÓN GENERAL
Fecha Firma: 20/12/2024
HASH: c9abf84135c943675bdb9eb6e64db8748

Ayuntamiento de Sant Joan d'Alacant

Seguridad de la Información

PLS-GLB-001

Política General de Seguridad de la Información

AJUNTAMENT DE SANT JOAN D'ALACANT

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 1 de 31

CONTROL DE EDICIÓN

FECHA	VERSIÓN	APROBACIÓN	CAMBIOS
Fecha de la firma electrónica	01	Órgano Competente	Versión inicial
Las aprobaciones formales de los documentos figuran en sus actas correspondientes.			

CLASIFICACIÓN

PÚBLICO

LISTA DE DISTRIBUCIÓN

PERSONA	CARGO
Difusión pública	----------

El presente documento está dirigido EXCLUSIVAMENTE a las personas nombradas en la lista de distribución, quienes podrán, en base a su criterio, divulgarlo a quienes consideren oportuno. Se recomienda encarecidamente una divulgación controlada en la que todos los cesionarios del documento conozcan inequívocamente su CLASIFICACIÓN y se comprometan a mantener la consecuente confidencialidad en todo su ciclo de uso y, en su caso, archivo y/o destrucción.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 2 de 31

ÍNDICE

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 3 de 31

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 4 de 31

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 5 de 31

1. Contenido y objetivos del presente documento.

Este documento contiene la Política General de Seguridad de la Información (PGSI en adelante) del Ayuntamiento de Sant Joan d'Alacant ("el Ayuntamiento" en adelante).

El objetivo fundamental de esta Política se centra en definir las estructuras organizativas, roles, responsabilidades, criterios e iniciativas de este Ayuntamiento respecto a la Seguridad de la Información que almacena y gestiona, así como el cumplimiento de los diferentes marcos normativos que la regulan.

2. Datos del Ayuntamiento de Sant Joan d'Alacant

Organismo	Ayuntamiento de Sant Joan d'Alacant
NIF	P0311900E
Domicilio	Plaza España 1
Población	Sant Joan d'Alacant
Código Postal	03550
Provincia	Alicante

3. Justificación de una Política General de Seguridad de la Información.

Los marcos normativos vigentes en materia de Seguridad de la Información requieren la disponibilidad de una Política de Seguridad corporativa que, aprobada por el denominado "Órgano Competente" y adecuadamente difundida entre el personal y todas las entidades afectadas, implemente los requerimientos de dichos Marcos con el fin de preservar los derechos y libertades de los interlocutores sociales con quienes interactúa el Ayuntamiento, englobados todos ellos en adelante bajo la denominación genérica "interlocutores", "interlocutores sociales", "terceros" o "partes interesadas".

La diversidad de marcos normativos, sus diferentes ámbitos objetivos y subjetivos, así como la evolución permanente de los mismos, aconsejan desarrollar una PGSI unificada y permitir con ello eliminar redundancias en actividades, documentos y controles, optimizando con ello las actuaciones corporativas y el nivel de cumplimiento normativo.

4. Ámbito objetivo de la PGSI.

La PGSI abarca todos los medios, automatizados o no, que el Ayuntamiento utiliza para el desarrollo de sus competencias y actividades, así como todos los medios por los cuales interopera con otras entidades, públicas y/o privadas. Las actividades incluyen:

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 6 de 31

(1). Las relaciones de carácter jurídico-económico-administrativo entre los interlocutores sociales y el Ayuntamiento.

(2). La realización de las funciones, obligaciones y competencias del Ayuntamiento, tanto las desarrollados por medios electrónicos como los manuales.

(3). El tratamiento de la información gestionada por el Ayuntamiento en el ejercicio de sus competencias, especialmente aquélla relacionada con datos personales.

(4). Las relaciones del Ayuntamiento con otras Administraciones Públicas.

5. Ámbito subjetivo de la PGSI.

La PGSI será aplicada por todos los servicios, departamentos, secciones, áreas, unidades administrativas y personal del Ayuntamiento y, en general, por todas las entidades internas y externas de cualquier tipo vinculadas a al Ayuntamiento mediante cualquier modelo de relación. Con el fin de unificar la terminología, las estructuras organizativas internas serán denominadas “departamentos” en adelante.

La PGSI afecta a todo el personal del Ayuntamiento, sea cual sea su relación laboral con el mismo. Asimismo, la PGSI afecta a todo el personal que presta servicios en el Ayuntamiento a través de empresas externas y que, en razón de esta relación, acceda, almacene y/o trate información cuya competencia y/o responsabilidad recaiga sobre el Ayuntamiento.

La PGSI será aplicada en las relaciones del Ayuntamiento con los interlocutores sociales, empresas y entidades públicas y/o privadas con las que interactúe, por lo que las personas que intervengan en estas relaciones están incluidas en los sujetos a quienes resulta de aplicación esta política.

6. Misión y servicios prestados.

El Ayuntamiento de Sant Joan d’Alacant tiene como misión el cumplimiento de las obligaciones y competencias legales atribuidas a un Ayuntamiento por la legislación vigente, cumpliendo los marcos normativos que les afectan, aportando a los Ciudadanos y resto de interlocutores sociales una administración eficiente, proactiva y actuando en todo momento en defensa de sus derechos y libertades.

7. Marcos normativos referenciales de la PGSI.

Los marcos normativos referenciales aplicables al Ayuntamiento de Sant Joan d’Alacant se encuentran en el registro corporativo de marcos normativos:

SANT JOAN-RGS-GLB-610-Normativa Aplicable

Documento público accesible.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 7 de 31

8. Alineamiento con el Esquema Nacional de Seguridad.

El Ayuntamiento de Sant Joan d'Alacant adopta el Esquema Nacional de Seguridad (Real Decreto 311/2022 de 3 de mayo, ENS en adelante) como marco normativo referencial, desarrollando la presente política en cumplimiento de lo requerido en su artículo 12 y alineando sus actuaciones con sus principios básicos, recogidos en su artículo 5:

> *Artículo 5. Principios básicos del Esquema Nacional de Seguridad.*
>
> *El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:*
>
> *a) Seguridad como proceso integral.*
> *b) Gestión de la seguridad basada en los riesgos.*
> *c) Prevención, detección, respuesta y conservación.*
> *d) Existencia de líneas de defensa.*
> *e) Vigilancia continua.*
> *f) Reevaluación periódica.*
> *g) Diferenciación de responsabilidades.*

Desarrollados en los artículos 6 al 11 del Real Decreto 311/2022 de 3 de mayo. Algunos de estos puntos se amplían en este documento.

Asimismo, el Ayuntamiento de Sant Joan d'Alacant adopta los requisitos mínimos recogidos en el artículo 12 del ENS:

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*

Desarrollados en los artículos 13 a 27 del Real Decreto 311/2022. Algunos de estos puntos se amplían en este documento.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 8 de 31

En consecuencia, se implementará y mantendrá un Sistema de Gestión de Seguridad de la Información (SGSI en adelante) basado en el ENS y, donde apliquen, en otros marcos normativos y/o referenciales en materia de seguridad de la información, tal como recoge en el registro corporativo de marcos normativos aplicables.

9. Órgano Competente.

A los efectos de las actuaciones previstas en el SGSI y encomendadas al denominado "Órgano Competente", este Órgano, en el Ayuntamiento de Sant Joan d'Alacant, será Alcaldía y, en su caso, en quien se establezca la oportuna y formal delegación.

10. Organización de la Seguridad.

10.1. Definición de roles.

Tal como indican las normas de referencia, la seguridad deberá comprometer a todos los miembros del Ayuntamiento. La Política de Seguridad debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros del Ayuntamiento.

Adicionalmente, otros marcos normativos requieren asimismo la creación de roles específicos, tales como el rol Delegado de Protección de Datos en el RGPD-LOPDGDD.

Se establecen por tanto los siguientes roles en el Ayuntamiento de Sant Joan d'Alacant relacionados con la Seguridad de la Información:

10.2. Responsable de Servicio + Responsable de la Información.

Este rol concentra, tal como permite el ENS, los roles de Responsable de Servicio y Responsable de la Información. La razón de esta unificación se basa en:

1. Los servicios municipales y su información asociada están íntimamente ligados, no necesitando un rol diferenciado para el servicio y otro para la información que trata.
2. Mejora de la operativa en materia de seguridad ante la cantidad de unidades administrativas, áreas o departamentos existentes en el Ayuntamiento de Sant Joan d'Alacant, con lo que la gestión individual de cada departamento dificulta la operatividad en materias como la ciberseguridad y la protección de datos personales, haciendo necesaria esta concentración y asignando a las personas responsables departamentales un rol delegado de este rol global.

Entre sus funciones como Responsable de Servicio:

- Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de los servicios bajo su responsabilidad.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 9 de 31

- Responsable de la disponibilidad de los servicios bajo su responsabilidad.
- Determinará y aprobará formalmente los niveles de seguridad de los servicios, en colaboración con los responsables departamentales, con el Responsable de Seguridad y el Responsable del Sistema, en cada dimensión de seguridad de cada servicio, dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, a los que se suele añadir requisitos de disponibilidad, accesibilidad, interoperabilidad, etc.

Entre sus funciones como Responsable de la Información:

- En cuanto al RGPD - LOPDGDD, por delegación del Responsable del Tratamiento se encomienda el desarrollo de las tareas relacionadas con la gestión de los tratamientos de datos personales que se realizan bajo su responsabilidad, tanto automatizados como no automatizados (papel).
- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos almacenados y tratados por Ayuntamiento de Sant Joan d'Alacant, con el fin de evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección.
- Establece los requisitos de la información en materia de seguridad, por lo que determinará los niveles de seguridad, en colaboración con el Responsable de Seguridad y el Responsable del Sistema, en cada dimensión dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad, pudiendo recabar el asesoramiento y supervisión del Delegado de Protección de Datos.
- Verificará que la prestación de un servicio atienda a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, así como otros relacionados con la accesibilidad, interoperabilidad, integridad, autenticidad, trazabilidad, etc.

Este rol puede ser asumido por el Comité de Seguridad de la Información o por la Oficina Municipal de Protección de Datos y Seguridad de la Información.

10.3. Responsable de Departamento / Unidad Administrativa (RDEP).

Competencia y responsabilidades en materia de seguridad en una Unidad Administrativa.

Ejerce las funciones de Responsable delegado de Servicio y Responsable delegado de la Información para los servicios e informaciones desarrollados en su departamento / unidad / área, estando obligado a realizar, con la máxima prioridad, las siguientes actividades:

1. Ofrecer toda la información que el Responsable de Servicio + Responsable de la Información le requiera.
2. Asistir a todas las sesiones de trabajo donde sea convocado por el Responsable de Servicio + Responsable de la Información, sesiones que tendrán la máxima prioridad en su planificación de trabajos.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 10 de 31

3. Implementar inmediatamente todas las medidas de seguridad que reciba del Responsable de Servicio + Responsable de la Información, del Responsable de Seguridad o del Responsable del Sistema, requiriendo y controlando su cumplimiento por parte del personal bajo su responsabilidad.

10.4. Responsable de Seguridad de la Información. (RSEG o CISO).

El rol de Responsable de Seguridad debe asumir las siguientes funciones:

- Tareas y controles asignados al rol Responsable de Seguridad en el ENS. Coordinará y controlará las medidas definidas en las políticas, normas, procedimiento e instrucciones sobre Seguridad y, en general, se encargará del cumplimiento de las medidas de seguridad que detalla el ENS.
- Reportará directamente al Comité de Seguridad de la Información.
- Actuará como Secretario del Comité de Seguridad de la Información.
- Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.
- Mantendrá la Seguridad de la Información tratada 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.
- Promoverá la formación y concienciación en materia de Seguridad de la Información dentro de su ámbito de responsabilidad.
- Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema.
- Realizará el Análisis y Gestión de Riesgos.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme a lo requerido en las Normas, al Anexo II del ENS (cuando aplique) 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 el Órgano Competente.
- Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de las normativas, procedimientos e instrucciones sobre 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).

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 11 de 31

- Elaborará, junto al Responsable de Sistema, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- 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.
- Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistema, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistema.
- 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.
- Actuará en plena coordinación con el Delegado de Protección de Datos.
- En el caso de servicios externalizados, 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, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.
- Asumirá el rol de Responsable de Seguridad de la Información en relación con la legislación en materia de Infraestructuras Críticas, si dicha legislación fuera aplicable en el Ayuntamiento de Sant Joan d'Alacant.

10.5. Responsable de Sistema (RSIS o CIO).

Las funciones del Responsable de Sistema (o Responsables de Sistemas si así se establece) son:

- Desarrollar, operar y mantener los Sistemas de Información durante todo su ciclo de vida, así como de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir el sistema de gestión de los Sistemas 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.
- El Responsable de 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 de los Sistemas de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- Elaborar los Planes de Continuidad del Sistema (cuando proceda) para que sean

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 12 de 31

validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.
- Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema (cuando proceda) 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.

10.6. Administrador de la Seguridad del Sistema (ADS).

Al rol Administrador de la Seguridad del Sistema le corresponden las siguientes funciones:

- Implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los Sistemas de Información.
- Asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la Política de Seguridad vigente.
- Aplicar a los sistemas de información, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los procedimientos de seguridad, instrucciones técnicas y los mecanismos y servicios de seguridad requeridos.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información y los mecanismos y servicios de seguridad requeridos.
- Gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los Sistemas de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Aprobar los cambios en la configuración vigente de los sistemas de información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
- Informar a los Responsables de la Seguridad y de Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Monitorizar el estado de la seguridad del sistema.

En caso de ocurrencia de incidentes de Seguridad de la Información:

- Llevar a cabo el registro, seguimiento y gestión de los incidentes de seguridad en los sistemas bajo su responsabilidad.
- Ejecutar el plan de seguridad aprobado.
- Aislar los incidentes para evitar la propagación a elementos ajenos a la situación de riesgo.
- Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves.
- Asegurar la integridad de los elementos críticos del sistema si se ha visto afectada la disponibilidad de los mismos.
- Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- Investigar incidentes. Determinar el modo, los medios, los motivos y el origen del incidente, su causa raíz, sus mecanismos de solución y documentar “lecciones aprendidas”.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 13 de 31

10.7. Responsable de Recursos Humanos (DRRHH).

Competencias y responsabilidades en:

1. Formación y concienciación del personal del Ayuntamiento de Sant Joan d'Alacant, tanto en desempeño profesional como en el cumplimiento de las leyes y normas relacionadas con la seguridad de la información.
2. Procesos internos relacionados con la selección de personas, acciones disciplinarias, gestión de permisos de acceso y relación laboral.
3. Comunicación de las políticas corporativas del SGSI, instrucciones de seguridad y comunicaciones periódicas al personal del Ayuntamiento de Sant Joan d'Alacant en materia de seguridad para mantener la concienciación.
4. Caracterización de puestos de trabajo en relación con la seguridad de la información, donde aplique.

10.8. Jefe de seguridad física de las instalaciones.

Competencias y responsabilidades en materia de seguridad física en las instalaciones del Ayuntamiento de Sant Joan d'Alacant. Entre sus funciones:

1.- Implantar las medidas de seguridad que le competan dentro de las determinadas por el Responsable de Seguridad, e informar a éste de su grado de implantación, eficacia e incidentes.
2.- Competencias y responsabilidades en el mantenimiento y disponibilidad de las instalaciones.

10.9. Equipo de Respuesta a Incidentes y Continuidad.

- Detección, recepción y actuación ante las incidencias relacionadas con la seguridad de la información. Procedimientos de escalada.
- Evaluación de incidentes y líneas de actuación, incluyendo el lanzamiento de los Planes de Continuidad, en su caso.
- En su caso, propuestas de comunicación a los organismos pertinentes (CCN, AEPD).
- Desarrollo de un entorno de "lecciones aprendidas" para evitar que se repita un incidente.
- Métricas e indicadores de incidencias, informando al Comité de Seguridad.
- Integrado en el Comité de Seguridad de la Información.

10.10. Responsable Gabinete Legal (RLEGAL o CLO).

La persona responsable del Gabinete Legal debe mantener el cumplimiento de los marcos normativos aplicables en el Ayuntamiento de Sant Joan d'Alacant, así como dirigir todas las actuaciones que, en materia jurídica, deban realizarse en defensa de los intereses corporativos.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 14 de 31

10.11. Delegado de Protección de Datos (DPD).

El rol de Delegado de Protección de Datos (DPD) es requerido por el RGPD en base a su Art. 37:

> *Artículo 37 Designación del delegado de protección de datos*
>
> *1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:*
>
> *a) El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.*
> *b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.*
> *c) Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 RGPD y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10 RGPD.*

En base a estas al artículo 37.1.a del RGPD, el Ayuntamiento de Sant Joan d'Alacant asume la necesidad de disponer del rol Delegado de Protección de Datos.

Por tanto, se identificará y nombrará un Delegado de Protección de Datos corporativo, si bien este rol podrá ser asignado a personal interno o a un servicio externo.

La titularidad concreta del DPD corporativo se determinará mediante designación del Órgano Competente, tras informe del Comité de Seguridad de la Información, y será dado de alta en el Registro de DPD de la Agencia Española de Protección de Datos (AEPD).

La posición y funciones del DPD están definidas en los artículos 38 y 39 del RGPD.

10.12. Infraestructuras Críticas.

En caso de que el Ayuntamiento de Sant Joan d'Alacant disponga de infraestructuras dentro del ámbito objetivo de la legislación en materia de Infraestructuras Críticas, los roles asociados son:

10.12.1. Responsable de Seguridad y Enlace (RSEN)

Persona designada por el operador crítico como representante y enlace con ante la Secretaría de Estado de Seguridad en todas las materias de seguridad de la protección de las infraestructuras críticas.

10.12.2. Responsable de Seguridad de la Información

Persona designada por el operador de servicios esenciales como punto de contacto y de coordinación técnica con las autoridades competentes en materia de seguridad de las redes y

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 15 de 31

sistemas de información. Coincide con el rol Responsable de Seguridad (RSEG) descrito anteriormente.

10.12.3. Delegados de Seguridad de la Infraestructura Crítica (DSEG)

Persona designada por el operador crítico como enlace operativo y el canal de información con las autoridades competentes en todo lo referente a la seguridad concreta de la infraestructura crítica.

10.13. Comité de Seguridad de la Información.

10.13.1. Funciones del Comité de Seguridad de la Información.

Órgano Colegiado cuyas funciones están definidas por el ENS, y son las siguientes:

- Atender los requerimientos, objetivos y necesidades de información del Órgano Competente y de los diferentes departamentos.
- Informar regularmente del estado de la Seguridad de la Información al Órgano Competente.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución del Ayuntamiento 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 Órgano Competente.
- Aprobar las normativas, procedimientos , instrucciones técnicas y, en general, todos los documentos sobre seguridad de la información.
- 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 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 Ayuntamiento 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.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 16 de 31

- Asegurar que la seguridad de la información se tenga en cuenta en todos los proyectos, desde su especificación inicial hasta su puesta en operación, incluyendo el principio de "Privacidad por diseño y por defecto" requerido por el RGPD. 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.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas del Ayuntamiento, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Recabar regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.
- Obtener asesoramiento sobre los temas 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 interna y/o externa.
    - Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.
- Aprobar el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente y plazos de ejecución, para su presentación al Órgano Competente y su correspondiente aprobación formal.
- Actuar como Equipo de Respuesta a Incidentes y Continuidad.
- Asumir el rol de Responsable de Servicio + Responsable de la Información.

10.13.2. Composición.

El Comité de Seguridad de la Información estará compuesto por los siguientes miembros:

Posición	Departamento / Área	Función
Presidente	Equipo de gobierno	Alcaldía o concejalía delegada. En su defecto, Secretario/a General.
Secretario	Tecnología de la Información	Responsable de Seguridad (RSEG / CISO)
Vocal 1	Secretaría	Secretaria/o General o persona designada al efecto.
Vocal 2	Tecnología de la Información	Responsable del Sistema
Vocal 3	Interno o externo	Delegado de Protección de Datos (con voz, sin voto).

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 17 de 31

Posición	Departamento / Área	Función

A requerimiento del Comité de Seguridad de la Información se convocará a otros responsables de departamento u otras personas cuya intervención sea requerida para el desarrollo de las actuaciones del Comité de Seguridad de la Información.

Corresponde al/a la Secretario/a del Comité de Seguridad de la Información:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Todos los miembros del Comité actuarán con voz y voto salvo el Delegado de Protección de Datos, que tendrá voz pero no voto en base al principio de independencia que rige este rol. Sus acuerdos requerirán, como mínimo, el voto de la mayoría simple de sus miembros.

10.13.3. Periodicidad de las sesiones de trabajo.

El Comité de Seguridad de la Información mantendrá sesiones de trabajo:

1. Planificadas. Plazo máximo de un mes.
2. No planificadas. Derivadas de incidentes de cualquier naturaleza cuya gravedad aconseje convocar la sesión de trabajo.

Las conclusiones del Comité de Seguridad de la Información se elevarán a Alcaldía o concejalía delegada en materia de seguridad corporativa, así como al Comité de Seguridad Corporativa (si se constituye).

10.13.4. Oficina Municipal de Protección de Datos y Seguridad de la Información (OMPDS).

Órgano Colegiado creado para concentrar los diferentes roles requeridos por el ENS, el RGPD y la LOPDGDD. La composición y periodicidad de las sesiones de trabajo de la OMPDS coincide con la del Comité de Seguridad de la Información.

Las funciones de la OMPDS integran:

1. Comité de Seguridad de la Información. ENS.
2. Por delegación del Órgano Competente, las funciones de Responsable de Tratamiento de datos personales. RGPD.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 18 de 31

3. Por delegación del Órgano Competente, las funciones de Encargado de Tratamiento de datos personales cuando el Ayuntamiento de Sant Joan d'Alacant actúe como tal.

10.14. Jerarquía en el proceso de decisiones y mecanismos de coordinación.

Los diferentes roles de Seguridad de la Información (autoridad principal y posibles delegadas) actuarán en base a:

10.14.1. Comité de Seguridad de la Información.

El Comité de Seguridad de la Información da instrucciones al Responsable de Seguridad de la Información y al Responsable de Sistema, quienes se encargan de cumplimentarlas, supervisando que todos los actores implicados implementan las medidas de seguridad según lo establecido en esta PGSI.

10.14.2. Responsable de Seguridad de la Información.

El Responsable de la Seguridad de la Información:

1. Informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
2. Informa al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
3. Rinde cuentas al Comité de Seguridad de la Información, como secretario:

    - Resumen consolidado de actuaciones en materia de seguridad.
    - Resumen consolidado de incidentes relativos a la Seguridad de la Información.
    - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

4. Rinde cuentas al Órgano Competente y (en su caso) al Comité de Seguridad Corporativa, según lo acordado en el Comité de Seguridad de la Información.

    - Resumen consolidado de actuaciones en materia de seguridad.
    - Resumen consolidado de incidentes relativos a la Seguridad de la Información.
    - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

5. Cuando no exista un Comité de Seguridad Corporativa, el Responsable de la Seguridad informará al Órgano Competente.

10.14.3. Responsable de sistema.

El Responsable de Sistema:

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 19 de 31

1. Informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
2. Informa al Responsable de Servicio de las incidencias funcionales relativas al servicio que le compete.
3. Da cuenta al Responsable de la Seguridad de:

   - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
   - Resumen consolidado de los incidentes de seguridad.
   - Indicadores de la eficacia de las medidas de protección.

10.14.4. Oficina Municipal de Protección de Datos y Seguridad de la Información.

La Oficina Municipal de Protección de Datos y Seguridad de la Información:

1. Actuando como Responsable de Tratamiento o Encargado de Tratamiento de datos personales, y consultando con el Delegado de Protección de Datos, toma las decisiones pertinentes en materia de cumplimiento del RGPD y la LOPDGDD, informando al Órgano Competente de los asuntos relacionados con brechas de seguridad graves.
2. Actuando como Comité de Seguridad de la Información desarrolla sus funciones e informa tal como se describe en su capítulo correspondiente.

10.15. Procedimientos de designación.

El Órgano Competente nombrará formalmente, mediante las resoluciones pertinentes:

- Comité de Seguridad Corporativa, en caso de constituirse.
- Oficina Municipal de Protección de Datos y Seguridad de la Información, en caso de constituirse.
- Comité de Seguridad de la Información.
- Responsable/s de la Información.
- Responsable/s del Servicio.
- Responsable/s de Seguridad.
- Responsable/s de Sistema.
- Administrador/es de Seguridad del Sistema, a propuesta del Responsable de Sistema o del Responsable de Seguridad de la Información.

10.16. Segregación de funciones.

Las normativas estándares, recogen el principio de “seguridad como función diferenciada”.
Este principio exige:

- Responsable de Seguridad de la Información debe ser independiente del Responsable de Sistema, a menos que, por indisponibilidad de recursos, deba recaer en la misma persona, circunstancia que deberá ser motivada y documentada.
- Responsable de Seguridad debe ser independiente de Responsables de Servicio.
- Responsable de Seguridad debe ser independiente de Responsables de Información.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 20 de 31

- Responsable de Servicio o de Información debe ser independiente de Responsable de Sistema, salvo excepcio0nes justificadas circunstancia que deberán ser motivadas y documentadas.
- Delegado de Protección de Datos debe ser independiente de funciones que comprometan su independencia. Con una adecuada política de actuación, el rol Delegado de Protección de Datos puede coincidir en la misma persona que el rol Responsable de Seguridad de la Información en caso de indisponibilidad de recursos.

La asignación de roles y responsabilidades tendrá en cuenta la preceptiva segregación de funciones, de forma que las actuaciones de las personas titulares de los mismos no comprometan la seguridad de Informaciones y Servicios en cualquiera de sus dimensiones (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad).

En casos excepcionales, sobre todo cuando no están disponibles los recursos necesarios, pueden exceptuarse estas reglas de segregación de funciones, estableciendo las medidas compensatorias apropiadas para la resolución de los conflictos de intereses que puedan surgir.

10.17. Suplencias y delegaciones.

Los roles requeridos por los marcos normativos referenciales de esta PGSI deben estar permanentemente operativos. El Ayuntamiento establecerá suplencias y/o delegaciones de forma que la ausencia de una persona, por cualquier motivo, no cause la carencia de las funciones y/o competencias que desarrolla.

11. Datos personales.

11.1. Tratamiento.

Para la prestación de los servicios corporativos deben ser recabados, tratados y almacenados datos personales. Es compromiso del Ayuntamiento de Sant Joan d'Alacant respetar y proteger los derechos recogidos en la Constitución Española respecto a la intimidad, privacidad, imagen y honor de las personas, por lo que el cumplimiento de los marcos normativos que los regulan y, por ende, la implementación de las medidas de seguridad y control requeridas constituye un objetivo prioritario de este Ayuntamiento.

El cumplimiento de RGPD, LOPDGDD y el resto de los marcos normativos que los desarrollen y evolucionen será una iniciativa prioritaria. Se adoptarán las medidas necesarias para que este Ayuntamiento cumpla en sus fechas de entrada en vigor todos los preceptos de los nuevos marcos, siendo uno de los puntos más importantes el nombramiento de la figura DPD (Delegado de Protección de Datos).

Asimismo, deberán realizarse los ciclos de formación y concienciación específicos para que el personal conozca las medidas que deben aplicar en sus puestos de trabajo y los medios disponibles para la resolución de dudas, problemas e incidentes relacionados.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 21 de 31

Será prioritario implementar las medidas organizativas y técnicas apropiadas para proteger los derechos y libertades de las personas físicas afectadas por los tratamientos de datos personales realizados por el Ayuntamiento.

11.2. Videovigilancia.

El Ayuntamiento de Sant Joan d'Alacant implantará los sistemas de videovigilancia necesarios, idóneos y proporcionales para las siguientes finalidades:

1. El mantenimiento de la seguridad de las personas, bienes e instalaciones (artículo 22 LOPDGDD).
2. La regulación, ordenación, gestión, vigilancia y disciplina del tráfico en las vías urbanas de titularidad municipal, así como la denuncia de las infracciones que se cometan en dichas vías y la sanción de las mismas (artículo 7 Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial.
3. Prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública (Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales).
4. Gestión de las cámaras y grabaciones en espacios públicos para fines de control y gestión de residuos y actuaciones ilícitas en la materia, incluyendo su posible repercusión penal.
5. En caso de las circunstancias lo aconsejen, y tras la información previa requerida en el artículo 89 de la LOPDGDD, control del desempeño laboral en base a la legitimación contenida en dicho artículo 89 de la LOPDGDD, adoptando todas las medidas necesarias para salvaguardar, simultáneamente, los derechos de las personas afectadas.

El Ayuntamiento de Sant Joan d'Alacant observará en todo momento la normativa vigente en materia de videovigilancia de los espacios públicos y privados, respetando los derechos de las personas captadas y suprimiendo las imágenes en los plazos establecidos por dicho ordenamiento.

Asimismo, se implementarán las medidas técnicas y organizativas adecuadas para salvaguardar la disponibilidad, confidencialidad e integridad de las imágenes grabadas, así como su posible comunicación a terceros en los casos en que dicha comunicación esté legitimada,

12. Inteligencia artificial.

El Ayuntamiento de Sant Joan d'Alacant es plenamente consciente de los relevantes avances que, en materia de Inteligencia Artificial (IA en adelante), se están desarrollando en los últimos

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 22 de 31

años, así como de los beneficios que puede aportar en las prestaciones del Ayuntamiento hacia la ciudadanía, por lo que se impulsará su implementación en todas aquellas actividades municipales donde aporte valor añadido a sus servicios.

Paralelamente, este Ayuntamiento también es consciente de los riesgos que supone una implementación desordenada y sin control de sistemas de IA, por lo que el CSI o la OMPDS deberán evaluar y, en su caso, aprobar cualquier sistema de IA antes de su despliegue y utilización por el personal municipal, así como la adecuada formación del personal para optimizar los resultados de estos sistemas y salvaguardar los derechos y libertades de la ciudadanía.

Todas las actuaciones en materia de IA se regirán, en todo momento, por la normativa legal vigente, muy especialmente el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, y sus desarrollos.

13. Gestión de riesgos.

13.1. Justificación.

Todos los sistemas sujetos a esta PGSI deberán realizar apreciaciones de riesgos, evaluando las amenazas a las que están expuestos, sus vulnerabilidades, el impacto que supondría la materialización de las amenazas y, por tanto, el nivel de riesgo que supone.

Respecto de todos los sistemas de información comprendidos en el alcance de esta Política se deberá realizar apreciaciones periódicas de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

Las apreciaciones de riesgos constituyen una de las bases fundamentales para determinar las medidas de seguridad que se deben adoptar, así como para los requerimientos del RGPD relacionados sobre Análisis de Riesgos y Evaluaciones de Impacto sobre Protección de Datos (EIPD) cuando procedan.

13.2. Criterios de apreciación de riesgos.

Para la armonización de las apreciaciones 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.

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que adoptará el Ayuntamiento de Sant Joan d'Alacant, basándose en estándares y buenas prácticas reconocidas. Esta metodología será MAGERIT V3 y las actualizaciones que pueda incorporar en el futuro.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión del Ayuntamiento, en base al impacto que los eventos

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 23 de 31

analizados supongan sobre los mismos, así como aquéllos que afecten a los derechos y libertades de las personas físicas afectadas por los tratamientos de datos personales.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los interlocutores sociales y los asociados a los tratamientos de datos personales.

13.3. Directrices de tratamiento.

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, documentando, justificando y promoviendo las inversiones adecuadas para su aprobación por el Órgano Competente.

13.4. Proceso de aceptación del riesgo residual.

Los riesgos residuales serán determinados por el Responsable de Seguridad de la Información.

Los niveles de riesgo residual sobre servicios e informaciones tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad contenidas en el Anexo II del ENS y aquéllas complementarias que fueran necesarias para el cumplimiento de RGPD y LOPDGDD) deberán ser aceptados previamente por los responsables de los servicios e informaciones afectadas y por el DPD en caso de afectar a datos personales.

Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

13.5. Necesidad de realizar o actualizar las apreciaciones de riesgos.

Las apreciaciones de riesgos deben ser actividades repetidas regularmente, según lo establecido en el Artículo 9 del ENS. Este proceso se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando se produzcan cambios normativos que así lo exijan o lo hagan conveniente.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 24 de 31

14. Gestión de incidentes de seguridad

Es obligación de todo el personal del Ayuntamiento de Sant Joan d'Alacant comunicar al Responsable de Departamento y al Responsable de Seguridad, sin dilación alguna, cualquier incidencia, real o sospechada, en materia de seguridad de la información.

Es obligación de todo el personal del Ayuntamiento de Sant Joan d'Alacant participar en todas las actividades que le sean requeridas durante el proceso de gestión de los incidentes de seguridad.

14.1. Prevención.

El Ayuntamiento de Sant Joan d'Alacant debe evitar, o, al menos, prevenir en la medida de lo posible, que la información o los servicios se vean afectados por incidentes de seguridad. Para ello, deben implementarse las medidas de seguridad determinadas por las normativas corporativas, así como cualquier control adicional identificado a través de una evaluación de riesgos.

Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados, existiendo una caracterización de puestos de trabajo donde se incluyan las cuestiones relacionadas con la seguridad.

Para garantizar el cumplimiento de la política, y bajo la supervisión del Comité de Seguridad de la Información, los responsable departamentales deben:

- Autorizar los sistemas antes de entrar en producción desde el prisma funcional, prestacional y legal.
- Evaluar regularmente la seguridad, incluyendo (juntamente con el Responsable de Seguridad) apreciaciones de riesgos, impulsando las iniciativas necesarias para resolver las situaciones no conformes o fuera de los márgenes de riesgo aceptables.
- Solicitar (si se considera necesaria) la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.
- Desarrollar Planes de Formación para su personal, así como reciclaje periódico y acciones de concienciación.

14.2. Detección – Vigilancia continua.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, pudiendo incluso provocar su detención, el Responsable de Sistema y los Administradores de Seguridad del Sistema deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, según lo establecido en los artículos 9 y 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa, práctica requerida por las normativas de referencia y en el artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 25 de 31

cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

14.3. Respuesta.

El equipo de respuesta ante incidentes debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros Organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT), autoridades competentes, organismos competentes (CCN, AEPD)y, en su caso a los afectados. Este precepto está recogido explícitamente en el ENS y en el RGPD (en este último caso, cuando el incidente afecte a datos personales).

14.4. Recuperación.

Para garantizar la disponibilidad de los servicios y las informaciones corporativas, el Ayuntamiento de Sant Joan d'Alacant desarrollará y mantendrá planes de continuidad de los sistemas de información como parte de su plan general de continuidad de servicio, así como actividades de recuperación en caso de caída total o parcial de los mismos. Estas actuaciones afectan tanto al ENS como a RGPD-LOPDGDD.

Estos planes de continuidad serán desarrollados teniendo en cuenta la categorización de los sistemas de información corporativos, en base a lo preceptuado en el Anexo I – Categoría de los sistemas, del ENS, y aplicar las medidas correspondientes de su Anexo II.

14.5. Aprendizaje.

Los incidentes serán analizados para determinar su causa raíz, las actuaciones desarrolladas en su resolución y recuperación y se extraerán las conclusiones apropiadas para prevenir su recurrencia.

14.6. Declaración.

Los incidentes serán evaluados por el Responsable de Seguridad de la Información, el Delegado de Protección de Datos y el Responsable de Seguridad Corporativa (si existe este rol), y se determinará la necesidad de su declaración ante los Organismos competentes:

1. Plataforma LUCIA del Centro Criptológico Nacional.
2. Agencia Española de Protección de Datos, en caso de estar implicados datos personales.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 26 de 31

3. Personas afectadas, si el incidente lo requiere en base a lo establecido en el RGPD para las brechas de seguridad.
4. Fuerzas y Cuerpos de Seguridad o Juzgados en caso de que el incidente pudiera suponer un ilícito civil o penal sustanciable en estas instancias.

15. Gestión del personal.

15.1. Obligaciones del personal.

El personal del Ayuntamiento de Sant Joan d'Alacant tiene la obligación de conocer y cumplir esta Política General de Seguridad de la Información (PGSI) y las Normativas y Procedimientos de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la PGSI y el resto de la documentación llegue a los afectados.

El personal del Ayuntamiento asistirá a sesiones de formación y concienciación en materia de Seguridad de la Información periodicamente, o cuando se realicen cambios significativos en medios y/o métodos relacionados. Se establecerá un programa de formación / concienciación continua para atender al personal, en particular en los casos de nueva incorporación.

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos del Ayuntamiento, constituyendo su incumplimiento una infracción a efectos de posibles procedimientos sancionadores, la cual será calificada en función del grado de incumplimiento y el impacto que éste haya generado sobre los servicios corporativos.

Asimismo, y sin perjuicio del procedimiento sancionador, el Ayuntamiento de Sant Joan d'Alacant denunciará ante las autoridades competentes las acciones que pudieran ser constitutivas de cualquier tipo de presunto delito.

15.2. Caracterización del puesto de trabajo.

El Ayuntamiento de Sant Joan d'Alacant incluirá en su descripción de puestos de trabajo los perfiles, titulaciones, acreditaciones y experiencia requeridos para aquellos puestos dedicados a tareas relacionadas con la Seguridad de la Información. Los procesos de selección tendrán en cuenta esta caracterización.

El Ayuntamiento de Sant Joan d'Alacant incluirá en su descripción de puestos de trabajo las funciones y responsabilidades en materia de seguridad de cada uno de dichos puestos.

15.3. Formación.

Las personas con responsabilidad en el uso (usuarios), operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en que

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 27 de 31

la necesiten para realizar su trabajo. La asistencia a las sesiones de formación es obligatoria y su aprovechamiento podrá ser evaluado.

El Ayuntamiento de Sant Joan d'Alacant elaborará anualmente un Plan de Formación, sobre el cual se realizará un seguimiento detallado, registrando todas las personas asistentes a los ciclos formativos.

15.4. Concienciación.

El Ayuntamiento de Sant Joan d'Alacant realizará actividades periódicas de concienciación hacia el personal, implementando mecanismos de comunicación de reglas de seguridad, cambios normativos, incidentes, resoluciones de Autoridades y, en general, toda información relevante para mejorar la conciencia del personal en cuanto a seguridad de la información y el cumplimiento de los marcos normativos aplicables.

15.5. Registro de actividad.

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

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

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

16. Terceras partes.

Cuando se presten servicios o se gestione información de otras Organizaciones, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 28 de 31

y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o se 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. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Las entidades terceras deberán seleccionarse atendiendo a los principios de idoneidad y cumplimiento de los marcos normativos exigibles, además del resto de criterios aplicables en su contratación.

Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

En caso de que algún aspecto de esta Política 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 servicio e información afectados antes de seguir adelante con la contratación.

En caso de que los tratamientos desarrollados por terceras partes involucren datos personales, se realizarán todas las actuaciones requeridas por el RGPD. En este último caso, se evaluará la idoneidad de los proveedores, tal como requiere el RGPD, y se firmarán los correspondientes contratos de “encargado de tratamiento” o “corresponsabilidad” con todo proveedor que desarrolle sus tareas tratando datos personales o “compromisos de confidencialidad y seguridad de la información” cuando los tratamientos de datos personales sean incidentales.

17. Revisión y aprobación de la Política de Seguridad

La Política General de Seguridad de la Información será revisada por el Comité de Seguridad de la Información y el Comité de Seguridad Corporativa (si se constituye) a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el Órgano Competente.

Cualquier cambio sobre la Política de Seguridad de la Información deberá ser difundido a todas las partes afectadas y, en su caso, objeto de reciclaje en la formación para el personal afectado.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 29 de 31

18. Documentación complementaria.

La Política de Seguridad de la Información se completará con documentos más detallados que ayudan a materializar sus preceptos. Para ello se utilizarán:

18.1. Normas de Seguridad.

Las normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto, los usos prohibidos y las responsabilidades de los usuarios. Son de carácter obligatorio.

18.2. Procedimientos de Seguridad.

Los procedimientos de seguridad detallan tareas concretas, indicando su operativa claramente.

18.3. Instrucciones de Seguridad.

Las instrucciones de seguridad desarrollan la operativa descrita en los procedimientos, explicando a nivel técnico su implementación.

18.4. Registros.

Repositorios conteniendo datos significativos respecto a eventos, resultados y, en general, información factual relevante u obligatoria para la seguridad de la información.

18.5. Gestión de la documentación.

El Ayuntamiento de Sant Joan d'Alacant dispone de un procedimiento de gestión de la documentación que incluye el inventario, las potestades de redacción y aprobación, control de versiones, clasificación de la información que contienen, formato, codificación y criterios de publicación.

Las aprobaciones son recogidas en actas del órgano potestativo correspondiente.

19. APROBACIÓN Y ENTRADA EN VIGOR.

Esta Política General de Seguridad de la Información es efectiva desde la fecha de su aprobación y será válida hasta que sea reemplazada por una nueva Política o sea derogada por resolución del Órgano Competente del Ayuntamiento de Sant Joan d'Alacant.

Este texto anula cualquier Política de Seguridad de la Información vigente hasta la fecha de aprobación de la presente.

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 30 de 31

Esta Política se complementa con el nombramiento formal de las personas concretas que asumen cada uno de los roles y funciones descritos, en base a la resolución o acuerdo correspondiente del Órgano Competente.

Texto aprobado en Sant Joan d'Alacant, mediante Decreto de Alcaldía de fecha <<FECHA DECRETO, sustituir este texto por la fecha del Decreto y su referencia>>

Cód. Validación: 7S355EYGNEZKLZCLLNX62AS6H
Verificación: https://santjoandalacant.sedelectronica.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 31 de 31