Seguridad de la Información

PLS-GLB-001

Política General de Seguridad de la Información

CONTROL DE EDICIÓN

FECHA	EDICION	REVISION	CAMBIOS
20/10/2017	01	AUREN CONSULTORES	Versión inicial
22/12/2020	02	AUREN CONSULTORES	Cambios en denominaciones de roles
6/07/2021	03	Responsable de Seguridad	Revisión para su aprobación por Pleno
Las aprobaciones formales de los documentos figuran en sus actas / resoluciones correspondientes.			

CLASIFICACIÓN: PUBLICO

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.

ÍNDICE

1 Contenido y objetivos del presente documento.....3
1 Datos del Ayuntamiento de San Vicente del Raspeig.....3
2 Justificación de una Política General de Seguridad de la Información.....3
3 Ámbito objetivo de la PGSI.....3
4 Ámbito subjetivo de la PGSI.....4
5 Misión y servicios prestados.....4
6 Marcos normativos referenciales de la PGSI.....4
7 Órgano Competente.....5
8 Organización de la Seguridad.....5
8.1 Definición de roles.....5
8.2 Responsable de Departamento (RDEP) – Unidad Administrativa.....6
8.3 Responsable de Recursos Humanos (DRRHH).....6
8.4 Responsable de Seguridad de la Información. (RSEG o CISO).....7
8.5 Responsable de Sistema (RSIS o CIO).....8
8.6 Administrador de la Seguridad del Sistema (ASS).....8
8.7 Jefe de seguridad física de las instalaciones (CFSO).....9
8.8 Equipo de Respuesta a Incidentes (IRT).....9
8.9 Responsable Gabinete Legal (RLEGAL o CLO).....10
8.10 Delegado de Protección de Datos (DPD).....10
8.11 Comité de Seguridad de la Información.....10
8.11.1 Composición.....10
8.11.2 Funciones del Comité de Seguridad de la Información.....11
8.12 Jerarquía en el proceso de decisiones y mecanismos de coordinación.....12
8.12.1 Comité de Seguridad de la Información.....12
8.12.2 Responsable de Seguridad de la Información.....12
8.12.3 Responsable de sistema.....13
8.13 Procedimientos de designación de personas.....13
8.14 Segregación de funciones.....13
8.15 Suplencias y delegaciones.....14
9 Datos de carácter personal.....14
9.1 Tratamiento.....14
9.2 Videovigilancia.....14
10 Gestión de riesgos.....14
10.1 Justificación.....14
10.2 Criterios de evaluación de riesgos.....15
10.3 Directrices de tratamiento.....15
10.4 Proceso de aceptación del riesgo residual.....15
10.5 Necesidad de realizar o actualizar las evaluaciones de riesgos.....15

11 Gestión de incidentes de seguridad....16
11.1 Prevención....16
11.2 Detección....16
11.3 Respuesta....17
11.4 Recuperación....17
11.5 Aprendizaje....17
12 Gestión del personal....17
12.1 Obligaciones del personal....17
12.2 Caracterización del puesto de trabajo....18
12.3 Formación....18
12.4 Concienciación....18
13 Terceras partes....18
14 Revisión y aprobación de la Política de Seguridad....19
15 Documentación complementaria....19
15.1 Normas de Seguridad....19
15.2 Procedimientos de Seguridad....19
15.3 Instrucciones de Seguridad....19
16 APROBACIÓN Y ENTRADA EN VIGOR....19

1 Contenido y objetivos del presente documento.

Este documento contiene la Política General de Seguridad de la Información (PGSI en adelante) del Ayuntamiento de San Vicente del Raspeig ("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.

1 Datos del Ayuntamiento de San Vicente del Raspeig

Razón social	Ayuntamiento de San Vicente del Raspeig
NIF	P0312200I
Domicilio	Plaza de la Comunitat Valenciana, 1,
Población	San Vicente del Raspeig
Código Postal	03690
Provincia	Alicante
País	España

2 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 Superior Competente", representado en el caso del Ayuntamiento de San Vicente del Raspeig por su **Pleno**, 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.

3 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:

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

2 La realización de las obligaciones y el ejercicio de competencias por parte del Ayuntamiento, tanto los 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 las Administraciones Públicas.

4 Ámbito subjetivo de la PGSI.

La PGSI será aplicada por todos los servicios, departamentos, secciones, áreas, unidades administrativas del Ayuntamiento y, en general, por todas las entidades internas y externas de cualquier tipo vinculadas a esta Entidad 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 la misma. Asimismo, la PGSI afecta a todo el personal que presta servicios al 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.

5 Misión y servicios prestados.

El Ayuntamiento, como Órgano de la Administración Pública, para la gestión de sus intereses, y en el ámbito de sus competencias, sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización y coordinación, promueve toda clase de actividades y presta los servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de los Ciudadanos, todo ello bajo los preceptos de los diversos marcos normativos que le afectan.

6 Marcos normativos referenciales de la PGSI.

Como base normativa para realizar la presente guía de seguridad, se ha analizado la legislación vigente, que afecta al desarrollo de las actividades de la Administración Local en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información. El marco legal, con carácter general en materia de seguridad de la información, viene establecido por la siguiente legislación:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que señala en su art. 17.3 que los medios o soportes en que se almacenen documentos , deberán contar con las medidas de seguridad que establece el Esquema Nacional de Seguridad, que garanticen una serie de principios (como integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados); y, establece también, en su art. 27.3 que las Administraciones Públicas deberán cumplir con el Esquema Nacional de Seguridad para garantizar la identidad y contenido de las copias electrónicas o en papel, es decir, el carácter de copias auténticas. Por último, dispone en su Disposición Adicional segunda que, tanto las Comunidades Autónomas, como las Entidades Locales, deberán garantizar su compatibilidad

informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes registros y plataformas mediante el cumplimiento, igualmente, del Esquema Nacional de Seguridad. Y que, además, deroga la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

- El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.
- Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Real Decreto Ley 12/2018, de 8 se septiembre,de Seguridad de las redes y sistemas de información que transpone la Directiva 2016/1148 del Parlamento Europeo y del Conseujo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión.

El documento se publicará en la Sede Electrónica del Ayuntamiento.

7 Órgano Competente.

La aprobación y las posteriores modificaciones de la presente Política de Seguridad de la Información se tramitarán por el Pleno de la corporación y, en su caso, en quien se establezca la oportuna delegación.

Las actuaciones derivadas de la aplicación de la presente Política de Seguridad serán aprobadas por Decreto de Alcaldía y, en su caso, en quien se establezca la oportuna delegación.

8 Organización de la Seguridad.

8.1 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 relacionados con la Seguridad de la Información.

8.2 Responsable de Departamento (RDEP) – Unidad Administrativa.

Competencia y responsabilidades en materia de seguridad en una Unidad Administrativa, desempeñando también el papel de "Propietario de Riesgo" en dicha Unidad Administrativa o Departamento.

Asume las funciones de Responsable de Servicio y Responsable de Información para los procesos desarrollados en su departamento / unidad / área si éstos no son asumidos por el Comité de Seguridad de la Información.

Entre sus funciones como Responsable de Servicio:

- En cuanto a 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 en su departamento concreto, tanto automatizados como no automatizados (papel).
- 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.
- Responsable de Información para toda aquélla gestionada por los servicios ofrecidos por su departamento.
- Tiene la responsabilidad última del uso que se haga de los servicios de su departamento y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que derive en un incidente sobre disponibilidad de los servicios.
- Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles de seguridad aplicar corresponda al Responsable del Sistema, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

Entre sus funciones como Responsable de la Información:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos almacenados y tratados por el Ayuntamiento de San Vicente del Raspeig, 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 una cierta información y, por tanto, de su protección. Por tanto, el Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establece los requisitos de la información en materia de seguridad.
    - En el marco del ENS, equivale a la potestad de determinar los niveles de Seguridad de la Información.
    - En el marco de RGPD y LOPDGDD, asume funciones delegadas por parte del Responsable del Tratamiento en el ámbito de su área de responsabilidad.
- Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad, pudiendo recabar opinión del Responsable de la Seguridad y Responsable del Sistema.

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.

8.3 Responsable de Recursos Humanos (DRRHH).

Competencias y responsabilidades en:

1 Formación y sensibilización del personal del Ayuntamiento de San Vicente del Raspeig, 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 "píldoras de seguridad" periódicas al personal del Ayuntamiento de San Vicente del Raspeig.

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

Se ha designado como tal al Coordinador del Área de Informática del Ayuntamiento al cual le corresponden las siguientes funciones:

- Tareas y controles asignados al rol Responsable de Seguridad en 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 manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en esta Política de Seguridad del Ayuntamiento.
- 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, la Política de Seguridad de la Información, para su aprobación por Dirección.
- Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.
- Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.
- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a Seguridad de la Información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.

- 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 Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.
- Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
- Actuará en plena coordinación con el Delegado de Protección de Datos (RGPD).

8.5 Responsable de Sistema (RSIS o CIO).

Se ha designado a uno de los técnicos del área de Informática y Modernización cuyas funciones 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 del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
- Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
- Monitorizar el estado de la seguridad 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 para que sean 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 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.

8.6 Administrador de la Seguridad del Sistema (ASS).

Se han nombrado como tales a los dos técnicos restantes del área de Informática y Modernización a los cuales les 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 establecida por el Ayuntamiento.
- Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los Procedimientos Operativos de Seguridad 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.
- La 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 del 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”.

8.7 Jefe de seguridad física de las instalaciones (CFSO).

Se designa como tal al Jefe de la Policía Local del Ayuntamiento, cuyas competencias y responsabilidades en materia de seguridad física en las instalaciones del Ayuntamiento de San Vicente del Raspeig serán las siguientes.

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.

8.8 Equipo de Respuesta a Incidentes (IRT).

Se designa como tal al personal del Área de Informátrica y Modernización sin perjuicio que se pueda contratar asesoramiento externo para la ejecución de determinadas tareas muy especíicas que requieren cierta especialización.

- Detección, recepción y actuación ante las incidencias relacionadas con la seguridad de la información. Procedimientos de escalada.
- Desarrollo de un entorno de "lecciones aprendidas" para evitar que se repita un incidente.
- Métricas e indicadores de incidencias, informando al Comité de Seguridad.
- Dirigido por RSEG / CISO.

8.9 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 San Vicente del Raspeig, así como dirigir todas las actuaciones que, en materia jurídica, deban realizarse en defensa de los intereses corporativos.

Se nombra como tal al responsable del área de Asesoría Jurídica y Patrimonio.

8.10 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.*

El Ayuntamiento de San Vicente del Raspeig asume la necesidad de disponer del rol Delegado de Protección de Datos (DPD en adelante), por lo que mediante resolución de Alcaldía n.º 417 del 12 de marzo de 2019 se designaron como Delegados de Protección de Datos del Ayuntamiento de San Vicente del Raspeig, para que de manera conjunta desarrollen las funciones que la normativa de aplicación atribuye al ese rol a los funcionarios Olga Pino Diez, Secretaria General del Ayuntamiento y Juan Manuel Ramos Crespo, Coordinador del Servicio de Informática, sin perjuicio de la contratación de soporte externo especializado.

Las funciones del DPD están definidas en el RGPD.

8.11 Comité de Seguridad de la Información.

8.11.1 Composición.

Mediante Resolución de Alaldía n.º 2291 del 28 de mayo de 2021 se creó el Órgano Colegiado denominado Comité de Seguridad de la Información, compuesto por los siguientes miembros:

Posición	Departamento / Área	Función
Presidencia	Equipo de gobierno	Alcaldía o representante del equipo de gobierno. En su defecto, Secretaría General.
Secretaría	Tecnología de la Información	Responsable de Seguridad (RSEG / CISO)
Vocal 1	Secretaria General	Secretaría General

Posición	Departamento / Área	Función
Vocal 2	Tecnología de la Información	Responsable de Sistema (RSIS / CIO)

A requerimiento del Comité de Seguridad de la Información se convocará a otros Responsables de Departamentos / Unidades Administrativas y/u otras personas cuya intervención sea requerida para el desarrollo de las actuaciones del Comité de Seguridad de la Información.

Corresponde al 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 y sus acuerdos requerirán, como mínimo, el voto de la mayoría simple de sus miembros.

8.11.2 Funciones del Comité de Seguridad de la Información.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Atender los requerimientos, objetivos y necesidades de información del Órgano Superior Competente y de los diferentes departamentos.
- Informar regularmente del estado de la Seguridad de la Información al Órgano Superior 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 la Dirección.
- Aprobar la normativa de 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 principales riesgos residuales asumidos por el Ayuntamiento y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de Seguridad de la Información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del 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.

- Asegurar que la Seguridad de la Información se tenga en cuenta en todos los proyectos TIC 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, para su presentación al Órgano Superior Competente y su correspondiente aprobación formal.
- Asumir los roles de Responsable de Servicio y Responsable de Información especificados en el ENS, teniendo en cuenta la opinión de los Responsables de Departamento o Unidad Administrativa afectados.

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

Los diferentes roles de Seguridad de la Información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple:

8.12.1 Comité de Seguridad de la Información.

El Comité de Seguridad de la Información da instrucciones al Responsable de Seguridad de la Información, quien se encarga de cumplimentarlas, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en esta PGSI.

8.12.2 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 Superior Competente, 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.

8.12.3 Responsable de sistema.

El Responsable del Sistema:

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:
   - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
   - Resumen consolidado de los incidentes de seguridad.
   - Medidas de la eficacia de las medidas de protección que se deben implantar.

8.13 Procedimientos de designación de personas.

El Órgano Competente nombrará formalmente, mediante las resoluciones pertinentes:

- Comité de Seguridad de la Información (ya creado mediante Resolución de Alaldía n.º 2291 del 28 de mayo de 2021).
- Responsable/s de la Información.
- Responsable/s del Servicio.
- Responsable/s de la Seguridad.
- Responsable/s de los Sistemas de Información.
- Administrador/es de Seguridad del Sistema, a propuesta del Responsable del Sistema o del Responsable de Seguridad de la Información.
- Delegado de Protección de Datos (ya creado mediante Resolución de Alcaldía n.º 417 del 12 de marzo de 2019).

8.14 Segregación de funciones.

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

- Responsable de Seguridad debe ser independiente del Responsable del Sistema.
- Responsable de Seguridad debe ser independiente de Responsables de Servicio.
- Responsable de Seguridad debe ser independiente de Responsables de Información.
- Responsable de Servicio o de Información debe ser independiente de Responsable del Sistema.

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.

8.15 Suplencias y delegaciones.

Los roles requeridos por los marcos normativos referenciales de esta PGSI deben estar permanentemente operativos. El Ayuntamiento establecerá un procedimiento formal de 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.

9 Datos de carácter personal.

9.1 Tratamiento.

Para la prestación de los servicios corporativos deben ser recabados, tratados y almacenados datos de carácter personal. Es compromiso del Ayuntamiento de San Vicente del Raspeig 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 sus marcos normativos que los desarrollan 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.

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.

9.2 Videovigilancia.

El Ayuntamiento 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 cancelando las imágenes en los plazos establecidos por dicho ordenamiento.

10 Gestión de riesgos.

10.1 Justificación.

Todos los sistemas sujetos a esta PGSI deberán realizar un análisis 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 análisis de riesgos periódicos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será 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.

10.2 Criterios de evaluación de riesgos.

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.

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que adoptará el Ayuntamiento, 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 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 de carácter personal.

10.3 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 Superior Competente.

10.4 Proceso de aceptación del riesgo residual.

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

Los niveles de riesgo residual esperados 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, ISO 27001 y aquéllas complementarias que fueran precisas para el cumplimiento de LOPDGDD) deberán ser aceptados previamente por los responsables de los servicios afectados 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.

10.5 Necesidad de realizar o actualizar las evaluaciones de riesgos.

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 9 del ENS y en la norma ISO 27001 y. Este análisis 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.

11 Gestión de incidentes de seguridad

11.1 Prevención.

El Ayuntamiento de San Vicente del Raspeig 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 departamentos / unidades administrativas deben:

- Autorizar los sistemas antes de entrar en producción desde el prisma funcional, prestacional y legal.
- Evaluar regularmente la seguridad, incluyendo apreciaciones de riesgos, impulsando las iniciativas necesarias para resolver las situaciones no conformes o fuera de los márgenes de riesgo aceptables.
- Solicitar 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.

11.2 Detección.

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 el Artículo 9 del ENS y en la norma ISO 27001.

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

11.3 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 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 de carácter personal).

11.4 Recuperación.

Para garantizar la disponibilidad de los servicios y las informaciones corporativas, el Ayuntamiento de San Vicente del Raspeig desarrolla y mantiene 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.

11.5 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.

12 Gestión del personal.

12.1 Obligaciones del personal.

El personal del Ayuntamiento tiene la obligación de conocer y cumplir esta Política General de Seguridad de la Información y las Normativas y Procedimientos de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la PGSI llegue a los afectados.

El personal del Ayuntamiento asistirá a sesiones de formación y concienciación en materia de Seguridad de la Información al menos una vez al año, 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 denunciará ante las autoridades competentes las acciones que pudieran ser constitutivas de cualquier tipo de presunto delito.

12.2 Caracterización del puesto de trabajo.

El Ayuntamiento de San Vicente del Raspeig 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 San Vicente del Raspeig incluirá en su descripción de puestos de trabajo las funciones y responsabilidades en materia de seguridad de cada uno de dichos puestos.

12.3 Formación.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La asistencia a las sesiones de formación es obligatoria y su aprovechamiento podrá ser evaluado.

El Ayuntamiento de San Vicente del Raspeig elaborará anualmente un Plan de Formación, sobre el cual se realizará un seguimiento detallado, registrando todas las personas asistentes a los ciclos formativos.

12.4 Concienciación.

El Ayuntamiento de San Vicente del Raspeig 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.

13 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 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 la 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 departamentales afectados antes de seguir adelante con la contratación.

En caso de que los tratamientos desarrollados por terceras partes involucren datos de carácter personal, 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", "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.

14 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 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.

15 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:

15.1 Normas de Seguridad.

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

15.2 Procedimientos de Seguridad.

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

15.3 Instrucciones de Seguridad.

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

16 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 San Vicente del Raspeig.

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