Anuncio Política de Seguridad de la Información del Ayuntamiento de Castelló de la Plana

En virtud del acuerdo adoptado por la Junta de Gobierno Local del Ayuntamiento de Castelló de la Plana, en sesión de 24 de abril de 2025, se deja sin efecto el documento de Política de Seguridad que fue aprobado mediante acuerdo de la Junta de Gobierno Local del Ayuntamiento de Castelló de la Plana, en fecha 31 de marzo de 2022, se aprueba la Política de Seguridad de la Información del Ayuntamiento de Castelló de la Plana, en cumplimiento de lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y demás normativa concordante, como documento en el que se reflejan las directrices que rigen la forma en que el Ayuntamiento de Castelló de la Plana y sus organismos dependientes deben gestionar y proteger la información y los servicios, y se designa a los cargos unipersonales u órganos colegiados indicados en el documento de la Política de Seguridad, para ocupar los distintos roles de seguridad.

En cumplimiento del citado acuerdo, se publica el texto íntegro del documento de Política de Seguridad de la Información:

«POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN AYUNTAMIENTO DE CASTELLÓ DE LA PLANA”

CONTROL DE VERSIONES

FECHA	VERSIÓN	CAMBIOS REALIZADOS
07/12/2021	01	Edición inicial del documento
11/10/2023	02	Actualización al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
02/11/2023	03	Homogeneización
12/11/2024	04	Revisión y actualización

Ajuntament de Castelló

Sumario

1. INTRODUCCIÓN

1.1. Misión y valores de la entidad

La misión del Ayuntamiento de Castelló de la Plana es prestar los servicios públicos municipales en el ámbito de sus competencias, bajo atributos de calidad, eficaces, eficientes, fiables y seguros, con una gestión transparente, mediante el uso de las nuevas tecnologías y la Administración Electrónica, impulsando la participación y colaboración de la ciudadanía, facilitando que Castelló de la Plana sea una ciudad moderna, innovadora, emprendedora, abierta, dinámica y cohesionada territorialmente.

Los valores del Ayuntamiento de Castelló de la Plana (en adelante, el Ayuntamiento) es convertir a la Ciudad de Castelló de la Plana en un referente y modelo de ciudad que promueva la economía basada en la sostenibilidad, creatividad e innovación, y al Ayuntamiento en una administración innovadora, eficiente en la utilización de los recursos y responsable, sujeta a los principios de participación, colaboración y transparencia, que mejore el nivel de calidad y eficiencia del servicio prestado para una mayor satisfacción de ciudadanos y empresas.

2. JUSTIFICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

2.1. Necesidad de Seguridad en los Sistemas

Para el cumplimiento de su misión, la prestación de los servicios y el cumplimiento de sus objetivos, el Ayuntamiento, depende de los sistemas TIC (Tecnologías de la Información y Comunicaciones).

Estos sistemas deben ser administrados con diligencia, adoptando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan

afectar a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada o de los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria, prevenir los incidentes y reaccionar con presteza en su caso.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Es por ello que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, Esquema Nacional de Seguridad), establece en su artículo 12 que todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá de acuerdo con los principios básicos recogidos en su artículo 5, y se desarrollará aplicando los requisitos mínimos enumerados en el artículo 12.1 de la citada norma.

2.2. REQUISITOS DE SEGURIDAD EN LOS DEPARTAMENTOS

Todos los departamentos del Ayuntamiento deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 8 del Esquema Nacional de Seguridad.

3. MARCO NORMATIVO

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

4. ORGANIZACIÓN DE LA SEGURIDAD

4.1. DEFINICIÓN DE ROLES

Tal como indica el artículo 13 del Esquema Nacional de Seguridad , la seguridad deberá comprometer a todos los miembros del Ayuntamiento.

La Política de Seguridad, según detalla el Anexo II del ENS, en su sección 3.1, debe identificar los responsables de velar por su cumplimiento y ser conocida por todos los miembros del Ayuntamiento.

La responsabilidad del éxito del Ayuntamiento, en última instancia, en su Dirección. como responsable de organizar las funciones y responsabilidades, la política de

seguridad del Ayuntamiento, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

La estructura organizativa de seguridad, y jerarquía en el proceso de decisiones la componen:

Rol	Funciones
Dirección	Órganos colegiados o unipersonales que deciden la misión y los objetivos del Ayuntamiento.
Comité de Seguridad	Órganos colegiados o unipersonales que toman decisiones que concretan cómo alcanzar los objetivos marcados por los órganos de gobierno.
Responsable de la Información	A nivel de gobierno. Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por del Ayuntamiento.
Responsable de Servicio	A nivel de gobierno o, en ocasiones baja a nivel ejecutivo. Tiene la responsabilidad última de determinar los niveles de servicio aceptables por del Ayuntamiento.
Responsable de Seguridad	A nivel ejecutivo. Funciona como supervisor de la operación del sistema y vehículo de reporte al Comité de Seguridad de la Información.
Responsable del Sistema	A nivel operacional. Toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día

4.2. RESPONSABLE DE LA INFORMACIÓN

El Responsable de la Información debe ser una persona que ocupa un alto cargo en la dirección del Ayuntamiento.

Compatibilidades. Este rol únicamente podrá coincidir con el de Responsable de Servicio y el Responsable de Información en organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable del Sistema y el de Administrador de Seguridad del Sistema, aunque se trate de organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento**.**

Se ha designado responsable de la Información al Alcalde/desa del Ayuntamiento o concejal/a en el/la que delegue.

Al responsable de la información corresponden las siguientes funciones:

Función	Detalle
Establecer requisitos de seguridad sobre la información	Establece los requisitos de la información en materia de seguridad. En el marco del Esquema Nacional de Seguridad, equivale a la potestad de determinar los niveles de seguridad de la información.
Determinar niveles de seguridad en cada dimensión	Determinar los niveles de seguridad en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta del Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.
Adoptar medidas sobre los datos personales	Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten 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.
Responder del uso	Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

4.3. Responsable del servicio

El Responsable del Servicio puede ser una persona concreta o puede ser un órgano corporativo, que revestirá la forma de órgano colegiado de acuerdo con la normativa administrativa.

Compatibilidades.

Es posible que coincidan en la misma persona u órgano las responsabilidades de la información y del servicio. La diferenciación tiene sentido:

- Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
- Cuando la prestación del servicio no depende de la unidad que es Responsable de la Información.

Incompatibilidades.

Este rol no podrá coincidir con el de Responsable de Seguridad, salvo en organizaciones de reducida dimensión que funcionen de forma autónoma.

Este rol no podrá coincidir con el de Responsable de Sistema ni con el de Administrador de la Seguridad del Sistema, ni siquiera cuando se trate de organizaciones de reducida dimensión que funcionen de forma autónoma.

Se ha designado como Responsables de Servicio a las personas que ostentan el puesto de mayor responsabilidad administrativa/operativa en cada Servicio. Estos puestos figuran en la RPT anual y se mantienen actualizados vía cambios en la denominación del cargo o en la propia RPT.

Los Servicios son los siguientes:

Nombre del servicio
Alcaldía
Grupos políticos
Secretaría general
Intervención general municipal
Asesoría Jurídica
Planificación y proyección económica
Gestión presupuestaria y contabilidad
Tesorería
Gestión Tributaria
Recursos humanos
Contratación
Estadística y padrón
Atención integrada y registro general
Gestión Catastral
Policía Local
Servicio De Extinción De Incendios Y Protección Civil
Bienestar Social
Vivienda
Educación

Cultura
Archivo
Participación Ciudadana
Juventud
Igualdad
Comercio y Mercados
Urbanismo
Medio Ambiente
Aguas, Saneamiento Y Recogida De Residuos
Mantenimiento, infraestructuras y comunicaciones
Movilidad
Fiestas
Deportes
Agencia de Desarrollo Local
Turismo
Informática
Consumo
Servicios Funerarios
Familia e infancia
Sanidad
Modernización y calidad de los servicios
Gente mayor
Pacto Local para el Empleo

Las funciones e información manejadas por dichos servicios son los siguientes:

Nombre del servicio	Descripción
Alcaldía	Gestión de las agendas y la actividad de alcaldía.
Grupos políticos	Gestión de las agendas y la actividad de los

Nombre del servicio	Descripción
	grupos políticos
Secretaría general	Gestión, seguimiento y control sobre los actos municipales y los miembros de la corporación local. Gestión de expedientes relacionados con la actividad municipal
Intervención general municipal	Control y fiscalización interna de la gestión económica, financiera y presupuestaria.
Asesoría Jurídica	Defensa jurídica
Planificación y proyección económica	Identificación, solicitud, gestión y justificación de líneas de ayuda y subvenciones públicas que puedan ser de interés municipal.
Gestión presupuestaria y contabilidad	Gestión económica y contable del Ayuntamiento. Realización de pagos correspondientes, gestión de la facturación, control presupuestario y gestión fiscal.
Tesorería	Gestión de los recursos financieros, incluyendo dinero, valores o créditos por operaciones presupuestarias o extra presupuestarias.
Gestión Tributaria	Gestión de inspección y trámites relacionados con tributos y otros ingresos de derecho público
Recursos humanos	Gestión del personal interno (vacaciones, bajas, consultas, etc.). Prevención de riesgos laborales y accidentes de trabajo. Gestión y publicación de ofertas de empleo público de personal de la entidad local.

Nombre del servicio	Descripción
Contratación	Gestión de los procedimientos de contratación pública, así como el seguimiento y control de los adjudicatarios. Gestión patrimonial.
Estadística y padrón	Gestión del Padrón municipal.
Atención integrada y registro general	Gestión de la entrada de escritos o comunicaciones presentados en el Ayuntamiento, así como la salida de los escritos y comunicaciones oficiales dirigidas a otros órganos o particulares.
Gestión Catastral	Gestión de la información catastral en el marco del convenio con catastro.
Policía Local	Servicios de Policía Local incluyendo la seguridad ciudadana, seguridad de las instalaciones municipales y la regulación del tráfico, gestión del estacionamiento de vehículos y el servicio de grúa y depósito municipal.
Servicio De Extinción De Incendios Y Protección Civil	Servicios de extinción de incendios y Protección Civil.
Bienestar Social	Servicios de evaluación y orientación para personas en situaciones de necesidad social, así como la atención inmediata a personas en situación o riesgo de exclusión social. Gestión de las prestaciones y actuaciones sociales a personas y colectivos vulnerables incluyendo las relacionadas con la atención a la dependencia y la cooperación al desarrollo.

Nombre del servicio	Descripción
Vivienda	Cooperación con las administraciones con competencias en vivienda.
Educación	Cooperación con las administraciones con competencias en educación.
Cultura	Promoción de la cultura y equipamientos culturales. Gestión de la biblioteca municipal. Gestión de museos municipales.
Archivo	Organización y localización de expedientes, documentos o registros del Ayuntamiento que han pasado al Archivo Municipal. Gestión de las consultas, copias y préstamos de documentos del Archivo Municipal. Conservación y consulta de los documentos recibidos y producidos por la entidad local.
Participación Ciudadana	Procesos participativos. Gestión de entidades ciudadanas y voluntariado del municipio. Publicidad activa y derecho de acceso a la información. Gestión de solicitudes de información, quejas, reclamaciones e iniciativas recibidas en el Ayuntamiento.
Juventud	Asesoramiento e información a la población joven del municipio, así como la realización de actividades y eventos enfocados a este colectivo.
Igualdad	Promoción de la igualdad entre hombres y mujeres, así como contra la violencia de género.
Comercio y Mercados	Ferias, abastos, mercados, lonjas y comercio

Nombre del servicio	Descripción
	ambulante.
Urbanismo	Tramitación y resolución de solicitudes, autorizaciones y licencias de obras. Gestión de desarrollos urbanístico y obras públicas.
Medio Ambiente	Mantenimiento de parques y jardines públicos. Gestión de la limpieza de viaria. Promoción, prevención e inspecciones relacionadas con la contaminación acústica, lumínica y atmosférica.
Aguas, Saneamiento Y Recogida De Residuos	Gestión y control de los servicios municipales de aguas y saneamiento y recogida de basuras.
Mantenimiento, infraestructuras y comunicaciones	Mantenimiento de la vía pública e instalaciones municipales.
Movilidad	Gestión del Tráfico, estacionamiento de vehículos y movilidad. Transporte colectivo urbano.
Fiestas	Promover, fomentar organizar las Fiestas de la Ciudad de Castelló de la Plana cuya organización correspondan al Excmo. Ayuntamiento de Castelló de la Plana y colaborar y asesorar en la celebración de otras fiestas que se organicen en la Ciudad por asociaciones, entidades, calles y barrios etc., siempre que tales fiestas tengan carácter público.
Deportes	Gestión de instalaciones deportivas y promoción del deporte en la entidad local.

Nombre del servicio	Descripción
Agencia de Desarrollo Local	Orientación laboral. Subvenciones de empleo. Emprendimiento.
Turismo	Promoción de la entidad local mediante la organización de diversas actividades, así como la promoción del turismo.
Informática	Gestión y control de los sistemas informáticos y de comunicaciones del Ayuntamiento, así como la gestión de la seguridad de los mismos. WIFI público. Gestión de las obligaciones en materia de protección de datos.
Consumo	Servicios de mediación en materia de consumo.
Servicios Funerarios	Gestión del cementerio municipal y de los servicios funerarios.
Familia e infancia	Atención preventiva e integral de menores y sus familias. En esta línea el Negociado de Familia e Infancia se orienta a la gestión de los servicios, recursos y proyectos municipales dirigidos al apoyo a familias y destinados a la prevención y abordaje de situaciones de riesgo social y a la promoción de la convivencia familiar.
Sanidad	Información de sanidad. Gestión de tenencia de animales.
Modernización y calidad de los servicios	Gestión y mejora de la calidad en los servicios municipales.
Gente mayor	Asesoramiento e información a la gente mayor del municipio, así como la realización de

Nombre del servicio	Descripción
	actividades y eventos enfocados a este colectivo.
Pacto Local	Formación, intermediación y observatorio socioeconómico en materia de empleo.

Las funciones del/los/las Responsable/s del Servicio son las siguientes:

Función	Detalle
Responsabilidad	Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
Establecer los requisitos de seguridad del servicio	Tiene la potestad de establecer los requisitos del servicio en materia de seguridad o, en terminología del Esquema Nacional de Seguridad, la potestad de determinar los niveles de seguridad de los servicios. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
Riesgos	Aprobar el riesgo residual (el resultante una vez aplicados los controles de seguridad).
Gestionar los Registros de actividad de los tratamientos del RGPD	Por delegación del Responsable de tratamiento se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión de los tratamientos de datos personales que se realizan en su área en concreto.

Consideraciones. El Responsable del Servicio deberá tener en cuenta las siguientes consideraciones:

- La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.
- Sigue siendo válido el/la responsable de cada Servicio aunque su nomenclatura no coincida exactamente con la indicada en esta tabla-relación, siempre y cuando sus funciones, roles y responsabilidades no hayan variado.

4.4. RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

El Responsable de Seguridad de la Información es una figura clave, ya que a él le corresponde dinamizar y gestionar el día a día de todo el proceso de seguridad de la información.

Se ha designado como Responsable de Seguridad de la Información a el/la Jefe/a de la Sección de Innovación y Desarrollo Tecnológico (SIDT).

Las **funciones** del Responsable de Seguridad son las siguientes:

Función	Detalle
Política, Normativa y Procedimientos	• Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política y Normativa de Seguridad de la Información, para su aprobación por Dirección. • Elaborará y someterá a la aprobación del Comité los Procedimientos Operativos de Seguridad de la Información.
Documento de Seguridad	• Coordinará y controlará las medidas definidas en el Documento de Seguridad y en general se encargará del cumplimiento de las medidas de seguridad que detalla el reglamento de desarrollo de la LOPD. • Coordinará la elaboración de la Documentación de Seguridad del Sistema.
Formación y concienciación	• Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. • 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
Gestión de la Seguridad	• 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 la Política de Seguridad del Ayuntamiento. • Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema. • Realizará el 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 Esquema Nacional de Seguridad. • Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del Esquema Nacional de Seguridad y del resultado del Análisis de Riesgos. • Elaborará, junto al Responsable del Sistema, el Plan de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información. • Validará los Planes de Continuidad de Sistemas que elabore el Responsable del Sistema, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable del Sistema. • Aprobará las directrices propuestas por el Responsable del 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. • Elaborar la memoria anual sobre el estado de la seguridad de la información, con el progreso de los proyectos de los planes de mejora, resumen de las actuaciones en materia de seguridad, de los incidentes relativos a seguridad de la información, del estado de la seguridad del sistema, y en particular del nivel de riesgo residual al que está expuesto el sistema.
Monitorizar	• Monitorizará los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos. • Monitorizará el desempeño de los procesos de gestión de incidentes de seguridad y recomendará posibles actuaciones respecto de ellos. En particular, velará por la

	coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
Asesoramiento	• Asesorará a otros responsables en la determinación de las medidas de seguridad necesarias a partir de los requisitos de seguridad establecidos por el contexto interno y externo del ámbito del Ayuntamiento.
Comité de Seguridad.	• 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).

Delegación de funciones

En caso de que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad, se podrá designar cuantos Responsables de Seguridad Delegados considere necesarios.

La designación corresponde al Responsable de la Seguridad. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable de la Seguridad.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad. Es habitual que se encarguen de la seguridad de sistemas de información concretos o de sistemas de información horizontales.

Cada delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reportan.

4.5. RESPONSABLE DEL SISTEMA

El/la Responsable del Sistema es la persona que toma las decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.

Compatibilidades. Este rol podrá coincidir con el de Administrador de Seguridad del Sistema en organizaciones de una dimensión reducida o intermedia que tengan una estructura autónoma de funcionamiento.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Información, con el de Responsable de Servicio ni con el de Responsable de Seguridad Corporativa o de la Información.

Se ha designado como Responsable del Sistema el/la Jefe/a del Negociado de Sistemas y Seguridad Informática.

Las funciones del/la Responsable del Sistema son las siguientes:

Función	Detalle
Gestionar el Sistema	• Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. • Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. • 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.
Establecer directrices y medidas	• Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. • Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema. • Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo. • Determinar la configuración autorizada de hardware y software a utilizar en el Sistema. • Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
Elaborar	• Elaborar procedimientos operativos de seguridad. • Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
Aprobar	• Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema. • Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
Monitorizar	• Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la

	Información.

Delegación de funciones.

En caso de que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, se podrá designar cuantos Responsables del Sistema Delegados considere necesarios.

La designación corresponde al Responsable del Sistema. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable del Sistema.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de información. Es habitual que se encarguen de subsistemas de información de cierta envergadura o de sistemas de información que presten servicios horizontales.

4.6. ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA.

El Administrador de seguridad es la persona encargada de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.

Se han designado como Administrador/es de la Seguridad del Sistema a los/las Técnicos/as del Negociado de Sistemas y Seguridad Informática junto con el/la Técnico/a en Seguridad de la Información.

Las funciones del Administrador de la Seguridad del Sistema son las siguientes:

Función	Detalle
Implementar, gestionar y mantener la seguridad	• La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información. • Asegurar que los controles de seguridad establecidos son cumplidos estrictamente. • Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad. • Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
Gestión,	• La gestión, configuración y actualización, en su caso, del

configuración y actualización	hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información. • Aprobar los cambios en la configuración vigente del Sistema de Información. • Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
Gestión de las autorizaciones	• La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
Aplicar los procedimientos	• La aplicación de los Procedimientos Operativos de Seguridad. • Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
Monitorizar la seguridad	• Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

4.7. RESPONSABLE DE SEGURIDAD FÍSICA

Cuando la seguridad física (de las instalaciones) esté segregada de la seguridad lógica, esta se ajustará a lo establecido por el Esquema Nacional de Seguridad en materia de protección física de forma análoga a lo establecido en los puntos anteriores.

El Responsable de la Seguridad Física implantará las medidas de seguridad que le competan dentro de las determinadas por el Responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

Se ha designado como Responsable de Seguridad Física al/la Comisario/a Principal/Jefe/a Policía Local.

4.8. RESPONSABLE DE GESTIÓN DEL PERSONAL

Se ha designado como responsable de Gestión de Personal al/la Jefe/a de la Sección de Gestión y Desarrollo de RR.HH. a quien le corresponde implantar las medidas de seguridad que le competan dentro de las determinadas por el Esquema Nacional de

Seguridad colaborando con éste en su implantación, eficacia y resolución de incidentes.

4.9. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Se ha creado el Comité de Seguridad de la Información que estará compuesto por los siguientes miembros:

PRESIDENTE/A: Alcalde/sa (que actuará como Responsable de Información o concejal/a en quien delegue)

SECRETARIO/A: Responsable de Seguridad de la Información.

VOCALES PERMANENTES:

- Secretario/a General de la Administración Municipal.
- Titular de Asesoría Jurídica.
- Responsable del Sistema
- Responsable de Seguridad de la información (actuará como Secretario del Comité)
- Responsable de Seguridad Física.
- Delegado/a de Protección de Datos.
- Jefe del servicio de Mantenimiento, infraestructuras y comunicaciones.

OTROS VOCALES:

- Responsables de Servicio (serán convocados/as según lo requieran los temas a tratar).

Funciones del Secretario/a. 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.

Funciones de los Vocales. Corresponde a los vocales del Comité de Seguridad de la Información:

- Participar en las reuniones.
- Contribuir con ideas y sugerencias para el buen desarrollo de las reuniones.

Todos miembros del Comité actuarán con voz y voto y sus acuerdos requerirán, como mínimo, el voto de la mayoría simple de sus miembros.

Funciones del Comité. Corresponde al Comité de Seguridad de la Información:

Función	Detalle
Informar	• Atender las inquietudes de Dirección del Ayuntamiento y de los diferentes departamentos/áreas. • Informar regularmente del estado de la seguridad de la información a la Dirección del Ayuntamiento.
Promover	• Promover la mejora continua del Sistema de Gestión de la 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.
Coordinar	• 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. • 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.
Elaborar	• Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección. • Elaborar la estrategia de evolución del Ayuntamiento en lo que respecta a la seguridad de la información.
Aprobar	• Aprobar la normativa de seguridad de la información. • Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información • 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.
Controlar	• 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. • Velar para que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su

		especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

Para dotar de mayor agilidad al Comité, se creará una comisión operativa de carácter técnico, que ejercerá las funciones ejecutivas. Esta comisión estará formado por el Responsable de Seguridad de la Información y por dos Administradores de Seguridad y mantendrá reuniones de carácter mensual. A estas reuniones podrán acudir asesores externos invitados por la comisión.

4.9.1. 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: el Comité de Seguridad de la Información da instrucciones al Responsable de la Seguridad de la Información que se encarga de cumplimentar, supervisando qué administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada por el Ayuntamiento.

El/la **Responsable de la Seguridad**:

- Informa al/la 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.
- Informa al/la 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.
- Da cuenta 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.
- Da cuenta a la Junta de Gobierno Local, 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.

El **Responsable del Sistema**:

- Informa al/la Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
- Informa al/la Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.
- Da cuenta al/la 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.

4.9.2. Procedimientos de designación de personas

La Dirección del Ayuntamiento nombrará formalmente mediante su publicación en el Boletín Oficial correspondiente:

- Al/la Responsable de la Información; puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).
- Al/la Responsable del Servicio; puede ser el mismo que el Responsable de la Información; puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).
- Al/la Responsable de la Seguridad, que debe reportar directamente a la Dirección o, cuando existan, a los comités de seguridad de la información y seguridad corporativa.
- Al/la Responsable del Sistema, que debe reportar directamente a la Dirección o, cuando existan, a los comités de seguridad de la información y seguridad corporativa.

La Dirección de la Organización designa a la persona Responsable del Sistema:

- A propuesta del/la Responsable de la Información tratada, cuando el Sistema de información trate una única información.
- A propuesta del/la Responsable del Servicio prestado, cuando el Sistema de información preste un único servicio.
- Directamente cuando el Sistema de información trata diferentes informaciones o presta diferentes servicios, oídos los responsables de las informaciones y los servicios afectados.

La Dirección del Ayuntamiento designa al/la Administrador de Seguridad del Sistema a propuesta del/la Responsable del Sistema.

5. GESTIÓN DE RIESGOS

5.1. Justificación

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

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 7.

5.2. 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 elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos.

5.3. 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, promoviendo inversiones de carácter horizontal.

5.4. Proceso de Aceptación del Riesgo Residual

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

Los niveles de Riesgo residual esperados sobre cada Información tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del Esquema Nacional de

Seguridad) deberán ser aceptados previamente por su Responsable de esa Información.

Los niveles de Riesgo residual esperados sobre cada Servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del Esquema Nacional de Seguridad) deberán ser aceptados previamente por su Responsable de ese Servicio.

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.

5.5. 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 10 del Esquema Nacional de Seguridad. 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.

6. GESTIÓN DE INCIDENTES DE SEGURIDAD

6.1. Prevención de incidentes

Los departamentos del Ayuntamiento deben prevenir que la información o los servicios se vean perjudicados por incidentes de seguridad.

El Esquema Nacional de Seguridad establece la que los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. De igual forma, el artículo 18 del Esquema Nacional de Seguridad define que los sistemas de instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el Esquema Nacional de Seguridad, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos

controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Establecer áreas seguras para los sistemas de información crítica o confidencial.
- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

6.2. Monitorización y detección de incidentes

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios 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 10 del Esquema Nacional de Seguridad.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del Esquema Nacional de Seguridad. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos del Ayuntamiento , verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.

Se deberán establecer, en función de las necesidades, las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel sistema.
- Sistemas de detección de intrusos a nivel físico

6.3. Respuesta ante incidentes

Los departamentos del Ayuntamiento deben:

- 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).

6.4. Recuperación ante incidentes y planes de continuidad

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

7. OBLIGACIONES DEL PERSONAL

Los empleados/as del Ayuntamiento tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Los empleados/as del Ayuntamiento atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un programa de concienciación continua para atender a los miembros de la organización, en particular a los de nueva incorporación.

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

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos la organización, constituyendo su incumplimiento infracción grave a efectos laborales.

8. 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 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.

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.

Cuando 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 de la información y los servicios afectados antes de seguir adelante.

9. ESTRUCTURA NORMATIVA Y DESARROLLO DE LA POLÍTICA DE SEGURIDAD

La estructura jerárquica de la documentación de seguridad es la siguiente:

Documento	Detalle
Política	• Define las metas y expectativas de seguridad. • Describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos. • Debe ser elaborada por el Comité de Seguridad y ser aprobada por la Dirección.
Normativa	• Establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema. • Es de carácter obligatorio. • Debe ser escrita por personas expertas en la materia o por el Responsable de Seguridad y aprobada por el Comité de Seguridad.
Procedimiento	• Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar. • Un procedimiento puede apoyarse en otros documentos para especificar, con el nivel de detalle que se desee, las diferentes tareas. Para ello, puede relacionarse con otros

	procedimientos o con instrucciones técnicas de seguridad. • Debe ser elaborado por el Responsable del Sistema y aprobado por el Responsable de Seguridad.
Instrucciones técnicas	• Determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.). • Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar. • Una instrucción técnica debe ser clara y sencilla de interpretar. • Debe documentar los aspectos técnicos necesarios para que la persona que ejecute la instrucción técnica no tenga que tomar decisiones respecto a la ejecución de la misma. A mayor nivel de detalle, mayor precisión y garantía de su correcta ejecución. • Pueden ser elaborados por el Responsable del Sistema o Administrador del Sistema y deben ser aprobados por el Responsable de Seguridad.
Guías	• Tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. • Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas. • Deben ser aprobadas por el Responsable de Seguridad.

10. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política 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 la Junta de Gobierno Local, de acuerdo con el artículo 12 del Esquema Nacional de Seguridad.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

11. ANEXO. GLOSARIO DE TÉRMINOS

Análisis de riesgos

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal

Cualquier información concerniente a personas físicas identificadas o identificables.

Gestión de incidentes

Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Política de seguridad

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos.

Principios básicos de seguridad

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema

Persona que se encarga de la explotación del sistema de información.

Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición.”

Castelló de la Plana
El Jefe de Sección de Innovación y Desarrollo Tecnológico,
David López López
(Documento firmado electrónicamente)