MUNICIPIOS

Ayuntamiento de Tavernes de la Valldigna

2025/12494 *Anuncio del Ayuntamiento de Tavernes de la Valldigna sobre la aprobación definitiva de la modificación del Reglamento Regulador de la Política de Seguridad de la Información. Expediente 2297743K – Interno: 003250008.*

ANUNCIO

Para hacer público que, por Resolución de la Concejalía delegada en materia de personal, nuevas tecnologías, cultura, fiestas, educación y relaciones con los grupos políticos n.º.3251 de 14 de octubre de 2025, se ha elevado a definitiva la aprobación de la modificación de la Política de Seguridad de la Información del Ayuntamiento, con el texto siguiente:

VER ANEXO

Lo cual se hace pública a los efectos del que dispone el artículo 131 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Tavernes de la Valldigna, 16 de octubre de 2025.—El concejal-delegado, Emilio Fonseca Martí.

VERSIÓN 1.0 **Redacción vigente**	**VERSIÓN 1.1** **Modificaciones**
2. INTRODUCCIÓN 3r párrafo: *Precisamente, el Real Decreto 3/2010, de 8 de enero, de Despliegue del Esquema Nacional de Seguridad, fija los principios básicos y requisitos mínimos, además de las medidas de protección para implantar en los sistemas de la administración.*	2.INTRODUCCIÓN 3r párrafo *Precisamente, el Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad, fija los principios básicos y requisitos mínimos, además de las medidas de protección para implantar en los sistemas de la administración.*
8º párrafo: *Los departamentos tienen que estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 7 del ENS.*	8º párrafo: *Los departamentos tienen que estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 8 del ENS.*
2.2 Detección *Dado que los servicios se pueden degradar rápidamente a causa de incidentes, que van desde una simple desaceleración hasta la detención, los servicios tienen que monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según el artículo 9 del ENS. La monitorización es especialmente relevando cuando se establecen líneas de defensa de acuerdo con el artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y repuerto que reúnen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan establecido como normales.*	2.2 Detección *Dado que los servicios se pueden degradar rápidamente a causa de incidentes, que van desde una simple desaceleración hasta la detención, los servicios tienen que monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según el artículo 10 del ENS. La monitorización es especialmente relevando cuando se establecen líneas de defensa de acuerdo con el artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y repuerto que reúnen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan establecido como normales.*
5. MARCO NORMATIVO *La normativa básica a que se sujeta la acción del Ayuntamiento es la siguiente:* *- Carta Europea de Autonomía Local. Hecho en Estrasburgo el 15 de octubre de 1985.*	*5. MARCO NORMATIVO* *La normativa básica a que se sujeta la acción del Ayuntamiento es la siguiente:* *- Carta Europea de Autonomía Local. Hecho en Estrasburgo el 15 de octubre de 1985.*

- Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local. *- Real decreto legislativo 781/1986, de 18 de abril, por el cual se aprueba el texto refundido de las Disposiciones Legales Vigentes en Materia de Régimen Local.* *- Ley 8/2010, de 23 de junio, de Régimen Local de la Comunidad Valenciana.* *- Real Decreto 2568/1986, de 28 de noviembre, por el cual se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.* *Hay que hacer constar que en la administración local las decisiones ejecutivas en materia de asignación de recursos humanos, materiales y financieros recaen en el ámbito de las competencias de los órganos decisorios (ayuntamiento pleno, alcalde, regidores delegados y junta de gobierno local), de forma que la responsabilidad última en la toma de decisiones corresponde a estos.*	*- Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local.* *- Real decreto legislativo 781/1986, de 18 de abril, por el cual se aprueba el texto refundido de las Disposiciones Legales Vigentes en Materia de Régimen Local.* *- Ley 8/2010, de 23 de junio, de Régimen Local de la Comunidad Valenciana.* *- Real Decreto 2568/1986, de 28 de noviembre, por el cual se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.* *Hay que hacer constar que en la administración local las decisiones ejecutivas en materia de asignación de recursos humanos, materiales y financieros recaen en el ámbito de las competencias de los órganos decisorios (ayuntamiento pleno, alcalde, regidores delegados y junta de gobierno local), de forma que la responsabilidad última en la toma de decisiones corresponde a estos..* ***- Específicamente, toda la normativa aplicable figurará en el correspondiente registro, el cual será objeto de actualización sin necesidad de modificar esta Política y que estará disponible por su consulta en la Sede electrónica y en el Portal de Transparencia del Ayuntamiento.***
6. ORGANIZACIÓN DE LA SEGURIDAD 6.1. Comité de Seguridad de la Información (CSI): composición, funciones i responsabilidades 7º párrafo: *El administrador de seguridad del sistema (ASS): los titulares de los puestos de trabajo A011, A013 y A020. En el ejercicio de esas responsabilidades, están facultados por el CSI para acceder a todos los sistemas y aplicaciones, con los permisos y privilegios adecuados, a fin de verificar la implantación de las medidas aprobadas por el CSI y efectuar las*	6. ORGANIZACIÓN DE LA SEGURIDAD 6.1. Comité de Seguridad de la Información (CSI): composición, funciones i responsabilidades 7º párrafo: El administrador de seguridad del sistema (ASS): los titulares de los puestos de trabajo A011, A013, A020 y A021. En el ejercicio de esas responsabilidades, están facultados por el CSI para acceder a todos los sistemas y aplicaciones, con los permisos y privilegios adecuados, a fin de verificar la implantación de las medidas aprobadas por el CSI y efectuar las comprobaciones necesarias. Se tiene

comprobaciones necesarias. Se tiene que dar cuenta al CSI del resultado de esas medidas.	que dar cuenta al CSI del resultado de esas medidas.
10. DATOS DE CARÀCTER PERSONAL. EVALUACIÓN DE IMPACTO 5º párrafo: *En cualquier caso, la evaluación de impacto se tiene que integrar en el análisis de riesgos a que se refiere el arte. 13 del ENS, de acuerdo con los criterios derivados de los artes. 25 y 32 delRGPD.*	*10. DATOS DE CARÀCTER PERSONAL. EVALUACIÓN DE IMPACTO* *5º párrafo:* *En cualquier caso, la evaluación de impacto se tiene que integrar en el análisis de riesgos a que se refiere el arte. 14 del ENS, de acuerdo con los criterios derivados de los artes. 25 y 32 delRGPD*
11. GESTIÓN DE RIESGOS 1º párrafo: *Todos los sistemas sujetos a esta Política tienen que hacer un análisis de riesgos, de acuerdo con el arte. 13 y concordantes del ENS, que evalúo las amenazas y los riesgos a que están expuestos. Esta análisis hay que repetirla:*	11. GESTIÓN DE RIESGOS 1º párrafo: *Todos los sistemas sujetos a esta Política tienen que hacer un análisis de riesgos, de acuerdo con el arte. 14 y concordantes del ENS, que evalúo las amenazas y los riesgos a que están expuestos. Esta análisis hay que repetirla:*
12. DESPLIEGE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN *Esta Política se desarrollará mediante la normativa de seguridad que afronto aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesitan conocerla, en particular los que usen, operan o administran los sistemas de información y comunicaciones.* *La normativa de seguridad estará disponible en la intranet http://intranet/intranet/index.php y en la sede electrònica del Ayuntamiento https://tavernesdevalldigna.sede.dival.es/*	*12. DESPLIEGE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN* *Esta Política se desarrollará mediante la normativa de seguridad que afronto aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesitan conocerla, en particular los que usen, operan o administran los sistemas de información y comunicaciones.* *La normativa de seguridad estará disponible en la intranet http://intranet/intranet/index.php y en la sede electrònica del Ayuntamiento https://tavernesdevalldigna.sede.dival.es/* ***Los procedimientos e instrucciones técnicas que se aprueban en ejecución de la presente Política estarán disponibles en los lugares citados en el párrafo anterior.***
15. DISPOSICIÓN FINAL 2º párrafo:	15. DISPOSICIÓ FINAL 2º párrafo:

Por lo tanto, antes tienen que adoptarse las medidas necesarias para elaborar la auditoría de seguridad a que se refiere el arte. 34 del ENS, por medio de la contratación del servicio consistente a definir los detalles del sistema hasta un nivel que proporciono evidencias suficientes y relevantes, dentro del alcance establecido para la auditoría.	*Por lo tanto, antes tienen que adoptarse las medidas necesarias para elaborar la auditoría de seguridad a que se refiere el arte. 31 del ENS, por medio de la contratación del servicio consistente a definir los detalles del sistema hasta un nivel que proporciono evidencias suficientes y relevantes, dentro del alcance establecido para la auditoría..*
16. ANEXO A. GLOSSARIO DE TÉRMINOS Y ABREVIATURAS Último párrafo: *RD **3/2010*** *Real Decreto 3/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Seguridad en el Ámbito de la Administración Electrónica.*	16. ANEXO A. GLOSSARIO DE TÉRMINOS Y ABREVIATURAS Último párrafo: *RD 311/2022* ***Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad**.*
17. ANEXO B. REFERENCIAS *CCN-STIC-402* *Organización y Gestión para la Seguridad de los Sistemas TIC. Diciembre 2006.* *CCN-STIC-801* *ENS - Responsables y funciones. 2010.* *CCN-STIC-805* *ENS - Política de Seguridad de la Información. 2011.* *Ley 39/2015* *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.* *Ley 40/2015* *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.*	*17. ANEXO B. REFERENCIAS* *CCN-STIC-402* *Organización y Gestión para la Seguridad de los Sistemas TIC. Diciembre 2006.* *CCN-STIC-801* *ENS - Responsables y funciones. 2010.* *CCN-STIC-805* *ENS - Política de Seguridad de la Información. 2011.* *Ley 39/2015* *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.* *Ley 40/2015* *Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.* ***Real Decreto 203/2021*** ***Real Decreto 203/2021, de 30 de marzo, por el cual se aprueba el Reglamento de actuación y***

CARTA EUROPEA De AUTONOMÍA LOCAL *Carta Europea de Autonomía Local. Hecho en Estrasburgo el 15 de octubre de 1985.* *Ley 7/1985* *Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.* *Ley 15/1999* *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE de 14 de diciembre de 1999.* *RD 1720/2007* *Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de Despliegue de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE de 19 de enero de 2008.* *RD 3/2010* *Real Decreto 3/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Seguridad en el Ámbito de la Administración Electrónica.*	***funcionamiento del sector público por medios electrónicos.*** *CARTA EUROPEA De AUTONOMÍA LOCAL* *Carta Europea de Autonomía Local. Hecho en Estrasburgo el 15 de octubre de 1985.* *Ley 7/1985* *Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.* *Ley 15/1999* *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE de 14 de diciembre de 1999.* *RD 1720/2007* *Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de Despliegue de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE de 19 de enero de 2008.* *RD 311/2022* *Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad.*

ANEXO: TEXTO REFUNDIDO DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE TAVERNES DE LA VALLDIGNA

«POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN VERSIÓN 2 (EXP. 1063215N– INTERNO: 003220023 – ENS_POL_01_PSI_V2**)**

Título:	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN VERSIÓN 2
Tipo de documento:	Normativa
Nombre del fichero:	003220023.018 ORG.1 POL_01_PSI_V2
Clasificación:	Normativa

Control de cambios

Versión	Fecha	Autor	Descripción del cambio
1.0	04/10/2018	Ayuntamiento en Pleno	Versión Inicial
1.1	28/07/2025	Ayuntamiento en Pleno	Versión 1.1

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por acuerdo de 28 de julio de 2025 del Ayuntamiento en pleno, elevado a definitivo por Resolución n.º 3251, de 14 de octubre de 2025.

Esta Política de Seguridad de la Información es efectiva desde esa fecha hasta que la reemplazo una nueva política.

Este texto deroga el anterior, elevado a definitivo por Resolución de la concejalía delegada en materia de nuevas tecnologías n.º 3351/2018, de 4 de octubre de 2018.

2. INTRODUCCIÓN

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC) en todos los ámbitos de la sociedad ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y dónde hay ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la Ley 40/2015, del 1.º de octubre, de Régimen Jurídico del Sector Público (LRJSP), que en el arte. 156.2 indica que el Esquema Nacional de Seguridad (ENS) tiene como finalidad establecer la política de seguridad en el uso de medios electrónicos en el ámbito de esta Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Precisamente, el Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad, fija los principios básicos y requisitos mínimos, además de las medidas de protección para implantar en los sistemas de la administración.

El Ayuntamiento depende de los sistemas TIC (tecnologías de información y comunicaciones) para lograr sus objetivos. Estos sistemas se tienen que administrar con diligencia, tomando las medidas adecuadas para protegerlos contra daños accidentales o deliberados que puedan afectar la disponibilidad, integridad o confidencialidad de la información tratada o los servicios proporcionados.

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 y reaccionante con celeridad ante los incidentes.

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

Los diferentes departamentos se tienen que cerciorar que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde la concepción hasta la 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 se tienen que identificar e incluir en la planificación, en la solicitud de ofertas y en pliegos de licitación para proyectos de TIC o servicios que afectan los sistemas de información.

Los departamentos tienen que estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 8 del ENS.

2.1. Prevención

Los departamentos tienen que evitar o, cuando menos, prevenir tanto como sea posible que la información o los servicios se vean perjudicados por incidentes de seguridad. Para hacerlo, tienen que implementar las medidas mínimas de seguridad determinadas por el ENS, y también cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los papeles y responsabilidades de seguridad de todo el personal, tienen que estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos tienen que:

- Autorizar los sistemas antes de entrar en operación.

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración llevados a cabo de forma rutinaria.

- Solicitar la revisión periódica por parte de terceros a fin de obtener una evaluación independiente.

2.2. Detección

Como que los servicios se pueden degradar rápidamente a causa de incidentes, que van desde una simple desaceleración hasta la detención, los servicios tienen que monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según el artículo 10 del ENS.

La monitorización es especialmente relevando cuando se establecen líneas de defensa de acuerdo con el artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y repuerto que reúnen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan establecido como normales.

2.3. Respuesta

Los departamentos tienen que:

- Establecer mecanismos para responder eficazmente en los incidentes de seguridad.

- Designar un punto de contacto para las comunicaciones 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).

2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos tienen que llevar a cabo planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

Esta política se aplica a todos los sistemas de información del Ayuntamiento, a todas las personas que forman parte de la organización, sin excepciones y a los prestamistas de servicios o proveedores de soluciones TIC del Ayuntamiento.

4. MISIÓN

Los objetivos de servicio del Ayuntamiento se concretan en el ejercicio de las competencias que la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local, le atribuye en los artículos 25 y 26, en función de la población y sin perjuicio

de las competencias que, en materia de administración electrónica, el arte. 36.1.g) de esa Ley atribuye a las diputaciones provinciales, así como el resto de competencias atribuidas por la legislación sectorial.

En materia de seguridad, los objetivos que el Ayuntamiento pretende garantizar con esta política de seguridad son los siguientes:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.

- Implementar medidas de seguridad en función del riesgo.

- Formar y concienciar los integrantes del Ayuntamiento respecto de la seguridad de la información. Implementar medidas de seguridad que permiten la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de los usuarios en relación con la información que conocen en el desempeño de sus funciones.

- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentran en áreas seguras, protegidos por controles de acceso, atendidos los riesgos detectados.

- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, para conseguir que la información transmitida a través de redes de comunicaciones sea adecuadamente protegida.

- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, a fin de garantizar la seguridad por defecto.

- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.

- Gestionar los incidentes de seguridad para una correcta detección, contención, mitigación y resolución, y adoptar las medidas necesarias porque no vuelven a producirse.

- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.

- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorante y corrigiendo las ineficiencias detectadas.

5. PRINCIPIOS RECTORES DE LA POLÍTICA

- Alcance estratégico: la seguridad de la información tiene que contar con el compromiso y apoyo de todos los niveles de la entidad y tendrá que coordinarse e integrarse con el resto de las iniciativas estratégicas de manera coherente.

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

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

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

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

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

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

- Diferenciación de responsabilidades. En aplicación de este principio las funciones del responsable de la seguridad y del responsable del sistema estarán diferenciadas.

6. MARCO NORMATIVO

La normativa básica a que se sujeta la acción del Ayuntamiento, con carácter general, es la siguiente:

- Carta Europea de Autonomía Local. Hecho en Estrasburgo el 15 de octubre de 1985.

- Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local.

- Real decreto legislativo 781/1986, de 18 de abril, por el cual se aprueba el texto refundido de las Disposiciones Legales Vigentes en Materia de Régimen Local.

- Ley 8/2010, de 23 de junio, de Régimen Local de la Comunidad Valenciana.

- Real Decreto 2568/1986, de 28 de noviembre, por el cual se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

- Real Decreto 4/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

- Real Decreto 203/2021, de 30 de marzo, por el cual se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

- Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad.

Hay que hacer constar que en la administración local las decisiones ejecutivas en materia de asignación de recursos humanos, materiales y financieros recaen en el ámbito de las competencias de los órganos decisorios (ayuntamiento lleno, alcalde, regidores delegados y junta de gobierno local), de forma que la responsabilidad última en la toma de decisiones corresponde a estos.

Específicamente, toda la normativa aplicable figurará en el correspondiente registro, el cual se actualizará sin necesidad de modificar esta Política y que estará disponible para consulta en la sede electrónica y en el Portal de Transparencia del Ayuntamiento.

7. ORGANIZACIÓN DE LA SEGURIDAD

7.1. Comité de Seguridad de la Información (CSI): composición, funciones y responsabilidades

Composición:

El Comité de Seguridad TIC está formado por:

- El responsable de la información (RINFO): el alcalde o regidor delegado con competencias en TIC.

- El responsable del servicio (RSERV): el alcalde y los regidores delegados situados al frente de cada área municipal y, dependiendo jerárquicamente y funcionalmente de ellos, los jefes de unidad, servicio y actividad.

- El responsable de seguridad (RSEG): el titular del puesto de trabajo A010.

- El responsable de sistemas (RSIS): el titular del puesto de trabajo A011, encargado de sistemas de la información, con atribuciones en materia de sistemas.

- el administrador de seguridad del sistema (ASS): los titulares de los puestos de trabajo A011, A013, A020 y A021. En el ejercicio de esas responsabilidades, están facultados por el CSI para acceder a todos los sistemas y aplicaciones, con los permisos y privilegios adecuados, a fin de verificar la implantación de las medidas aprobadas por el CSI y efectuar las comprobaciones necesarias. Se tiene que dar cuenta al CSI del resultado de esas medidas.

- El delegado de protección de datos (DPD) (colegiado).

- El titular del puesto de trabajo A002, encargado de transparencia y protección de datos.

- El secretario del Ayuntamiento.

- El jefe de la Policía como responsable de seguridad física.

- El jefe del Departamento de Recursos Humanos como responsable de la gestión de personal.

- El interventor del Ayuntamiento.

- El tesorero del Ayuntamiento.

- El jefe de la Sección de Contratación.

- El jefe de la Sección de Urbanismo y Medio Ambiente.

El secretario del Comité de Seguridad TIC es el titular del lugar A013 y tendrá como funciones hacer las convocatorias, preparar la documentación, levantar actas de las reuniones y documentar los acuerdos, además de trasladar las instrucciones necesarias a los responsables de cada unidad organizativa, verificar el cumplimiento e informar el CSI de cualquier incidencia que se produzca en el curso de las actividades encomendadas por el CSI. Cualquier discrepancia o impedimento a su actuación por parte de los responsables de las unidades organizativas se tiene que hacer saber inmediatamente al CSI, que tiene que adoptar las medidas oportunas para garantizar el cumplimiento de sus recomendaciones, instrucciones, medidas o, en su defecto, proponer la apertura de expedientes disciplinarios y de responsabilidad patrimonial.

El Comité de Seguridad TIC tiene que hacer el repuerto en el Ayuntamiento en pleno, Alcaldía, concejalía delegada con competencias en TIC y, si procede, a la Junta de Gobierno Local, como órganos competentes para adoptar acuerdos y resoluciones.

Es misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento. La Política lo aprueba el Ayuntamiento lleno y se difunde porque la conozcan todas las partes afectadas.

Además, veáis el punto 7, «Funciones y responsables».

7.2 Responsable de la información (RINFO)

El alcalde o regidor delegado con atribuciones en materia de TIC.

Tiene la responsabilidad última del uso que se haga de una información concreta y, por lo tanto, de su protección. Es el responsable último de cualquier error o negligencia que conduzca a un incidente de confidencialidad o de integridad. Tiene la potestad de establecer los requisitos de la información en materia de seguridad, es decir, de determinar los niveles de seguridad de la información.

Además, veáis el punto 7, «Funciones y responsables».

7.3 Responsable del servicio (RSERV)

El alcalde y los regidores delegados situados al frente de cada área municipal y, dependiendo jerárquicamente y funcionalmente de ellos, los jefes de unidad, servicio y actividad.

Tiene la potestad de establecer los requisitos del servicio en materia de seguridad, es decir, los niveles de seguridad de los servicios, a propuesta del responsable de la seguridad y con informe previo no vinculante del responsable del sistema.

Además, veáis el punto 7, «Funciones y responsables».

7.4 Responsable de seguridad (RSEG)

El titular del puesto de trabajo A010.

El artículo 10 del Esquema Nacional de Seguridad recoge el principio de “la seguridad como función diferenciada”. Este principio exige que el responsable de la seguridad sea independiente del responsable del sistema.

Tiene las atribuciones siguientes:

- Mantener la seguridad de la información empleada y de los servicios proporcionados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con la política de seguridad de la organización.

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

- Específicamente, dar las instrucciones necesarias sobre seguridad física de los sistemas en el jefe de la Policía Local, a través de la Alcaldía o concejalía delegada correspondiente.

Además, veáis el punto 7, «Funciones y responsables».

7.5 Responsable de sistemas (RSIS)

El titular del puesto de trabajo A011. Tiene las responsabilidades siguientes:

- Desarrollar, operar y mantener el sistema de información durante todo el ciclo de vida, las especificaciones, instalación y verificación del funcionamiento correcto.

- Definir la topología y sistema de gestión del sistema de información y establecer los criterios de uso y los servicios disponibles.

- Cerciorarse que las medidas específicas de seguridad se integran adecuadamente dentro del marco general de seguridad.

- Acordar la suspensión del uso de una información concreta o la prestación de un servicio concreto si es informado de deficiencias graves de seguridad que puedan afectar la satisfacción de los requisitos establecidos. Esta decisión tiene que ser acordada con los responsables de la información afectada, del servicio afectado y del responsable de la seguridad, antes de ser ejecutada.

Además, veáis el punto 7, «Funciones y responsables».

7.6 Administrador de la seguridad del sistema (ASS) (colegiado)

Los titulares de los puestos de trabajo A011, A013, A020 y A021. Tienen las responsabilidades siguientes:

- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información.

- Gestionar, configurar y actualizar, si procede, el hardware y el software en que se basan los mecanismos y servicios de seguridad del sistema de información.

- Gestionar las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización que la actividad llevada a cabo en el sistema se ajusta a la autorización.

- Aplicar los procedimientos operativos de seguridad.

- Aprobar los cambios en la configuración vigente del sistema de información.

- Asegurar que los controles de seguridad establecidos se cumplen estrictamente.

- Asegurar que se aplican los procedimientos aprobados para usar el sistema de información.

- Supervisar las instalaciones de hardware y software, las modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de los acontecimientos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

- Informar 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 la detección hasta la resolución.

Además, veáis el punto 7, «Funciones y responsables».

7.7 Delegado de protección de datos colegiado (DPD)

Con independencia de las funciones auxiliares que se puedan encomendar a la Diputación Provincial o, si procede, a un sujeto jurídico privado que disponga del certificado correspondiente, el órgano colegiado DPD asume la supervisión, asesoramiento en la aplicación de la normativa de PDP, y también la firma de toda clase de documentos de su competencia, en los términos del RGPD y normativa de derecho interno aplicable.

El órgano colegiado lo integran:

- El secretario general (puesto de trabajo A001).

- El jefe del Departamento TIC (puesto de trabajo A010).

- El jefe de Actividad de Régimen Interior, Modernización y Protección de Datos (lugar A002).

Sus funciones son las siguientes:

- Participar de forma adecuada y dentro del tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

- Informar y asesorar el responsable o el encargado del tratamiento y los trabajadores que se ocupan del tratamiento de las obligaciones que los incumben en virtud de este Reglamento y otras disposiciones de protección de datos de la Unión o de los estados miembros.

- Supervisar el cumplimiento del RGPD, otras disposiciones de protección de datos de la Unión o de España y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

- Ofrecer el asesoramiento que se le solicito sobre la evaluación de impacto relativo a la protección de datos y supervisar la aplicación de conformidad con la normativa aplicable.

- Cooperar con la autoridad de control.

- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y hacer consultas, si procede, sobre cualquier otro asunto.

El delegado de protección de datos tiene que llevar a cabo sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y las finalidades del tratamiento.

8. FUNCIONES Y RESPONSABILIDADES

En la mesa se usan las abreviaturas siguientes:

CSI - Comité de Seguridad de la Información

RINFO - Responsable de la información

RSERV - responsable del servicio

RSEG - Responsable de la seguridad

RSIS - Responsable del sistema

ASS - Administrador de la seguridad del sistema función responsable

DPD - Delegado de protección de datos colegiado

FUNCIÓN	RESPONSABLE
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o CSI + DPD
Determinación de la categoria del sistema	RSEG + DPD
Anàlisis de riesgos	RSEG + DPD
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG + DPD
Configuración de seguridad	elabora: RSEG aplica: ASS
Implantación de les medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV + DPD

Documentación de seguridad del sistema	RSEG
Política de seguridad	elabora: CSI aprueba: Ayuntamiento en pleno
Normativa de seguridad	elabora: RSEG + DPD aprueba: CSI
Procedimentos operatius de seguridad	elabora: RSIS + DPD aprueba: RSEG aplica: ASS
Estado de la seguridad del sistema	monitora: ASS reporta: RSEG
Planes de mejor de la seguridad	elaboran: RSIS + RSEG + DPD aprueba: CSI
Planes de conscienciación y formación	elabora: RSEG + DPD aprueba: CSI
Planes de continuidad	elabora: RSIS valida: RSEG coordina y aprueba: CSI ejerce: RSIS
Suspensió temporal del servicio	RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS aprueba: RSEG

Respuesta a incidentes de seguridad de la información:

- ASS: llevar el registro, contabilidad y gestión de los incidentes de seguridad en los sistemas bajo su responsabilidad.

- ASS: aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.

- ASS: tomar decisiones a corto plazo si la información se ha visto comprometida de tal manera que pueda tener consecuencias graves (estas actuaciones tendrían que tener un procedimiento para reducir el margen de discrecionalidad de la ASS al mínimo número de casos).

- ASS: asegurar la integridad de los elementos críticos del sistema si se ha visto afectada la disponibilidad (estas actuaciones tendrían que tener un procedimiento para reducir el margen de discrecionalidad de la *ASS al mínimo número de casos).

- ASS: mantener y recuperar la información almacenada por el sistema y sus servicios asociados.

- ASS: investigar el incidente: determinar la manera, los medios, los motivos y el origen del incidente.

- RSEG: analizar y proponer salvaguardias que prevengan incidentes parecidos en el futuro.

- RSIS: planificar la implantación de las salvaguardias en el sistema.

- Comité de Seguridad: aprobar el plan de mejora de la seguridad, con la dotación presupuestaria correspondiente.

- RSIS: ejecutar el plan de seguridad aprobado.

- *DPD: cuando los incidentes de seguridad afectan sistemas que involucran datos de carácter personal.

9. PROCEDIMENTOS DE DESIGNACIÓN

El arte. 5.2 de la Ley 40/2015, del 1.º de octubre, de Régimen Jurídico del Sector Público (LRJSP), indica que corresponde a cada administración pública delimitar, en su respectivo ámbito competencial, las unidades administrativas que configuran los órganos administrativos propios de las especialidades derivadas de su organización.

Por otra parte, el arte. 74 del Real decreto legislativo 5/2015, de 30 de octubre, por el cual se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado público, dice que las administraciones públicas tienen que estructurar en su organización, a través de relaciones de puestos de trabajo u otros instrumentos organizativos similares, que tienen que comprender, cuando menos, la denominación de los lugares, los grupos de clasificación profesional, los cuerpos o escalas, si procede, a que están adscritos, los sistemas de provisión y las retribuciones complementarias. Por lo tanto, la designación de los diferentes sujetos definidos en esta política de seguridad tiene que basarse, inexcusablemente, en el detalle de las funciones y responsabilidades asignadas en la Relación de Puestos de trabajo, hecho que determina la necesidad de modificarla a fin de incluir esas funciones y responsabilidades, después de un análisis y valoración previas.

Según el arte. 21.1.h) de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local (*LRBRL), el alcalde es el presidente de la corporación y tiene la atribución de ejercer la dirección superior de todo el personal, y acordar su nombramiento.

Por otra parte, el arte. 22.2.y) de la *LRBRL atribuye en el Ayuntamiento lleno la aprobación de la plantilla de personal y de la relación de puestos de trabajo, la fijación de la cuantía de las retribuciones complementarias fijas y periódicas de los funcionarios y el número y régimen del personal eventual.

De acuerdo con este criterio, se tramitará un plan de ocupación que permita la atribución de esas funciones y responsabilidades a los lugares que se detallan, con la consiguiente valoración a efectos de adecuar las retribuciones complementarias que correspondan.

*Mentrimentres, se establecerá un programa específico de productividad que permita retribuir la asunción de funciones y responsabilidades.

Por lo tanto, todas las funciones y responsabilidades asignadas quedan condicionadas, lógicamente, al hecho que los órganos decisorios competentes adoptan las medidas necesarias en cuanto a aprobación de gastos, expedientes de contratación y, en general, todas las decisiones tendentes a la efectividad de las medidas de seguridad.

Los nombramientos podrán ser revisados cada dos años, pero podrán hacerse antes cuando el lugar quedo vacante o por un incumplimiento reiterado de sus funciones, con prevención previa. El Ayuntamiento dispone de los procedimientos de provisión de puestos de trabajo previstos en la normativa vigente para hacer los nombramientos, atendida su vinculación a los puestos de trabajo identificados en la Relación de Puestos de trabajo.

En casos de ausencias de larga duración o las de menor duración, pero que puedan provocar ineficiencias en las funciones de cada uno que afectan el sistema, el mecanismo para la sustitución de los responsables designados es el previsto tanto en la Relación de Puestos de trabajo como en la normativa aplicable al personal al servicio del Ayuntamiento (sistemas de provisión definitiva de los puestos de trabajo o sistemas de provisión no definitiva, como por ejemplo las comisiones de servicio y los nombramientos accidentales o interinos).

10. RESOLUCIÓN DE CONFLICTOS

En caso de conflictos entre los diferentes responsables, la Alcaldía o concejalía delegada en materia de personal los resolverá con informe previo no vinculante del Comité de Seguridad de la Información.

11. TRATAMIENTO DE DATOS DE CARÀCTER PERSONAL. EVALUACIÓN DE IMPACTO

El Ayuntamiento trata datos de carácter personal, según se describe en el Registro de Actividades de Tratamiento. Tendrá que evaluar los riesgos relacionados con los datos personales tratados y proponer un plan de actuación para la corrección de los riesgos que superen el umbral autorizado.

El análisis de riesgos será reevaluado de manera periódica, contará con el asesoramiento y supervisión del delegado de protección de datos, y, en todo caso, cuando se detecte un tratamiento de alto riesgo; se tendrá que hacer, en su caso, una evaluación de impacto. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestamistas de servicios o la respuesta a incidentes y/o brechas de datos personales.

La evaluación de impacto relativa a la protección de datos, a la cual tendrán acceso solo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información del Ayuntamiento se tienen que ajustar a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidas en la evaluación, que, como mínimo, tiene que detallar:

- la evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como por ejemplo la elaboración de perfiles, sobre la cual se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que las afectan significativamente de manera similar.

- El tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 del RGPD.

- La observación sistemática a gran escala de una zona de acceso público.

En cualquier caso, la evaluación de impacto se tiene que integrar en el análisis de riesgos a que se refiere el arte. 14 del ENS, de acuerdo con los criterios derivados de los artes. 25 y 32 del RGPD.

12. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política tienen que hacer un análisis de riesgos, de acuerdo con el arte. 14 y concordantes del ENS, que evalúo las amenazas y los riesgos a que están expuestos. Este análisis hay que repetirla:

- Regularmente, al menos una vez en el año.

- Cuando cambio la información que se usa.

- Cuando cambian los servicios prestados.

- Cuando ocurra un incidente grave de seguridad

- Cuando se reportan vulnerabilidades graves.

- Cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para armonizar los análisis de riesgos, el Comité de Seguridad TIC tiene que establecer una valoración de referencia para las diferentes clases de información utilizadas y los diferentes servicios prestados. El Comité de Seguridad tiene que dinamizar la disponibilidad de recursos para atender las necesidades de seguridad de los diferentes sistemas, a fin de promover inversiones de carácter horizontal.

Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del delegado de protección de datos; además se coordinarán los planes del tratamiento del riesgo.

13. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información tendrá que ser tenida en cuenta cuando se aprueban otras políticas del Ayuntamiento en diferentes materias.

Esta Política se desarrollará mediante la normativa de seguridad que afronto aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesitan conocerla, en particular los que usen, operan o administran los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet http://intranet/intranet/index.php y en la sede electrónica del Ayuntamiento https://tavernesdevalldigna.sede.dival.es/

Los procedimientos e instrucciones técnicas que se aprueban en ejecución de esta Política estarán disponibles en los lugares indicados en el párrafo anterior.

14. OBLIGACIONES DEL PERSONAL

Todos los miembros del Ayuntamiento tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad. Es responsabilidad del Comité de Seguridad TIC disponer los medios necesarios porque la información reúno a los afectados.

Todos los miembros del Ayuntamiento tienen que asistir a una sesión de concienciación en materia de seguridad TIC al menos una vuelta en el año. Se establecerá un programa de concienciación continua para atender todos los miembros del Ayuntamiento, en particular los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el uso seguro de los sistemas en la medida que la

necesitan para hacer su trabajo. La formación es obligatoria antes de asumir una responsabilidad, tanto si es la primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades.

15. TERCERAS PARTES/PRESTADORES DE SERVICIOS/PROVEEDORES DE SOLUCIONES

Cuando el Ayuntamiento presto servicios a otros organismos o use información otros organismos, los tiene que hacer partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los servicios; se establecerán canales para el repuerto y coordinación de los respectivos comités de seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad y procedimientos de actuación por la reacción ante incidentes de seguridad. Además, el responsable de seguridad será el punto de contacto (POC).

Cuando el Ayuntamiento uso servicios de terceros o ceda información a terceros, los tiene que hacer partícipes de esta Política de Seguridad y de la normativa de seguridad que afecto esos servicios o información, sin perjuicio del cumplimiento otras obligaciones en materia de protección de datos. Esta tercera parte queda sujeta a las obligaciones establecidas en esa normativa, pero puede llevar a cabo sus propios procedimientos operativos para satisfacerla, de forma que el Ayuntamiento pueda supervisarlos o solicitar evidencias del cumplimiento, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de repuerto y resolución de incidencias que tendrán que ser canalizadas por el POC de los terceros implicados y, además, cuando afecte datos personales, por el delegado de protección de datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se tiene que requerir un informe del responsable de seguridad que preciso los riesgos en que se incurre y la forma de tratarlos. Se requiere que los responsables de la información y los servicios afectados aprueban este informe antes de seguir adelante.

En la contratación de prestamistas de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir el ENS.

En la adquisición de derechos de uso de activos en la nube se tendrá en cuenta los requisitos establecidos en las medidas de seguridad del anexo II del ENS y en las guías de desarrollo.

Cuando la entidad adquiera, desarrollo o implanto un sistema de inteligencia artificial, además de cumplir la normativa vigente en la materia, tendrá que disponer del informe del responsable de la seguridad, que consultará el responsable de la información y del servicio y, cuando sea menester, el del sistema. El delegado de protección de datos también tiene que emitir su parecer.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD

El Ayuntamiento dispondrá de un procedimiento para la gestión ágil de los acontecimientos e incidentes de seguridad que suponen una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad otras normas sectoriales como la de protección de datos personales o cualquier otra que afecto el Ayuntamiento para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando haga falta, a las fuerzas y cuerpos de seguridad el Estado o los juzgados.

17. APROBACIÓN DE LA POLÍTICA Y ENTRADA EN VIGOR

Las modificaciones de esta Política que representan cambios o adaptaciones ante ineficiencias las aprobará el Comité de Seguridad de la Información, siempre que no sean significativas y dará cuenta al Pleno de manera inmediata. El Comité de Seguridad tendrá que revisar anualmente la Política de Seguridad de la Información.

En caso de que los cambios suponen una modificación sustancial, significativa o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que tendrán que ser aprobados, en su caso, por el Pleno.

DISPOSICIÓN FINAL

Las responsabilidades asignadas a los integrantes del CSI lo son a efectos de impulso de las acciones concretas que escapan de sus competencias y recaen en la Alcaldía y equipo de gobierno en cuanto a la asignación de recursos personales, materiales y financieros. Mientras esto no paso, no se pueden exigir responsabilidades a los integrantes del CSI si, como mínimo, no se ha llevado a cabo la auditoría de seguridad e informe de auditoría consiguiente.

Por lo tanto, antes tienen que adoptarse las medidas necesarias para elaborar la auditoría de seguridad a que se refiere el arte. 31 del ENS, por medio de la contratación del servicio consistente a definir los detalles del sistema hasta un nivel que proporciono evidencias suficientes y relevantes, dentro del alcance establecido para la auditoría.

Además, tiene que proporcionarse a todos los integrantes del CSI la formación adecuada para cumplir sus funciones, en cumplimiento de la DA 1.ª del ENS.

ANEXO A. HERRAMIENTAS PARA IMPLEMENTAR LA POLÍTICA

Dado que la Política de Seguridad está escrita a un nivel muy amplio, se requiere complementarla con documentos más precisos que ayudan a llevarla a cabo. Para lo cual se utilizan otros instrumentos que reciben diferentes nombres, de los cuales los más comunes son los siguientes:

- Normas de seguridad (security standards) que en el ámbito de la administración pública se podrán equiparar a instrucciones de servicio.

- Guías de seguridad (security guides).

- Procedimientos de seguridad (security procedures).

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

Las guías tienen un carácter formativo y buscan ayudar los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos en que no hay procedimientos precisos. Por ejemplo, suele haber una guía sobre como escribir procedimientos de seguridad. Las guías ayudan a prevenir que se pasan por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

Los procedimientos (operativos) de seguridad afrontan tareas concretas e indican qué hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Las organizaciones no siempre separan nítidamente estos diferentes tipos de herramientas, sino que a veces se generan manuales y reglamentos de seguridad que tienen un poco de todos los elementos anteriormente mencionados, a fin de buscar siempre más efectividad en la concienciación y formación de los usuarios del sistema.

Si bien los manuales y reglamentos de carácter mixto pueden servir como herramientas importantes, a menudo es útil distinguir claramente entre el que es política (abstracta) y su aplicación concreta. De este modo se es más flexible y se consigue cierta uniformidad de resultados incluso cuando cambia la tecnología o los mecanismos empleados.

ANNEX B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Análisis de riesgos

Uso sistemático de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal

Cualquier información referida a personas físicas identificadas o identificables. 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 cuanto al tratamiento de

datos personales y a la libre circulación de estos datos y por el cual se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), así como la normativa interna aplicable.

Gestión de incidentes

Plano de acción para atender las incidencias que se produzcan. Además de resolverlas, tiene que incorporar medidas de cumplimiento que permiten conocer la calidad del sistema de protección y detectar tendencias antes de que acontezcan problemas graves. ENS.

Gestión de riesgos

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

Incidente de seguridad

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

Información

Caso concreto de cierta clase de información.

Política de seguridad

Conjunto de directrices plasmadas en un documento escrito, que rigen la manera en que una organización gestiona y protege la información y los servicios que considera críticos. ENS.

Principios básicos de seguridad

Cimientos que tienen que regir toda acción orientada a asegurar la información y los servicios. ENS.

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 determina 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.

Delegado de protección de datos

Órgano colegiado que asume las funciones atribuidas por la normativa de protección de datos personales.

Servicio

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

Sistema de información

Conjunto organizado de recursos porque la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. ENS.

ABREVIATURAS

CCN Centro Criptológico Nacional

CERT Computer Emergency Reaction Team

ENS Esquema Nacional de Seguridad

STIC Seguridad TIC

TIC Tecnologías de la información y las comunicaciones

17. ANEXO B. REFERENCIAS

CCN-*STIC-402

Organización y Gestión para la Seguridad de los Sistemas TIC. Diciembre 2006.

CCN-*STIC-801

ENS - Responsables y funciones. 2010.

CCN-STIC-805

ENS - Política de Seguridad de la Información. 2025.

Ley 39/2015

Ley 39/2015, del 1.º de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Ley 40/2015

Ley 40/2015, del 1.º de octubre, de Régimen Jurídico del Sector Público.

Real Decreto 203/2021

Real Decreto 203/2021, de 30 de marzo, por el cual se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

CARTA EUROPEA De AUTONOMÍA LOCAL

Carta Europea de Autonomía Local. Hecho en Estrasburgo el 15 de octubre de 1985.

Ley 7/1985

Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

Ley 3/2018

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

RD 1720/2007

Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba el Reglamento de Despliegue de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE de 19 de enero de 2008.

RD 311/2022

Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad.