Cesareo Reborado Rozas (1 para 1)
CONCELLEIRO
Data de Sinatura: 18/08/2022
HASH: 6658e01c77f317f39d148e5a401f9448
CONCELLO DE LALÍN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI)

Concello de Lalín

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 1 a 33

CONTROL DE VERSIONES

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	ELABORADO	REVISADO	APROBADO
1.0	Primera versión del documento	10/06/2022	17/08/2022	

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 2 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

INDICE

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 3 a 33

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 4 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

1 Aprobación y entrada en vigor

La Política de Seguridad de la Información, en adelante, PSI, será aprobada el Comité de Seguridad del Ayuntamiento de Lalín.

Esta Política de Seguridad de la Información, es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva política.

2 Introducción

El Ayuntamiento de Lalín depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada a 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 y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implican que 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 los servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

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

El Ayuntamiento de Lalín debe estar preparado para prevenir, detectar, reaccionar, recuperarse de incidentes y conservar la información, de acuerdo con el Artículo 5 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en adelante (ENS).

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 5 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

3 Alcance y misión de la PSI

La presente Política es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios al Ayuntamiento de Lalín, especialmente, los responsables de los Servicios de Explotación de los Sistemas de Información y los propios usuarios, como actores ambos, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de Información.

En el ámbito de la presente Política, se entiende por usuario cualquier empleado/empleada público perteneciente o ajeno al Ayuntamiento de Lalín, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con el Ayuntamiento de Lalín y que utilice o posea acceso a sus Sistemas de Información

Esto implica que las diferentes áreas del Ayuntamiento de Lalín 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 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.

Esta Política es de aplicación a todo el ámbito de actuación del Ayuntamiento de Lalín, y sus contenidos se refieren de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad del Ayuntamiento.

El Ayuntamiento para la gestión de sus intereses y de las funciones y competencias que tiene encomendadas, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y expectativas de la población y de todos los grupos de interés.

El Ayuntamiento desea potenciar el uso de las nuevas tecnologías tanto internamente como en sus relaciones con la ciudadanía.

Los principales objetivos que se persiguen son, entre otros, los siguientes:

- Mejorar la calidad de los servicios públicos.
- Mejorar la seguridad de la información tratada por el Ayuntamiento.
- Fomentar la relación electrónica de la ciudadanía con el Ayuntamiento, creando la confianza necesaria entre ciudadano y el Ayuntamiento en esa relación.
- Hacer transparente la actividad del Ayuntamiento.
- Fomentar la participación y colaboración.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 6 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

4 Marco normativo

Se toma como referencia básica en materia de Seguridad de la Información las normativas siguientes:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- 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.
- Ley 34/2002, de 11 de junio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Reglamento (UE) nº 910/2014: relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

5 Principios básicos

5.1 Prevención

El Ayuntamiento de Lalín debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS, así como

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 7 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, van a estar claramente definidos y documentados.

5.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación y actuar en consecuencia según lo establecido en el Artículo 8 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

5.3 Respuesta

Para garantizar la disponibilidad de los servicios críticos, las distintas áreas del Ayuntamiento de Lalín deben desarrollar, cuando sea necesario, la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

5.4 Conservación

Sin perjuicio de los demás principios establecidos por el Ayuntamiento de Lalín, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

6 Organización de la seguridad

La implantación de la Política de Seguridad en el Ayuntamiento de Lalín requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) El Comité de Seguridad de la Información

b) Responsable del Servicio

c) Responsable de la Información

d) Responsable de Seguridad

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 8 a 33

e) Responsable de Sistemas

f) Responsable de Seguridad Física

g) Delegado de Protección de Datos

6.1 Comité de seguridad de la información

El Comité de Seguridad de la Información coordina la seguridad de la información en el Ayuntamiento de Lalín. Estará constituido por:

- Presidente: José Crespo Iglesias – (Alcalde).
- Secretario: Carlos Vence Lago (Técnico informático).
- Vocales:
    - César López Arribas (Secretario General).
    - Cesáreo Reboredo Rozas (Concejal de Novas Tecnoloxías).
    - Alberto Viz Vázquez (Técnico Informático).
    - Responsables de las unidades organizativas municipales será convocados por el presidente en función de los temas a tratar (si afectan a su área)
    - DPD (en este caso puede ser vocal sin derecho a voto al ser personal externo)
    - Oficina técnica (vocal sin derecho a voto)

Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas.

El Comité se deberá reunir con carácter ordinario cada tres meses y con carácter extraordinario por razones de urgencia y causa justificada o cuando lo decida su Presidencia.

El Comité podrá recabar del personal técnico propio o externo la información pertinente para la toma de sus decisiones, así como invitar a dicho personal a las reuniones con voz y sin voto.

El Comité ajustará su funcionamiento a las previsiones contenidas en el capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El Responsable de la Seguridad, actuará como Secretario, con voz y voto, y como tal:

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 9 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

- Convoca las reuniones del Comité de Seguridad de la Información.
- Levantará actas de las reuniones del Comité de Seguridad.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

Se convocará al resto de personas con responsabilidades en los roles del ENS según las necesidades del Comité de Seguridad de la Información.

De igual manera, se convocará a las personas responsables de Seguridad de ENS de cada área en función de las necesidades del Comité de Seguridad de la Información.

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

a) Elaborar los borradores de modificación y actualización de la PSI.

b) Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.

c) Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.

d) 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.

e) Aprobar las Normas de Seguridad TIC (documentación de segundo nivel normativo).

f) Asegurar la coordinación de las diferentes áreas implicadas en la gestión de incidentes de seguridad de la información.

g) Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

h) 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.

i) Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

j) Velar porque 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

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 10 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

k) Impulsar el cumplimiento y difusión de la PSI, promoviendo las actividades de concienciación y formación en materia de seguridad para el personal de la organización.

l) Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas del Ayuntamiento.

El Comité de Seguridad de la Información no es un comité técnico, pero recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría interna y/o externa.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

6.2 Responsable de la Información - (CSI)

Conforme a los artículos 11 y 41 del ENS, el Responsable de la Información es la persona que establece las necesidades de seguridad de la información que se maneja y efectúa las valoraciones del impacto que tendría un incidente que afectara a su seguridad. Tiene, además, la potestad de modificar el nivel de seguridad requerido para la misma (Anexo II.5.7.2 del ENS).

Serán personas con alto cargo en la dirección de la organización y pertenecientes al comité directivo del mismo. Este cargo tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestione cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestione.

La persona u órgano que lo asuma deberá ser identificada para cada Información que trate la organización.

Son funciones del Responsable de la Información, dentro de su ámbito de actuación, las siguientes:

a) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información (artículo 41

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 11 a 33

del ENS). Para ello, puede recabar el asesoramiento del Responsable de Seguridad y del Responsable del Sistema.

b) Es el responsable, junto al Responsable del Servicio, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control. Esta tarea podrá delegarla, de acuerdo con el Responsable del Servicio, en el Responsable de Seguridad y en el Responsable del Sistema.

c) 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.

d) Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

e) El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

f) Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.

g) Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta al Responsable de Seguridad y conviene que escuche la opinión del Responsable del Sistema.

Compatibilidad con otros roles

Este rol podrá coincidir con el del Responsable de Servicio.

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 siquiera cuando se trate de organizaciones de reducida dimensión que funcionen de forma autónoma.

Esta responsabilidad recaerá sobre el Comité de Seguridad de la Información (CSI).

6.3 Responsable del Servicio (CSI)

Conforme al artículo 13 del ENS, el Responsable del Servicio es la persona que determina los requisitos de seguridad del servicio prestado.

Respecto al proceso de gestión del riesgo, el Responsable del Servicio es el encargado, junto al Responsable de la Información, de aceptar los riesgos residuales calculados en el

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 12 a 33

análisis de riesgos, y de realizar su seguimiento y control. Esta tarea podrá delegarla, de acuerdo con el Responsable del Servicio, en el Responsable de Seguridad y en el Responsable del Sistema.

El Responsable del Servicio puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio, si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información, Responsable de Seguridad y Responsable de Sistemas, antes de ser ejecutada.

Sus funciones podrán ser asignadas a personas individuales, o bien ser asumidas por el Comité de Seguridad de la Información.

La persona u órgano que lo asuma deberá ser identificada para cada Servicio que preste la organización.

Funciones asociadas

Sus funciones serán las siguientes:

a) Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.

b) Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.

c) El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.

d) Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

e) Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

f) 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.

Compatibilidad con otros roles:

- Podrá coincidir en la misma persona u órgano colegiado el rol de Responsable de la Información y del Responsable del Servicio, aunque generalmente no coincidirán cuando:

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 13 a 33

- El servicio gestione información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
- La prestación del servicio no dependa de la unidad a la que pertenece el Responsable de la Información.
- Este rol no podrá coincidir con el de Responsable de Seguridad, salvo en organizaciones de reducida dimensión que funcionen de forma autónoma.

Esta responsabilidad recaerá sobre el Comité de Seguridad de la Información (CSI).

6.4 Responsable de Seguridad

Conforme al artículo 13 del ENS, el Responsable de Seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y del servicio.

Se nombrará formalmente como tal, por parte del órgano de gobierno, a una única persona en la organización.

El rol no podrá ser desarrollado por un órgano colegiado, ni podrá haber más de una persona asumiendo el rol en la organización, aunque pueda delegar parte de sus funciones en otras personas.

Tal como se describe en la Guía CCN-STIC-801: “La figura del “Responsable de la Seguridad” aparece en ambas normativas (ENS y LOPD) con un papel muy similar como persona que vela para que los sistemas de información efectivamente respondan a los requisitos establecidos. Las organizaciones harán bien en hacer coincidir estas responsabilidades en una única figura, recopilando todas las funciones en la Política de Seguridad”.

Por tanto, se decide asimismo que el Responsable de Seguridad ejerza también de Responsable de Seguridad a efectos de cumplimiento de la normativa en materia de protección de datos de carácter personal.

Serán funciones del Responsable de Seguridad las siguientes:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información, con la responsabilidad y autoridad para asegurarse de que el Sistema de Gestión de la Seguridad de la Información cumple con los requisitos del Esquema Nacional de Seguridad.

b) Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas.

c) Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables del Servicio y de la

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 14 a 33

Información, siguiendo en todo momento lo exigido en el Anexo II del ENS, declarando la aplicabilidad de dichas medidas.

d) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.

e) Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación al Esquema Nacional de Seguridad, en colaboración con el Responsable de Sistemas.

f) Realizar con la colaboración del Responsable del Sistema, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable del Sistema, podrá aceptar los riesgos residuales calculados en el análisis de riesgos cuando el Responsable de la Información y el Responsable del Servicio hayan delegado en él esta tarea.

g) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y analizar los informes de auditoría, elaborando las conclusiones a presentar al Responsable del Sistema, a los Responsables del Servicio y los Responsables de la Información para que adopten las medidas correctoras adecuadas.

h) Coordinar el proceso de Gestión de la Seguridad, en colaboración con el Responsable de Sistemas.

i) Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema (artº. 28 y Anexo II.2 del ENS).

j) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el Responsable de Sistemas.

k) Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS.

l) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

m) Preparar los temas a tratar en las reuniones del Comité de Seguridad, en coordinación con el Responsable del Sistema, aportando información puntual para la toma de decisiones.

n) Responsable de la ejecución directa o delegada de las decisiones del Comité de Seguridad.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 15 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

o) Colaborar estrechamente con el Delegado de Protección de Datos en relación a las obligaciones y disposiciones del Reglamento General de Protección de Datos y la LOPDGDD.

p) Participará en la elaboración, en el marco del Comité de Seguridad de la Información, la Política de Seguridad de la Información, para su aprobación por Dirección.

q) 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).

r) Elaborará, junto al Responsable de Sistema, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.

s) Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.

t) Aprobará las directrices propuestas por el Responsable de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

En caso de ocurrencia de incidentes de seguridad de la información:

- Analizará y propondrá salvaguardas que prevengan incidentes similares en un futuro.

Compatibilidad con otros Roles

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

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

Delegación de Funciones

Para determinados Sistemas de Información 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 podrán designar los Responsables de Seguridad Delegados que se consideren necesarios.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 16 a 33

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

Los Responsables de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad, pudiendo ser, por ejemplo, la seguridad de sistemas de información concretos o de sistemas de información horizontales.

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

Respecto a la documentación, y apoyándose en el Responsable del Sistema, son funciones del Responsable de Seguridad:

a) Proponer al Comité de Seguridad para su aprobación la documentación de seguridad de segundo nivel (Normas de Seguridad TIC y Procedimientos Generales del Sistema de Gestión de la Seguridad de la Información –SGSI–) y firmar dicha documentación.

b) Aprobar la documentación de seguridad de tercer nivel y firmar dicha documentación.

c) Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

Para el desarrollo de cualquiera de sus funciones el Responsable de Seguridad podrá recabar la colaboración del Responsable del Sistema.

Este rol será asumido por el técnico informático y podrá recabar ayuda de la Oficina Técnica.

6.5 Responsable del Sistema

Serán funciones del Responsable del Sistema las siguientes:

a) Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 17 a 33

d) Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.

e) Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.

f) Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el Responsable de Seguridad.

g) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

h) Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de dicha información o servicio y con el Responsable de Seguridad.

i) Realizar con la colaboración del Responsable de Seguridad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable de Seguridad, podrá aceptar los riesgos residuales calculados en el análisis de riesgos cuando el Responsable de la Información y el Responsable del Servicio hayan delegado en él esta tarea.

j) Elaborar en colaboración con el Responsable de Seguridad, la documentación de seguridad de tercer nivel.

k) Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad.

l) Elaborar los Planes de Continuidad del Sistema para que sean validados por el Responsable de Seguridad, y coordinados y aprobados por el Comité de Seguridad de la Información.

m) Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.

n) Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad para su aprobación.

En caso de ocurrencia de incidentes de seguridad de la información:

a) Planificará la implantación de las salvaguardas en el sistema.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 18 a 33

b) Ejecutará el plan de seguridad aprobado.

Compatibilidad con otros roles

Este rol no podrá coincidir con el de Responsable de Información, con el de Responsable de Servicio ni con el de Responsable de Seguridad

Esta responsabilidad será asumida al Técnico informático que podrá recabar en sus funciones ayuda de la Oficina Técnica.

6.6 Administrador de Sistemas

Se designara como Administrador de la Seguridad del Sistema a un técnico informático que podrá recurrir a la Oficina de Técnica para la implementación de trabajos en el ENS. al que, como tal, le corresponden las siguientes funciones:

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

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 19 a 33

- Monitorizar el estado de la seguridad del sistema.
- En caso de ocurrencia de incidentes de seguridad de la información:
- Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
- Ejecutar el plan de seguridad aprobado.
- Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
- Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar reflejadas en un procedimiento documentado para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
- Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.

6.7 Responsable de Seguridad Física

Serán funciones del Responsable de Seguridad Física las siguientes:

a) Establecer medidas que protejan y aseguren la integridad e indemnidad de las instalaciones y dependencias del Ayuntamiento de Lalín. Especialmente, en las siguientes materias que se señalan con carácter enunciativo no limitativo:
    - o Autorización y control de accesos a dependencias e instalaciones.
    - o Protección de las instalaciones.
    - o Protección de la información almacenada y en tránsito.

b) Implantar y ejecutar directamente las medidas de seguridad física que le competan.

c) Implantar y ejecutar medidas propuestas y aprobadas previamente por el Comité de Seguridad de la Información

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 20 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

d) Asegurar la integridad, disponibilidad y confidencialidad de los elementos críticos del sistema de información en soporte físico.

e) Informar al Comité de Seguridad del grado de implantación de las medidas, su eficacia y los incidentes de seguridad física con carácter anual.

f) En caso de ocurrencia de incidentes de seguridad física que afecte a la información del Ayuntamiento:

- Planificar la implantación de medidas de protección de la información, para que el incidente no vuelva a producirse.
- Tomar decisiones a corto plazo si la información se ha visto comprometida y pudiera tener consecuencias graves.

g) Investigar el incidente: determinar el modo, los medios, los motivos y el origen del incidente y promover e implantar directamente las medidas que permitan evitar el mismo en el futuro.

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

La responsabilidad será asumida por la Jefatura de Policía.

6.8 Delegado de Protección de Datos

Siguiendo lo indicado en el RGPD y la LOPDGDD, el Delegado de Protección de Datos tendrá como mínimo las siguientes funciones:

- Asesorar y supervisar el cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
- Asesorar y supervisar que se han definido plazos de conservación para los datos y que existen y se aplican procedimientos correctos para su destrucción cuando corresponda.
- Supervisar que los tratamientos disponen de bases jurídicas o legitimación
- Asesorar sobre la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Asesorar sobre la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 21 a 33

- Asesorar y supervisar el diseño e implantación de medidas de información a los afectados por los tratamientos de datos (cláusulas).
- Asesorar y supervisar que existen mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
- Supervisar las solicitudes de ejercicio de derechos por parte de los interesados.
- Supervisar la diligencia en la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
- Asesorar y supervisar sobre los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Asesorar y supervisar el diseño e implantación de políticas de protección de datos.
- Revisar los controles y auditorías de Seguridad y protección de datos y reportar conclusiones a la Dirección.
- Supervisar la primera versión de los registros de actividades de tratamiento, así como los cambios que se realicen en los mismos.
- Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Asesorar, revisar y validar los análisis de riesgo y Evaluaciones de Impacto realizados.
- Asesorar y supervisar la implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
- Asesorar y supervisar en la Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Supervisar los procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Comunicar las violaciones de seguridad a las autoridades e interesados cuando se requiera.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 22 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

- Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Supervisar las evaluaciones de impacto sobre la protección de datos.
- Mantener las relaciones con las autoridades de supervisión.
- Mantener el contacto con los interesados.
- Asesorar y supervisar en el diseño de programas de formación, concienciación y sensibilización de usuarios.
- Reportar periódicamente al CSI sobre el estado de cumplimiento en la materia y las acciones que haya que acometer, así como reportar ante incidencias y circunstancias que se produzcan puntualmente.

El delegado de protección de datos está nombrado formalmente y comunicado a la Agencia Española de Protección de Datos, pudiéndose comunicar los ciudadanos en el correo **dpd@lalin.gal**.

7 Procedimientos de designación

La creación del Comité de Seguridad, el nombramiento de sus integrantes y la designación del Responsable de Seguridad del Responsable del Sistema y del Responsable de la Seguridad Física, serán propuestos y aprobados por el alcalde del ayuntamiento de Lalín.

El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Se designan las siguientes responsabilidades:

- **Responsable de Información:** (CSI). Alcalde.
- **Responsables del Servicio:** (CSI). Secretario.
- **Responsable de Seguridad**: Técnico informático.
- **Responsable del Sistema**: Técnico informático.
- **Administrador del Sistema**: Técnico informático.
- **Responsable de Seguridad Física**: Policía Local..
- **Delegado de Protección de datos**: dpd@lalin.gal.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 23 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

8 Revisión de la política de seguridad de la información

Será misión del Comité de Seguridad de la Información (CSI) la revisión anual de esta Política de Seguridad de la Información y la propuesta de modificación o mantenimiento de la misma. La Política será aprobada por este y difundida para que la conozcan todas las partes afectadas.

Esta Política se desarrollará por medio de normativa de seguridad que aborde aspectos específicos. Esta normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y de comunicaciones.

La normativa de seguridad estará disponible en la intranet del organismo.

9 Datos de carácter personal

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal. El Registro de Actividades del Tratamiento detalla los tratamientos afectados y los responsables correspondientes, así como las medidas adoptadas derivadas de las evaluaciones de impacto realizadas sobre los tratamientos.

Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro de Actividades del Tratamiento.

En todo caso, se deberá atender a los principios regulados en el artículo 5 RGPD, que se considerar auténticas obligaciones para esta entidad.

9.1 Figuras vinculadas a la protección de datos de carácter personal

9.1.1 Responsable del Tratamiento

El Responsable del tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento.

A esos efectos se ha atribuido la condición de Responsable de Tratamiento a la persona jurídico-pública, es decir, al propio Ayuntamiento de Lalín. De manera que, se ha entendido que el Ayuntamiento es Responsable del Tratamiento de los datos de carácter personal que obran en sus sistemas de información, y que derivan de la prestación de los servicios públicos atribuidos a nivel de competencias. Cabe decir que la consideración de Responsable de Tratamiento no debe ser asociada a persona física representante del Ayuntamiento, en calidad del cargo o puesto (como, por ejemplo, el Alcalde o Secretario).

Las funciones del Responsable del Tratamiento son, principalmente:

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 24 a 33

- 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.
- Deberá informar a los titulares de los datos los derechos que les asisten y en los términos en los que pueden ejercerlos.
- Deberá excluir del tratamiento los datos relativos al afectado que se oponga al tratamiento de los mismos.
- Deberá cesar en la utilización o cesión ilícita de los datos cuando así lo requiera el interesado.
- Obligación de hacer efectivo el derecho de rectificación o supresión del interesado en el plazo máximo de 1 mes.
- Notificar las rectificaciones o cancelaciones efectuadas en los datos personales a quien se haya comunicado dichos datos, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

9.1.2 Delegado de Protección de datos

El Delegado de Protección de Datos (DPD) puede ser interno o externo a la organización, pudiendo revestir asimismo la forma de un órgano colegiado (Comité Delegado de Protección de Datos), velando siempre por evitar conflicto de intereses en cualquiera de sus miembros. Además de ello, podrá designarse un único DPD para varias autoridades u organismos públicos, teniendo en consideración su estructura y tamaño.

El Delegado de Protección de Datos en la entidad es **TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES S.A.**

Para cualquier comunicación se realizará mediante el correo electrónico: dpd@lalin.gal

Las funciones asociadas son:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros 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.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 25 a 33

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.
- 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, y realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento. Para ello **deberá ser capaz** de:

- Recabar información para determinar las actividades de tratamiento.
- Analizar y comprobar la conformidad de las actividades de tratamiento.
- Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
- Recabar información para supervisar el registro de las operaciones de tratamiento.
- Asesorar en la aplicación del principio de la protección de datos por diseño y por defecto.
- Asesorar sobre:
    - Si se debe llevar a cabo o no una evaluación de impacto de la protección de datos.
    - Qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos.
    - Si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa.
    - Qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos de intereses de los afectados.
    - Si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos.
    - Si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes al Reglamento.
- Priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 26 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

- Asesorar al responsable del tratamiento sobre:
    - Qué metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos.
    - Qué áreas deben someterse a auditoría de protección de datos interna o externa.
    - Qué actividades de formación internas proporcionar al personal o a los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

El DPD deberá reunir conocimientos especializados del Derecho y la práctica en materia de protección de datos. Se han identificado, en consecuencia, aquellos **conocimientos, habilidades o destrezas** necesarias que tiene que saber o poseer el Delegado de Protección de Datos para llevar a cabo una de las funciones propias de su puesto.

Estas funciones genéricas del DPD se pueden concretar en tareas de asesoramiento y supervisión, entre otras, en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 27 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

- Auditoría de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento.
- Análisis de riesgos de los tratamientos realizados.
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Realización de evaluaciones de impacto sobre la protección de datos.
- Relaciones con las autoridades de supervisión.
- Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

9.1.3 Funciones y obligaciones de usuarios con acceso a datos

Todos los empleados de la entidad están sujetos a funciones y obligaciones que se definan en este sentido.

Todo el personal de la entidad que disponga de acceso a los datos de carácter personal debe cumplir con las siguientes obligaciones generales:

- No se permite la difusión de datos de carácter personal ni confidencial perteneciente a la entidad, estando obligado a guardar secreto de la información incluso terminada la relación laboral.
- El usuario se responsabilizará de notificar toda incidencia según el procedimiento de gestión de incidencias. No notificar una incidencia será considerada una omisión del deber del trabajador.
- El usuario se responsabilizará de todos los accesos que se realicen bajo su identificador y contraseña, por tanto, no deberá revelar la contraseña.
- No se permite la copia de datos de carácter personal, en soportes, sin la autorización expresa del delegado de protección de datos.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 28 a 33

- De cualquier forma, conforme referido, cada usuario de los sistemas de información de la entidad deberá respetar las normativas que estén vigentes y aprobadas en cada momento.

9.1.4 Funciones y obligaciones del Encargado del Tratamiento

El **apartado 8 del artículo 4 del RGPD** define al Encargado de Tratamiento como <<*la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*>>.

El Encargado del Tratamiento deberá aplicar 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.

Igualmente, deberá implementar las medidas de seguridad a que se refiere el párrafo anterior y que aparecerán estipuladas en el contrato con el Responsable del Tratamiento.

En concreto, sus funciones son las de:

- Tratar los datos del tratamiento.
- Realizar el control de tratamiento, calidad y seguridad de los datos.
- Controlar la forma y requisitos para proceder a las adiciones y cancelaciones.
- Controlar los soportes de seguridad.
- Control y acceso de contraseñas.
- Mantenimiento del registro de incidencias.
- Crear una lista para las situaciones en la que un afectado no desee que sus datos personales se almacenen en el tratamiento.
- Dar traslado al responsable del tratamiento de aquellas solicitudes de ejercicio de derecho que se reciban por parte de los interesados.

En consecuencia, el Ayuntamiento de Lalín deberá llevar a cabo un documento actualizado donde se identificarán los Encargados de Tratamiento que están prestando servicios en la entidad, así como la indicación de la formalización del pertinente contrato con estos prestadores de servicios con acceso a datos.

10 Gestión de riesgos

Para todos los sistemas sujetos a esta Política de Seguridad de la Información debe realizarse periódicamente una evaluación de los riesgos a los que están expuestos. Este análisis se repetirá:

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 29 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal

- Regularmente, al menos una vez al año.
- Cuando cambie la información gestionada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos (artículo 7 del ENS) y reevaluación periódica (artículo 10 del ENS).

El Responsable de Seguridad junto al Responsable de Sistemas, son los encargados de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

El Responsable de la Información y el del Servicio son los responsables de los riesgos sobre la información y sobre el servicio, respectivamente, y por tanto de aceptar los riesgos residuales calculados en el análisis y de realizar su seguimiento y control sin perjuicio de la posibilidad de delegar esta tarea.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse cada año por parte del Responsable de Seguridad con la colaboración del Responsable del Sistema, que elevarán un informe al Comité Seguridad de la Información.

11 Desarrollo de la política de seguridad de la información. Documentación de Seguridad

Esta Política de Seguridad de la Información se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Las normas y procedimientos contemplarán, al menos, los siguientes aspectos:

- Protección de datos de carácter personal: se implantarán medidas técnicas y organizativas que permitan cumplir los requisitos normativos en esta materia.
- Gestión de activos de información: los activos de información se encontrarán inventariados, categorizados y estarán asociados a un responsable.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 30 a 33

- Seguridad ligada a los recursos humanos: la seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios, para lo que se implantarán los mecanismos que permitan a los usuarios conocer sus responsabilidades y cómo cumplir con ellas.
- Seguridad física: las instalaciones del Ayuntamiento de Lalín mantendrán una correcta seguridad física para evitar los accesos no autorizados así como cualquier otro tipo de daño o interferencia externa.
- Seguridad lógica: se establecen medidas organizativas y técnicas para el control de accesos, la protección frente a códigos dañinos, la seguridad de las comunicaciones, la realización de copias de seguridad, etc.
- Gestión de incidentes de seguridad: se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El cuerpo normativo sobre seguridad de la información será de obligado cumplimiento y se desarrollará en cuatro niveles según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: Política de Seguridad de la Información del Ayuntamiento. Documento de obligado cumplimiento por todo el personal, interno y externo, recogido en el presente documento.

b) Segundo nivel normativo: Políticas Específicas de Seguridad de la Información y Normas de Seguridad TIC, que desarrollan con un mayor grado de detalle la PSI dentro de un ámbito determinado. Las Normas dan respuesta, sin entrar en detalles de implementación ni tecnológicos, a qué se puede hacer y qué no en relación a un cierto tema desde el punto de vista de la seguridad: qué se considera un uso apropiado o inapropiado, las consecuencias derivadas del incumplimiento, entre otros aspectos.

También pertenecen a este nivel la documentación de Procedimientos Generales del Sistema de Gestión de la Seguridad de la Información (SGSI) que implementa, mantiene y mejora de manera continua el SGSI. Los documentos relativos a este segundo nivel normativo serán aprobados por Comité de Seguridad a propuesta del Responsable de Seguridad.

c) Tercer nivel normativo: Procedimientos Operativos e Instrucciones Técnicas. Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la organización, y los procesos internos en ella establecidos. Procedimientos STIC e Instrucciones Técnicas STIC serán

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 31 a 33

aprobados por el Responsable de Seguridad y con la participación en su elaboración del Responsable del Sistema.

d) Cuarto Nivel: Informes, registros y evidencias electrónicas. Documentos de carácter técnico que pueden estar soportados en formatos normalizados que recogen el resultado y las conclusiones de un estudio, una actividad o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información. La responsabilidad de que existan este tipo de documentos es del Responsable del Sistema.

Aparte de los documentos solicitados en el punto anterior, la documentación de seguridad del sistema podrá contar, bajo criterio del Responsable de Seguridad, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, etc.

El Responsable de Seguridad y el Responsable del Sistema, serán responsables de mantener la documentación de seguridad actualizada y organizada y de gestionar los mecanismos de acceso a la misma.

12 Formación y concienciación

Todos los miembros del Ayuntamiento de Lalín 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.

Todos los miembros del Ayuntamiento de Lalín asistirán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros del Ayuntamiento de Lalín, 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.

13 Incumplimiento

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 32 a 33

14 Terceras partes

Las empresas y organizaciones externas que con ocasión de su colaboración con el Ayuntamiento de Lalín para la prestación de un servicio, accedan o gestionen activos de información del Ayuntamiento de Lalín o de sus usuarios, directa o indirectamente (en sistemas propios o ajenos), comparten la responsabilidad de mantener la seguridad de los sistemas y activos del Ayuntamiento de Lalín, por lo que deberán asumir las siguientes obligaciones:

- No difundir ninguna información relativa a los servicios proporcionados al Ayuntamiento de Lalín sin autorización expresa para ello.
- Informar y difundir a su personal las obligaciones establecidas en esta Política.
- Aplicar las medidas estipuladas por RGPD en el tratamiento de los datos personales responsabilidad del Ayuntamiento de Lalín que traten por razón de la prestación del servicio.
- Aplicar los procedimientos para la gestión de seguridad relacionados con los servicios proporcionados al Ayuntamiento de Lalín. Especialmente se deben aplicar los procedimientos relacionados con la gestión de usuarios, tales como notificaciones de altas y bajas, identificación de los usuarios, gestión de contraseñas, etc., en el sentido descrito en la presente política y normativa reguladora que sea de aplicación.
- Notificar cualquier incidencia o sospecha de amenaza a la seguridad de algún sistema o activo del Ayuntamiento de Lalín a través de los mecanismos que se determinen, colaborando en la resolución de las mismas relacionados con los sistemas, servicios o personal de la propia entidad.
- Implantar medidas en sus propios sistemas y redes para prevenir la difusión de virus y/o código malicioso a los sistemas del Ayuntamiento de Lalín. Específicamente, cualquier equipo conectado a la red corporativa del Ayuntamiento de Lalín debe disponer de un antivirus actualizado preferiblemente de forma automática.
- Implantar medidas en sus propios sistemas y redes para prevenir el acceso no autorizado a los sistemas del Ayuntamiento de Lalín desde otras redes. Entre otros, se deben aplicar las actualizaciones de seguridad en sus sistemas y se debe mantener un sistema cortafuegos para proteger las conexiones desde Internet y otras redes no confiables.

El Ayuntamiento de Lalín se reserva el derecho de revisar la relación con la entidad externa en caso de incumplimiento de las anteriores obligaciones.

Cod. Validación: 39934ZSKNQRJE6ELMC5GAT2GH | Corrección: https://lalin.sedelectronica.gal/
Documento asinado electronicamente desde a plataforma xestiona esPublico | Páxina 33 a 33

Praza de Galicia, 1. 36500 Lalín (Pontevedra). / Tfno. 986 78 70 60 / Fax 986 78 06 38 / www.lalin.gal / informatica@lalin.gal