**AMPARO TABOADA GIL, Secretaria General de la Diputación Provincial de A Coruña.**

**CERTIFICA:** Que el PLENO DE LA CORPORACIÓN de la Diputación Provincial de A Coruña, en la sesión ordinaria celebrada el 25 de marzo de 2022, adoptó el siguiente acuerdo:

---

**25. Aprobación de la modificación de la política de seguridad de la información de la Diputación provincial de A Coruña revisada en marzo de 2022.**

Aprobar la modificación de la política de seguridad de la información de la Diputación Provincial de la Coruña que es del siguiente tenor literal:

## 1. INTRODUCCIÓN

Este documento constituye la Política de Seguridad de la Información de la Diputación Provincial de A Coruña, en adelante "La Diputación", en cumplimiento del artículo 11 (Requisitos mínimos de Seguridad del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica) y de la medida de seguridad org.1 contemplada en el Anexo II de dicho Real Decreto.

En este sentido, el mencionado artículo 11 establece que "*Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.*"

La estructura de este documento sigue las pautas establecidas por la guía CCN-STIC-805(publicada por el Centro Criptológico Nacional, ente adscrito al Centro Nacional de Inteligencia) para la redacción de la Política de Seguridad en el ámbito del Esquema Nacional de Seguridad.

La Política de Seguridad de la Información recoge la postura de la Diputación en cuanto a la seguridad de la información y establece los criterios generales que deben regir la actividad del organismo en cuanto a la seguridad.

El objetivo de la seguridad de la información es garantizar la calidad de la información y laprestación continuada de los servicios, actuando preventivamente, supervisando la actividaddiaria y reaccionando con presteza a los incidentes.

Los sistemas de información deben estar protegidos contra amenazas de rápida evolución con potencialpara incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, usoprevisto y valor de la información y los servicios. Para defenderse de estas amenazas, serequiere una estrategia que se adapte a los cambios en las condiciones del entorno paragarantizar la prestación continua de los servicios.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Esquema

Nacional de Seguridad y la Ley Orgánica de Protección de Datos y garantía de derechos digitales (en adelante ENS y LOPD-gdd), así comorealizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar lasvulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizarla continuidad de los servicios prestados.

## 2. Misión de la Diputación de A Coruña

La Diputación de A Coruña es una institución de gobierno local que promueve el desarrollo y el bienestar de la ciudadanía en los municipios que componen la provincia de A Coruña. Actúa prestando servicios directamente a los ciudadanos y sobre todo en cooperación con los ayuntamientos. La Diputación, tiene como misión la asistencia técnica, económica y material a los ayuntamientos para que puedan prestar servicios locales de calidad de forma homogénea en toda la provincia, coordinando servicios y organizando servicios públicos de carácter supramunicipal.

## 3. Marco Normativo

La normativa la que se encuentra sometida la Diputación de la Coruña, más relacionada con su actividad, se recoge a continuación (por orden cronológico ascendente):

- Ley 7/85 Reguladora de las Bases de Régimen Local.
- Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.
- Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.
- Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 27/2013 de Racionalización y Sostenibilidad de la Administración Local.
- Orden HAP/2425/2013, de 23 de diciembre, por la que se publican los límites de los distintos tipos de contratos a efectos de la contratación del sector público a

partir del 1 de enero de 2014.

- Real Decreto-ley 8/2014, de 4 de julio, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
- Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

## 4. Política General de Seguridad

El objeto de la presente Política es establecer la postura de la Diputación respecto a la Seguridad que afecta a los procesos relacionados con el desempeño de sus funciones y, muy particularmente, con los relacionados con la administración electrónica, tanto desde el punto de vista de los usuarios de los servicios, como desde el punto de vista interno, para la gestión de la propia Entidad.
La Diputación utiliza las Tecnologías de la Información y las Comunicaciones para prestar sus servicios, por lo que es consciente de que estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados.
Asimismo, también es consciente de que los incidentes de seguridad pueden estar provocados desde lugares remotos, a través de las conexiones a redes de comunicaciones de las que se dispone y, muy concretamente, a través de las conexiones a la Internet (ciber-ataques).
El fin de la política es contrarrestar las amenazas mencionadas anteriormente con los medios suficientes, dentro de las posibilidades presupuestarias. Para este fin, se establecerá una estructura de seguridad, junto con los mecanismos apropiados para su gestión, y un conjunto de instrumentos de apoyo de forma que se garantice:

- el cumplimiento de los objetivos de su misión y de prestación de servicios
- el cumplimiento de la legislación y normativa aplicables

Para ello,

- se preverán y desplegarán medidas para evitar incidentes de seguridad que pudieran afectar al cumplimiento de objetivos o poner en riesgo la información.

- se diseñarán medidas de respuesta ante incidentes de seguridad, física o lógica, de forma que se minimice el impacto de los mismos, en caso de que ocurrieran.

Como norma general, se tendrá un enfoque de orientación al riesgo a la hora de diseñar las medidas de seguridad necesarias, poniendo más foco y esfuerzo en la mitigación de lo que suponga un mayor riesgo.
Las distintas unidades bajo cuya responsabilidad se encuentran los servicios prestados deberán contemplar la seguridad desde el mismo momento en que se concibe un nuevo sistema o servicio, aplicando para estos y para los ya existentes, las medidas de seguridad prescritas por el Esquema Nacional de Seguridad para garantizar la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad de los servicios y de la información.
Los requisitos de seguridad de los sistemas, las necesidades y requisitos de formación de los usuarios, y las necesidades de financiación deben ser identificados e incluidos en la planificación de los sistemas y en los pliegos de prescripciones utilizados para la realización de proyectos que involucren a las Tecnologías de la Información y Comunicaciones (TIC).
Se deben articular mecanismos de prevención, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad.
En cuanto a la prevención, se debe evitar que los servicios y la información resulten afectados por un incidente de seguridad. Para ello, la Diputación implementará las medidas de seguridad establecidas en el Anexo II del ENS, así como medidas adicionales que pudieran ser identificadas en el proceso de análisis de riesgos.
En cuanto a la reacción, se establecerán mecanismos de detección, comunicación y gestión de incidentes de seguridad, de forma que cualquier incidente pueda ser tratado en el menor plazo posible. Siempre que sea posible, se detectarán de forma automática los incidentes de seguridad, utilizando elementos de monitorización de los servicios o de detección de anomalías y poniendo en marcha los procedimientos de respuesta al incidente en el menor plazo posible. Para los incidentes detectados por los usuarios, ya sean internos o externos, se establecerán los pertinentes canales de comunicación de incidentes.
En cuanto a la recuperación, para aquellos servicios que se consideren críticos, en base a la valoración que de los mismos realicen sus responsables, se deberán desarrollar planes que permitan la continuidad de dichos servicios en el caso de que, a raíz de un incidente de seguridad, quedaran indisponibles.

## 5. Alcance

Esta Política de Seguridad es de aplicación a todos los servicios prestados por la Diputación así como a todo el personal, sin excepciones.

## 6. Organización de la Seguridad

La seguridad en La Diputación está soportadas obre las estructuras y roles que se describen a continuación:

- Estructura de especificación, que es la que se encarga de establecer los requisitos de seguridad asociados a los servicios prestados.

- Estructura de supervisión, que es la que se encarga de verificar el cumplimiento de los requisitos de seguridad y el alineamiento continuo con los objetivos de la organización.

- Estructura de operación, que se encarga de implantar las medidas de seguridad identificadas.

## 6.1. Estructura de especificación

Esta estructura es la encargada de determinar los requisitos de seguridad que serán de aplicación a los servicios prestados por la Diputación y a garantizar el cumplimiento normativo asociado que le es de aplicación, en concreto el Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad.
Se describen a continuación las funciones y responsabilidades de los roles asociados a la especificación.

### 6.1.1 Responsable de la Información

Es el responsable último de la protección de la información, garantizando su disponibilidad, confidencialidad e integridad.
Tiene la potestad de establecer los requisitos de seguridad de la información, en el sentido de asignarle a la misma una valoración que determinará el nivel de protección que requiere.
El establecimiento de requisitos podrá realizarse a propuesta del Responsable de Seguridad de la Información y contando con la opinión del Responsable del Sistema.
Este rol podrá recaer en una o varias personas, e incluso en un órgano colegiado, pudiendo coincidir con el Responsable del Servicio.

### 6.1.2 Responsable del Servicio

Este rol es el responsable de establecer los niveles de seguridad (o requisitos de seguridad) que requieren los servicios prestados, que determinarán las medidas de protección necesarias, así como su intensidad.
El establecimiento de requisitos podrá realizarse a propuesta del Responsable de Seguridad de la Información y contando con la opinión del Responsable del Sistema. Los requisitos del servicio deben tener en cuenta los requisitos de la información que manejen.
Este rol podrá recaer en una o varias personas, e incluso en un órgano colegiado, pudiendo coincidir con el Responsable de la Información.

### 6.1.3 Responsable del Tratamiento

El Responsable del Tratamiento es la persona física o jurídica sobre la que recaen las funciones genéricas recogidas en la normativa de protección de datos aplicable y vigente en cuanto a responsabilidad última de los tratamientos de datos personales que se lleven a cabo.

En general, esta figura determina los fines y los medios relacionados con el tratamiento de los datos personales.
Sus funciones son las siguientes:

- Garantizar el cumplimiento de principios relativos al tratamiento recogidos en la normativa vigente en materia de protección de datos personales.

- Garantizar el cumplimiento de las normativas existentes en la Diputaciónde A Coruña en materia de protección de datos personales.

- Garantizar el mantenimiento adecuado, y conforme a la legislación vigente, del Registro de Actividades de Tratamiento.

- Garantizar el cumplimiento del deber de información al interesado recogido en la normativa vigente en materia de protección de datos personales.

- Establecer los mecanismos necesarios para recibir, gestionar y resolver solicitudes de ejercicio de derechos por parte de los interesados.

- Evaluar el riesgo para los derechos y libertades de los afectados en las brechas de seguridad y la posible notificación a las autoridades de control y a los afectados.

- Determinar las medidas técnicas y organizativas apropiadas que se deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con la normativa vigente de protección de datos personales.

- Actuar como punto de contacto con las autoridades de control, conjuntamente con el Delegado de Protección de Datos.

- Implantar y seguir los programas de formación y sensibilización del personal de la Diputación de A Coruña en materia de protección de datos personales.

## 6.2 Estructura de supervisión

La estructura de supervisión de la seguridad se encarga de verificar la correcta implantación y operación de los requisitos de seguridad que se hayan establecido, de cara a mantener la alineación con los objetivos y de cumplir con las normas y legislación aplicable.
En la supervisión global de todas las actividades relativas a la seguridad de la información se encuentra el Responsable de Seguridad de la Información.
En la supervisión global de las actividades relativas a la seguridad física se encuentra el Responsable de Seguridad Física.
Para la coordinación global e integral de la seguridad se encuentra el Comité de Seguridad de la Información.
Las funciones y responsabilidades de cada una de las figuras se describen a continuación:

### 6.2.1. Responsable de Seguridad de la Información

Es responsable de la definición, coordinación, difusión y verificación de los requisitos de seguridad de la información en la Diputación.

Este Responsable forma parte del Comité de Seguridad de la Información, siendo el encargado de elevar a dicho Comité los asuntos de interés relacionados con la seguridad de la información.
Sus responsabilidades comprenden:

- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de la Diputación.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de las normas y procedimientos establecidos.
- Conseguir que se elabore el presupuesto anual de seguridad de tecnologías de la información y las comunicaciones (TIC) de la Diputación.
- Supervisar la implantación práctica de la estrategia de seguridad de la información de la Diputación.
- Supervisar las situaciones excepcionales (o incidentes) de ciberseguridad producidas en la Diputación.
- Promover la realización de análisis de riesgos de seguridad de la información, así como los planes para mitigarlos, de forma periódica, elevando las conclusiones al Comité de Seguridad de la Información para su aprobación.
- Promover y coordinarla realización de programas de formación y sensibilización en materia de seguridad de la información.
- Analizar los indicadores de seguridad para medir la eficacia y eficiencia de las medidas implantadas.
- Analizar los incidentes de seguridad de la información reflejados en los registros de estos y verificar que se han establecido los planes para su resolución.
- Mantener actualizada la documentación asociada a la gestión de la seguridad de la información: normativas, procedimientos y registros.
- Velar por que se elaboren procedimientos operativos para la realización de las actividades que se encuentren reguladas por la normativa interna de seguridad.
- Verificar el cumplimiento de las normas y procedimientos establecidos.
- Velar por la inclusión de cláusulas de seguridad en los contratos con terceras partes y por su cumplimiento.
- Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos de TIC desde su especificación inicial hasta su puesta en operación.
- Autorizar por escrito la ejecución de procedimientos de recuperación de datos en los casos en que se requiera.
- Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad.

- Impulsar la realización de las auditorías ordinarias regulares, al menos cada dos años, que permitan verificar el cumplimiento de las obligaciones de la Diputación en materia de seguridad.

- Colaborar con las auditorías externas/internas en materia de seguridad de la información, revisarlas y encargar a los responsables de los sistemas la implantación de las correcciones que se deriven.

### 6.2.2. Delegado de Protección de Datos

El Delegado de Protección de Datos es la figura que actúa como asesor, supervisor e interlocutor del Responsable del Tratamiento en el ámbito de las competencias marcadas por la normativa en materia de protección de datos vigente.
Sus funciones son:

- Informar y asesorar a la Diputación de A Coruña, y a todo el personal que se ocupe del tratamiento de datos personales, de las obligaciones que se deriven del Reglamento General de Protección de Datos y de otras disposiciones relacionadas con la protección de datos.

- Supervisar el cumplimiento del Reglamento General de Protección de Datos en la Diputación de A Coruña.

- Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

- Cooperar con la Autoridad de Control.

- Actuar como punto de contacto de la Autoridad de Control conjuntamente con el Responsable del Tratamiento.

Además, asesorará al Responsable del Tratamiento o, en general, a aquella figura que lo necesite, en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos.

- Identificación de las bases jurídicas de los tratamientos.

- Valoración de la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

- 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 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 entre la Diputación de A Coruña y los encargados del tratamiento.

### 6.2.3. Responsable de Seguridad Física

Es responsable de la definición, coordinación, difusión y verificación de los requisitos de seguridad física de las instalaciones donde se alojen los sistemas de información
Este Responsable forma parte del Comité de Seguridad de la Información, siendo el encargado de elevar a dicho Comité los asuntos de interés relacionados con la seguridad física de los locales y las infraestructuras.
Sus responsabilidades comprenden:

- Identificación de necesidades de seguridad física.

- Conseguir la elaboración de un presupuesto anual de inversiones y actuaciones en seguridad física.

- Supervisar la instalación y el mantenimiento posterior de los elementos y servicios destinados a la seguridad física.

- Analizar los incidentes de seguridad física que se puedan haber producido y establecer actuaciones para dar respuesta a los mismos.

- Mantener actualizada la documentación asociada a la gestión de la física: normativas, procedimientos y registros.

### 6.2.4. Comité de Seguridad de la Información

La misión del Comité de Seguridad es la coordinación general de las actividades que tienen relación con la seguridad integral.
Un objetivo fundamental del Comité de Seguridad es la puesta en común de aspectos importantes de la seguridad entre todos los responsables. Con ello se evitará que actividades referentes a la seguridad, que puedan afectar a varias o todas las unidades de la organización, queden sin el suficiente conocimiento por parte de sus responsables, o sin el suficiente apoyo o compromiso, perjudicando la eficacia.
Las funciones del Comité de Seguridad son:

- Establecer unos objetivos de seguridad de la información corporativos alineados con la encomienda de gestión del organismo.

- Informar regularmente del estado de la seguridad a la Presidencia.

- Revisar regularmentela Política de Seguridad y proponer cambios, si procede.

- Revisar las normativas internas de seguridad que se puedan derivar de la Política de Seguridad, a propuesta del Responsable de Seguridad de la Información,aprobarlas,

en su caso.

- Elaborar y proponer los requisitos de formación para el personal clave que maneja información, sistemas e infraestructuras físicas.

- Asumir el papel de dueño de los riesgos de seguridad de la información (quien tiene la potestad para aceptar los riesgos residuales sobre los activos), aprobando las apreciaciones de riesgos realizadas y aceptando el riesgo residual resultante, en su caso.

- Aprobar los planes de tratamiento de riesgos que surjan a raíz de las apreciaciones de riesgos realizadas.

- Seguir el desarrollo de los planes de acción aprobados.

- Coordinar las actuaciones en materia de seguridad que se puedan estar realizando en diferentes unidades de la Diputación, con objeto de evitar esfuerzos duplicados o desalineados con la Política de Seguridad

- Supervisar y participar en la resolución de los incidentes de seguridad que se puedan producir y plantear las estrategias y salvaguardas ante los mismos, velando por la adecuada coordinación de los diferentes actores involucrados en la gestión de estos incidentes.

- Analizar información de indicadores de seguridad que pudiera haber definidos. Tomar decisiones en caso de desviación respecto a los umbrales establecidos.

- Proponer soluciones de seguridad que deban tener un presupuesto aprobado.

- Promover la mejora continua de la seguridad de la información.

El Comité de Seguridad de la Información tendrá una composición de miembros fijos y otros que participarán en función de los temas a tratar.
Serán miembros fijos del Comité de Seguridad:

- El Presidente de la Diputación

- El Responsable de Seguridad de la Información

- El Responsable del Sistema

- El Responsable de Seguridad Física

- Los responsables de los diferentes Servicios de la Diputación, o el diputado que los represente.

Adicionalmente, podrán asistir al Comité de Seguridad los responsables de las materias específicas a tratar en las reuniones, que podrán ser invitados en función del contenido de la agenda.
Cuando los asuntos a tratar incidan o puedan incidir en tratamientos de datos personales, se deberá convocar al Delegado de Protección de Datos.

#### 6.2.4.1. Frecuencia de reuniones del Comité de Seguridad de la Información

El Comité de Seguridad de la Información se reunirá con carácter ordinario, como mínimo, una vez cada seis meses y, extraordinariamente, por convocatoria de alguno de sus miembros fijos.

#### 6.2.4.2. Convocatorias del Comité de Seguridad

Las convocatorias del Comité de Seguridad serán realizadas por el Secretario del Comité, quien velará por que se redacte un acta recogiendo los asuntos tratados y las decisiones tomadas.

### 6.3. Estructura de Operación

La estructura de operación de la seguridad debe asumir la administración operativa de la seguridad de los sistemas de información, implantando en dichos sistemas las medidas necesarias para satisfacer los requisitos de seguridad establecidos por la estructura de especificación.
Se describen a continuación las funciones y responsabilidades de las figuras asociadas a la estructura de operación.

#### 6.3.1. Responsable de los Sistemas de Información

Sus funciones y responsabilidades son:

- Definir, en coordinación con el Responsable de Seguridad de la Información, las especificaciones funcionales de seguridad de los Sistemas de Información de la Diputación.

- Garantizar que en el diseño de sistemas de información y redes de comunicaciones se contemplen desde el principio los aspectos necesarios de seguridad de la información en cuanto a disponibilidad, integridad, confidencialidad, autenticación, control de acceso, auditoría y registro.

- Revisar que la configuración de seguridad tras la instalación de un sistema nuevo es la adecuada.

- Revisar que la configuración de seguridad tras los cambios en un sistema sigue siendo la adecuada.

- Verificar el funcionamiento de mecanismos de Control de Acceso que eviten que un usuario acceda a datos o recursos con derechos distintos de los autorizados, sin que en ningún caso se puedan desactivar.

- Seguir los foros de vulnerabilidades y elaboración del calendario de aplicación de parches para los sistemas de información, en función de los que surjan y el impacto que tengan en la seguridad (los parches mismos los aplicarán los administradores de sistemas).

- Implantar las medidas de seguridad que resulten de los planes de tratamiento de riesgos o planes de acciones correctivas a raíz de las auditorías de seguridad de la información.
- Proporcionar datos para la alimentación de indicadores de seguridad de la información.
- Supervisar los procedimientos de copia de seguridad.
- Realizar auditorías técnicas periódicas de la infraestructura de tecnologías de la información, sistemas y aplicaciones.

### 6.4. Designación de roles de las estructuras de seguridad

Los roles de gobierno de la seguridad recogidos en la presente Política, que ejercerán sus funciones de forma horizontal para toda la información y servicios prestados por la Diputación de A Coruña, quedan designados como sigue:

| ROL | EJERCIDO POR |
|---|---|
| **Responsable de la Información** | **Comité de Seguridad de la Información** |
| **Responsable del Servicio** | **Comité de Seguridad de la Información** |
| **Responsable de Seguridad de la Información** | **Jefatura del Servicio de Informática y Administración Electrónica** |
| **Responsable de Seguridad Física** | **Jefatura del Servicio de Sistemas y Soporte** |
| **Responsable de los Sistemas de Información** | **Jefatura del Servicio de Sistemas y Soporte** |
| **Presidente del Comité de Seguridad** | **Presidente de la Diputación** |
| **Secretario del Comité de Seguridad** | **Responsable de Seguridad de la Información** |

RPT-7116849

| ROL | EJERCIDO POR |
|---|---|
| **Responsable del Tratamiento** | **Diputación de A Coruña** |
| **Delegado de Protección de Datos** | **Oficialía Mayor** |

Los roles de seguridad quedan asignados a los puestos organizativos recogidos en el cuadro anterior, quedando automáticamente designados sus titulares en cada momento. En caso de ausencia temporal o baja, la persona que lo sustituya en el puesto, asumirá los roles indicados en ésta política.

Se establece que el Comité de Seguridad es el órgano con potestad para modificar la designación de roles establecida anteriormente. En caso de modificación, se recogerá la misma en el acta de la sesión correspondiente, que constituirá el documento justificativo en tanto se realice una revisión del presente documento de Política de Seguridad.

### 6.5. Mecanismos de coordinación y de resolución de conflictos

La coordinación entre los diferentes roles participantes de las actividades de seguridad así como la resolución de conflictos que pudieran surgir entre ellos se llevará a cabo en el seno del Comité de Seguridad de la Información.

## 7. Funciones y obligaciones

Al margen de las funciones y atribuciones que atañen al personal que integra el esquema organizativo responsable de la seguridad, se establecen a continuación las obligaciones del personal de la Diputación así como de aquellos terceros que tengan acceso a sus sistemas de información.

### 7.1. Funciones y obligaciones del personal

Todo el personal de la Diputación tiene la obligación de conocer la Política de Seguridad y cumplirla. El Comité de Seguridad de la Información dispondrá los medios para que esta Política llegue a los afectados.
Así mismo, el personal deberá asistir a las sesiones de concienciación y formación en materia de seguridad para las que sea designado como asistente.

### 7.2. Funciones y obligaciones de terceras partes

Las terceras partes (entidades externas a la Diputación) que estén relacionadas con la

RPT-7116849

gestión, mantenimiento o explotación de los servicios prestados por la Diputación serán hechos partícipes de esta Política. Las terceras partes quedarán obligadas al cumplimiento de esta Política y a las normativas que se puedan derivar de ella.
Las terceras partes podrán desarrollar sus propios procedimientos operativos para satisfacer la Política.
Se deberán establecer procedimientos específicos de comunicación de incidencias para que los terceros afectados puedan reportarlas.
El personal de las Terceras Partes deberá recibir sesiones de concienciación, tal como se exige para el personal propio.
Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte, el Responsable de Seguridad de la Información deberá realizar un informe del riesgo en que se incurre. Ese riesgo deberá ser aceptado por el Comité de Seguridad de la Información.

## 8. Formación y concienciación

De manera sistemática se realizarán acciones de formación y concienciación en materia de seguridad de la información.
El objetivo de la acción formativa y de concienciación es doble:

- mantener informado al personal más directamente relacionado con el manejo de información y los sistemas que la tratan sobre los procedimientos existentes de seguridad, configuración segura de equipos, desarrollo seguro, gestión de incidentes de seguridad, riesgos, etc.

- concienciar al personal, en general, de la importancia de la seguridad y de los procedimientos básicos de manejo e intercambio de información.

Todo el personal deberá asistir a una sesión de concienciación en materia de seguridad de la información con la periodicidad que se determine por parte del Comité de Seguridad de la Información.
Las personas con responsabilidad en el uso, la gestión, mantenimiento o explotación de los servicios soportados en las 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.

## 9. Gestión de riesgos

Todos los sistemas, servicios e infraestructuras sujetos a la presente Política deberán ser objeto de un análisis de riesgos que evalúe las amenazas y los riesgos a los que están expuestos.
El análisis se repetirá regularmente, al menos una vez al año, elevándose las conclusiones al Comité de Seguridad de la Información.
Se realizará un análisis de riesgos de los sistemas de información en periodos inferiores a un año cuando:

- haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.

- ocurra un incidente de seguridad grave.

- se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

El Comité de Seguridad de la Información establecerá los niveles aceptables de riesgo y aprobará las actuaciones a llevar a cabo en caso de que se incurra en niveles de riesgo no aceptables.

## 10. Datos de carácter personal

La Diputación solo recogerá datos de carácter personal cuando seanadecuados, pertinentes y no excesivos y estos se encuentren en relación con el ámbito y lasfinalidades para los que se hayan obtenido. De igual modo,adoptará las medidas técnicas y organizativas necesarias para el cumplimiento de la legislación vigente en materia de protección de datos.

## 11. Desarrollo de la Política de Seguridad

Esta Política de Seguridad se desarrollará mediante la elaboración de otras políticas o normativas de seguridad que aborden aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.
La aprobación y revisión de los documentos anteriormente reseñados se hará conforme a lo siguiente:

- Política de Seguridad de la Información: será aprobada por el Pleno de la Diputación de A Coruña, siendo responsabilidad del Comité de Seguridad de la Información su revisión para elevar una propuesta de modificación cuando sea necesario.

- Normativa Interna de seguridad de la información: será aprobada por el Comité de Seguridad de la Información, siendo el Responsable de Seguridad de la Información el responsable de su elaboración y actualización.

- Procedimientos operativos de seguridad de la información: será aprobada por el Comité de Seguridad de la Información, siendo el Responsable de Seguridad de la Información el responsable de su elaboración y actualización.

La documentación de políticas y normativas de seguridad, así como esta Política de Seguridad se encontrará a disposición de todo el personal de la organización que necesite conocerla y, en particular, el personal que utilice, opere o administre los sistemas de información y comunicaciones o la información misma albergada en dichos sistemas o los servicios prestados por la Diputación.

## 12. Revisión de la Política de Seguridad

La presente política de seguridad será revisada con carácter anual por el Comité de Seguridad de la Información.

Y para que conste y sin perjuicio de los términos de la aprobación del acta, según lo dispuesto en el artículo 206 del Reglamento de organización, funcionamiento y régimen jurídico de las Corporaciones locales, expido la presente de orden y con el visto bueno del Sr. Presidente en A Coruña.

La Secretaria: Amparo Taboada Gil (firmado digitalmente)

El Presidente: Valentín González Formoso (firmado digitalmente)