MIGUEL IGLESIAS MARTÍNEZ, Secretario 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 30 de mayo de 2025, adoptó el siguiente acuerdo:

---

22. Aprobación de modificaciones en la política de seguridad.

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

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 12 (Política de seguridad y requisitos mínimos de seguridad) del 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 y de la medida de seguridad org.1 contemplada en el Anexo II de dicho Real Decreto. En este sentido, el mencionado artículo 12 establece que "Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente".

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 la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

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

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 LOPD-gdd), 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.

Así mismo, las áreas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

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.

Marco Normativo de la Diputación de A Coruña

La normativa legal a la que se encuentra sometida la Diputación de la Coruña, más relacionada con su actividad, se recoge a continuación, en 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 5/1997, de 22 de julio, de Administración Local de Galicia.
- Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.

**RPT-7116849

- Ley 38/2003, de 17 de noviembre, General de Subvenciones.

- Ley 58/2003, de 17 de diciembre, General Tributaria.

- 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.

- Ley 9/2007, de 13 de junio, de subvenciones de Galicia.

- 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.

- El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (reglamento eIDAS).

- Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.

- Ley 2/2015, de 29 de abril, del empleo público de Galicia.

- 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.

- 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.

- 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)

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

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

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

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

Adicionalmente, forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica de la Diputación de A Coruña derivadas de las relacionadas anteriormente y publicadas en las sedes electrónicas comprendidas dentro del ámbito de

**RPT-7116849

aplicación de esta Política.

Principios de la Política de Seguridad de la Información

Toda la actividad relacionada con el uso de los activos de información y el tratamiento de datos personales en la Diputación se regirá por los siguientes principios:

- Alcance estratégico: La Política de Seguridad de la Información contará con el compromiso de todos los niveles directivos de modo que la seguridad de la información y la protección de datos estén integradas y coordinadas con las decisiones estratégicas de la Diputación.

- Seguridad integral: La seguridad se entenderá como un proceso integral y planificado, constituido por todos los elementos técnicos, humanos, materiales, procedimentales y organizativos relacionados con los sistemas de información, evitando las actuaciones puntuales o tratamientos coyunturales.

- Gestión de la seguridad basada en los riesgos: El análisis y la gestión de los riesgos serán parte esencial y permanente del proceso de seguridad. Mediante el análisis de riesgos se detectan los problemas de seguridad y con su correcta gestión se persigue reducirlos a un nivel aceptable mediante la selección e implantación de medidas de seguridad.

- Prevención, detección, respuesta y conservación: La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección, respuesta y conservación, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o los servicios que presta.

- Existencia de líneas de defensa: Los sistemas de información dispondrán de una estrategia de protección constituida por múltiples capas de seguridad dispuesta de forma que, cuando una de las capas sea comprometida, permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

- Vigilancia continua: La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

**RPT-7116849

- Reevaluación periódica: La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

- Diferenciación de responsabilidades: En los sistemas de información se diferenciarán el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

- Ciclo completo y seguridad por defecto: Se contemplarán los aspectos de seguridad en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto. La seguridad debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

- Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación será proporcional, en sus costes económicos y operativos, a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

- Responsabilidad proactiva: El responsable del tratamiento deberá aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de la información se hace conforme a la normativa española y europea en la materia.

- Legitimación en el tratamiento de datos personales: Sólo se tratarán los datos de carácter personal cuando dicho tratamiento esté legitimado en alguna de las causas previstas en el Reglamento (UE) 2016/679.

- Licitud, lealtad y transparencia: Los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado.

- Limitación de la finalidad: Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

- Minimización de datos: Los datos tratados serán adecuados, pertinentes y limitados a

lo necesario en relación con los fines para los que sean tratados.

- Integridad y calidad: Se garantizará el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y, en su caso, actualización.

- Limitación del plazo de conservación: Los datos se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que pudieran derivarse de su tratamiento. Los datos podrán conservarse durante períodos más largos cuando sean tratados exclusivamente con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos de acuerdo con lo establecido en el Reglamento (UE) 2016/679. El tratamiento para estos fines se realizará con las medidas técnicas y organizativas adecuadas, respetando particularmente el principio de minimización de los datos personales, así como, cuando sea posible, su anonimización. En esta modalidad de tratamiento será a su vez de aplicación lo dispuesto en la normativa sobre archivos y documentación.

- Confidencialidad: Quienes intervengan en el tratamiento estarán obligados a guardar el deber de secreto, incluso después de haber finalizado el proceso de tratamiento.

- Profesionalidad: La seguridad de los sistemas de información estará implantada, atendida, revisada y auditada por personal cualificado y formado, que participará en todas las fases del ciclo de vida de los sistemas.

- Prevención, disponibilidad y recuperación: Se desarrollarán planes de acción y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad. Se asegurará el nivel de disponibilidad requerido para los activos y recuperación ante cualquier contingencia.

Requisitos mínimos y Directrices

Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información. La Política de Seguridad de la Información se establecerá de acuerdo con los principios básicos señalados y se desarrollará aplicando los siguientes requisitos mínimos y directrices:

- Protección de las instalaciones: Los activos de información se emplazarán en áreas

**RPT-7116849

seguras, protegidas por controles de acceso físico adecuados a su nivel de criticidad. Los sistemas y los activos de información ubicados en dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

- Autorizaciones y controles de acceso: El acceso a la información estará debidamente controlado y limitado a las personas usuarias, procesos, dispositivos u otros sistemas de información autorizados, y exclusivamente a las funciones permitidas. A tal fin se implantarán los mecanismos de identificación y autenticación adecuados para cada activo.

- Gestión de activos de información: Los activos de información se inventariarán y categorizarán. Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación.

- Autorización de sistemas y soluciones: Se deberá autorizar los sistemas y soluciones antes de entrar en operación. Se controlará y limitará los accesos a los sistemas de información. Se configurará y diseñará los sistemas de información de forma que se garantice la seguridad y protección de datos por defecto

- Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que, debidamente autorizada, acceda a los activos de información conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

- Protección de datos de carácter personal: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

- Registro de actividad: La actividad realizada por las personas usuarias de sistemas de información deberá ser registrada al objeto de verificar y auditar el buen uso de la información, siempre con plenas garantías a la intimidad y dignidad personal, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación. La monitorización deberá realizarse motivando su necesidad y aplicando el principio de proporcionalidad, eligiendo la medida menos invasiva. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

- Gestión de incidentes de seguridad: Los procedimientos de gestión permitirán identificar, registrar y dar una efectiva y pronta respuesta a los incidentes de seguridad, comunicando los procedentes a la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

- Protección de las comunicaciones: La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, sin perjuicio de las actuaciones realizadas con fines de registro de actividad.

- Especificaciones de seguridad: El desarrollo y mantenimiento de los sistemas de información irán acompañados de las especificaciones de seguridad y de los correspondientes procedimientos de control.

- Adquisición de productos de seguridad y contratación de servicios de seguridad: Se optará, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, por aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

- Monitorización continua: se desarrollarán servicios horizontales de seguridad que aumenten la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicaciones de la Diputación integrado en la Red Nacional de Centros de Operaciones de Ciberseguridad.

- Prevención ante otros sistemas de información interconectados: Se protegerá el perímetro de sistemas de información, en particular, si se conecta a redes públicas y se reforzarán las tareas de prevención, detección y respuesta a incidentes de seguridad.

- Mínimo privilegio: los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios y la funcionalidad imprescindible para que la organización alcance sus objetivos.

- Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

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 la misión de la Diputación y de prestación de sus servicios

- El cumplimiento de la legislación y normativa aplicables.

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

**RPT-7116849

de proyectos que involucren a las Tecnologías de la Información y Comunicaciones (TIC).

Se articularán mecanismos de prevención, detección, respuesta y conservación 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 y, en general, medidas que disuadan a posibles atacantes y que reduzcan la superficie de exposición para minimizar la probabilidad de que las amenazas lleguen a materializarse.

En cuanto a la detección, se implementarán las medidas adecuadas para descubrir la presencia de un incidente en la fase más temprana posible, con objeto de contenerlo y minimizar su impacto. 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. 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 respuesta, se pondrán en marcha mecanismos, asociados a los procedimientos de gestión de incidentes y de continuidad de las operaciones, para la restauración de la información y los servicios que pudieran haberse vistos afectados por un incidente de seguridad.

En cuanto a la conservación, se desplegarán medidas que garanticen la conservación de la información en soporte electrónico.

Alcance

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

Organización de la Seguridad

La seguridad en la Diputación está soportada sobre las estructuras y roles que se describen a continuación:

- Estructura de especificación, que es la que se encarga de establecer los requisitos

**RPT-7116849

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.

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 311/2022 de 3 de mayo 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.

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 requiera. El establecimiento de requisitos podrá realizarse a propuesta del Responsable de Seguridad de la Información y contando con la opinión del Responsable del Sistema.

El Responsable de la Información tiene, de forma exclusiva, la potestad de modificar en el tiempo la valoración mencionada anteriormente, si así fuera necesario.

Este rol podrá recaer en una o varias personas, e incluso en un órgano colegiado, pudiendo coincidir con el Responsable del Servicio.

Responsable del Servicio

Este rol es el responsable de establecer los niveles de seguridad (o requisitos de seguridad) que requieran 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.

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 Diputación de 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.

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. La implantación de todas las actividades relativas a la seguridad de la información, de acuerdo a las directrices del Responsable de Seguridad de la Información, corresponde al Administrador 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:

Responsable de Seguridad de la Información

Es responsable de la determinación de las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios 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:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información de la Diputación.
- Promover y coordinar la realización de programas de formación y sensibilización en materia de seguridad de la información.
- Llevar a cabo 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.
- Elaborar la normativa de seguridad derivada de la Política de Seguridad.
- Aprobar los procedimientos operativos para la realización de las actividades que se encuentren reguladas por la normativa interna de seguridad.
- Mantener actualizada la documentación asociada a la gestión de la seguridad de la información: normativas, procedimientos y registros.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de las normas y procedimientos establecidos.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de la Diputación.
- Conseguir que se elabore el presupuesto anual de seguridad de tecnologías de la información y las comunicaciones (TIC) de la Diputación.
- Supervisar las situaciones excepcionales (o incidentes) de ciberseguridad producidas en la Diputación.
- 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.
- Velar por la inclusión de cláusulas de seguridad en los contratos con terceras partes y por su cumplimiento.
- 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.
- Establecer la categoría de los sistemas de información de la Diputación.
- 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.

**RPT-7116849

- Notificar al CCN-CERT los incidentes de seguridad que se deban comunicar, en base a la legislación vigente.
- Constituirse en punto de contacto del CCN-CERT en materia de seguridad de la información.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas del CCN-CERT para su aplicación en el ámbito de la Diputación.

Administrador de Seguridad de la Información

Es responsable de la puesta en marcha de la implementación, gestión y mantenimiento de las medidas de seguridad que sean de aplicación a los sistemas de información de acuerdo a las directrices del Responsable de Seguridad de la Información.

Sus funciones son las siguientes:

- Monitorizar el estado de la seguridad del sistema.
- Aplicar los procedimientos operativos de seguridad de la información aprobados e informar al Responsable de Seguridad de la Información de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Elaborar procedimientos operativos de seguridad de la información y asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y se registren con la frecuencia deseada, de acuerdo con esta Política y normativa derivada.
- Colaborar en la elaboración de catálogos de activos y servicios, análisis de riesgos, evaluaciones de impacto, en la relación de auditorías, acciones de asesoramiento y en cualquier otra actividad relacionada con la Seguridad de la Información en que sea necesaria su participación.
- Coordinar el proceso de respuesta ante incidentes de seguridad en el sistema bajo la supervisión del Responsable de Seguridad de la Información y el Responsable de los Sistemas de Información.
- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema.
- Gestionar la configuración y actualización del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema.

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.

**RPT-7116849

- Mantenimiento de registro de encargados de tratamiento

- Asesoramiento a Contratación en relación con los encargados de tratamiento en cuanto al contenido de los contratos o actos jurídicos que regulen la relación entre la Diputación de A Coruña y los encargados del tratamiento.

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.

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.

**RPT-7116849

Las funciones del Comité de Seguridad son:

- Establecer unos objetivos de seguridad de la información corporativos alineados con los objetivos de prestación de servicios y gestión de la Diputación.
- Informar regularmente del estado de la seguridad a la Presidencia.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Elaborar y revisar regularmente la Política de Seguridad y proponer cambios, si procede, para su aprobación por el Pleno de la Diputación.
- Revisar las normativas internas de seguridad que se puedan derivar de la Política de Seguridad, a propuesta del Responsable de Seguridad de la Información, y aprobarlas, en su caso.
- Elaborar y proponer los requisitos de formación para el personal clave que maneje 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), teniendo en cuenta los requisitos de seguridad establecidos para los diferentes activos por parte de sus responsables correspondientes, aprobando las apreciaciones de riesgos realizadas y aceptando el riesgo residual resultante, en su caso.
- Aprobar los planes de tratamiento de riesgos y mejora de la seguridad que surjan a raíz de las apreciaciones de riesgos realizadas y velar por la coordinación de su ejecución en las distintas unidades.
- 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
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- 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. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- 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.

**RPT-7116849

- 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.
- Analizar información de indicadores de seguridad que pudiera haber definidos. Tomar decisiones en caso de desviación respecto a los umbrales establecidos.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Diputación, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- 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 Secretario General de la Diputación
- El Responsable de Seguridad de la Información
- La Administradora de Seguridad de la Información
- El Delegado de Protección de Datos
- 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.

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.

Convocatorias del Comité de Seguridad

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

El Secretario del Comité preparará la agenda de temas a tratar, aportando la información necesaria para la toma de decisiones y será el responsable de que las acciones acordadas se lleven a cabo, ya sea por ejecución directa o por delegación.

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.

Responsable de los Sistemas de Información

Sus funciones y responsabilidades son:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Definir, en coordinación con el Responsable de Seguridad de la Información, las

**RPT-7116849

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.

El Responsable del Sistema tiene la potestad para proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si apreciara deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La propuesta debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad y elevada al Presidente de la Diputación para su decisión final.

Designación de roles de las estructuras de seguridad

El Pleno de la Diputación de A Coruña designará, inicialmente, y ratificará en las sucesivas revisiones de esta Política 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.

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 no se realice una revisión del presente documento de Política de Seguridad, momento en el que se ratificarán los nuevos nombramientos por el Pleno.

Los roles de gobierno de la seguridad quedan establecidos como sigue:

ROL	EJERCIDO POR
Responsable de la Información	El Comité de Seguridad de la Información. El Comité de Seguridad delega en los responsables de las diferentes áreas organizativas de la Diputación para la operativa del día a día con la información propia de cada área (autorizaciones, calificación de información y otras actividades atribuibles al responsable de la información)
Responsable del Servicio	El Comité de Seguridad de la Información. El Comité de Seguridad delega en los responsables de las diferentes áreas organizativas de la Diputación para la operativa del día a día con los servicios ofrecidos por cada área para las actividades atribuibles al responsable del servicio.

**RPT-7116849

ROL	EJERCIDO POR
Responsable de Seguridad de la Información	Titular de la Jefatura del Servicio de Informática y Administración Electrónica.
Administrador de Seguridad de la Información	Titular de la Jefatura de Sección de Seguridad de la Información.
Responsable de Seguridad Física	Titular de la Jefatura del Servicio de Sistemas y Soporte.
Responsable de los Sistemas de Información	Titular de la Jefatura del Servicio de Sistemas y Soporte.
Presidente del Comité de Seguridad	Titular de la Presidencia de la Diputación.
Secretario del Comité de Seguridad	Secretario General de la Diputación.
Responsable del Tratamiento	Diputación de A Coruña.
Delegado de Protección de Datos	Titular de la 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.

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.

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.

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.

**RPT-7116849

Así mismo, el personal deberá asistir a las sesiones de concienciación y formación en materia de seguridad para las que sea designado como asistente.

Funciones y obligaciones de terceras partes

Las terceras partes (entidades externas a la Diputación) que estén relacionadas con la gestión, mantenimiento o explotación de los servicios prestados por la Diputación serán hechas 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.

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.

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 estuvieran 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.

Datos de carácter personal

La Diputación sólo recogerá datos de carácter personal cuando sean adecuados,

pertinentes y no excesivos, con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. De igual modo, la Diputación adoptará las medidas técnicas y organizativas necesarias para el cumplimiento de la legislación vigente en materia de protección de datos.

Desarrollo de la Política de Seguridad y Estructuración de la Documentación 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, revisión y nivel de acceso 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.
    - Será un documento de público acceso.
- 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.
    - La normativa de seguridad estará a disposición de todo el personal de la Diputación.
- Procedimientos operativos de seguridad de la información:
    - Serán aprobados por el Responsable de Seguridad, siendo el Responsable del Sistema o el responsable del servicio competente en la materia del procedimiento, el responsable de su elaboración y actualización.
    - Los procedimientos operativos estarán a disposición de todo el personal de la Diputación que los requiera llevar a cabo para su actividad.

Revisión de la Política de Seguridad

La presente política de seguridad será revisada con carácter anual por el Comité de Seguridad de la Información, que podrá modificarla y elevarla para su aprobación.

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.

El Secretario General: Miguel Iglesias Martínez (Firmado digitalmente)

El Presidente: Valentín González Formoso (Firmado digitalmente)