D. ANTONIO FERNANDO BENÍTEZ MARTÍN, SECRETARIO DELEGADO DE LA AGENCIA PÚBLICA ADMINISTRATIVA PATRONATO DE RECAUDACIÓN PROVINCIAL DE MÁLAGA,

CERTIFICA:

Que el Consejo Rector del Patronato de Recaudación Provincial, en sesión ordinaria celebrada el día 18 de octubre de 2023 adoptó entre otros, el siguiente acuerdo que se transcribe con el siguiente tenor literal:

"Punto nº 7.- Aprobación, si procede, de la actualización del documento de política de seguridad de la información y privacidad del Patronato de Recaudación Provincial de Málaga."

PROPUESTA *de la Iltma. Sra. Presidenta Delegada de la Agencia Pública de Servicios Económicos de Málaga-Patronato de Recaudación Provincial, Dña. María del Carmen Martínez Fernández, referente a:*

APROBACIÓN DE LA ACTUALIZACIÓN DEL DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DEL PATRONATO DE RECAUDACIÓN PROVINCIAL DE MÁLAGA

Exposición de motivos.

El Pleno de la Agencia Pública de Servicios Económicos Provinciales - Patronato de Recaudación Provincial (en adelante PRP), en sesión ordinaria celebrada el 23 de julio de 2012, aprobó el documento de Política de Seguridad del organismo como instrumento para generar seguridad en los tratamientos de la información y en las relaciones con la ciudadanía y con otros organismos de las administraciones públicas.

No obstante, debido a la rápida evolución de las TIC, de las demandas de usuarios y de la normativa aplicable, en el marco de la revisión continua, siendo precisa la adaptación de esta Política para reforzar el nivel de seguridad y para adecuarla a la nueva normativa aplicable en protección de datos, con fecha 23 de junio de 2020 el Consejo Rector aprobó una nueva Política de Seguridad de la Información, en la que se integró la política de Privacidad del Patronato de Recaudación Provincial (por la vinculación existente entre sus respectivos roles y materias, y por simplificación normativa).

La adopción de medidas relacionadas con la seguridad en el ámbito tecnológico ha constituido un importante criterio a la hora de establecer las relaciones de confianza entre las administraciones públicas y la ciudadanía, toda vez que éstas se están viendo comprometidas en los últimos tiempos por amenazas que suponen un reto tecnológico de enorme complejidad. La continuidad de los servicios y la protección de los datos de carácter personal deben ser una prioridad en cualquier actuación administrativa, y así se está reflejando en el actual marco normativo, que supone una importante evolución hacia un nuevo modelo de prestación de servicios por parte de las administraciones públicas, acorde con las demandas de una sociedad más tecnificada y consciente de los beneficios y riesgos de las TIC.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad sustituye al 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, que se actualiza para:

- *Alinear el ENS con el marco normativo y el contexto estratégico existentes para garantizar la seguridad en la Administración Digital.*
- *Introducir la capacidad de ajustar los requisitos del ENS para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza de los riesgos a los que están expuestos sus sistemas de información.*
- *Reforzar la protección frente a las tendencias en ciberseguridad mediante la revisión de los principios básicos, los requisitos mínimos y las medidas de seguridad que deben adoptarse por las entidades sujetas al ENS.*

Los sistemas afectados deberán adecuarse a lo dispuesto en el real decreto en un plazo de veinticuatro meses contados a partir de su entrada en vigor.

El objetivo del ENS es crear las condiciones necesarias de seguridad en el uso de los medio electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios; promover la gestión continuada de la seguridad; promover la prevención, detección y corrección, para una mejor resiliencia en el escenario de ciberamenazas y ciberataques; promover un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios públicos digitales cuando participan diversas entidades y; en definitiva, servir de modelo de buenas prácticas, en línea con lo apuntado en las recomendaciones de la OCDE Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document.

El mandato principal del ENS es el establecido en el artículo 12 'Política de seguridad y requisitos mínimos de seguridad', según el cual "cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente", la cual "es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta" y se establecerá de acuerdo con los principios básicos y se desarrollará aplicando los requisitos mínimos, en proporción a los riesgos identificados en cada sistema. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 del ENS deberá contar con una política de seguridad formalmente aprobada por el órgano competente. Por tanto, la Política es un documento aprobado formalmente por la Alta Dirección de la Organización (tal y como señala el punto 3.6 de la Guía de como elaborar una Política de Seguridad del Centro Criptológico Nacional), siendo un acto administrativo que no establece la normativa de funcionamiento de un servicio interno; sin tener, así, naturaleza reglamentaria.

El punto 3.6 de la Guía mencionada del CCN, también señala que esta normativa "estará sujeto a un proceso de revisión regular que lo adapte a nuevas circunstancias, técnicas u organizativas, y evite que quede obsoleto. Por ello se establecerá un proceso organizativo que asegure que regularmente se revisa la oportunidad, idoneidad, completitud y precisión de lo que la Política establezca y sea sometido a aprobación formal por la Alta Dirección. El proceso de elaboración y aprobación debe explicitarse en la misma Política".

En la Política de Seguridad y Privacidad del PRP se establece en el punto 28.1 que la responsabilidad de revisión, modificación, actualización de la Política, para su posterior propuesta (por la Presidencia del Organismo) para su aprobación (por el Consejo Rector) será competencia del Comité de Seguridad y Privacidad.

Si bien la Política de Seguridad y Privacidad del PRP aprobada por el Consejo Rector el 23 de junio de 2020 cumple con el actual ENS, en la sesión del Comité de Seguridad y Privacidad del organismo, de fecha 4 de octubre de 2023, se valoró y confirmó la necesidad de actualizarla para alinearla con los principios básicos y requisitos mínimos de seguridad que se establecen en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, así como para adaptar el marco de gobierno a la estructura y necesidades actuales de la Agencia. Igualmente, la actualización de esta Política se alinea con los nuevos criterios establecidos en las guías de seguridad actualizadas del Centro Criptológico Nacional (CCN-STIC), en particular, la colección de guías de la serie 800, y disponibles en el Portal del CCN-CERT, que ayudan al mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

La actualización de la Política de Seguridad y Privacidad del PRP que fue aprobada por el Consejo Rector el 23 de junio de 2020, consolida los cambios, deja sin efecto el anterior texto y, será efectiva desde la fecha de su aprobación por el Consejo Rector del Organismo, debiéndose publicar en el portal web del PRP y en la Intranet corporativa.

Dado que el Patronato de Recaudación Provincial está realizando todas las actuaciones necesarias para dar respuesta efectiva a los problemas de seguridad de las redes y sistemas de información (por las amenazas en ciberseguridad) y, para dar cumplimiento a las actuales obligaciones normativas, esta Presidencia, conocido el acuerdo por unanimidad del Comité de Seguridad y Privacidad del PRP para actualizar la Política de Seguridad y Privacidad, tal y como consta en su acta de 4 de octubre de 2023, propone al Consejo Rector del Organismo que acuerde lo siguiente:

a) *Aprobar la actualización del Documento de Política de Seguridad de la Información y Privacidad del Patronato de Recaudación Provincial de Málaga, en el marco de la revisión continua, para alinearla con los principios básicos y requisitos mínimos de seguridad que se establecen en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, así como para adaptar el marco de gobierno a la estructura y necesidades actuales del organismo, cuyo texto es el siguiente:*

"Política de Seguridad de la Información y de Privacidad del Patronato de Recaudación Provincial de Málaga

1. Objeto

El presente documento define y establece los principios que conforman la Política de Seguridad de la Información y de Privacidad de la Agencia Pública de Servicios Económicos Provinciales de Málaga - Patronato de Recaudación Provincial, (en adelante PRP), para garantizar en la mejor medida posible, la confidencialidad, integridad y disponibilidad de sus sistemas de información, de las comunicaciones y de los servicios telemáticos con el fin de proporcionar a los ciudadanos, a las entidades locales y a las entidades públicas, unos servicios fiables, de calidad y de confianza para permitirles el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. Para ello se establecen las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal.

En este documento se establece el compromiso del PRP con la seguridad de los Sistemas de Información, definiendo los objetivos y criterios básicos para el tratamiento de la misma, sentando los pilares del marco normativo de seguridad de esta administración y estableciendo una nueva estructura organizativa y de gestión de la seguridad y privacidad del PRP que velará por su cumplimiento.

2. Ámbito de aplicación

La presente Política es aplicable a toda la información y activos de información del PRP que la soportan, incluyendo todas las personas y terceras empresas u organismos que de una forma u otra acceden a ellos, independientemente de su situación física, dentro o fuera de las instalaciones del organismo. Afecta, por tanto, y son de aplicación directa a todos los sistemas, aplicaciones, servicios, información y ubicaciones del PRP, incluyendo al personal implicado en su tratamiento.

Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

La Política de Seguridad y Privacidad expuesta en el presente documento sirve de referencia, en ningún momento pretenden ser una política absoluta, pudiendo estar sometida a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad y privacidad marcados por el PRP.

Debe ser conocida y cumplida por todo el personal del PRP, independientemente del puesto, cargo y responsabilidad dentro del mismo, publicándose en la intranet del PRP.

3. Marco normativo

El marco normativo relevante en que se desarrollan las actividades del PRP, y, en particular, la prestación de sus servicios electrónicos a la ciudadanía está integrado por las siguientes normas:

- *Real Decreto por el que se regula el Esquema Nacional de Seguridad (ENS).*
- *Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.*
- *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.*
- *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 (RGPD).*
- *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).*
- *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.*
- *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 58/2003, de 17 de diciembre, General Tributaria.*

El PRP mantendrá un registro con el marco normativo que le es aplicable, incluyendo las instrucciones técnicas de seguridad de obligado cumplimiento tal y como se contempla en el Esquema Nacional de Seguridad que será publicado en el portal web PRP, siendo el Comité de Gestión de la Seguridad de la Información y Privacidad (en adelante, Comité de Seguridad y Privacidad el encargado del mantenimiento del precitado registro.

El Comité de Seguridad y Privacidad será responsable de identificar las guías de seguridad del CCN, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

4. CUMPLIMIENTO DE LOS PRINCIPIOS BÁSICOS Y REQUISITOS MÍNIMOS DE SEGURIDAD

Para lograr el cumplimiento del Real Decreto por el que se regula el Esquema Nacional de Seguridad (ENS), que recoge los principios básicos y el cumplimiento de los requisitos mínimos, el PRP ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger, teniendo en cuenta la categoría de los sistemas afectados.

La seguridad como un proceso integral y mínimo privilegio

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La

aplicación del Esquema Nacional de Seguridad al PRP estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) *El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.*
b) *Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.*
c) *En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.*
d) *Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.*

Vigilancia continua, reevaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad

La vigilancia continua por parte del PRP permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

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.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Gestión de personal y profesionalidad

Todo el personal, propio o ajeno relacionado con los sistemas de información del PRP, dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Incidentes de seguridad, prevención, detección, reacción y recuperación

El PRP, dispone de procedimientos de gestión de incidentes de seguridad acuerdo con lo previsto en el Esquema Nacional de Seguridad, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, 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 a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados

El PRP, ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa ha sido 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.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema del PRP se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Diferenciación de responsabilidades, organización e implantación del proceso de seguridad

El PRP, ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

Autorización y control de los accesos

El PRP, ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Protección de las instalaciones

El PRP, ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad el PRP, tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

Protección de la información almacenada y en tránsito y continuidad de la actividad

El PRP, prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación del ENS, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el ENS, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Registro de actividad y detección de código dañino

El PRP, con el propósito de satisfacer el objeto del ENS, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el RGPD y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, el PRP podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la

información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

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.

Infraestructuras y servicios comunes

El PRP, tendrá en cuenta que la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en el ENS.

Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras

El PRP, tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para entidades locales que sean de aplicación.

5. Objetivos generales de la Política de Seguridad

El PRP define los siguientes objetivos generales en la presente Política de Seguridad y Privacidad:

a) *Garantizar la seguridad TIC y proteger los recursos de Información y la tecnología para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de los mismos 24 horas al día durante los 365 días del año.*

b) *Crear la estructura de la organización de la seguridad y privacidad en el organismo.*

c) *Marcar las directrices, objetivos y principios que sirvan de base para el desarrollo de las normas, procedimientos y procesos de gestión de la seguridad.*

d) *Mantener el Registro de Actividades de Tratamiento que está publicado por medios electrónicos en el Portal de Transparencia del PRP, recogiendo asimismo las medidas de seguridad concretas aplicadas para cada actividad de tratamiento de datos personales.*

e) *Mantener la presente Política de Seguridad actualizada, realizando al menos, una revisión anual para confirmar y asegurar su vigencia y nivel de eficacia.*

f) *Incluir, en los planes de formación del personal al servicio del PRP acciones formativas y de concienciación relativas a la Seguridad de la Información y a la protección de datos de carácter personal.*

6. Responsabilidad de la Política de Seguridad y Privacidad

La responsabilidad general y última de la presente Política de Seguridad y Privacidad recae sobre el PRP.

7. Organización y gestión de la Seguridad de la Información

La estructura organizativa de la gestión de la seguridad de la información del PRP en relación con el Esquema Nacional de Seguridad está compuesta por los siguientes roles:

a) *Responsable de la Información y de los Servicios.*
b) *Responsable de Seguridad.*
c) *Responsable del Sistema.*

Así mismo, formarán parte de la estructura organizativa de la gestión de la seguridad los siguientes agentes:

a) *El Comité de Seguridad y Privacidad.*
b) *El Grupo de Respuesta a Incidentes de Seguridad y Privacidad (Comité de Crisis).*
c) *Unidad de Administración y Seguridad, dependiente del Servicio de Tecnologías de la Información, cuya persona responsable es el Director de Seguridad.*

Asignación de responsabilidades en materia de Seguridad

La asignación de responsabilidades en materia de seguridad será la siguiente:

- *El Responsable de la Información y el Responsable del Servicio será el Comité de Seguridad y Privacidad.*
- *El Responsable de la Seguridad será el Director de Seguridad, persona responsable de la Unidad de Administración y Seguridad del PRP.*
- *El Responsable del Sistema será el titular del puesto de Responsable de Sistemas del PRP, que es la persona al frente de la Unidad de Sistemas y Comunicaciones, dependiente del Servicio de Tecnologías de la Información.*

Comité de Gestión de la Seguridad de la Información y Privacidad

Se dispone de un Comité de Seguridad y Privacidad, como responsable de implementar la Política de Seguridad y Seguridad y como órgano de dirección y seguimiento en materia de Seguridad y Protección de Datos en el ámbito del PRP, formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en el organismo y que velará por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos y seguridad.

El Comité de Seguridad y Privacidad actuará como órgano colegiado que se regirá por el presente documento, y por lo previsto en la Sección 3ª del Capítulo 2º del Título preliminar de la Ley 40/2015 de Régimen Jurídico de las Administraciones Públicas.

- ### *Composición del Comité de Gestión de Seguridad de la información y Privacidad*

  El Comité de Seguridad y Privacidad estará compuesto por los siguientes miembros:

  a) *Presidente/a: Gerente del PRP.*
  b) *Vocales:*
     - *Tesorero/a del PRP.*
     - *Jefe/a de Unidades de Gestión Tributaria e Inspección.*
     - *Responsable de Seguridad.*

- *Delegado/a de Protección de Datos.*

c) *Secretario/a: Jefe/a de las Unidades de Atención al Público. Su participación podrá ser delegable en personal de su área.*

La participación del Presidente podrá ser delegada en cualquiera de los vocales titulares. La participación de los vocales podrá ser delegada en personal de su área.

El Comité de Seguridad y Privacidad podrá convocar a sus reuniones a las personas que estime pertinente a propuesta de alguno de sus miembros, en calidad de asesores. Esta convocatoria la efectuará la Presidencia. Asimismo, el Comité de Seguridad y Privacidad podrá recabar de personal técnico especializado, propio o externo, la información oportuna para la toma de decisiones.

El Delegado/a de Protección de Datos y los asesores del Comité de Seguridad y Privacidad dispondrán de voz, pero no de voto.

- *Funcionamiento del Comité de Gestión de la Seguridad de la Información y Privacidad*

El Comité de Seguridad y Privacidad, se reunirá con carácter ordinario, al menos una vez cada 6 meses, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

El Secretario/a del Comité levantará actas de sus reuniones, lo cual será firmada por todos los asistentes a la reunión.

De toda la documentación de funcionamiento del Comité de Gestión de la Seguridad de la Información y Privacidad quedará constancia en el expediente electrónico creado a tal efecto en que se recogerán las convocatorias, actas, así como los documentos que son llevados a cabo para su revisión o aprobación.

Si la necesidad de la convocatoria lo requiere, a las reuniones del Comité podrán asistir en calidad de asesores las personas que se estimen pertinentes, disponiendo de voz, pero no de voto.

El Comité se regirá por este Decreto, por la normativa reguladora de la Política de Seguridad y Privacidad, por el Esquema Nacional de Seguridad y por la normativa de protección de datos de carácter personal.

Grupo de Respuesta a Incidentes de Seguridad y Privacidad (Comité de Crisis)

El Comité de Seguridad y Privacidad nombrará un Grupo de Respuesta a Incidentes de Seguridad y Privacidad (Comité de Crisis), cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad y a la privacidad del PRP. Será la persona titular de la Presidencia del Comité de Seguridad y Privacidad quien determine la existencia de tales contingencias y las califique como graves. Las decisiones adoptadas por este grupo serán ratificadas por el Comité de Seguridad y Privacidad en su conjunto cuando sea necesario.

- *Composición del Grupo de Respuesta a Incidentes de Seguridad y Privacidad (Comité de Crisis)*

  El Grupo de Respuesta a Incidentes de Seguridad y Privacidad (Comité de Crisis) estará constituido por los siguientes integrantes:

  - *El Presidente del Comité de Seguridad y Privacidad.*
  - *Las personas responsables de los servicios que se vean afectados por el incidente/brecha de seguridad.*
  - *El Responsable de Seguridad.*
  - *El Delegado/a de Protección de Datos.*

  Pudiendo formar parte del mismo en función de las necesidades:

  - *Personas pertenecientes a asistencias externas con conocimientos en materia de ciberseguridad y/o con conocimiento sobre los sistemas de información afectados.*

  De las decisiones adoptadas por el Comité de Crisis se levantará acta quedando las mismas recogidas en el correspondiente expediente administrativo creado a tal efecto.
  Su composición podrá ser modificada mediante acuerdo del Comité de Seguridad y Privacidad.

- *Funcionamiento*

  Corresponde al Grupo de Respuesta a Incidentes de Seguridad y Privacidad (Comité de Crisis), entre sus funciones, notificar a la autoridad competente en materia de seguridad de las redes y sistemas de información, concretamente a su equipo de respuesta a incidentes de seguridad informática (CSIRT o CERT), los incidentes de seguridad TIC, en los casos y en los términos que determine la normativa aplicable.

  La notificación mencionada en el apartado anterior podrá realizarse bien directamente, bien a través de AndalucíaCERT o por el medio o procedimiento que disponga.

8. Funciones y responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS:

Funciones del Comité de Gestión de la Seguridad de la Información y Privacidad

El Comité de Seguridad y Privacidad coordinará todas las actividades relacionadas con la seguridad de los sistemas de información y ejercerá las siguientes funciones:

a) Aprobar el desarrollo de la política de seguridad de segundo nivel, según lo previsto en el apartado "ESTRUCTURA DE LA DOCUMENTACIÓN DE SEGURIDAD Y PRIVACIDAD" del presente documento.

b) Velar por el desarrollo, implantación, divulgación, cumplimiento y actualización de la Política de Seguridad.

c) *Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en todo el PRP.*

d) *Proporcionar los medios y recursos necesarios para posibilitar la realización de las iniciativas de seguridad planificadas, previéndolo en los presupuestos del PRP.*

e) *Establecer los requisitos de seguridad que se deben cumplir a nivel organizativo, técnicos y de control de los sistemas y servicios, de su disponibilidad y otros que permitan alcanzar los objetivos de Seguridad identificados.*

f) *Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.*

g) *Nombrar un Grupo de Respuesta a Incidentes de Seguridad y Privacidad (Comité de Crisis).*

h) *Aprobar los nombramientos de responsables y responsabilidades en materia de Seguridad de la Información que no sea TIC.*

i) *Comunicar a los terceros que colaboren en la explotación de los sistemas de información la realización de la misma conforme a los exigido en el ENS.*

j) *Valorar el grado de conformidad de los procedimientos implantados en el PRP con las normas definidas en la Política, estableciendo planes de mejora para aquellos que requieran de una modificación para su total conformidad.*

k) *Aprobar los procedimientos que se definan para dar cumplimiento a las normas derivadas de la Política de Seguridad.*

l) *Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.*

m) *Identificar, supervisar, controlar y monitorizar los cambios significativos en la exposición de los activos de información a las amenazas a que se encuentran expuestos.*

n) *Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la Política de Seguridad.*

o) *Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades de cada área.*

p) *Respaldar los planes estratégicos en materia de seguridad definidos por el PRP.*

q) *Establecer mecanismos para compartir la documentación de seguridad con el propósito de normalizarlo en la medida de lo posible en todo el ámbito de la Política de Seguridad.*

r) *Aprobar las actividades de tratamiento a incluir en el Registro de Actividades de Tratamiento, supervisarlo y, aprobar los cambios que se realicen en relación con los mismos, concretando su procedimiento en un documento de seguridad y privacidad de segundo nivel del artículo 20.1 de esta Política de Seguridad y Privacidad.*

s) *Aprobar una metodología de gestión de proyectos que traten datos personales, que garanticen desde el inicio el análisis de riesgo y sus medidas de mitigación, para cumplir la protección de datos desde el diseño y por defecto.*

t) *Aprobar los análisis de riesgo de los tratamientos realizados, así como la implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.*

u) *Aprobar si se debe llevar a cabo una evaluación de impacto sobre la protección de datos, con el asesoramiento previo del Delegado/a de Protección de Datos.*

v) Aprobar la destrucción, seudonimización o anonimización de todo dato personal contenido en los documentos electrónicos y las bases de datos correspondientes tras archivarse por finalizar el procedimiento administrativo, concretándose, en una norma de segundo nivel del artículo 20 de esta Política de Seguridad, tanto los principios como el procedimiento de actuación.

w) Aprobar la implantación del procedimiento de gestión de brechas de seguridad de los datos y, de la correspondiente notificación a la autoridad de control competente y a los afectados, a través de una norma de segundo nivel del artículo 20 de esta Política de Seguridad.

x) Resolver los conflictos de responsabilidades que puedan aparecer entre los diferentes roles y/o entre diferentes áreas en relación con la seguridad y con la protección de datos de carácter personal.

Funciones del Responsable de la información

El Responsable de la información tendrá asignadas las siguientes funciones:

- *Determinar los niveles de seguridad de la información tratada, o requisitos de la información en materia de seguridad, según los parámetros del Anexo I del ENS, siguiendo los criterios de valoración de la Política de Seguridad, recabando al efecto propuesta al Responsable de Seguridad y contando con la participación del Responsable del Sistema.*
- *Valorar las consecuencias de un impacto negativo sobre la seguridad de la información, que efectuará atendiendo a su repercusión en la capacidad del PRP para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de la ciudadanía.*
- *Tratar desde su nivel de responsabilidad los incidentes de seguridad conforme al procedimiento que se establezca al efecto.*
- *Aceptar los niveles de riesgo residual que afectan a la información.*
- *Poner en comunicación del Responsable de Seguridad, cualquier variación respecto a la Información de los que es responsable, especialmente la incorporación de nueva información a su cargo.*

Funciones del Responsable de los servicios

El Responsable de los servicios tendrá asignadas las siguientes funciones:

- *Determina los niveles de seguridad de los servicios, o requisitos de los servicios en materia de seguridad, según los parámetros del Anexo I del ENS, siguiendo los criterios de valoración de la Política de Seguridad, recabando al efecto propuesta al Responsable de Seguridad y contando con la participación del Responsable del Sistema.*
- *Valora las consecuencias de un impacto negativo sobre la seguridad de los servicios, que efectuará atendiendo a su repercusión en la capacidad del PRP para el logro de sus*

objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de la ciudadanía.

- *Tratar desde su nivel de responsabilidad los incidentes de seguridad conforme al procedimiento que se establezca al efecto.*
- *Aceptar los niveles de riesgo residual que afectan a los servicios.*
- *Poner en comunicación del Responsable de Seguridad, cualquier variación respecto a los servicios de los que es responsable, especialmente la incorporación de nuevos servicios a su cargo.*

Responsable de Seguridad

Son funciones del Responsable de Seguridad:

a) Supervisar el cumplimiento de Política de Seguridad, y de sus normas y procedimientos derivados.

b) Asesorar en materia de seguridad de la información a los integrantes del PRP que así lo requieran.

c) Coordinar la interacción con otros organismos especializados.

d) Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.

e) Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.

f) Preparar los temas a tratar en las reuniones del Comité de Seguridad y Privacidad, aportando información puntual para la toma de decisiones.

g) Responsable de la ejecución directa o delegada de las decisiones del Comité de Seguridad y Privacidad.

h) Aprobar la normativa de seguridad derivada de tercer nivel (procedimientos generales).

i) Coordinar y controlar el cumplimiento de las medidas de seguridad definida en los documentos de seguridad correspondientes a todos los ficheros o tratamientos de datos de carácter personal existentes.

j) Mantener el marco documental relativo al sistema de gestión de la seguridad de la información actualizado.

k) Determinar los controles de la ENS necesarios para mitigar el riesgo resultante del Análisis de Riesgos.

l) Elaborar el plan de proyectos anual y coordinar su ejecución.

m) Operar los recursos facilitados por el Comité de Seguridad y Privacidad.

n) Mantener la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

o) Gestionar los incidentes de seguridad de la información que se produzcan, informando de los más relevantes al Comité de Seguridad y Privacidad y, en todo caso, de los que conlleven información de datos personales, al Delegado/a de Protección de Datos.

p) *Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad de la información.*

q) *Aprobar la Categoría del Sistema en base a la valoración de la información y servicios realizada.*

En aquellos sistemas de información que, por su complejidad, distribución, separación física de sus elementos o números de usuarios se necesitara de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad de la Información, el Responsable de Seguridad podrá designar cuantos Responsables de Seguridad Delegados considere necesarios.

Los Responsables de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de Seguridad de la Información teniendo dependencias funcionales directas de él.

Funciones del Responsable del Sistema

Son funciones del Responsable del Sistema:

a) *Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.*

b) *Elaborando los procedimientos operativos necesarios.*

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

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

e) *Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y el Comité de Seguridad y Privacidad.*

f) *Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.*

g) *Llevar a cabo las funciones del administrador de la seguridad del sistema:*

- *La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.*
- *La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.*
- *Aprobar los cambios en la configuración vigente del Sistema de Información.*
- *Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.*
- *Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.*
- *Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.*
- *Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.*

Así mismo, el Responsable del Sistema podrá acordar la suspensión del manejo de determinada 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

deberá ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de Seguridad antes de ser ejecutada.

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

La designación y delegación de funciones en los Responsables del Sistema Delegados corresponde al Responsable de Sistemas, sin perjuicio de que la responsabilidad final siga recayendo sobre el Responsable del Sistema.

Los Responsables del Sistema Delegados se harán cargo en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de Información, así como también tendrán dependencia funcional directa con el Responsable del Sistema que es a quién reportan.

9. Otras responsabilidades

Se podrán designar otras responsabilidades para garantizar el cumplimiento y la implantación de las medidas de seguridad del anexo II del ENS.

10. Conflictos

En el caso de conflicto y, de acuerdo al principio de jerarquía que rige en el PRP, deberá ser resuelto por el superior jerárquico, a excepción de los siguientes conflictos:

- *En caso de conflicto de responsabilidades entre los diferentes roles y/o entre diferentes áreas en relación con la seguridad y con la protección de datos de carácter personal, este será resuelto por la Comisión de Seguridad y Privacidad.*
- *En caso de conflicto con la normativa de seguridad prevalecerá el criterio que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.*

11. Obligaciones del personal

Todos los miembros del PRP tienen la obligación de conocer y cumplir la presente Política de Seguridad y privacidad, las normativas y procedimientos derivados de la misma, tales como las relativas a la protección de datos de carácter personal, siendo responsabilidad del Comité de Seguridad y Privacidad disponer de los medios necesarios para que la información llegue a los afectados.

12. Asesoramiento especializado en materia de seguridad de la información

El Responsable de Seguridad de la Información será el encargado de coordinar los conocimientos y las experiencias disponibles en el PRP con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos o empresa especializada contratada exterior.

13. Tratamiento de datos de carácter personal

1. *Todos los sistemas de información del PRP se ajustarán a lo exigido por el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por el que se aprueba el Reglamento General de Protección de Datos, en adelante, Reglamento General de Protección de Datos (RGPD), además de a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantías y Derechos Digitales (LOPDGDD), así como al resto de la normativa general o sectorial de protección de datos de carácter personal que sea de aplicación. Todos los tratamientos de datos de carácter personal, automatizados o no automatizados, se sujetarán a la citada norma cuando se encuentren dentro de su ámbito de aplicación.*
2. *Las actividades de tratamiento de datos de carácter personal deberán catalogarse en atención a sus finalidades, y estarán recogidas en el Registro de Actividades de Tratamiento, con la información establecida en el art.30 del RGPD.*
3. *El PRP hará público el inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información incluida en el Registro de Actividades de Tratamiento y su base legal.*
4. *Se aplicarán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Las medidas de seguridad serán establecidas para cada actividad de tratamiento en virtud del resultado de los análisis de riesgos efectuadas a las mismas o, tras la oportuna evaluación de impacto de protección de datos, en caso de ser necesaria. En caso de conflicto con la normativa de seguridad prevalecerá el criterio que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.*

14. Registro de Actividades de Tratamiento

1. *El PRP dispone de un Registro de Actividades de Tratamiento del PRP, que es configurado como un registro administrativo en el que han de constar las actividades en las que se traten datos personales y que sean llevadas a cabo en el organismo. Su contenido se detalla en el artículo 30 del RGPD.*
2. *Este Registro de Actividades de Tratamiento será accesible en el portal web y en el portal de Transparencia del PRP.*
3. *Dicho Registro de Actividades de Tratamiento se cumplimentará de acuerdo a lo establecido en un documento de seguridad y privacidad de segundo nivel del artículo 20.1 de esta Política de Seguridad y Privacidad, teniendo en cuenta que el Comité de Seguridad y Privacidad será quien apruebe, modifique o suprima estos registros, a propuesta de la Delegado/a de Protección de Datos, o a propuesta del Jefe de servicio correspondiente con la supervisión previa de la Delegado/a de Protección de Datos.*

15. Responsables de los Tratamientos de datos de carácter personal

Será responsable del tratamiento de datos de carácter personal el PRP como organismo que determina las fines y medios del tratamiento.

El PRP es responsable/corresponsable de todos los tratamientos de datos de carácter personal que se realicen en el desarrollo de su actividad, salvo que se indique lo contrario en un tratamiento concreto.

Estos tratamientos se realizan sobre los datos de carácter personal de los usuarios de los servicios que ofrece en el desarrollo de su actividad que podrán ser obligados tributarios, sus representantes, empleados públicos o cualquier otra persona que utilice sus servicios. Todos ellos tienen el concepto de interesados.

16. Encargados de los Tratamientos de datos de carácter personal.

Si los Responsables de los Tratamientos designaran a un Encargado del Tratamiento lo harán únicamente por cada tratamiento a un Encargado de Tratamiento que ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al RGPD y garantice la protección de los derechos de las personas interesadas, de conformidad con el artículo 28 del RGPD.

Las principales funciones y responsabilidades, dentro de su ámbito de actuación, son las establecidas en el artículo 28 del RGPD y demás normativa de aplicación.

Tanto el Responsable como el Encargado del Tratamiento deberá determinar claramente cuándo el tratamiento se realiza bajo su autoridad, conforme a lo establecido en el artículo 29 del RGPD y cuándo se realiza mediante un Encargado de Tratamiento sujeto a lo establecido en el artículo 28 del RGPD.

17. Delegado/a de Protección de Datos

1. *La persona que ostente la condición de Delegado/a de Protección de Datos podrá poner en conocimiento del Comité de Seguridad y Privacidad las cuestiones relacionadas con la protección de datos que sea necesario y participará, desde el inicio, en todas las cuestiones y proyectos relacionados con la protección de datos, contribuyendo así al cumplimiento de la protección de datos personales desde el diseño y por defecto.*
2. *Son funciones de la persona que ostente la condición de Delegado/a de Protección de Datos, entre las demás que le corresponden de conformidad con el artículo 39 del RGPD y demás normativa de aplicación, las siguientes:*
    - *Informar y asesorar al PRP o a los encargados del tratamiento y al personal que se ocupe del tratamiento, de las obligaciones que les incumben en virtud del RGPD, así como de otras disposiciones de protección de datos de la Unión Europea y de sus Estados miembros.*
    - *Supervisar el cumplimiento de las políticas del PRP o de los encargados de tratamiento de éste en materia de protección de datos personales.*

- *Supervisar el cumplimiento de lo dispuesto en el RGPD y en la LOPDGDD, así como el cumplimiento de otras disposiciones de protección de datos de la Unión Europea y de sus Estados miembros.*
- *Proponer a la Comisión de Seguridad y Privacidad, para su aprobación, normas o metodologías internas referidas a la protección de datos en el PRP.*
- *Asesorar y supervisar 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.*
  - *Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos personales.*
  - *Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.*
  - *Establecimiento de mecanismos de recepción, gestión y 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 PRP – 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 implementación de políticas de protección de datos.*
  - *Auditoría de protección de datos.*
  - *Establecimiento y gestión de los registros de actividades de tratamiento.*
  - *Análisis de riesgo 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 libertados 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.*
- *Supervisar que el sistema de gestión de protección de datos es conveniente, adecuado y eficaz y promover la mejora continua.*
- *Supervisar si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con el RGPD.*
- *Supervisar los resultados de las auditorías de protección de datos.*

Los datos del Delegado/a serán comunicados a la autoridad de control competente para que actúe como punto de contacto entre ésta y el PRP.

18. Análisis y Gestión de Riesgos

1. *La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos, de conformidad con lo dispuesto en el ENS, y en la reevaluación periódica.*
2. *El Responsable de Seguridad es el encargado de que el análisis se realice en tiempo y forma, así como de identificar carencias y debilidades y ponerlas en conocimiento de los Responsables de la Información y del Servicio.*

19. Formación y concienciación

El objetivo es lograr la plena conciencia respecto a que la Privacidad y la Seguridad de la Información afecta a todos los miembros del PRP y a todas las actividades de acuerdo al principio de Seguridad Integral recogido en el ENS. A estos efectos, se propondrán y organizarán anualmente sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se gestionan.

20. Estructura de la Documentación de Seguridad y Privacidad

1. La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles de manera que cada documento de un nivel se fundamenta en los de nivel superior.

Todos estos niveles prestarán especial atención a las exigencias derivadas del Esquema Nacional de Seguridad, así como a la normativa aplicable en materia de protección de datos de carácter personal.

Se establecen los siguientes niveles.

> ***Primer nivel**: Política de Seguridad de la Información. Aprobado por el Consejo Rector a propuesta de la Presidencia del PRP. De obligado cumplimiento, y cuya responsabilidad de revisión, modificación, actualización y posterior propuesta para su aprobación será competencia del Comité de Seguridad y Privacidad.*

***Segundo nivel**: Normativas y Procedimientos de Seguridad y Privacidad. De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente. Estos documentos serán aprobados por el Comité de Seguridad y Privacidad a propuesta de cualquiera de sus miembros. Las normas de seguridad y privacidad deberán describir los principios a seguir y, serán concretadas por los procedimientos de seguridad y privacidad, que describirán las acciones a realizar de una manera más específica en los siguientes aspectos (listado meramente enunciativo):*

a. *Clasificación y tratamiento de la información.*
b. *Roles, responsabilidades de seguridad y personas autorizadas para tratar datos en atención a su trabajo diario en el aplicativo del PRP.*
c. *Seguridad física.*
d. *Gestión de operaciones de tratamiento de la información.*
e. *Control de accesos.*
f. *Adquisición y desarrollo de sistemas.*
g. *Gestión de incidentes de seguridad.*

***Tercer nivel**: Procedimientos Técnicos de Seguridad. Orientados a resolver tareas consideradas críticas por el perjuicio que causaría una actuación inadecuada de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. La responsabilidad de detectar los perjuicios y proponer las soluciones correspondientes es el Responsable del Sistema. La aprobación de estos procedimientos técnicos será del Responsable de Seguridad.*

***Cuarto nivel**: Informes, registros, evidencias electrónicas y plantillas. En este último nivel se puede incluir todo tipo de documentación técnica o especializada que se considere necesario para completar y facilitar el desarrollo de las medidas de seguridad. De esta manera, los informes son documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o de una evaluación. Los registros de actividad o alertas de seguridad son documentos de carácter técnico que recogen amenazas y vulnerabilidades a sistemas de información y son responsabilidad del equipo de seguridad. Las evidencias electrónicas se generan durante todo el ciclo de vida de los sistemas de información, pudiendo abarcar uno o más sistemas en función del aspecto tratado.*

2. El Comité de Seguridad y Privacidad establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la Política de Seguridad.

21. Revisión, distribución y cumplimiento

La Política de Seguridad y Privacidad deberá mantenerse actualizada permanentemente para adecuarla a los servicios de Administración Electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

El Comité de Seguridad y Privacidad velará por la revisión, distribución y cumplimiento de la presente Política de Seguridad y Privacidad. La revisión de la Política, de las Normas y Procedimientos derivados de ella se realizará al menos una vez al año, así como cada vez que

ocurran cambios significativos en los elementos del Sistema de Información que puedan afectarle directa o indirectamente, distribuyéndose a todo el personal afectado.

La versión más actualizada de la Política de Seguridad y Privacidad, se publicarán en la Intranet corporativa y el portal web del PRP.

22. Proceso disciplinario

Se seguirá el proceso disciplinario formal existente y contemplado en las normas internas del PRP para el personal que viole la Política de Seguridad y Privacidad, así como las Normas y Procedimientos derivados de ella.

23. Disposición final. Publicidad de la Política de Seguridad y Privacidad

La presente Política de Seguridad y Privacidad del PRP actualiza la aprobada por el Consejo Rector del PRP el 23 de junio de 2020 a la legislación vigente en la materia. Esta Política consolida los cambios, deja sin efecto el anterior texto y, será efectiva desde la fecha de su aprobación por el Consejo Rector del Organismo. Se publicará en el portal web del PRP y en la Intranet corporativa."

b) La actualización de esta Política de Seguridad y Privacidad es efectiva desde la fecha de su aprobación por el Consejo Rector de la Agencia y hasta que sea de nuevo actualizada, modificada o, reemplazada por una nueva Política. Esta Política, que consolida los cambios y deja sin efecto el anterior texto de 23 de junio 2020, se publicará en el portal web del PRP y, en la Intranet corporativa."

Sometida la propuesta anterior a votación, resulta aprobada por 12 votos a favor (10 del Grupo Popular, 1 del Grupo Socialista y 1 de Con Málaga) y 1 abstención del Grupo Vox, lo que representa la mayoría absoluta de los miembros que de hecho y derecho componen este Órgano colegiado.

Y para que conste y surta los efectos oportunos, expido la presente certificación de orden y con el Vº Bº de la Presidenta, con las advertencias y salvedades contenidas en el artículo 206 del Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.

Lo que le traslado a Vd. indicándole asimismo, en relación a los recursos que en su caso puede interponer contra este acuerdo, que dicho acto pone fin a la vía administrativa, conforme a lo dispuesto en el art. 52.2 de la Ley 7/1985, no obstante lo cual, contra el mismo podrá interponer, con carácter potestativo, y según dispone el art. 52.1 de la citada Ley 7/1985 y el 123 de la Ley 39/2015, de fecha 1 de octubre, Recurso de Reposición en el plazo de un mes contado desde la notificación, ante el mismo órgano que lo dictó; o bien interponer, directamente, Recurso Contencioso-Administrativo en el plazo de dos meses contados desde la notificación, ante el Juzgado de lo Contencioso-Administrativo con Sede en Málaga. Si optara por interponer el Recurso de Reposición potestativo, no podrá interponer Recurso Contencioso-Administrativo hasta que aquél sea resuelto expresamente o se haya producido su desestimación por silencio. No obstante podrá interponer cualquier recurso que estime procedente bajo su responsabilidad.

Patronato de Recaudación Provincial

Hacienda electrónica local y provincial
DIPUTACIÓN DE MÁLAGA

DOCUMENTO ELECTRÓNICO

CÓDIGO DE VERIFICACIÓN DEL DOCUMENTO ELECTRÓNICO

2f562b2d42dcb60bc385893b1a6b8aa100ba9b68

Dirección de verificación del documento: **https://sede.malaga.es/patronatoderecaudacion**
Hash del documento: 08e42e0639dd7d09ad163253cf5f12653286861f8809235dc14d19d0af3bb67b16779055d6670585f2c44
1ab5aa4928d2225f81f3a820f91822f609672688f02

METADATOS ENI DEL DOCUMENTO:

Version NTI: http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e

Identificador: ES_LA0010492_2023_00000000000000000000017897849

Órgano: LA0003318

Fecha de captura: 18/10/2023 12:17:44

Origen: Administración

Estado elaboración: Original

Formato: PDF

Tipo Documental: Certificado

Tipo Firma: XAdES internally detached signature

Valor CSV: 2f562b2d42dcb60bc385893b1a6b8aa100ba9b68

Regulación CSV: Decreto 3628/2017 de 20-12-2017

Código QR para validación en sede

Código EAN-128 para validación en sede

Ordenanza reguladora del uso de medios electrónicos en el ámbito de la Diputación Provincial de Málaga:
https://sede.malaga.es/normativa/ordenanza_reguladora_uso_medios_electronicos.pdf

Política de firma electrónica y de certificados de la Diputación Provincial de Málaga y del marco preferencial para el sector público provincial (texto consolidado):
https://sede.malaga.es/normativa/politica_de_firma_1.0.pdf

Procedimiento de creación y utilización del sello electrónico de órgano de la Hacienda Electrónica Provincial:
https://sede.malaga.es/normativa/procedimiento_creacion_utilizacion_sello_electronico.pdf

Acuerdo de adhesión de la Excma. Diputación Provincial de Málaga al convenio de colaboración entre la Administración General del Estado (MINHAP) y la Comunidad Autónoma de Andalucía para la prestación mutua de soluciones básicas de Administración Electrónica de fecha 11 de mayo de 2016:
https://sede.malaga.es/normativa/ae_convenio_j_andalucia_MINHAP_soluciones_basicas.pdf

Aplicación del sistema de Código Seguro de Verificación (CSV) en el ámbito de la Diputación Provincial de Málaga:
https://sede.malaga.es/normativa/decreto_CSV.pdf