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 23 de junio de 2020 adoptó entre otros, el siguiente acuerdo que se transcribe con el siguiente tenor literal:

"Punto nº 7.- Aprobación, si procede, de Política de Seguridad de la Información y Privacidad del Patronato de Recaudación Provincial de Málaga.

Llegado a este Punto incluido en el Orden del día, se procede al tratamiento de la siguiente Propuesta:

PROPUESTA DE LA PRESIDENCIA

Exposición de motivos.

El Pleno del Patronato de Recaudación Provincial, en sesión ordinaria celebrada el 23 de julio de 2012, aprobó por unanimidad el documento de Política de Seguridad del organismo, según lo dispuesto en la legislación vigente y 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.

La rápida evolución de las TIC, de las demandas de usuarios y del marco normativo requiere de una constante adaptación de estos instrumentos para que dicho nivel de seguridad no solo se mantenga, sino que se vea reforzado. Para ello, desde la administración central del estado se han dispuesto herramientas y normativas que regulan y coordinan estas adaptaciones, que en definitiva son las que se reflejan en las presentes propuestas.

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 marco normativo reciente, 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.

En el ámbito europeo, el 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 - RGPD), pretende sentar las bases de una normativa de privacidad que se adecue a la nueva realidad

tecnológica y social, dando un paso más en la defensa de los derechos de los ciudadanos, ante la creciente preocupación de éstos durante los últimos años por la falta de control sobre sus propios datos que han podido percibir cuando los han facilitado a terceros. La LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPD), complementa al RGPD en los ámbitos en los que este permite ser desarrollado.

El RGPD establece la obligación de designar un Delegado de Protección de Datos (en adelante DPD) a todas las Administraciones Públicas (a excepción de los Tribunales de Justicia cuando actúen en el ejercicio de la función judicial) como garante del cumplimiento de la normativa de protección de datos en las organizaciones. El Patronato de Recaudación tiene designado un DPD interno cuyos datos de contacto han sido comunicados a la Agencia Española de Protección de Datos. La Agencia garantizará que el DPD participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales en el organismo.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, reconoce, como derecho de las personas en sus relaciones con las Administraciones Públicas, la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas (artículo 13.h).

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, determina, en su artículo 3.2, que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

El Esquema Nacional de Seguridad (ENS) se regula por el Real Decreto 3/2010, de 8 de enero, modificado a su vez por el Real Decreto 951/2015, de 23 de octubre, y tiene como finalidad fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. Al mismo tiempo, establece el marco regulatorio de la Política de Seguridad de la Información que deberá ser plasmado en un documento, accesible y comprensible para todos los miembros, que define lo que significa la seguridad de la información en una organización determinada y que rige la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

El artículo 11.1 del ENS establece que "Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente". 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.

Con la aprobación de esta nueva política de Seguridad y Privacidad, se reemplaza y se deja sin efecto a la anterior Política del organismo, aprobada por el Pleno del Patronato de Recaudación el 23 de julio de 2012.

Como es sabido, la materia de seguridad y de privacidad (protección de datos) están estrechamente vinculadas por lo que, en este Patronato, van a ser tratadas de manera integral, dado que todas las actividades de tratamientos de datos personales deben tener analizados sus riegos para concretar las medidas técnicas y organizativas de seguridad a implantar. Aunque en la Seguridad Informática se debe distinguir dos propósitos de protección -la Seguridad de la Información (cuyo objetivo de protección son los datos mismos) y la Protección de Datos (cuyo objetivo de protección es el contenido de la información sobre personas)-, las medidas de protección aplicadas normalmente van a ser las mismas (y previstas en el ENS, donde se incluyen las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado).

La nueva la Política de Seguridad permitirá garantizar en la mejor medida posible, la confidencialidad, la integridad y disponibilidad de los 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 los medios electrónicos.

Así, para dar cumplimiento a los anteriores requerimientos, se considera oportuno constituir en el ámbito del Patronato de Recaudación Provincial de Málaga un Comité de Gestión de la Seguridad de la Información y de Privacidad como órgano colegiado, según lo previsto en la Sección 3ª del Capítulo 2º del Título preliminar de la Ley 40/2015 de Régimen Jurídico de las Administraciones Públicas.

Por tanto, el objetivo es adecuar y actualizar la Política de Seguridad a las nuevas normas, así como integrarla con la política de privacidad del organismo y, cumplir las dos obligaciones básicas en materia de seguridad TIC recogidas en el Esquema Nacional de Seguridad:

- *Por un lado, estableciendo una nueva estructura de organización y gestión de la seguridad y privacidad de la Agencia acorde con la actual legislación y reorganización del PRP. A este respecto, mediante este nuevo documento, se crea un nuevo Comité de Seguridad y Privacidad y, se establece su composición, funciones y régimen de funcionamiento. Se incluye de este modo, en un mismo texto normativo, la Política de Seguridad y la regulación de la composición y funcionamiento del Comité de Seguridad (y privacidad), dado que este último forma parte de la estructura que sustenta la propia política de seguridad. Para la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad del organismo, también se ordena la formación, dentro del Comité, de un Grupo de Respuesta a Incidentes de Seguridad y Privacidad.*

- *Por otro lado, aprobando el Documento de Política de Seguridad y de Privacidad del Patronato de Recaudación. Para ello define los roles o funciones de seguridad, prevé las normas para su desarrollo, establece los principios de la política de seguridad del organismo, la gestión de riesgos, obligaciones del personal y, por último, refleja las obligaciones de auditoría de seguridad ya establecidas legalmente. Finalmente, también se definen aspectos organizativos referente a la materia de protección de datos que afectan directamente a la seguridad TIC. Entre ellos el principio de integridad y confidencialidad de los datos de carácter personal recogido en el artículo 5.1.f) del RGPD que supone que los datos personales serán tratados de tal*

manera que se garantice una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Asimismo, mediante este documento, se crea el Registro de Actividades de Tratamiento, y se definen las figuras fundamentales de la protección de datos respecto a la política de seguridad de la Agencia: el Responsable del Tratamiento, el Encargado del Tratamiento y el Delegado de Protección de Datos.

Dado que el Patronato de Recaudación Provincial está realizando todas las actuaciones necesarias para alcanzar el compromiso de dar cumplimiento a las obligaciones normativas, esta Presidencia, conocido el informe emitido por el Director de Seguridad y la Delegada de Protección de Datos, propone al Consejo Rector del Organismo que acuerde lo siguiente:

a) Aprobar un nuevo Documento de Política de Seguridad de la Información y Privacidad del Patronato de Recaudación Provincial de Málaga, que tenga por objeto garantizar la seguridad de los sistemas de información y las comunicaciones, de la información y los servicios utilizados por estos sistemas, así como el crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo 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, así como establecer una nueva estructura de organización y gestión de la seguridad y privacidad de la Agencia, integrando la regulación del Comité dentro de la Política de Seguridad (por simplificación normativa), cuyo texto es el siguiente:

"POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y DE PRIVACIDAD DEL PATRONATO DE RECAUDACIÓN PROVINCIAL DE MALAGA

Texto refundido

1. *Objeto*

El presente documento define y establece los principios que conforman la Política de Seguridad de la Información del Patronato de Recaudación Provincial de Málaga, en adelante el Patronato, 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 Patronato 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 de la Agencia que velará por su cumplimiento.

2. *Ámbito de aplicación*

La presente Política es aplicable a toda la información y activos de información del Patronato 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 Patronato, 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 Patronato.

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

3. *Principios básicos de la Seguridad de la Información*

Los principios básicos que regirán la política de seguridad TIC del Patronato de Recaudación serán, además de los establecidos en el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, los siguientes:

a) *Principio de disponibilidad de la información. Se permitirá el acceso autorizado a la información, siempre que sea necesario.*
b) *Principio de prevención. Todos aquellos activos (infraestructura, soportes, sistemas comunicaciones, etc.) donde la información reside, viaja o es procesada, deben estar adecuadamente protegidos. Se evitará, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella en función de una evaluación de amenazas y riesgos.*
c) *Principio de detección. La Seguridad de la Información no es algo estático, por lo que debe ser constantemente controlada y periódicamente revisada. Los servicios se pueden degradar rápidamente debido a incidentes que pueden producir desde una simple desaceleración hasta la detención de los mismos, por lo que se monitorizará la operación de los servicios de manera continua para detectar anomalías en los niveles de prestación requeridos, actuando en consecuencia.*
d) *Principio de reacción. Se deberá minimizar la probabilidad de ocurrencia de incidentes, así como reducir su frecuencia y duración de los mismos, en especial los incidentes a través de Internet y de los Sistemas de Información puestos a disposición de los ciudadanos. Se establecerán mecanismos para responder eficazmente a los incidentes de seguridad, designando un punto de contacto para centralizar y gestionar el intercambio de información asociada a los incidentes de seguridad, así como estableciendo protocolos para el intercambio de información relacionada con dichos incidentes.*
e) *Principio de recuperación. Se deberá garantizar la disponibilidad de los servicios ofrecidos a la ciudadanía, en la medida de lo posible y en función de la criticidad de los mismos.*
f) *Principio de responsabilidad. Todas las personas que tienen acceso a la información del Patronato son responsables de observar las normas de seguridad establecidas, por lo que deben estar adecuadamente formadas y concienciadas. Los roles y responsabilidades de seguridad de todo el personal estarán claramente definidos y documentados.*
g) *Integridad y confidencialidad de los datos de carácter personal. Los datos personales serán tratados de tal manera que se proteja contra accesos y alteraciones no autorizados o ilícitos y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.*

4. *Objetivos generales de la política de Seguridad*

El Patronato define los siguientes objetivos generales en la presente Política de Seguridad:

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) *Crear el Registro de Actividades de Tratamiento, el cual deberá mantenerse, publicarse por medios electrónicos en la web del Patronato y, recoger 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 Patronato acciones formativas y de concienciación relativas a la Seguridad de la Información y a la protección de datos de carácter personal.*

5. *Responsabilidad de la Política de Seguridad*

La responsabilidad general y última de la presente Política de Seguridad recae sobre el Patronato de Recaudación Provincial de Málaga.

6. *Organización y gestión de la Seguridad de la Información*

La estructura organizativa de la gestión de la seguridad de la información del Patronato de Recaudación Provincial en relación con el Esquema Nacional de Seguridad está compuesta por los siguientes agentes:

a) *El Comité de Gestión de la Seguridad de la Información y Privacidad, en adelante Comité de Seguridad y Privacidad y, el Grupo de Respuesta a Incidentes de Seguridad y Privacidad.*
b) *Unidad de Seguridad, Sistemas y comunicaciones, cuya persona responsable (Director de Seguridad) tendrá la condición de Responsable de Seguridad TIC.*
c) *Responsables de la Información y Responsables de los Servicios.*
d) *Responsable de Sistemas.*

7. *Creación del Comité de Gestión de la Seguridad de la Información y Privacidad*

1. *Se crea un Comité de Gestión de Seguridad de la Información y Privacidad como responsable de implementar la Política de Seguridad y como órgano de dirección y seguimiento en materia de Seguridad y Protección de Datos en el ámbito del Patronato,*

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.

2. *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.*

8. *Funciones del Comité de Seguridad 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 artículo 28.1 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 Patronato.*
d) *Proporcionar los medios y recursos necesarios para posibilitar la realización de las iniciativas de seguridad planificadas, previéndolo en los presupuestos del Patronato.*
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 (protección de datos de carácter personal).*
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 Patronato 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 Patronato.*
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 art. 28.1 de esta Política de Seguridad.*
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 art. 28 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 art. 28 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.*

9. *Composición del Comité de Seguridad y Privacidad*

1. *El Comité de Seguridad y Privacidad estará compuesto por los siguientes miembros:*
   a) *Presidente/a: Gerente del Patronato.*
   b) *Vocales:*
      - *Jefe/a de las Unidades de Recaudación/Tesorería.*
      - *Responsable de Gestión Tributaria e Inspección.*
      - *Responsable de Seguridad.*
      - *Delegado/a de Protección de Datos.*
   c) *Secretario/a: Jefe/a del Servicio de Planificación y Modernización. Con voz y voto. Su participación podrá ser delegable en personal de su área.*
2. *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.*
3. *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 podrá recabar de personal técnico especializado, propio o externo, la información oportuna para la*

toma de decisiones. Los asesores del Comité de Seguridad y Privacidad dispondrán de voz, pero no de voto.

10.*Funcionamiento del Comité de Seguridad y Privacidad*

El Comité de Seguridad, 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 del Comité levantará actas de sus reuniones.

De toda la documentación de funcionamiento del Comité de Seguridad quedará constancia en registro electrónico.

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, por el Esquema Nacional de Seguridad y por la normativa de protección de datos de carácter personal.

11.*Grupo de Respuesta a Incidentes de Seguridad y Privacidad*

1. *El Comité de Seguridad y Privacidad nombrará un Grupo de Respuesta a Incidentes de Seguridad y Privacidad, 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 en su conjunto cuando sea necesario.*
2. *La composición mínima de este grupo será la siguiente:*
    a) *La persona titular de la Presidencia del Comité de Seguridad y Privacidad.*
    b) *Las personas titulares de los Servicios que se vean afectados por el incidente.*
    c) *El Responsable de Seguridad.*
    d) *El Delegado/a de Protección de Datos.*
3. *Su composición podrá ser modificada mediante acuerdo del Comité de Seguridad y Privacidad.*
4. *Corresponde al Grupo de Respuesta a Incidentes de Seguridad y Privacidad, 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.*
5. *La notificación mencionada en el apartado anterior podrá realizarse bien directamente, bien a través de AndalucíaCERT o por el medio o procedimiento que disponga.*

12. *Unidad de Seguridad, Sistemas y comunicaciones*

1. *La Agencia, de acuerdo con el acuerdo plenario de la Diputación Provincial de Málaga de fecha 20 de abril de 2018 (que ratifica el acuerdo del Consejo Rector del PRP de 17 de abril de 2018), cuenta con una Unidad de Seguridad, Sistemas y comunicaciones, en el que habrá personal adscrito a funciones de seguridad y personal adscrito a funciones que velen por el correcto funcionamiento de los sistemas de información, garantizándose el principio de función diferenciada recogido en el ENS.*
2. *El Director de Seguridad de la Unidad de Seguridad, Sistemas y comunicaciones, tiene la condición de Responsable de Seguridad TIC, cuya función esencial es planificar lo que se ha de hacer en materia de seguridad, así como supervisar que se haya hecho adecuadamente, y todo ello atendiendo a los principios de:*
    a. *Autenticación.*
    b. *Confidencialidad: la información asociada a los servicios electrónicos al ciudadano del Patronato sólo debe poder ser conocida por las personas autorizadas para ello.*
    c. *Integridad: la información asociada a los servicios electrónicos al ciudadano del Patronato no debe ser alterada por personas no autorizadas.*
    d. *Disponibilidad: garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma siempre que lo requieran, así como garantía de que los servicios relativos a la Administración Electrónica permanecerán disponibles 24 horas al día durante 365 días al año.*
    e. *Trazabilidad.*

13. *Responsable de Seguridad TIC*

Son funciones del Responsable de Seguridad TIC:

- *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 Patronato 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.*
- *h. Aprobar la normativa de seguridad derivada de tercer nivel (procedimientos generales).*
- *i. Coordinar y controlar el cumplimiento de las medidas de seguridad definidas 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.*
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 y, en todo caso, de los que conlleven información de datos personales, al DPD.*
p. *Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad de la información.*

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 Responsables 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.

14.*Responsables de la Información y responsables de Servicio*

Los Responsables de la Información y los Responsables del Servicio dentro de su ámbito de actuación y de sus competencias, tienen la potestad de establecer en materia de seguridad, los requisitos de los servicios y de la información que manejan. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.

Serán responsables de la prestación del servicio, que debe atender a requisitos de seguridad de la información tratada en cuanto a disponibilidad, accesibilidad, interoperabilidad, autenticidad, trazabilidad, confidencialidad e integridad.

15.*Responsable del Sistema*

Son funciones del Responsable de Sistemas:

1. *Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, sus especificaciones, instalación y verificación de su correcto funcionamiento.*

2. *Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de seguridad*
3. *Elaborar los procedimientos operativos de seguridad de los sistemas de información*
4. *Elaborar los Planes de Continuidad de los Sistemas de Información*

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 de Sistema, el Patronato podrá designar cuantos Responsables de Sistemas Delegados considere necesario.

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

Los Responsables de Sistemas 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.

16.*Asignación de responsabilidades en materia de Seguridad.*

- *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 Seguridad, Sistemas y comunicaciones del PRP.*
- *El* ***Responsable del Sistema*** *será el titular del puesto de Responsable de sistemas del PRP, que es la persona al frente del Departamento de Sistemas.*

17.*Otras responsabilidades*

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

18.*Conflictos*

En el caso de conflicto y, de acuerdo al principio de jerarquía que rige en el Patronato de Recaudación Provincial de Málaga, 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.*

19.*Obligaciones del personal*

Todos los miembros del Patronato 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.

20.*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 Patronato 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.

21.*Tratamiento de datos de carácter personal*

1. *Todos los sistemas de información de la Agencia 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, además de a la Ley Orgánica 3/20178, de 5 de diciembre, de Protección de Datos y Garantías y Derechos Digitales, 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 Patronato de Recaudación Provincial 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.*

22.*Creación del Registro de Actividades de Tratamiento*

1. *Se crea el Registro de Actividades de Tratamiento del Patronato de Recaudación, 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 Patronato de Recaudación Provincial.*
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 art. 28.1 de esta Política de Seguridad, teniendo en cuenta que el Comité de Seguridad y privacidad será quien apruebe, modifique o suprima estos registros, a propuesta de la Delegada de Protección de Datos, o a propuesta del Jefe de servicio correspondiente con la supervisión previa de la Delegada de protección de Datos.*

23.*Responsables de los Tratamientos de datos de carácter personal.*

Será responsable del tratamiento de datos de carácter personal el Patronato de Recaudación Provincial como organismo que determina las fines y medios del tratamiento. La Agencia Pública Administrativa de Servicios Económicos "Patronato de Recaudación Provincial" (en adelante "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.

24.*Encargados de los Tratamientos de datos de carácter personal.*

1. *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 Reglamento General de Protección de Datos y garantice la protección de los derechos de las personas interesadas, de conformidad con el artículo 28 del Reglamento General de Protección de Datos.

2. *Las principales funciones y responsabilidades, dentro de su ámbito de actuación, son las establecidas en el artículo 28 del Reglamento General de Protección de Datos y demás normativa de aplicación.*
3. *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 Reglamento General de Protección de Datos y cuándo se realiza mediante un Encargado de Tratamiento sujeto a lo establecido en el artículo 28 de dicho Reglamento General de Protección de Datos.*

25.*Delegado de Protección de Datos*

1. *La persona que ostente la condición de Delegado 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 de Protección de Datos, entre las demás que le corresponden de conformidad con el artículo 39 del Reglamento General de Protección de Datos y demás normativa de aplicación, las siguientes:*
   - *Informar y asesorar al Patronato 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 Patronato 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 LOPD y GDD, 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 la Agencia.*
   - *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 Patronato – 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 Reglamento.*
- *Supervisar los resultados de las auditorías de protección de datos.*

El DPD formará parte del Comité de Seguridad y Privacidad del PRP como vocal del mismo, y sus datos de contacto habrán sido comunicados a la autoridad de control competente para que actúe como punto de contacto entre ésta y el Patronato.

26.*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 artículo 6 del ENS, y en la reevaluación periódica.*
2. *El Responsable de Seguridad TIC 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.*

3. *La gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionadas a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el Responsable de Seguridad TIC, recogiéndose en un Plan de Acción anual.*
4. *En particular, para realizar el análisis de riesgos se utilizará la herramienta PILAR que facilita el seguimiento de la aplicación de las medidas de seguridad seleccionadas y proporciona un valor de riesgo residual estabilizado y comparable entre diferentes sistemas de información. Se utilizará la metodología MAGERIT como metodología de realización de análisis de riesgos.*
5. *El Responsable de Sistemas realizará, con periodicidad al menos anual, un análisis de riesgos cuyas conclusiones se plasmarán en actuaciones para tratar y mitigar el riesgo, o incluso replantear la seguridad de los sistemas en caso necesario.*

   Se realizarán análisis de riesgos en periodos inferiores a un año cuando:

   a) Se modifique la información manejada.
   b) Se modifiquen los servicios prestados.
   c) Ocurran incidentes graves de seguridad.
   d) Se reporten vulnerabilidades graves.

   Las conclusiones de los análisis de riesgos serán elevadas al Responsable de Seguridad, al Delegado/a de Protección de Datos y, al Comité de Seguridad y Privacidad.

27. *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 Patronato y a todas las actividades de acuerdo al principio de Seguridad Integral recogido en el art. 5 del 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.

28. *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 de la Agencia. 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.*

La siguiente tabla resume el marco normativo y la responsabilidad de su aprobación:

Nivel normativo	***Documento***	***Aprueba***
Primero	*Política de Seguridad*	*Consejo Rector*
Segundo	*Normas y procedimientos de Seguridad y privacidad*	*Comité de Seguridad y Privacidad*
Tercero	*Procedimientos Técnicos de seguridad*	*Responsable de Seguridad TIC*
Cuarto	*Informes, registros, evidencias y plantillas*	*Responsable de Sistemas*

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.*

29.*Revisión, distribución y cumplimiento*

La Política de Seguridad 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, sus Normativas y Procedimientos asociados, se publicarán en la Intranet del Patronato.

30.*Proceso disciplinario*

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

Disposición final. Publicidad de la Política de Seguridad y Privacidad

El presente documento por el que se establece la Política de Seguridad y Privacidad del Patronato de Recaudación Provincial de Málaga, una vez aprobado por el Consejo Rector del Organismo, se publicará, además de en el Boletín Oficial de la Provincia de Málaga, en la Intranet del Patronato."

b) *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 reemplazada por una nueva Política. La entrada en vigor de la presente Política, supone dejar sin efecto la anterior Política de Seguridad aprobada por el Pleno del Patronato de Recaudación el 23 de julio de 2012."*

Sometida la propuesta anterior a votación, resulta aprobada por 10 votos a favor (9 del Grupo Popular y 1 del Grupo Ciudadanos) y 1 abstención del Grupo Adelante Málaga, 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.

diputación de **málaga**
patronato de recaudación

Hacienda electrónica
local y provincial
DIPUTACIÓN DE MÁLAGA

DOCUMENTO ELECTRÓNICO

CÓDIGO DE VERIFICACIÓN DEL DOCUMENTO ELECTRÓNICO

9b331c2593783f4214fd65e2e52fc1a0e9ca8907

Dirección de verificación del documento: **https://sede.malaga.es**

METADATOS ENI DEL DOCUMENTO:

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

Identificador: ES_LA0010492_2020_00000000000000000000003079359

Órgano: LA0003318

Fecha de captura: 23/06/2020 12:41:56

Origen: Administración

Estado elaboración: Original

Formato: PDF

Tipo Documental: Certificado

Tipo Firma: XAdES internally detached signature

Valor CSV: 9b331c2593783f4214fd65e2e52fc1a0e9ca8907

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