CIUDAD AUTÓNOMA DE MELILLA

CONSEJERIA DE PRESIDENCIA Y SALUD PUBLICA

Dirección General de la Sociedad de la Información

29. ACUERDO DEL CONSEJO DE GOBIERNO DE FECHA 8 MAYO DE 2019, RELATIVO A LA APROBACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA CIUDAD AUTÓNOMA DE MELILLA.

El Consejo de Gobierno de la Ciudad Autónoma de Melilla en sesión extraordinaria celebrada el 24 de abril de 2019 adoptó el siguiente Acuerdo registrado al número 2109000340 de 08 de mayo de 2019:

I.- Que el Consejo de Gobierno de la Ciudad Autónoma de Melilla con fecha 16 de diciembre de 2013 procedió a la aprobación de la Política de Seguridad de la Ciudad Autónoma de Melilla.
II.- Que, tras la entrada en vigor de la Ley 39/2015, de 01 de octubre, del procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015 de 01 de octubre, del Régimen Jurídico del Sector Público, hace que se deba proceder a la actualización de la citada Política de Seguridad, adaptándola a la nueva realidad normativa y técnica.
III.- Que el 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 en su artículo 1.2 establece: "*El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias*".
IV.- Que la Ciudad Autónoma de Melilla ha puesto en funcionamiento una Plataforma de Tramitación Electrónica de procedimientos administrativos, ajustándose a lo dispuesto en la Ley 40/2015, de 01 de octubre, del Régimen Jurídico del Sector Público, y la Ley 39/2015, de 01 de octubre del Procedimiento Administrativo Común de las Administraciones Públicas.
V.- Que el artículo 11 del Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica señala 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.*"
VI.- Que de acuerdo con el artículo 17 de la Ley Orgánica 2/1995, que aprueba el Estatuto de Autonomía de Melilla al Consejo de Gobierno le corresponde la dirección de la política de la ciudad y el ejercicio de las funciones ejecutivas y administrativas correspondientes.
VII.- Que el artículo 16.1.9 del Reglamento del Gobierno y Administración de la Ciudad Autónoma de Melilla establece como competencia del Consejo de Gobierno el adoptar las medidas necesarias para la ejecución, en su propio territorio, de las disposiciones de carácter general que afecten a las materias que sean competencia de la Ciudad Autónoma de Melilla.
VIII.- Que, de acuerdo con el vigente Decreto de Distribución de Competencias de la Ciudad Autónoma de Melilla, le corresponde a la Consejería de Presidencia y Salud Pública entre otras atribuciones: la Automatización de procedimientos y procesos de gestión; las actuaciones en el ámbito de la Administración Electrónica; y la coordinación e interlocución con la AGE en la implantación de iniciativas de e-Administración, Interoperabilidad y cualquiera otra en el ámbito de las TIC.
IX.- Que con fecha 28 de marzo de 2019 se emite informe justificativo de la necesidad de la aprobación de la Política de Seguridad de la Información de la Ciudad Autónoma de Melilla por parte de la Dirección General de la Sociedad de la Información.
X.- Que con fecha 09 de abril de 2019 se procede a dar el visto bueno a la Política de Seguridad de la Información de la Ciudad Autónoma de Melilla por parte del Comité de Seguridad en Tecnologías de la Información y la Comunicación.
XI.- Que con fecha 09 de abril de 2019 se procede a emitir informe de legalidad favorable por parte de la Secretaría Técnica de Presidencia y Salud Pública.

En virtud de lo anteriormente expuesto, visto informe de la Dirección General de la Sociedad de la Información, visto bueno favorable del Comité de Seguridad en Tecnologías de la Información y la Comunicación e Informe de la Secretaría Técnica de Presidencia y Salud Pública, y de acuerdo con el artículo 33.5 h) del Reglamento de Gobierno y Administración de la Ciudad Autónoma de Melilla, **VENGO EN DISPONER**:

Primero.- La modificación de la **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CIUDAD AUTÓNOMA DE MELILLA**, que se incluye en la presente disposición.

Segundo.- La aprobación de la presente Política de Seguridad de la Información de la Ciudad Autónoma de Melilla supone la derogación de cualquier otra que existiera en esta Administración.
Tercero.- Que se proceda a la publicación del texto de la Política de Seguridad de la Información de la Ciudad Autónoma de Melilla en el BOME y en la Sede Electrónica de la Ciudad Autónoma de Melilla. La presente Política de Seguridad tendrá efectos desde la publicación en el BOME.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CIUDAD AUTÓNOMA DE MELILLA

1. APROBACIÓN Y ENTRADA EN VIGOR
El órgano competente para la aprobación de la Política de Seguridad de la Ciudad Autónoma de Melilla es el Consejo de Gobierno.

Esta Política de Seguridad de la Información es efectiva desde la fecha de su aprobación por el Consejo de Gobierno y hasta que sea reemplazada por una nueva Política.

La entrada en vigor de la presente Política de Seguridad de la Información de la Ciudad Autónoma de Melilla supone la derogación de cualquier otra que existiera en esta Administración.

2. INTRODUCCIÓN
La Ciudad Autónoma de Melilla depende de los sistemas TIC (Tecnologías de la Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

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

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que toda la organización debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad. Se debe además realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

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

Las diferentes áreas que utilizan los sistemas TIC deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

3. ALCANCE
Ésta política se aplica sin excepciones a todos los sistemas TIC de la Ciudad Autónoma de Melilla y a todos los miembros de la organización así como a los recursos de las diferentes Direcciones Generales, Gabinetes, Organismos Autónomos y entidades asimiladas, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

4. MISIÓN
La Ciudad Autónoma de Melilla, para la gestión de sus intereses y en el ámbito de sus competencias, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población de la Ciudad de Melilla.

La Ciudad Autónoma de Melilla ejerce sus competencias, en los términos previstos en la legislación del Estado y en su Estatuto de Autonomía.

Para ejercer éstas competencias la Ciudad Autónoma de Melilla hace uso de sistemas de información que deben ser protegidos de una forma efectiva y eficiente.

5. MARCO NORMATIVO
Se toma como referencia, sin carácter exhaustivo, la siguiente legislación:

- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
- Ley Orgánica 2/1995, de 13 de marzo del Estatuto de Autonomía de Melilla
- Reglamento de la Asamblea de la Ciudad Autónoma de Melilla
- Reglamento del Gobierno Y de La Administración de La Ciudad Autónoma De Melilla.
- Reglamento de Organización Administrativa de la Ciudad Autónoma de Melilla
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- 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 (Reglamento general de protección de datos (RGPD))
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

6. PRINCIPIOS GENERALES DE LA POLÍTICA DE SEGURIDAD

Con el desarrollo de ésta Política de Seguridad, la Ciudad Autónoma de Melilla establece un marco de gestión de la seguridad de la información acorde con el 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, reconociendo así como activos estratégicos la información y los sistemas que la soportan.

Uno de los objetivos fundamentales de la implantación de este marco de referencia es el asentar las bases sobre las cuales los trabajadores públicos y los ciudadanos puedan acceder a los servicios en un entorno de gestión seguro, anticipándonos a sus necesidades, y preservando sus derechos.

La Política de Seguridad de la Información protege a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Ciudad Autónoma de Melilla.

La gestión de la seguridad de la información ha de garantizar el adecuado funcionamiento de las actividades de control, monitorización y mantenimiento de las infraestructuras e instalaciones generales, necesarias para la adecuada prestación de servicios, así como de la información derivada del funcionamiento de los mismos. Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

1. Contribuir desde la gestión de la seguridad de la información a cumplir con la misión y objetivos establecidos por la Ciudad Autónoma de Melilla.
2. Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.
3. Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
4. Proteger los recursos de información de la Ciudad Autónoma de Melilla y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

7. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte.

7.1. Comités: Funciones y responsabilidades.

7.1.1. Consejo de Gobierno de la Ciudad Autónoma de Melilla.

En materia de seguridad de la información, el Consejo de Gobierno de la Ciudad Autónoma de Melilla tiene las siguientes funciones:

- Aprobar la Política de Seguridad de la Información de la Ciudad Autónoma de Melilla.
- Adoptar las medidas pertinentes, en materia de seguridad de la información a propuesta del Comité de Seguridad TIC.
- La resolución de conflictos que pudieran aparecer entre las diferentes áreas de la Ciudad Autónoma de Melilla a la hora de aplicar la ésta Política de Seguridad y las normas que se desarrollen.
- Designar a los diferentes responsables recogidos en ésta Política de Seguridad.

7.1.2. Comité de Seguridad en Tecnologías de la Información y la Comunicación (Comité STIC).

Se crea el Comité STIC que eleva al Consejo de Gobierno de la Ciudad Autónoma de Melilla todas sus propuestas. Éste comité tiene las siguientes funciones:

- Elaborar y evaluar la Política de Seguridad de la Información de la Ciudad Autónoma de Melilla y sus normas organizativas.
- Velar por el alineamiento de las actividades de seguridad de la información y los objetivos de la organización municipal, llevando a cabo acciones orientadas a la mejora continua de los procesos de seguridad de la información.
- Evaluar e informar sobre los riesgos de seguridad en los activos TIC.
- Creación y aprobación de las normas que enmarcan el uso de los servicios TIC en la Ciudad Autónoma de Melilla.
- Aprobará los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de la seguridad de las TIC.

Este Comité estará formado al menos por los siguientes roles:

- El titular de la Consejería que tenga las atribuciones en materia de Tecnologías de la Información y la Comunicación.
- El Director General que tenga las atribuciones en materia de Tecnologías de la Información y la Comunicación.
- El Secretari@ Técnic@ de la Consejería que tenga las atribuciones en materia de Tecnologías de la Información y la Comunicación.
- El Responsable de Seguridad de la Información.

El Comité STIC podrá incorporar a los técnicos y asesores que considere oportunos para el desarrollo de sus competencias.

7.2. Roles: Funciones y responsabilidades

7.2.1. Responsables de la Información

Son responsables de la Información de acuerdo con el Esquema Nacional de Seguridad las personas siguientes dentro de la organización administrativa de la Ciudad Autónoma de Melilla:

- Los titulares de las Direcciones Generales de las Consejerías de la Ciudad Autónoma de Melilla, ajustándose a la estructura organizativa vigente en cada momento.
- Los titulares de las Jefaturas o responsables de los Gabinetes, Organismo Autónomos o asimilados, que no estén incardinados jerárquicamente en una Dirección General de una Consejería de la Ciudad Autónoma de Melilla.
- El titular de la Intervención de la Ciudad Autónoma de Melilla.
- El titular de la Tesorería de la Ciudad Autónoma de Melilla.
- El titular de la Secretaría General de la Asamblea de la Ciudad Autónoma de Melilla.
- El titular de la Secretaría del Consejo de Gobierno de la Ciudad Autónoma de Melilla.
- Asimismo, podrá designarse a un cargo o puesto específico como responsable de la información y los servicios, si se estima necesario. En todo caso, dicha designación se efectuaría mediante resolución del titular de la Consejería que tenga las atribuciones en materia de Tecnologías de la Información y la Comunicación.

Los diferentes Responsables de la Información tienen la responsabilidad última del uso que se haga de la información de las áreas de las cuales son responsables y por tanto de su protección.

Los Responsables de la Información tendrán además la potestad de determinar los niveles de seguridad de la información, de acuerdo con las aportaciones del Responsable de Seguridad y del Responsable del Sistema.

Cada uno de los Responsables de la Información será a su vez Responsable del Tratamiento de aquellos datos personales que sean de su competencia, de acuerdo con el Reglamento General de Protección de Datos.

7.2.2. Responsables de los Servicios

Son responsables de los Servicios de acuerdo con el Esquema Nacional de Seguridad las mismas personas que son Responsables de la Información, quedando así unificados los roles de Responsables de la Información y de los Servicios.

Se entiende como servicio aquel que se presta dentro del ámbito de aplicación de la las Leyes 39/2015, 40/2015 y demás normativa concordante.

Los diferentes Responsables de los Servicios tendrán la potestad de determinar los niveles de seguridad de los servicios, que siempre deberán atender a los requisitos de seguridad de la información que manejan.

En el caso de que el Servicio sea prestado por una Dirección General u órgano asimilado al efecto de esta Política de Seguridad y los datos que se manejan sean responsabilidad de otra, prevalecerán los requisitos de seguridad de mayor nivel.

7.2.3. Responsable de Seguridad TIC

Cumplirá funciones relativas a la seguridad de los sistemas de información de la Ciudad Autónoma de Melilla, lo cual incluye determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios usados en la Ciudad Autónoma de Melilla. Este rol recaerá sobre el titular del puesto de trabajo denominado “Jefe de la Sección de Infraestructuras y Seguridad TIC”.

Serán responsabilidades del responsable STIC las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Ciudad Autónoma de Melilla.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Resolver los conflictos que surjan a nivel operacional mediante la interpretación de la Política de Seguridad de la Ciudad Autónoma de Melilla y las diferentes normas que sean de aplicación.
- Ejercerá las funciones de Delegado de Protección de Datos, de acuerdo con lo indicado en el RGPD.
- Ejercerá las funciones de Secretario del Comité STIC y como tal:
    - Convoca las reuniones del Comité STIC.
    - Prepara los temas a tratar en las reuniones del Comité, aportando información para la toma de decisiones.
    - Es responsable de supervisar y velar por la ejecución de las decisiones del Comité.

7.2.4. Responsable del Sistema.

El Responsable del Sistema será el Director General que tenga las atribuciones en materia de TIC.

Desde el punto de vista de la seguridad, sus responsabilidades, utilizando todos los recursos internos y externos asignados a su Director General y las correspondientes delegaciones de tareas, serán entre otras las siguientes:

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

El Responsable del Sistema podrá acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

7.2.5. Designación formal de los roles.
El nombramiento en los cargos y/o puestos de la organización administrativa de la Ciudad Autónoma de Melilla señalados en este apartado de la Política implica la designación formal de su rol correspondiente de acuerdo con el Esquema Nacional de Seguridad.

8. ANALISIS Y GESTIÓN DE RIESGOS
Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).
- Cuando ocurra un incidente grave de seguridad.

Para la armonización de los análisis de riesgos, el Comité STIC establecerá una valoración de referencia, mediante rangos, para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité STIC, si fuera necesario, trasladará al Consejo de Gobierno las necesidades de inversión en materia de seguridad detectadas mediante dichos análisis.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD
Ésta Política de Seguridad podrá desarrollarse si se considera necesario, por medio de normativa de seguridad que afronte aspectos específicos. Se podrán utilizar los siguientes instrumentos:

- Reglamentos: Serán aprobados por el Consejo de Gobierno a propuesta del Comité STIC y serán de obligado cumplimiento por todo el personal de la Ciudad Autónoma de Melilla, así como de las entidades que participen en el funcionamiento o hagan uso de los sistemas TIC.
- Guías de seguridad: Serán aprobadas por el Comité STIC, tendrán un carácter informativo y buscarán ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos en los casos en los que no existan procedimientos precisos.
- Instrucciones técnicas: Serán dictadas por el Responsable STIC, y serán de obligado cumplimiento para el personal y servicios encargados de la operación de los sistemas. Afrontarán tareas concretas, indicando lo que hay que hacer de forma precisa.

La normativa de seguridad estará a disposición de todos los miembros de la organización de la Ciudad Autónoma de Melilla que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

10. TRATAMIENTO DE DATOS PERSONALES
Para la consecución de sus objetivos, la Ciudad Autónoma de Melilla realiza el tratamiento de datos personales. Todos los sistemas de información de la Ciudad Autónoma de Melilla se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de estos datos, siempre que esos requisitos de seguridad sean mayores que los establecidos por el Esquema Nacional de Seguridad.

11. OBLIGACIONES DEL PERSONAL
Todas las personas que realicen de forma directa o indirecta actuaciones dentro de la Ciudad Autónoma de Melilla tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad que pudiera desarrollarse, siendo responsabilidad del Comité STIC disponer los medios necesarios para que la información llegue a los afectados.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12. TERCERAS PARTES
Cuando la Ciudad Autónoma de Melilla utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad si existiera y que atañe a dichos servicios o información relacionada con los mismos. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se

garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se indica en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Melilla a 09 de mayo de 2019
El Secretario del Consejo de Gobierno
José Antonio Jiménez Villoslada