# POLITICA DE PRIVACIDAD Y SEGURIDAD DE DATOS PERSONALES

La Política de Privacidad y Seguridad de los datos personales del CONSORCIO DE TRANSPORTE METROPOLITANO DEL AREA DE JAEN (CTMAJ) es el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco del cumplimiento del Reglamento General de Protección de Datos (RGPD).

La información personal es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad del CTMAJ. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

Mantener la privacidad y seguridad de los datos personales es proteger este activo, con la finalidad de garantizar el respeto a los derechos y libertades de las personas a las que pertenece, asegurar la calidad de la información y la continuidad del servicio público, minimizar el riesgo y permitir maximizar el retorno de las inversiones en beneficio de la sociedad.

La privacidad es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos y en el que es fundamental la máxima colaboración e implicación de todo el personal del CTMAJ.

La dirección del CTMAJ, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento.

## Propósito

El propósito de esta Política de Privacidad y Seguridad de los datos personales es proteger los activos de información personal de la organización, asegurando para ello la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y de las instalaciones, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos de los servicios prestados y la legislación vigente. Asimismo, pretende preservar el respeto por los derechos y libertades de los interesados que puedan verse afectados por el tratamiento de sus datos personales, fruto de la actividad de esta organización.

## Objetivos y Fundamentos de esta Política

La información personal debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción, o cualquier otra operación de tratamiento. Por ello, se establecen los siguientes principios mínimos:

**Principio de confidencialidad:** la información personal deberá estar accesible únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

**Principio de integridad y calidad:** se deberá garantizar el mantenimiento de la integridad y calidad de la información personal, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de registro, tratamiento, almacenamiento y distribución de la información personal contribuyen a preservar su exactitud y corrección.

**Principio de disponibilidad y continuidad:** se garantizará un nivel de disponibilidad en los datos personales y se dotarán los planes y medidas necesarias para asegurar la continuidad de los servicios que los tratan y la recuperación ante posibles contingencias graves.

**Principio de gestión del riesgo:** se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la privacidad y seguridad de los datos personales.

**Principio de proporcionalidad en coste:** la implantación de medidas que mitiguen los riesgos de los tratamientos de datos personales deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegurará que los recursos necesarios para la gestión de la privacidad y seguridad estén disponibles.

**Principio de concienciación y formación:** se articularán iniciativas que permitan a las personas usuarias de los datos personales conocer sus deberes y obligaciones en cuanto al tratamiento de la información personal. De igual forma, se

fomentará la formación específica en materia de privacidad y seguridad de todas aquellas personas que gestionan y administran los soportes, sistemas de información, telecomunicaciones y seguridad física.

**Principio de prevención:** se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la privacidad.

**Principio de detección y respuesta:** los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia respondiendo eficazmente, a través de los mecanismos establecidos al efecto, a los incidentes de seguridad.

**Principio de mejora continua:** se revisará el grado de cumplimiento de los objetivos de mejora de la privacidad y seguridad planificados de forma periódica y el grado de eficacia de los controles implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico actual.

**Principio de licitud y transparencia:** se articularán mecanismos que permitan garantizar que el tratamiento de datos personales sea realizado en todo momento de forma lícita, leal y transparente en relación con su titular, el interesado.

**Principio de exactitud y limitación de la finalidad:** se garantizará que los datos personales objeto de tratamiento sean recogidos con fines determinados, explícitos y legítimos y no serán tratados posteriormente de manera incompatible con los fines que motivaron su tratamiento. Asimismo, solo serán tratados los datos personales que sean exactos y se adoptarán medidas razonables para su continua actualización y/o rectificación en caso de ser inexactos.

**Principio de minimización de datos:** serán objeto de tratamiento únicamente aquellos datos personales que sean adecuados, pertinentes y estrictamente necesarios para el cumplimiento de la finalidad que motiva el tratamiento, y no serán mantenidos durante más tiempo del necesario para cumplir con dicha finalidad.

**Principio de privacidad desde el diseño:** se aplicarán, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, concebidas para aplicar de forma efectiva los principios de protección de datos personales e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos de la legislación vigente y proteger los derechos de los interesados.

**Principio de privacidad por defecto:** se garantizará que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Este principio se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

**Principio de responsabilidad proactiva:** la organización adoptará todas las medidas que sean necesarias para cumplir todos los principios enumerados en esta Política y estar, en todo momento, en posición de demostrar dicho cumplimiento.

**La Política de Privacidad y Seguridad de los datos personales es aprobada por la Dirección de esta organización y su contenido y el de las normas y procedimientos que la desarrollan es de obligado cumplimiento.**

- Todos los usuarios con acceso a la información personal tratada por el CTMAJ tienen la obligación y el deber de custodiarla y protegerla.
- La Política y las Normas de Privacidad y Seguridad se adaptarán a la evolución de los sistemas y de la tecnología y a los cambios organizativos y legales y con los estándares y mejores prácticas de las normas de reconocimiento internacional, así como a los códigos de conducta que puedan aparecer.
- Las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán en los Documentos de Seguridad apropiados y se deberá establecer una planificación para su implantación y gestión.
- Las medidas de seguridad y los controles establecidos serán proporcionales a la criticidad de la información a proteger y a su clasificación.
- Los usuarios que incumplan la Política de Privacidad y Seguridad de los datos personales o las normas y procedimientos complementarios podrán ser sancionados de acuerdo con lo establecido en los contratos que amparen su relación con esta organización y con la legislación vigente y aplicable.

## Requisitos Legales

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril del 2016 relativo a la protección de

las personas físicas en lo que respecta al tratamiento de datos personales (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).

## Alcance

Esta política debe integrarse dentro de un Sistema de Gestión de la Privacidad y Seguridad de los datos personales (SGP), que engloba los tratamientos de datos personales que soportan los procesos necesarios, tanto principales como auxiliares y complementarios, para la prestación de los servicios de esta organización que se realizan físicamente en las instalaciones del responsable o mediante sistemas de información que permiten un tratamiento equivalente al realizado in situ. Dichas instalaciones son identificadas en el Inventario de Activos.

La presente Política de Privacidad y Seguridad se aplica a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información personal conocida, gestionada o bajo tratamiento de la organización para los procesos descritos.

El personal sujeto a esta política incluye a todas las personas con acceso a la información personal descrita, independientemente del soporte en el que se encuentre esta y de si el individuo es empleado o no de la empresa. Por lo tanto, también se aplica a los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información personal, a los sistemas de información empleados para su tratamiento o a las instalaciones que se emplean para su custodia o tratamiento.

Para garantizar que el proceso de privacidad y seguridad implantado será actualizado y mejorado de forma continua, se implantará y documentará un SGP. De esta forma, el contenido de la Política de Privacidad y Seguridad de los datos personales será desarrollado en normas y procedimientos complementarios.

## Contexto

El contexto describe los aspectos que ayuden a comprender el alcance especificado en esta Política de privacidad y seguridad de los datos personales.

El CTMAJ se constituye con el objeto de articular la cooperación económica, técnica y administrativa entre las Administraciones consorciadas a fin de ejercer de forma conjunta y coordinada las competencias que les corresponden en materia de creación y gestión de infraestructuras y servicios de transporte, en el ámbito territorial de los Municipios Consorciados, que, a fecha de esta política, son: Jaén, Fuerte del Rey, La Guardia de Jaén, Mengíbar, Torredelcampo, Los Villares, Villatorres, Jamilena, Martos, Torredonjimeno, Mancha Real, Pegalajar, junto con la Diputación Provincial de Jaén y la Junta de Andalucía, a través de la Consejería de Fomento y Vivienda.

Los tratamientos de datos del responsable se justifican bajo la necesidad de identificación de los perceptores de los servicios que el responsable proporciona mediante la ejecución de los poderes públicos que se le confieren por parte de la Administración Autonómica, siempre que dichos servicios precisen de identificación del perceptor.

Este responsable percibe servicios y productos por parte de proveedores que, en determinados casos, pueden tener la forma de persona física y/o precisar la identificación de trabajadores por cuenta ajena que formen parte de los mencionados proveedores. Por tanto, desde un punto de vista tanto administrativo como técnico, puede ser preciso tratar datos personales tanto de unos como de otros.

Dentro de la organización del responsable se encuentra personal laboral interno. El tratamiento de datos personales de este personal, de identificación, hoja curricular, desempeño laboral habitual, contraprestaciones por su trabajo, aptitud para el desempeño laboral, y otros, se establece indispensable para el responsable.

El responsable realiza (o puede necesitar realizar) contrataciones laborales para cubrir bajas, por exigencias del servicio o aumento de la producción. Para ello, precisa mantener una bolsa de empleo, formada por los datos incluidos en las hojas curriculares de los candidatos.

## Requisitos de los actores principales respecto a la Privacidad y Seguridad de la información

Siempre referidos al alcance descrito, los diferentes actores principales que participan en las actividades de esta organización presentan los siguientes requisitos:

Los usuarios del CTMAJ requieren:

- La protección de la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de los datos personales sometidos a tratamiento por parte del CTMAJ.
- Respecto para los derechos y libertades de los usuarios, en lo referente al tratamiento de sus datos personales y a las consecuencias que dichos tratamientos pudieran tener sobre ellos.
- La protección de la información personal de manera que se eviten riesgos, errores o fallos en los servicios prestados por el CTMAJ.
- El cumplimiento de las condiciones de servicio definidos en los acuerdos entre los usuarios y el CTMAJ.
- El Cumplimiento de la legislación vigente.

Los proveedores del CTMAJ requieren:

- La protección de la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de los datos personales sometidos a tratamiento por el CTMAJ.
- Respecto para los derechos y libertades de los proveedores y sus empleados, en lo referente al tratamiento de sus datos personales y a las consecuencias que dichos tratamientos pudieran tener sobre estos.
- La protección de la información personal de manera que se eviten riesgos, errores o fallos en los servicios prestados por el CTMAJ.
- El cumplimiento de los requisitos definidos en los contratos suscritos entre los proveedores y el CTMAJ.
- Cumplimiento de la legislación vigente.

La dirección del CTMAJ requiere:

- Cumplir los requerimientos de servicio exigidos en los acuerdos con los usuarios.
- Proporcionar a los usuarios el soporte y el servicio que estos puedan necesitar para disfrutar de los diferentes servicios proporcionados por el CTMAJ en el alcance establecido.
- Proteger los activos del CTMAJ.
- La aplicación de las mejores prácticas de privacidad y seguridad de la información personal respecto al alcance descrito.
- Maximizar el retorno de la inversión en términos de beneficios para la ciudadanía.

Los empleados del CTMAJ requieren:

- Procedimientos y herramientas que les permitan mantener los aspectos de seguridad y privacidad que esta organización exige en los soportes y sistemas utilizados.
- Les sean proporcionadas las formaciones y actividades de concienciación que les permitan cumplir con sus obligaciones respecto a la privacidad de los datos personales.
- El respeto y protección de sus datos personales, como si de cualquier ciudadano se tratase.

## Roles, Responsabilidades y Deberes

La dirección asigna y comunica las responsabilidades, autoridades y roles en lo referente a la privacidad y seguridad de la información personal. También se asegurará de que los usuarios conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados.

**Usuarios**

Toda persona o sistema que acceda a la información personal tratada por el CTMAJ se considerará un usuario. Más concretamente, el rol del Usuario no debe ser confundido con la figura del Usuario de los servicios públicos ofrecidos por el CTMAJ como Actor Principal bajo el alcance de esta Política.

Los usuarios son responsables de su conducta cuando, en el desarrollo del tratamiento, acceden a la información personal o utilizan los sistemas de información o acceden a los lugares o soportes que la contienen y/o custodian. El usuario es responsable de todas las acciones realizadas utilizando sus identificadores o credenciales personales.

Los usuarios tienen la obligación de:

- Cumplir la Política de Privacidad y Seguridad de los datos personales y las normas, procedimientos e instrucciones complementarias.
- Proteger y custodiar la información personal bajo tratamiento, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida.
- Conocer y aplicar la Política de Privacidad y Seguridad de los datos personales, las Normas de Uso de los Sistemas de Información y el resto de políticas, normas, procedimientos y medidas de privacidad y seguridad aplicables.

**Dirección**

La dirección del CTMAJ está profundamente comprometida con la política descrita en este documento y es consciente del valor de la información personal y del grave impacto personal, económico y de imagen que puede producir un incidente de seguridad.

La dirección asume las siguientes responsabilidades:

- Demostrar liderazgo y compromiso con respecto al sistema de gestión de la privacidad
- Asegurar que se establecen la política y los objetivos de privacidad y seguridad y que estos son compatibles con la dirección estratégica de la organización.
- Aprobar y comunicar la Política de Privacidad y Seguridad de los datos personales, las Normas de Uso de los Sistemas de Información y la importancia de su cumplimiento a todos los usuarios, internos o externos, y a los demás agentes a quienes deba interesar.
- Reunirse al menos una vez al año, y cuando cualquier evento o solicitud extraordinaria lo demande, con el Responsable de Privacidad y de ser distinta persona, con el Delegado de Protección de Datos, para ser informados sobre el SGP y actualizar la estrategia en materia de privacidad y seguridad.
- Fomentar una cultura corporativa de privacidad y seguridad de la información de carácter personal.
- Apoyar la mejora continua de los procesos de privacidad y seguridad de los datos personales.
- Asegurar que están disponibles los recursos necesarios para el cumplimiento de la política de privacidad y seguridad de los datos personales, de las normas de uso de los sistemas y para el funcionamiento del sistema de gestión de la privacidad (SGP).
- Definir el enfoque para el análisis y la gestión de los riesgos inherentes a los tratamientos de datos personales y los criterios para asumir los riesgos y asegurar la evaluación de los mismos al menos con una periodicidad anual.
- Asegurar que se realizan auditorías internas sobre la privacidad y seguridad de los tratamientos y que se revisan sus resultados para identificar oportunidades de mejora.
- Definir y controlar el presupuesto para mantener la privacidad y seguridad de los datos personales.
- Aprobar los planes de formación y las mejoras y proyectos relacionados con la privacidad y seguridad de la información personal y su tratamiento.
- Aprobar la documentación hasta su segundo nivel de normas y procedimientos.
- Determinar las medidas, sean disciplinarias o de cualquier otro tipo, que pudieran aplicarse a los responsables de violaciones de seguridad en la información personal tratada.

**Responsable de la Privacidad**

La persona con el cargo de Responsable de la Privacidad asumirá las siguientes funciones:

- Promover la privacidad y seguridad de la información personal y de los servicios prestados a través de su tratamiento, con la responsabilidad y autoridad para asegurarse de que el Sistema de Gestión de la Privacidad cumple con los requisitos establecidos por la organización y por la legislación vigente.
- Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad y privacidad de los tratamientos.
- Establecer las medidas encaminadas a preservar la privacidad y seguridad de los datos personales que sean adecuadas y eficaces para cumplir los requisitos establecidos por la organización y la legislación.

- Promover las actividades de concienciación y formación en materia de privacidad y seguridad en su ámbito de responsabilidad.
- Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación al RGPD, en colaboración con el Delegado de Protección de Datos.
- Realizar con la colaboración del Delegado de Protección de Datos, los preceptivos análisis de riesgos de los tratamientos de datos personales, de seleccionar los controles a implantar y de revisar el proceso de gestión del riesgo inherente a los tratamientos. Asimismo, junto a la Dirección y con la participación del Delegado de Protección de Datos, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de privacidad y seguridad y analizar los informes de auditoría, elaborando las conclusiones a presentar a la Dirección y al Delegado de Protección de Datos para que sean adoptadas las medidas correctoras adecuadas.
- Coordinar el proceso de Gestión de la Privacidad, en colaboración con la Dirección.
- Firmar la Declaración de Aplicabilidad, que comprende la relación de controles seleccionados para el SGP.
- Elaborar informes periódicos que incluyan los incidentes más relevantes en cada período, en coordinación con el Delegado de protección de datos.
- Verificar que las medidas aplicadas son adecuadas para la protección de la información personal y los servicios que la precisan.
- Preparar los temas a tratar en las reuniones de la Dirección, en coordinación con el Delegado de Protección de Datos, aportando información puntual para la toma de decisiones.
- Responsable de la ejecución directa o delegada de las decisiones de la Dirección, se reunirá con esta y con el Delegado de protección de datos, al menos con una frecuencia anual, para asegurar la estrategia.

Respecto a la documentación, y apoyándose en el Delegado de protección de datos, son funciones del Responsable de la Privacidad:

- Proponer, a la Dirección y al Delegado de protección de datos para su aprobación, la documentación de segundo nivel (Normas y Procedimientos Generales del Sistema de Gestión de la Privacidad –SGP) y firmar dicha documentación.
- Aprobar la documentación de tercer nivel (Procedimientos Operativos e Instrucciones Técnicas).
- Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

Para el desarrollo de cualquiera de sus funciones el Responsable de la Privacidad podrá recabar la colaboración del Delegado de Protección de datos o de cualquier responsable de departamento o área de la organización.

**Delegado de Protección de Datos**

Siguiendo lo indicado en el RGPD y en la LOPDGDD, el Delegado de Protección de Datos tendrá como mínimo las siguientes funciones:

- Informar y asesorar al responsable del tratamiento y a sus empleados de las obligaciones que les incumben en relación al RGPD y otras disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

Además, respecto a este SGP, le corresponden las siguientes funciones y responsabilidades:

- Dar apoyo, asesoramiento y supervisión a aquellos temas que le sean planteados por el Responsable de la Privacidad.

**Responsable del Sistema**

Es la persona o departamento encargado de asumir la responsabilidad del funcionamiento de cada sistema de información utilizado para tratar los datos personales. Sus funciones, en referencia a la privacidad y seguridad de la información personal, son 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, y cualquier otra que, al margen del tratamiento de datos personales, le sean asignados.
- Asegurarse de que las instrucciones y medidas al respecto del tratamiento de datos personales proporcionadas por el Responsable de la Privacidad, previamente aprobadas por la Dirección, sean implementadas en los sistemas de información bajo su responsabilidad.
- Implantar las medidas necesarias para garantizar la privacidad y seguridad de los datos personales tratados a través del sistema durante todo su ciclo de vida, de acuerdo con el Responsable de la Privacidad.
- Suspender el tratamiento de una determinada información personal si es informado de deficiencias graves de privacidad y seguridad, previo acuerdo con el Responsable de la Privacidad y la Dirección.
- Realizar con la colaboración del Responsable de la Privacidad los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable de la Privacidad, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Elaborar en colaboración con el Responsable de la Privacidad, la documentación de privacidad y seguridad de tercer nivel (Procedimientos Operativos e Instrucciones Técnicas) que afectan a los sistemas de información.

**Comité de Privacidad y Seguridad**

Compuesto por el responsable de la privacidad, el delegado de protección de datos y la dirección (al menos un representante) se reúne al menos semestralmente para coordinar la privacidad y seguridad de la información personal a nivel de la organización.

Sus funciones son las siguientes:

- Atender las inquietudes de la dirección y de los responsables de privacidad y DPD.
- Obtener una fotografía del estado de la privacidad de la información personal.
- Promover la mejora continua del SGP.
- Elaborar la estrategia de evolución
- Revisar la Política de privacidad y seguridad, Normativa y procedimientos al menos anualmente
- Aprobar los requisitos de formación
- Priorizar actuaciones
- Promover la realización de auditorías del SGP.
- Comprobar que la Privacidad y seguridad de la Información personal está presente en todos los proyectos

## Clasificación de la Información

La información se clasificará de acuerdo con la sensibilidad requerida en su tratamiento y a los niveles de seguridad y privacidad exigibles según el riesgo.

## Evaluación de Riesgos

Conocer los riesgos, tanto para los derechos y libertades de los interesados como para la seguridad de la información personal, y elaborar una estrategia para gestionarlos adecuadamente es primordial para el CTMAJ, ya que únicamente si se conoce el estado de privacidad y seguridad podrán tomarse las decisiones adecuadas para mitigar los riesgos a los que se enfrenta.

Se utilizará una metodología basada en la identificación de los factores de riesgo más relevantes, que afectan a los tratamientos de datos personales, para analizar los riesgos. Por ello, se realizará una identificación de los principales factores de riesgo en base a su probabilidad e impacto, extrayendo dichos factores de riesgo, por ejemplo, de un catálogo previamente configurado.

La organización debe determinar los niveles de riesgo a partir de los cuales tomará acciones de tratamiento sobre los mismos. Un Riesgo se considera aceptable cuando implantar más controles se estima que consumiría más recursos que el posible impacto asociado.

Una vez llevado a cabo el proceso de evaluación de riesgos, la dirección de esta organización será responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgo.

## Proyectos

Todos los proyectos relacionados o que afecten a los tratamientos de datos personales deberán incluir, en su proceso de análisis, una evaluación de los requisitos de privacidad y seguridad y definir un modelo de gestión consensuado con el responsable de la privacidad.

En el diseño, implantación y gestión de los tratamientos de datos personales y en los proyectos se tendrán en cuenta y aplicarán los conceptos de privacidad desde el diseño y por defecto, y los controles y medidas para mitigación de riesgos que proceda según el documento de aplicabilidad aprobado por el CTMAJ.

## Contratación y adquisiciones

Todas las contrataciones y adquisiciones que supongan o requieran acceso o tratamiento de información personal, deberán realizarse amparadas por un contrato que incluya cláusulas destinadas a garantizar la salvaguarda de la confidencialidad, integridad y disponibilidad de la información personal.

En aquellos casos en los que los servicios contratados supongan acceso o tratamiento por el proveedor de datos de carácter personal se deberá incluir en el contrato el clausulado requerido para el cumplimiento del Reglamento Europeo de Protección de Datos y de la Ley Orgánica de Protección de Datos de Carácter Personal.

Las empresas y personas que con motivo de contrataciones de servicios o adquisiciones de cualquier tipo accedan a información personal, deberán conocer la Política de Privacidad y Seguridad de los datos personales y las normas y procedimientos complementarios que sean de aplicación para el objeto de la contratación.

Las empresas y personas externas que accedan a la información personal bajo tratamiento de esta organización deberán considerar dicha información, por defecto, como confidencial.

La única información que podrán considerar como no confidencial es aquella que se haya obtenido a través de los medios de difusión pública.

## Concienciación, Divulgación y formación

La presente Política de privacidad y seguridad de datos personales debe ser conocida por todos los usuarios internos y externos y por las entidades que accedan, gestionen o traten datos personales bajo tratamiento del CTMAJ

El conjunto de Políticas, normas y procedimientos complementarios a esta Política de privacidad y seguridad de los datos personales también deberán ser adecuadamente comunicados y puestos en conocimiento de las personas, empresas e instituciones afectadas o implicadas en cada caso.

Se definirán, periódicamente, programas de comunicación, concienciación y formación y se entregará copia de la normativa correspondiente a los usuarios.

## Desconexión Digital y Teletrabajo

Los usuarios que tengan autorizado el régimen de teletrabajo total o parcialmente deberán conocer y respetar las medidas de seguridad que afectan a la información, sea de carácter personal o no, que por objeto de su régimen y función especifica deban conocer y tratar. Se realizaran cuantas acciones y se desarrollaran cuantas medidas técnicas y organizativas sean precisas para permitir un entorno seguro de teletrabajo con las mismas garantías que se establecen para el trabajo en las propias instalaciones del responsable, respetando, en cualquier caso, la protección mínima necesaria para los derechos y libertades de los interesados y para la seguridad de la información tratada.

Asimismo, el responsable establecerá los mecanismos que permitan al empleado una desconexión digital efectiva.

## Respuesta a incidentes de seguridad

Cualquier compromiso de la confidencialidad, integridad o disponibilidad de la información personal bajo tratamiento del CTMAJ se considera un incidente de seguridad. Esto incluye, entre otros, el acceso, la eliminación, la destrucción, la modificación o la interrupción de la disponibilidad no autorizadas. También se consideran incidentes de seguridad los meros intentos de compromiso de las condiciones anteriores, los de evitar, alterar o modificar las medidas de privacidad y seguridad o las violaciones o incumplimientos de la Política de Privacidad y seguridad de los datos personales o de las normas y procedimientos complementarios.

Los usuarios son responsables de informar, de forma inmediata, de cualquier incidente de seguridad, a través de los canales y procedimientos definidos en la organización para la comunicación de incidencias.

## Revisión y Auditorías

El responsable de la privacidad revisará esta política anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por la dirección.

Las revisiones comprobarán la efectividad de la política, valorando los efectos de los cambios legislativos, tecnológicos y de servicio.

La dirección será responsable de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a las situaciones de riesgo establecidas en el presente documento.

El sistema de gestión de la privacidad se auditará cada año, según un plan de auditorías desarrollado por el responsable de la privacidad.