



SP25-00373

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES QUE HA DE REGIR EL PROCEDIMIENTO DE CONTRATACIÓN DEL SERVICIO DE ALOJAMIENTO EXTERNO DE LA PLATAFORMA DE SERVIDORES CORPORATIVOS, CORRESPONDIENTES A LA SOCIEDAD MERCANTIL MUNICIPAL MADRID DESTINO CULTURA TURISMO Y NEGOCIO S.A., A ADJUDICAR MEDIANTE PROCEDIMIENTO ABIERTO SIMPLIFICADO.

NOTA: Registro Oficial de Licitadores y Empresas Clasificadas del Sector Público (ROLECE)

De conformidad con el artículo 159.4 a) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, todos los licitadores que se presenten a licitaciones realizadas a través del procedimiento abierto simplificado deberán estar inscritos en el Registro Oficial de Licitadores y Empresas Clasificadas del Sector Público – también conocido como ROLECE - en la fecha final de presentación de ofertas siempre que no se vea limitada la concurrencia.

En consecuencia, será obligatorio para participar en las licitaciones tramitadas mediante el procedimiento abierto simplificado, estar inscrito en el Registro Oficial de Licitadores y Empresas Clasificadas del Estado, también conocido como ROLECE.

A estos efectos, también se considerará admisible la proposición del licitador que acredite haber presentado la solicitud de inscripción en el correspondiente Registro junto con la documentación preceptiva para ello, siempre que tal solicitud sea de fecha anterior a la fecha final de presentación de las ofertas. La acreditación de esta circunstancia tendrá lugar mediante la aportación del acuse de recibo de la solicitud emitido por el correspondiente Registro y de una declaración responsable de haber aportado la documentación preceptiva y de no haber recibido requerimiento de subsanación.

ÍNDICE

1 OBJETO DEL CONTRATO

2 REQUERIMIENTOS DEL SERVICIO

- 2.1 Situación actual
- 2.2 Condiciones generales
- 2.3 Requisitos mínimos del centro de alojamiento
- 2.4 Ubicación
- 2.5 Requisitos de comunicación
- 2.6 Requisitos de seguridad y accesos
- 2.7 Servicios adicionales
- 2.8 Organización de los trabajos
- 2.9 Acuerdo de nivel de servicio

3 ESQUEMA NACIONAL DE SEGURIDAD



4 RESPONSABILIDAD

5 RÉGIMEN JURÍDICO Y CARACTERÍSTICAS DEL PERSONAL

6 CLÁUSULAS SOCIALES

7 CUMPLIMIENTO NORMATIVO

8 SOSTENIBILIDAD Y PRINCIPIO DNSH (DO NO SIGNIFICANT HARM)

8.1 Objeto y alcance

8.2 Principios y obligaciones

8.3 Prohibición de prácticas perjudiciales

ANEXO I.- DATOS PERSONALES OBJETO DEL CONTRATO

ANEXO II.- MEDIDAS DE SEGURIDAD



SP25-00373

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES QUE HA DE REGIR EL PROCEDIMIENTO DE CONTRATACIÓN DEL SERVICIO DE ALOJAMIENTO EXTERNO DE LA PLATAFORMA DE SERVIDORES CORPORATIVOS, CORRESPONDIENTES A LA SOCIEDAD MERCANTIL MUNICIPAL MADRID DESTINO CULTURA TURISMO Y NEGOCIO S.A., A ADJUDICAR MEDIANTE PROCEDIMIENTO ABIERTO SIMPLIFICADO.

NOTA: Registro Oficial de Licitadores y Empresas Clasificadas del Sector Público (ROLECE)

De conformidad con el artículo 159.4 a) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, todos los licitadores que se presenten a licitaciones realizadas a través del procedimiento abierto simplificado deberán estar inscritos en el Registro Oficial de Licitadores y Empresas Clasificadas del Sector Público – también conocido como ROLECE - en la fecha final de presentación de ofertas siempre que no se vea limitada la concurrencia.

En consecuencia, será obligatorio para participar en las licitaciones tramitadas mediante el procedimiento abierto simplificado, estar inscrito en el Registro Oficial de Licitadores y Empresas Clasificadas del Estado, también conocido como ROLECE.

A estos efectos, también se considerará admisible la proposición del licitador que acredite haber presentado la solicitud de inscripción en el correspondiente Registro junto con la documentación preceptiva para ello, siempre que tal solicitud sea de fecha anterior a la fecha final de presentación de las ofertas. La acreditación de esta circunstancia tendrá lugar mediante la aportación del acuse de recibo de la solicitud emitido por el correspondiente Registro y de una declaración responsable de haber aportado la documentación preceptiva y de no haber recibido requerimiento de subsanación.

1 OBJETO DEL CONTRATO

La sociedad mercantil municipal Madrid Destino Cultura, Turismo y Negocio, S.A. (en adelante, “MADRID DESTINO”) tiene, entre otros objetivos, la gestión de programas y actividades culturales, formativas y artísticas, la organización, apoyo y difusión de las mismas, la prestación de todos los servicios e infraestructuras integrantes o complementarios de estos programas y actividades, la gestión de cualesquiera centros, espacios, recintos, dependencias y/o servicios culturales cuya gestión le fuera encomendada temporal o indefinidamente, o cuyo uso le fuera cedido por el Ayuntamiento de Madrid. Asimismo, MADRID DESTINO asume la contratación y ejecución de las obras, instalaciones, servicios y suministros necesarios para el desarrollo de sus actividades, la gestión de las políticas municipales de promoción e información turística de la Ciudad de Madrid y la proyección de su imagen a nivel nacional e internacional, así como la gestión y explotación de los derechos de propiedad intelectual derivados de las obras susceptibles de generar tales derechos resultantes de las anteriores actividades. Además, presta por cuenta propia o ajena todo tipo de servicios relacionados con la organización, dirección, producción y administración de eventos, ya sean deportivos, exposiciones, congresos, convenciones, seminarios, ferias, y cualquier otro evento de naturaleza similar.



Para alcanzar estos objetivos, MADRID DESTINO dispone de una infraestructura tecnológica compuesta por una variedad de equipos y sistemas informáticos diseñados para ofrecer servicios de computación y comunicaciones en todos sus centros de trabajo. El Departamento de Informática y Telecomunicaciones es responsable de diseñar, administrar, controlar y actualizar dicha infraestructura, con el objetivo de proporcionar soluciones tecnológicas de calidad que incrementen la productividad de los empleados y garanticen la continuidad y seguridad de los servicios prestados.

En este contexto, y con el fin de asegurar la máxima disponibilidad, seguridad y eficiencia operativa, MADRID DESTINO requiere la contratación de un servicio de **alojamiento de servidores en modalidad de housing** en un centro de datos externo. Este servicio debe permitir albergar la plataforma tecnológica principal de la organización, compuesta por dispositivos críticos como firewalls, servidores físicos, cabinas de almacenamiento, switches, routers y sistemas de respaldo, que requieren un espacio de rack completo con suministro eléctrico y condiciones óptimas de operación. Además, el centro de alojamiento debe cumplir con los más altos estándares de seguridad, disponibilidad y certificación, así como facilitar la conectividad necesaria para la integración con la red corporativa de MADRID DESTINO, permitiendo la intervención inmediata de su personal técnico y el acceso seguro a los recursos alojados.

La mera presentación de propuestas implica la aceptación sin reservas por parte del licitador y en todo caso por el adjudicatario, de las condiciones establecidas en los Pliegos que rigen la presente contratación.

2 REQUERIMIENTOS DEL SERVICIO

Es objeto de este contrato es mejorar la disponibilidad de los servicios tecnológicos de Madrid Destino mediante la contratación un alojamiento en modalidad housing para su plataforma de servidores en un centro de datos especializado. El cual garantice un suministro estable de la corriente eléctrica además de unas condiciones de temperatura y humedad específicas para este tipo servicio.

El responsable del contrato, por parte de MADRID DESTINO, será el Área de Informática y Comunicaciones (en adelante "IT"), previa designación de la persona correspondiente antes del inicio de la prestación del Servicio.

2.1.- Situación actual

Actualmente MADRID DESTINO tiene alojada toda su plataforma de servidores en un centro de procesamiento de datos especializado. Dicha plataforma se encuentra en un rack individual de 42U.

2.2 Condiciones generales

En este apartado se detallan las características mínimas exigidas. El incumplimiento de cualquiera de ellas supondrá que la propuesta correspondiente no sea valorada, quedando en consecuencia excluida de la presente contratación.

Se requiere de espacio en modalidad de housing para albergar la siguiente plataforma electrónica:

- 2 firewalls: NSA 4600 (1U)
- 1 servidor físico (controlador): HPE ProLiant DL360 Gen10 Server (1U)
- 2 servidores físicos (virtualización): HPE ProLiant DL160 Gen10 Server (1U)



- 1 cabina de almacenamiento: Huawei OceanStorm Dorado 3000 (2U)
- 2 switches de enlaces: DGS-1520-28MP (1U)
- 2 routers para la conectividad con el proveedor de servicios de comunicaciones de MADRID DESTINO (1U)
- 2 switches para la conectividad con el proveedor de servicios de comunicaciones de MADRID DESTINO (1U)
- 1 NAS SYNOLOGY RS2818RP+ (3U) para copias
- Panel de fibra óptica y cableado estructurado necesario

Para ello se requiere de un espacio de un rack de al menos 42U.

El rack suministrado deberá de ser para uso único de MADRID DESTINO, por lo que no podrá compartirse con otros clientes.

Se considera incluido el servicio de suministro eléctrico, los consumos necesarios para la operación y el espacio para albergar la infraestructura.

Sobre las marcas de fabricantes y/o tecnologías citadas en este pliego

Todas las marcas de fabricantes y/o las tecnologías a las que se hace referencia en este documento se citan porque MADRID DESTINO, en la actualidad, tiene ya instalados equipos y hace uso del software basado en dichas marcas y/o tecnologías. Por lo tanto, en los casos en los que se haga referencias a determinadas marcas y/o tecnologías, los licitadores deberán tener en cuenta la dependencia tecnológica de MADRID DESTINO con las plataformas ya implantadas y en producción.

La mención expresa a una determinada marca comercial y/o modelo determinado debe entenderse también como realizada a una marca y/o modelo equivalente o superior.

2.3 Requisitos mínimos del centro de alojamiento

Se considera que el centro de alojamiento debe cumplir de manera indispensable los siguientes requisitos:

- El centro de alojamiento ofertado debe cumplir el nivel TIER 3 del estándar TIA 942, así como asumir el compromiso a evolucionar hacia normativas más exigentes incluyendo aquellas que se vayan estandarizando a lo largo del contrato.

A estos efectos, los licitadores deberán acompañar en el Sobre Único (Declaración responsable y de Oferta de criterios valorables en cifras o porcentajes), una declaración responsable de su cumplimiento debidamente firmada por el representante legal de la mercantil. La falta de presentación de la declaración responsable será causa de exclusión.

- El Centro de Proceso de Datos (CPD) en el que se alojen los servidores y sistemas relacionados con el presente contrato deberá cumplir con los requisitos establecidos en el **Esquema Nacional de Seguridad (ENS), en su nivel medio**, conforme al Real Decreto 311/2022, de 3 de mayo.



La acreditación de su cumplimiento por parte de los licitadores deberá realizarse de conformidad con lo establecido en el Apartado 3 del presente Pliego, correspondiente al *Esquema Nacional de Seguridad*.

La documentación acreditativa deberá acompañarse en el Sobre Único (Declaración responsable y Oferta de criterios valorables en cifras o porcentajes). La falta de acreditación será causa de exclusión.

- Proporcionar una infraestructura de altas prestaciones bajo un entorno de seguridad física y lógica:
 - El Centro de Alojamiento debe ser un entorno seguro, fiable, dotado de medidas de seguridad físicas y control ambiental.
 - El Centro de Alojamiento debe disponer de una infraestructura de alta disponibilidad tanto en elementos físicos, eléctricos y comunicaciones.
 - Sistema de Control: la empresa deberá contar con un sistema de adquisición y control de datos en planta de las instalaciones del edificio que aloje la plataforma de MADRID DESTINO. A través de este sistema, se controlará y gestionarán como mínimo los sistemas que se indican a continuación: Seguridad y Control de Accesos, Electricidad en Media y baja tensión, transformadores, UPS, Grupos Electrógenos, Protección contra incendios (detección y extinción), Aire Acondicionado, Temperatura en la Sala y Detección de humedad en salas. Toda esta información se explotará por parte del adjudicatario en tiempo real e histórico mediante un software gráfico. De cada sistema se gestionarán y tomarán los datos y alarmas para su posterior procesado. MADRID DESTINO podrá pedir un informe de los parámetros de funcionamiento de la sala y control de cumplimiento de los diferentes ANS (acuerdos de nivel de servicio).
- La alimentación eléctrica de los equipos informáticos y de comunicaciones de datos de MADRID DESTINO tiene que ser realizada mediante Sistemas de Alimentación Ininterrumpida (SAIs), y protegida mediante grupos electrógenos redundantes de configuración “n+1” de conmutación automática.
- La potencia eléctrica inicial en la sala donde estarán alojados los equipos de MADRID DESTINO será como mínimo de 1000 W/m².
- Se deberá de ofertar un consumo eléctrico máximo de 3kw.
- El rack donde se instalen los equipos deberá suministrarse con una corriente eléctrica monofásica redundada de al menos 32A y 4 bases C13.
- Sistema de aire con enfriadoras más equipos autónomos que mantendrán la temperatura del CPD en torno a 22°C ± 3°C y una humedad ambiental mantenida del 50% ± 10%. La temperatura en los armarios no deberá superar bajo cualquier circunstancia la temperatura de 29°C.



- Es requisito mínimo la posesión de certificación actualizada a fecha de la licitación del siguiente certificado: ISO/IEC 27001: para la seguridad de la información.

La documentación acreditativa deberá acompañarse en el Sobre Único (Declaración responsable y Oferta de criterios valorables en cifras o porcentajes). La falta de acreditación será causa de exclusión.

2.4 Ubicación

La ubicación geográfica debe garantizar una proximidad que permita la actuación inmediata in situ del personal técnico de MADRID DESTINO. Por ello será necesario que todas las instalaciones, infraestructuras y equipamientos necesarios para la prestación del servicio de alojamiento se encuentren dentro de la Comunidad de Madrid.

2.5 Requisitos de comunicación

Actualmente, MADRID DESTINO dispone de una red de datos privada basada en tecnología MPLS, contratada con la UTE TELEFÓNICA DE ESPAÑA / TELEFÓNICA MÓVILES, que proporciona conexiones seguras mediante accesos de fibra óptica con diferentes velocidades y caudales.

Esta solución se implementa a través de una Red Privada Virtual (VPN) sobre infraestructura de red IP/MPLS, conforme al estándar RFC 2547bis.

Habrán dos posibles escenarios:

- Escenario A: no hay cambio de CPD. En este caso, no habrá necesidad ni de instalación de la línea ni de trasladar equipos al ser el actual CPD.
- Escenario B: hay cambio de CPD. En este caso la UTE TELEFÓNICA DE ESPAÑA / TELEFÓNICA MÓVILES deberá instalar un acceso FlexWan de 1 Gbps simétrico en el centro de datos que resulte adjudicatario de esta licitación. Por tanto, el adjudicatario deberá disponer de la infraestructura física necesaria (accesos y cableado) que permita la correcta instalación y operación de dicho acceso.

Condiciones de Coordinación y Plazos

En el caso de producirse el escenario B, el adjudicatario deberá facilitar el acceso a las instalaciones para que Telefónica de España pueda realizar los trabajos de adecuación necesarios.

Estos trabajos deberán poder iniciarse tras la firma del contrato con al menos dos meses de antelación al arranque del servicio.

Traslado de equipos

Igualmente y en el caso de producirse el escenario B, una vez formalizado el contrato de adjudicación y completada la instalación de comunicación mencionada en el punto 2.5 MADRID DESTINO realizará un traslado de equipos al nuevo centro de alojamiento de datos.



El traslado de los equipos no es objeto del presente contrato y será asumido por MADRID DESTINO. Dicho traslado será en fin de semana y será necesario que el adjudicatario asegure que se podrá contar con muelle de descarga con acceso seguro para poder llevar a cabo este trabajo de la manera más segura posible.

2.6 Requisitos de seguridad y accesos

El servicio de alojamiento deberá respetar como mínimo, las siguientes condiciones de seguridad de las instalaciones:

- Que el sistema de detección de incendios deberá constar de múltiples detectores, situados en techo y suelo de la sala. El sistema de extinción automático se basará en la inundación de la sala mediante gas inerte o similar.
- Que exclusivamente el personal autorizado pueda tener acceso a los locales donde se encuentren ubicados los equipos físicos objeto del Servicio de Alojamiento.
- Que se aplicará un procedimiento para la entrada y/o salida de los distintos soportes informáticos.
- Que en ningún caso el personal de la empresa que preste el Servicio de alojamiento tenga acceso a los datos contenidos o soportados en los equipos o recursos alojados, ni realice tratamiento de estos sin autorización de MADRID DESTINO.
- MADRID DESTINO facilitará al adjudicatario un listado con nombres y DNI del personal que podrá tener acceso permanente a las instalaciones y equipos. Cualquier otro acceso será comunicado previamente mediante correo electrónico por parte del responsable del servicio.
- Control de acceso al recinto mediante las siguientes medidas de seguridad:
 - Vigilancia perimetral mediante cámaras
 - Vigilancia interior de movilidad en plantas mediante cámaras
 - Sistemas de seguridad y control de acceso.
 - Sistema de videovigilancia en la zona donde se alojen los equipos.
 - Grabaciones que deberán ser accesibles por el personal que indique la Dirección del Contrato
- Para los casos en los que se vaya a movilizar material el adjudicatario deberá de poder facilitar, bajo petición previa de MADRID DESTINO, una plaza de aparcamiento en un ambiente seguro.

2.7 Servicios adicionales

A parte de todo lo previamente mencionado, se requiere de los siguientes servicios adicionales:

- **Gestión de apagado o encendido.** En caso de que sea necesario realizar un apagado o encendido físico de los servidores la empresa adjudicataria tendrá que poner a disposición de MADRID DESTINO un teléfono de atención en el que puedan contactar con un técnico que pueda realizar esta gestión. Este servicio se tendrá que ofrecer en modalidad 12x7.



- **Gestión de informes.** Se podrán solicitar informes estadísticos de las siguientes variables:
 - Consumo eléctrico
 - Temperatura
 - Humedad
 - Accesos
 - Incidencias captadas en el sistema de video vigilancia

2.8 Organización de los trabajos

Interlocutor

El Responsable del contrato de MADRID DESTINO supervisará y controlará la ejecución del servicio objeto del contrato, dando en su caso la conformidad a su recepción de acuerdo con lo establecido en el presente documento.

Si las deficiencias en la ejecución fueran reiteradas o el retraso evidente, MADRID DESTINO podrá llegar a la resolución del contrato.

Es obligación del adjudicatario informar por escrito al Responsable del contrato de MADRID DESTINO acerca de la ejecución del servicio cuando éste lo solicite y, en todo caso, en aquellos supuestos en los que se produzca alguna incidencia.

Para ello, la empresa seleccionada designará una persona que actuará como interlocutor permanente con MADRID DESTINO, encargándose de la coordinación de la ejecución del contrato. La empresa seleccionada se compromete a facilitar la identidad de este interlocutor, juntamente con los datos necesarios para su fácil localización, especialmente número de teléfono móvil y correo electrónico, antes del comienzo del inicio del contrato.

El interlocutor deberá emitir un parte con las incidencias que, en su caso, hubieran podido existir en la ejecución del servicio.

MADRID DESTINO facilitará al adjudicatario toda la información necesaria para facilitar el correcto cumplimiento del contrato.

Responsable del contrato de MADRID DESTINO

Corresponderá de forma exclusiva al responsable del contrato de MADRID DESTINO la realización de cualesquiera indicaciones relacionadas con la ejecución del contrato y que se encuadren dentro del concepto de coordinación técnica.

Dichas indicaciones se realizarán a la persona que haya sido designada por el adjudicatario como responsable del servicio o su sustituto. Las indicaciones se trasladarán preferiblemente por escrito y en su defecto, en caso de ser necesario, de forma verbal.



El responsable del contrato de MADRID DESTINO, en general cualquier empleado de MADRID DESTINO que intervenga durante la fase de ejecución del contrato, se abstendrá de realizar indicaciones de cualquier tipo referidas a las condiciones de trabajo (horarios, turnos, jornada laboral, vacaciones, permisos y demás) al personal de la empresa adjudicataria.

Asimismo, se abstendrán de trasladar de forma directa al personal de la empresa adjudicataria, distintos al responsable del servicio o su sustituto designado por ésta, cualquier tipo de orden, instrucción o indicación referida a la organización y dirección del trabajo, control, distribución de los tiempos y cuestiones de análoga naturaleza.

2.9 Acuerdo de nivel de servicio

Los Indicadores y sus Niveles expuestos a continuación son los mínimos para considerar. Para cada uno de los niveles de servicio, serán tenidas en cuenta las alternativas propuestas por el adjudicatario siempre que sean razonables y ofrezcan beneficios adicionales (p.e. menor coste, mayor funcionalidad con igual coste, etc.).

El seguimiento de los acuerdos de nivel de servicio (ANS) se llevará a cabo mensualmente, para lo que el adjudicatario suministrará a MADRID DESTINO una herramienta y/o información que facilite la monitorización de los indicadores.

El adjudicatario deberá proveer con carácter mensual informes de situación, grado de cumplimiento y evolución de los ANS. Cualquier incumplimiento del compromiso del adjudicatario podrá provocar la aplicación de penalidades económicas y en última instancia, la cancelación del del contrato.

Disponibilidad del servicio

Salvo indicación contraria en el ámbito correspondiente, la disponibilidad se define como la máxima parada no planificada de un entorno, por año.

Esta medida anual no incluye cualquier parada planificada solicitada por MADRID DESTINO.

- Franja de disponibilidad de servicio: 24x7
- Porcentaje de disponibilidad del servicio: 99.982%
- Máximo tiempo de parada no planificada: Cada 1,6 horas de parada contabilizará como un nuevo incumplimiento de la disponibilidad del servicio

Cualquier parada planificada que afecte a los sistemas alojados en el CPD deberá ser notificada con suficiente antelación (mínimo de 7 días naturales) para que permita tomar las acciones oportunas por parte de MADRID DESTINO, que evite o minimice los efectos de esta.

3 ESQUEMA NACIONAL DE SEGURIDAD

Atendiendo al objeto del contrato y de acuerdo con lo establecido en el artículo 65.2 de la LCSP, la mercantil seleccionada deberá cumplir la normativa legal aplicable en materia de seguridad en el marco de los servicios prestados, específicamente, con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y las guías de



apoyo elaboradas por el Centro Criptológico Nacional (CCN). La conformidad con lo dispuesto en el ENS se alcanza mediante la adecuada implantación de las medidas de seguridad contempladas en el Anexo II del citado real decreto, para la siguiente categorización:

Nivel de confidencialidad: Medio.

Nivel de integridad: Medio.

Nivel de trazabilidad: Medio.

Nivel de autenticidad: Medio.

Nivel de disponibilidad: Medio.

En consecuencia, los licitadores deberán acreditar en el Sobre Único (Declaración responsable y Oferta de criterios valorables en cifras o porcentajes):

- Bien estar en posesión de la correspondiente Declaración de Conformidad para el tratamiento de sistemas de información de categoría **MEDIA**, exigidas en la Guía de Seguridad CCN-STIC-809, con el objetivo de garantizar el compromiso de la entidad en cuestión con la seguridad de los sistemas, respecto de la información que trata o los servicios que presta. No obstante, el proveedor del servicio deberá permitir, de forma adicional, el acceso por parte de MADRID DESTINO al informe de auditoría emitido, con el objetivo de verificar las posibles deficiencias del sistema.
- Bien acreditar estar en **proceso de certificación del ENS en nivel medio** para los servicios de consultoría objeto del presente contrato y fecha estimada para la obtención de la certificación, para lo cual deberán aportar una carta de la entidad certificadora en la que conste que la mercantil se encuentra en proceso de certificación del ENS en nivel medio y la fecha estimada para la obtención de la mencionada certificación, que deberá estar comprendida dentro del plazo de cinco (5) meses a contar desde el inicio de la ejecución del contrato.

La falta de acreditación implica que el contrato no pueda serle adjudicado y se entenderá que la mercantil ha retirado su oferta, procediéndose a exigirle el importe del 3 por ciento del presupuesto base de licitación, IVA excluido, en concepto de penalidad.

Para la acreditación de su cumplimiento no cabe su acumulación en caso de UTEs (deberán cumplir el requisito todos los miembros integrantes de la UTE) -Resolución 1099/2021 TACRC y Resolución 113/2022 TACRC -, dado que afecta a la totalidad de los servicios objeto del contrato y no solo a una parte de los mismos. De modo análogo, tampoco cabe su integración por medios externos vía subcontratación- Resolución 294/2021 TACRC-, por el mismo motivo esgrimido para la acumulación, dado que es la totalidad del objeto del contrato la que motiva su exigencia y no tan solo una parte del mismo.

Esta obligación tiene atribuidas las penalidades que se prevén el apartado 28 del Anexo I del PCAP.

El proveedor del sistema notificará a MADRID DESTINO, con carácter urgente, la existencia de cualquier incidente que conociera en el desarrollo de las tareas y que pudieran afectar a la seguridad de los Sistemas de Información de MADRID DESTINO.

MADRID DESTINO podrá exigir las responsabilidades oportunas al proveedor del servicio para el supuesto de que surjan o se verifiquen deficiencias relativas a las obligaciones contenidas en esta cláusula. Para valorar el impacto de las deficiencias verificadas, se tendrán en cuenta conceptos como la gravedad de la



deficiencia detectada, el carácter negligente o doloso de la misma o las consecuencias y perjuicios que se pudieran ocasionar en el desarrollo de la actividad de MADRID DESTINO, y de su relación con terceros.

4 RESPONSABILIDAD

El adjudicatario será responsable de todos los daños y perjuicios directos e indirectos que se causen a terceros y/o al personal de MADRID DESTINO, incluido el lucro cesante y el daño emergente, como consecuencia de su culpa o negligencia y/o de las personas que, por cuenta de esta, intervengan en la ejecución material de la presente contratación.

Asimismo, la Sociedad se compromete a satisfacer el importe de todos los desperfectos ocasionados por culpa o negligencia imputable a la misma y/o al personal por cuenta de esta y/o bajo su responsabilidad, a los espacios o lugares donde el servicio sea prestado.

El licitador que resulte propuesto como adjudicatario deberá presentar a MADRID DESTINO con carácter previo a la adjudicación, las condiciones particulares y el recibo de pago del seguro de responsabilidad señalado en el Apartado 16 del Anexo I al Pliego de Cláusulas Administrativas Particulares.

5 RÉGIMEN JURÍDICO Y CARACTERÍSTICAS DEL PERSONAL

En caso de accidente o perjuicio de cualquier género ocurrido al personal con ocasión del ejercicio de sus trabajos, la empresa adjudicataria cumplirá lo dispuesto en las normas vigentes bajo su responsabilidad, sin que ésta alcance, en modo alguno, a MADRID DESTINO.

El personal contratado por el adjudicatario dependerá única y exclusivamente del mismo, el cual tendrá todos los derechos y obligaciones respecto al citado personal sin que en ningún caso resulte responsable MADRID DESTINO de las obligaciones existentes entre ellos.

El adjudicatario de la prestación cumplirá en todos sus ámbitos con la normativa vigente en materia laboral y de Seguridad Social, incluyendo la normativa sobre prevención de riesgos laborales establecida en el presente Pliego.

A la extinción del contrato, no podrá producirse en ningún caso la consolidación de las personas que hayan realizado los trabajos objeto del contrato, como personal del ente, organismo o entidad del sector público contratante.

El adjudicatario deberá acreditar, mediante declaración responsable, la afiliación y el alta en la Seguridad Social de las personas trabajadoras destinadas a la ejecución del contrato. Esta obligación se extenderá a todo el personal subcontratado por la entidad adjudicataria principal, destinado a la ejecución del contrato. Para la acreditación del cumplimiento de esta obligación, la entidad adjudicataria aportará una declaración responsable al efecto, al inicio del contrato, en la que se señale que las personas trabajadoras destinadas a la ejecución de este se encuentran afiliadas y dadas de alta en la Seguridad Social.

El adjudicatario se compromete a tener asegurados a todos sus trabajadores que realicen el servicio, cubriendo incluso la responsabilidad civil que cualquier accidente pudiera ocasionar, así como dotar a las personas que ejecuten el servicio de todos los medios materiales referido a Seguridad y Salud Laboral que ordena la legislación vigente.



Si se verificara la defectuosa prestación del Servicio, MADRID DESTINO procederá a imponer la penalización de corresponda, de conformidad con lo establecido en los pliegos que rigen la presente contratación.

Si las deficiencias en la prestación del Servicio fueran reiteradas y/o graves, MADRID DESTINO podrá acordar la resolución del contrato.

El adjudicatario asignará el personal que resulte necesario en cada momento en función de su categoría y especialización, siempre con la experiencia necesaria para desempeñar correctamente las funciones requeridas.

6 CLÁUSULAS SOCIALES

De conformidad con lo establecido en el Decreto de 19 de enero de 2016 del Delegado de Gobierno de Economía y Hacienda por el que se aprueba la Instrucción 1/2016, relativa a la incorporación de cláusulas sociales en los contratos celebrados por el Ayuntamiento de Madrid, sus organismos autónomos y entidades del sector público municipal, serán de obligado cumplimiento por la adjudicataria, las cláusulas sociales establecidas en el presente Pliego que se relacionan a continuación, sin perjuicio de lo establecido en el Pliego de Cláusulas Administrativas Particulares.

El incumplimiento de las mismas implicará la imposición de penalidades de conformidad con el Apartado 28 del Anexo I al Pliego de Cláusulas Administrativas Particulares.

1.- La adjudicataria estará obligada a que los bienes o servicios objeto del contrato hayan sido producidos o se desarrollen respetando las normas sociolaborales vigentes en España y en la Unión Europea o de la Organización Internacional del Trabajo.

En el cumplimiento del presente contrato se tendrá en cuenta lo establecido en la Convención de Naciones Unidas sobre los derechos de las personas con diversidad funcional, así como los criterios de accesibilidad universal y de diseño universal o diseño para todas las personas, tal como son definidos estos términos en el Texto Refundido de la Ley General de derechos de personas con diversidad funcional y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013, de 29 de noviembre (en adelante TRLGDPD).

2.- En toda documentación, publicidad, imagen o materiales especiales que, en su caso, deban aportar los licitadores o que sean necesarios para la ejecución del contrato, deberá hacerse un uso **no sexista del lenguaje**, evitar cualquier imagen discriminatoria de las mujeres o estereotipos sexistas y fomentar con valores de igualdad la presencia equilibrada, la diversidad y la corresponsabilidad.

Corresponderá al Responsable del contrato de MADRID DESTINO, la comprobación del cumplimiento de esta obligación, a cuyo fin llevará a cabo la revisión de la cartelería y documentación, así como de cualquier otro soporte que garantice el cumplimiento de esta obligación.



3. En materia de seguridad y salud laboral:

La adjudicataria tiene la obligación de adoptar las medidas de seguridad y salud en el trabajo que sean obligatorias para prevenir de manera rigurosa los riesgos que puedan afectar a la vida, integridad y salud de las personas trabajadoras.

Asimismo, deberá acreditar el cumplimiento de las obligaciones siguientes:

- La evaluación de riesgos y planificación de la actividad preventiva correspondiente a la actividad contratada.
- La formación e información en materia preventiva a las personas adscritas a la ejecución del contrato.
- El justificante de la entrega de equipos de protección individual que, en su caso sean necesarios.

De conformidad con lo anterior, la adjudicataria está obligada a respetar y cumplir la normativa vigente en materia laboral, de seguridad social, de integración social de minusválidos y de prevención de riesgos laborales, conforme a lo dispuesto en la Ley 31/1995, de 8 de noviembre, sobre Prevención de Riesgos Laborales y en el Reglamento de los Servicios de Prevención, aprobado por Real Decreto 39/1997, de 17 de enero. Igualmente es de aplicación el Real Decreto 773/1997, 30 de mayo sobre disposiciones mínimas de seguridad y salud relativas a la utilización por los trabajadores de equipos de protección individual, así como el Real Decreto 171/2004, de 30 de enero, de coordinación de actividades empresariales, y toda aquella normativa que sea de aplicación y/o se promulgue durante la vigencia del presente procedimiento de contratación.

4. En materia de empleo

Afiliación y alta en la Seguridad Social de las personas trabajadoras destinadas a la ejecución del contrato, así como de todas las sucesivas incorporaciones que puedan producirse.

La adjudicataria se compromete a tener asegurados a todos sus trabajadores que presente el Servicio, cubriendo incluso la responsabilidad civil que cualquier accidente pudiera ocasionar, así como dotar a las personas que presten el Servicio de todos los medios materiales referido a Seguridad y Salud Laboral que ordena la legislación vigente.

La adjudicataria deberá acreditar, mediante declaración responsable, la afiliación y el alta en la Seguridad Social de las personas trabajadoras destinadas a la ejecución del contrato. Esta obligación se extenderá a todo el personal subcontratado por la entidad adjudicataria principal, destinado a la ejecución del contrato.

Para la acreditación del cumplimiento de esta obligación, la entidad adjudicataria aportará una declaración responsable al efecto a requerimiento de MADRID DESTINO, en la que se señale que las personas trabajadoras destinadas a la ejecución del mismo se encuentran afiliadas y dadas de alta en la Seguridad Social.



En todo caso, el Responsable del contrato de MADRID DESTINO y/o en su caso el Órgano de contratación podrán solicitar, cuando lo consideren oportuno, la aportación de la documentación que acredite el contenido de la declaración responsable.

CONTROL DE EJECUCIÓN DE LAS CLÁUSULAS SOCIALES

El Responsable del contrato de MADRID DESTINO supervisará el cumplimiento de las obligaciones que en relación a las Cláusulas sociales sean impuestas a la mercantil adjudicataria en el presente Pliego y en el correspondiente a las Cláusulas Administrativas Particulares, así como las que se deriven de la legislación social y laboral vigente.

Con carácter previo a la finalización del contrato, la mercantil adjudicataria deberá presentar un informe relativo al cumplimiento de las obligaciones sociales que le fueran exigibles legal o contractualmente. El incumplimiento de las mismas implicará la imposición de penalidades, de conformidad con lo establecido en el Apartado 28 del Anexo I al Pliego de Cláusulas Administrativas Particulares.

Junto con las Cláusulas Sociales descritas, el Apartado 22 del Anexo I al Pliego de Cláusulas Administrativas Particulares señala las **CONDICIONES ESPECIALES DE EJECUCIÓN**, que son de aplicación al presente procedimiento de contratación.

7 CUMPLIMIENTO NORMATIVO

La adjudicataria manifiesta que dispone en su organización interna de medidas suficientes de control, prevención y detección de la comisión de cualquier tipo de conducta que pudiera ser considerada como ilícito penal, cometida con los medios o bajo la cobertura de la propia compañía y/o a través de cualquier persona física integrante o dependiente de la misma.

A los efectos de lo expuesto en el párrafo anterior, la adjudicataria manifiesta que su actuación en el ámbito del presente contrato estará regida en todo momento por los principios de la buena fe contractual y convenientemente sujeta a Derecho, de manera que en ningún momento participará ni colaborará en la comisión de ninguna conducta que pudiera encontrarse tipificada penalmente en el ordenamiento jurídico. Asimismo, se compromete expresamente a denunciar en todo momento ante las autoridades policiales y/o judiciales competentes, cualquier conducta que pudiera apreciar como consecuencia de la ejecución de este contrato, y que puedan considerarse delictivas de conformidad con lo dispuesto en el Código Penal. En el caso previsto en el párrafo anterior, la Adjudicataria colaborará en lo posible con las autoridades policiales y/o judiciales, para esclarecer las responsabilidades penales dimanantes de los hechos denunciados.

El ejercicio por cualquiera de las partes contratantes y/o cualquiera de las personas físicas integrantes o dependientes de las mismas, de alguna de las conductas que pudieran ser calificadas como ilícitas y constitutivas de responsabilidad penal, podrá constituir un incumplimiento contractual y, por tanto, erigirse en causa de resolución del presente contrato, dando lugar a la indemnización que pudiera resultar procedente en concepto de daños y perjuicios.

Las partes manifiestan que la firma del presente contrato se ha realizado atendiendo a las condiciones particulares de cada una, y únicamente, basándose en los criterios comerciales y/o de programación de ambos, sin que el contrato se haya firmado como consecuencia de una promesa, ofrecimiento o concesión



por ninguna de las partes, de un beneficio o ventaja de cualquier naturaleza no justificados que pudieran favorecer a las partes o a otros terceros.

La Adjudicataria, en el caso en el que ofrezca como mejora un Sistema Digital de Registro de Actividad, se compromete a prestar los servicios objeto del presente contrato de forma tal que los sistemas de información de MADRID DESTINO queden en todo momento protegidos frente a posibles intrusiones por parte de terceros, adoptando todas las medidas de precaución y protección que sean necesarias para prevenir, evitar y detectar ataques de virus informáticos, troyanos, programas espía (“spyware”) u otros mecanismos de intrusión informática que puedan afectar al normal desenvolvimiento y desarrollo del presente contrato. Para ello, la Adjudicataria mantendrá actualizados, programas antivirus y cualesquiera otros mecanismos de detección de intrusiones que monitoricen los posibles intentos de introducirse en los sistemas sin la debida autorización y tendrá implementados procedimientos internos de control para asegurar que los empleados de la Adjudicataria eviten situaciones que puedan implicar un riesgo en los sistemas de información de la MADRID DESTINO.

La Adjudicataria se compromete a cumplir en todo momento los estándares de MADRID DESTINO en lo que a requerimientos de seguridad de la información se refiere y sus posibles modificaciones, siempre y cuando MADRID DESTINO le comunique por escrito cuáles son estos. Su inobservancia por parte de la Adjudicataria podrá dar lugar a la resolución del contrato por parte de MADRID DESTINO conforme a lo estipulado en la cláusula 47 del PCAP.

Igualmente, la Adjudicataria se compromete a comunicar de forma inmediata a MADRID DESTINO cualquier incidente o anomalía relativa a las medidas de seguridad que puedan afectar a la misma o a sus clientes, así como cualquier posible incidencia que afecte o pueda afectar a los sistemas de información de la MADRID DESTINO, a fin de que ésta pueda adoptar las medidas que considere oportunas en defensa de sus propios intereses y de los de sus clientes.

Asimismo, si como consecuencia de la ejecución del presente contrato, los sistemas y aplicaciones informáticos de MADRID DESTINO estuvieran, de cualquier forma, conectados a los sistemas de la Adjudicataria, MADRID DESTINO se reserva el derecho de poder revocar el acceso o de interrumpir la conexión entre los sistemas de ambas partes.

MADRID DESTINO dispone de un Código Ético de carácter vinculante y obligado cumplimiento para todos sus empleados y colaboradores publicado en la documentación de la sección de Buen Gobierno de la página web corporativa, www.madrid-destino.com, que se incorpora al presente expediente por referencia, para conocimiento y compromiso de la adjudicataria, así como de los licitadores a los efectos de preparar sus ofertas.

8 SOSTENIBILIDAD Y PRINCIPIO DNSH (DO NO SIGNIFICANT HARM)

8.1.- Objeto y alcance

El adjudicatario deberá garantizar que la prestación del servicio de alojamiento en modo *housing* se realiza conforme al principio de “No causar un perjuicio significativo” (DNSH), en línea con lo establecido en el **Reglamento (UE) 2020/852 del Parlamento Europeo y del Consejo**, relativo a la taxonomía para actividades sostenibles, así como con la normativa ambiental vigente.



8.2.- Principios y obligaciones

El adjudicatario se compromete a:

- **Eficiencia energética y reducción de emisiones:**
 - Implementar medidas para optimizar el consumo energético en el centro de datos, incluyendo sistemas de refrigeración eficientes y tecnologías de ahorro energético.
 - Priorizar el uso de energía procedente de fuentes renovables, acreditando el porcentaje anual de energía verde utilizada.
 - Mantener un **PUE (Power Usage Effectiveness)** inferior a 1,5 o justificar las acciones para su mejora.
- **Gestión responsable de residuos:**
 - Aplicar procedimientos para la correcta gestión y reciclaje de residuos electrónicos y materiales asociados al servicio.
 - Cumplir con la normativa sobre residuos peligrosos y RAEE (Residuos de Aparatos Eléctricos y Electrónicos).
- **Cumplimiento normativo y certificaciones:**
 - Acreditar el cumplimiento de la normativa ambiental aplicable.
 - Disponer de certificaciones reconocidas como **ISO 14001 (Gestión Ambiental)** y, en su caso, **ISO 50001 (Gestión Energética)** o contar con medidas de gestión medioambiental, que deberán ser equivalentes a las exigidas con arreglo a los sistemas o normas de gestión indicados.
- **Informe de sostenibilidad:**
 - Presentar un informe anual que detalle las medidas adoptadas para garantizar el respeto al medio ambiente y la aplicación del principio DNSH, incluyendo indicadores como:
 - PUE del centro de datos.
 - Porcentaje de energía renovable utilizada.
 - Toneladas de CO₂ evitadas.
 - Cantidad de residuos reciclados.

8.3.- Prohibición de prácticas perjudiciales

Queda prohibida cualquier práctica que implique:

- Vertidos contaminantes.
- Uso de tecnologías obsoletas con alto consumo energético.
- Incumplimiento de la normativa europea y nacional en materia ambiental.

El incumplimiento de las obligaciones y/o la inobservancia de las prohibiciones, implicará la imposición de penalidades de conformidad con el Apartado 28 del Anexo I al Pliego de Cláusulas Administrativas Particulares.

En Madrid, a la fecha de la firma electrónica

MADRID DESTINO

EL ADJUDICATARIO

Fdo.: Responsable del contrato

Fdo.: Órgano de contratación



ANEXO I.- DATOS PERSONALES OBJETO DEL CONTRATO

Descripción general del tratamiento de Datos Personales a efectuar:

El objeto del contrato incluye el tratamiento de datos de carácter personal.

Disposición de los datos al terminar el Servicio

Una vez finalice el encargo, el adjudicatario debe:

a) Devolver al responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

No obstante, el Responsable del Tratamiento podrá requerir al encargado para que en vez de la opción a), cumpla con la b) o con la c) siguientes:

b) Devolver al encargado que designe por escrito el responsable del tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

c) Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento. No obstante, el encargado puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.



ANEXO II.- MEDIDAS DE SEGURIDAD

Dando cumplimiento la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, es objeto del presente Anexo la determinación por parte de MADRID DESTINO, como “Responsable de Ficheros”, de las medidas de seguridad que el adjudicatario, como “Encargado del Tratamiento”, deberá adoptar en la captación, el acceso y el tratamiento de los datos de carácter personal a los que acceda por cuenta de MADRID DESTINO para la prestación de los servicios contratados.

El adjudicatario dispone de un Documento de Seguridad que recoge las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

El Documento de Seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento, o bien, podrá consistir en distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

El Documento deberá contener, como mínimo, los siguientes aspectos:

- a. Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- b. Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
- c. Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
- d. Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- e. Procedimiento de notificación, gestión y respuesta ante las incidencias.
- f. Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
- g. Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, el Documento de seguridad deberá contener, además:

- a. La identificación del responsable o responsables de seguridad.
- b. Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.



MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS AUTOMATIZADOS.

MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO.

- Funciones y obligaciones del personal.
 - Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.
 - También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.
 - El adjudicatario, como encargado del tratamiento, adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.
- Registro de incidencias.
 - El adjudicatario, como encargado del tratamiento, deberá disponer de un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.
- Control de acceso.
 - Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
 - El adjudicatario se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
 - El adjudicatario establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
 - Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el adjudicatario.
 - En caso de que exista personal ajeno al adjudicatario que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.
- Gestión de soportes y documentos.
 - Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.
 - Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.
 - La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del adjudicatario deberá ser autorizada por el adjudicatario o encontrarse debidamente autorizada en el documento de seguridad.
 - En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.



- Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
- La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.
- Identificación y autenticación.
 - El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
 - El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
 - Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
 - El Documento de Seguridad debe establecer la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.
- Copias de respaldo y recuperación.
 - Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
 - Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
 - Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.
 - El adjudicatario se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
 - Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.
 - Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.



MEDIDAS DE SEGURIDAD DE NIVEL MEDIO.

Además de las medidas de seguridad de nivel básico, indicadas anteriormente, deberán implantarse las siguientes medidas de seguridad.

- Responsable de seguridad.
 - En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.
 - En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.
- Auditoría.
 - A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del Título VIII del Reglamento de desarrollo de la LOPD.
 - Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.
 - El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
 - Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al adjudicatario para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.
- Gestión de soportes y documentos.
 - Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
 - Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.
- Identificación y autenticación.
 - El adjudicatario establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.



- Control de acceso físico.
 - Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.
- Registro de incidencias.
 - En el registro regulado en el PUNTO 2 de las Medidas de Seguridad de nivel Básico deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
 - Será necesaria la autorización del adjudicatario para la ejecución de los procedimientos de recuperación de los datos.

MEDIDAS DE SEGURIDAD DE NIVEL ALTO.

Además de las medidas de seguridad de nivel básico y medio, indicadas anteriormente, deberán implantarse las siguientes medidas de seguridad.

- Gestión y distribución de soportes.
 - La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.
 - La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.
 - Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.
 - Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.
- Copias de respaldo y recuperación.
 - Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.
- Registro de accesos.
 - De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
 - En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
 - Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
 - El período mínimo de conservación de los datos registrados será de dos años.



- El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
- No será necesario el registro de accesos definido en este artículo en caso de que concurren las siguientes circunstancias:
 - Que el responsable del fichero o del tratamiento sea una persona física.
 - Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.
 - La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el Documento de Seguridad.
- Telecomunicaciones.
 - Cuando, conforme al artículo 81.3 Reglamento de desarrollo de la LOPD deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS

MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO.

- Criterios de archivo.
 - El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.
 - En aquellos casos en los que no exista norma aplicable, el adjudicatario deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.
- Dispositivos de almacenamiento.
 - Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.
- Custodia de los soportes.
 - Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

MEDIDAS DE SEGURIDAD DE NIVEL MEDIO.

Además de las medidas de seguridad de nivel básico, indicadas anteriormente, deberán implantarse las siguientes medidas de seguridad.

- Responsable de seguridad.
 - Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el PUNTO 6 del apartado correspondiente a las MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS AUTOMATIZADOS.



- Auditoría.
 - Los ficheros comprendidos en el nivel de seguridad medio se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del Título VIII del Reglamento de desarrollo de la LOPD.

MEDIDAS DE SEGURIDAD DE NIVEL ALTO.

Además de las medidas de seguridad de nivel básico y medio, indicadas anteriormente, deberán implantarse las siguientes medidas de seguridad.

- Almacenamiento de la información.
 - Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.
 - Si atendidas las características de los locales de que dispusiera el adjudicatario, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.
- Copia o reproducción.
 - La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el Documento de Seguridad.
 - Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.
- Acceso a la documentación.
 - El acceso a la documentación se limitará exclusivamente al personal autorizado.
 - Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
 - El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.
- Traslado de documentación.
 - Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

VERIFICACIÓN DEL CUMPLIMIENTO POR EL RESPONSABLE

MADRID DESTINO se reserva la facultad de auditar, sin previo aviso, los sistemas e instalaciones del adjudicatario, a los únicos efectos de comprobar el cumplimiento de las medidas de seguridad establecidas en el presente Anexo.

El adjudicatario acepta dicha facultad de MADRID DESTINO y pondrá a su disposición la ayuda y colaboración necesaria para llevar a cabo dicha comprobación, la cual nunca podrá obstaculizar, de forma sustancial, la actividad del adjudicatario.