



**Nº DE EXPEDIENTE: SP23-00238 y SP23-00240**

**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES QUE HAN DE REGIR LA CONTRATACIÓN DEL SERVICIO DE ALOJAMIENTO DE LAS DIFERENTES PLATAFORMAS WEB DE MADRID DESTINO CULTURA TURISMO Y NEGOCIO, S.A., A ADJUDICAR MEDIANTE PROCEDIMIENTO SUJETO A REGULACIÓN ARMONIZADA.**



## ÍNDICE

<b>1. INTRODUCCIÓN .....</b>	<b>1</b>
<b>2. REQUERIMIENTOS TÉCNICOS MÍNIMOS DEL SERVICIO .....</b>	<b>1</b>
<b>3. MARCAS DE FABRICANTES Y/O TECNOLOGÍAS CITADAS EN ESTE PLIEGO.....</b>	<b>1</b>
<b>4. LOTE 1 SERVICIO DE ALOJAMIENTO EN LA NUBE DE LA PLATAFORMA DE TURISMO (SP23-00238) .....</b>	<b>2</b>
4.1.1. Objeto del contrato .....	2
4.1.2. Plataforma a alojar .....	3
4.1.3. Requisitos genéricos.....	3
4.1.3.1. Requisitos mínimos del centro de alojamiento .....	3
4.1.3.2. Requisitos mínimos para comunicaciones .....	5
4.1.3.3. Requisitos mínimos para copias de respaldo y recuperación .....	5
4.1.4. Requisitos alojamiento .....	6
4.1.4.1. Requisitos mínimos de la electrónica de red .....	6
4.1.4.2. Requisitos mínimos del centro de alojamiento .....	6
4.1.4.3. Requisitos seguridad .....	7
4.1.4.4. Gestión de incidencias .....	9
4.1.5. Descripción de la plataforma actual.....	9
4.1.5.1. Entornos COM, MOD y PRO .....	9
4.1.5.2. Entorno Centro de Inteligencia Turística .....	12
4.1.5.3. Otros servidores Cloud de la plataforma de Turismo .....	12
4.1.5.4. Tabla resumen.....	12
4.1.5.5. Potencial de crecimiento entorno Cloud .....	13
4.1.6. Procedimiento de migración .....	13
4.1.6.1. Requisitos mínimos de la migración y puesta en producción.....	13
4.1.7. Perfiles asignados al proyecto .....	13
<b>5. LOTE 2 SERVICIO DE ALOJAMIENTO EN LA NUBE DE LA PLATAFORMA DE UNIFICACIÓN DE LAS WEBS CULTURALES (SP23-00240).....</b>	<b>14</b>
5.1.1. Objeto del contrato .....	14
5.1.2. Plataforma a alojar .....	15
5.1.3. Requisitos genéricos.....	15
5.1.3.1. Requisitos mínimos del centro de alojamiento .....	15
5.1.3.2. Requisitos mínimos para comunicaciones .....	17
5.1.3.3. Requisitos mínimos para copias de respaldo y recuperación .....	18
5.1.4. Requisitos alojamiento .....	18
5.1.4.1. Requisitos mínimos de la electrónica de red .....	18
5.1.4.2. Requisitos mínimos del centro de alojamiento .....	18
5.1.4.3. Requisitos seguridad .....	20
5.1.4.4. Gestión de incidencias .....	21
5.1.5. Descripción de la plataforma actual.....	21
5.1.5.1. Inventario de servidores actuales .....	23
5.1.5.1. Tabla resumen.....	25
5.1.5.1. Potencial de crecimiento entorno Cloud .....	25
5.1.6. Procedimiento de migración .....	25
5.1.6.1. Requisitos mínimos de la migración y puesta en producción.....	25
5.1.7. Perfiles asignados al proyecto .....	26
<b>6. SEGURIDAD DE LA INFORMACIÓN.....</b>	<b>26</b>



<b>7. RESPONSABLE DEL SERVICIO / SUSTITUTO.....</b>	<b>27</b>
<b>8. OBLIGACIONES LABORALES Y SOCIALES .....</b>	<b>27</b>
<b>9. CLÁUSULAS SOCIALES DE OBLIGADO CUMPLIMIENTO .....</b>	<b>28</b>
<b>10. PROTECCIÓN DE DATOS Y CONFIDENCIALIDAD .....</b>	<b>30</b>
<b>Normativa.....</b>	<b>30</b>
<b>Tratamiento de Datos Personales .....</b>	<b>30</b>
<b>Estipulaciones como Encargado de Tratamiento.....</b>	<b>31</b>
<b>Sub-encargos de tratamiento asociados a Subcontrataciones .....</b>	<b>36</b>
<b>Información.....</b>	<b>36</b>
<b>11. SOLICITUD DE INFORMACIÓN .....</b>	<b>37</b>
<b>ANEXO I “TRATAMIENTO DE DATOS PERSONALES” .....</b>	<b>37</b>
<b>ANEXO II MEDIDAS DE SEGURIDAD .....</b>	<b>41</b>

## 1. INTRODUCCIÓN

La sociedad mercantil municipal Madrid Destino Cultura Turismo 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, incluida la contratación y ejecución de las obras, instalaciones, servicios y suministros para los mismos, la gestión de las políticas municipales de promoción e información turística de la Ciudad de Madrid, la proyección de su imagen a nivel nacional e internacional y la gestión y explotación de los derechos de propiedad intelectual derivados de las obras susceptibles de generar tales derechos resultantes de las anteriores actividades, así como la prestación por cuenta propia o ajena de 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.

Por todo lo anterior y para el correcto ejercicio de sus competencias, Madrid Destino requiere la prestación de los siguientes servicios:

- **Lote 1:** Servicio de alojamiento en la nube de las plataformas de turismo. Portal de turismo, plataforma profesional, sistemas relacionados con la modernización de los puntos de atención, sitios web de eventos de interés turístico, etc.
- **Lote 2:** Servicio de alojamiento en la nube de la plataforma de las webs culturales y web corporativa. Plataforma destinada a la gestión y explotación de las webs de los espacios culturales de la empresa, a saber, Teatro Fernán Gómez, Matadero Madrid, Teatro Español, etc., así como posibles campañas puntuales relacionadas con programación cultural (Carnaval, San Isidro, Veranos del Villa, etc.) y web corporativa.

A estos efectos, Madrid Destino está llevando a cabo el correspondiente procedimiento de contratación conforme al cual se solicita a las empresas del sector que presenten sus mejores ofertas.

## 2. REQUERIMIENTOS TÉCNICOS MÍNIMOS DEL SERVICIO

La necesidad de que las proposiciones de las empresas licitadoras se adecúen a los requisitos exigidos con carácter de mínimos obligatorios en los pliegos, obedece a la propia finalidad de la contratación que se quiere llevar a cabo y a las necesidades que con ella se pretende satisfacer. En consecuencia, las ofertas de las empresas que no los cumplan, no pueden ser objeto de valoración y, por tanto, serán excluidas de la licitación.

## 3. 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 instaladas soluciones basadas en las mismas. Por lo tanto, los licitadores deberán tener en cuenta la dependencia tecnológica de Madrid Destino con las plataformas ya implantadas y en producción.



#### 4. Lote 1 Servicio de alojamiento en la nube de la plataforma de turismo (SP23-00238)

##### 4.1.1. Objeto del contrato

MADRID DESTINO necesita contratar los servicios de alojamiento de un data-center especializado cubriendo los siguientes aspectos:

- Plataforma en cloud para el alojamiento de los servidores.
- Monitorización 24x7.
- Servicios gestionados de administración de los sistemas.
- Backup / Restore.
- Comunicaciones entre cliente y proveedor, así como caudal de salida a Internet.
- Electrónica de red.
- Seguridad (antivirus y servicios SOC).
- Ciertas licencias de software que se especifican en este documento y que deben ser incluidas en la propuesta en modo servicio.

El servicio servirá en su mayor parte para albergar la plataforma de turismo que gestiona directa o indirectamente Madrid Destino. También están en esta plataforma servicios como la web de gestión de cupos de MCB, Bloggin' Madrid, todas ellas relacionadas con la actividad de Madrid Destino en relación con la promoción turística.

Las Web serán independientes de manera funcional, pero trabajarán bajo una estructura lógica común y basada casi en su totalidad en una arquitectura de tres capas (presentación, lógica de negocio y datos) por lo que la infraestructura de servidores virtuales deberá estar agrupada en grupos de servidores, que deberán estar dotados de redundancia a nivel de servidor frontal, NFS y backend.

La infraestructura donde se da el servicio deberá tener redundancia hardware implementada.

Los servicios se solicitarán bajo demanda y deberán permitir flexibilidad de crecimiento o decrecimiento según las necesidades de Madrid Destino.

El servicio deberá permitir la creación e VPNs tanto para Madrid Destino como para dar acceso a terceros colaboradores de Madrid Destino.

La conexión entre Madrid Destino y el proveedor deberá estar soportada por una línea punto a punto o por un acceso con caudal garantizado de al menos 10 Mbps.



#### 4.1.2. Plataforma a alojar

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

#### 4.1.3. Requisitos genéricos

##### 4.1.3.1. *Requisitos mínimos del centro de alojamiento*

Son requisitos indispensables que ha de incluir el centro de alojamiento los siguientes:

- 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 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/m<sup>2</sup>.
- La empresa proveedora de los servicios contará con un centro de operaciones y soporte en modalidad 24x7 con personal propio presencial en dicho centro de operaciones.
- Será requisito mínimo el disponer de técnicos especialistas para la gestión de servicio bajo metodología ITIL con certificación Foundation o similar. El adjudicatario deberá garantizar que al menos 4 de las personas asignadas a la operación de la plataforma poseen dicha certificación.
- Que todas las instalaciones, infraestructuras y equipamientos necesarios para la prestación del servicio de alojamiento se encuentren en España.



- Instalación del software requerido por MADRID DESTINO. Esta instalación puede ser desde un sistema operativo (Ubuntu, Red Hat, CentOS, Windows, etc.) hasta un servicio (ftp, base de datos, etc.). En el caso de que este software requiera licencia, dicho software será proporcionado por MADRID DESTINO. Ciertas licencias de software podrán ser incluidas en modo servicio.
- Instalación de servidores si es requerido por MADRID DESTINO. También se incluirá la instalación y configuración del software básico de monitorización, backup, etc... que sea necesario para dar el servicio.
- Cumplimiento Esquema Nacional de Seguridad:

El adjudicatario deberá cumplir la normativa legal aplicable en materia de seguridad en el marco de los servicios prestados, específicamente, con el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y las guías de apoyo elaboradas por el CCN en este sentido.

La conformidad con lo dispuesto en el ENS se alcanza satisfaciendo los mandatos contenidos en su texto articulado y mediante la adecuada implantación de las medidas de seguridad contempladas en el Anexo II del citado Real Decreto 3/2010, para la siguiente categorización:

- Nivel de Disponibilidad: Medio
- Nivel de Integridad: Medio
- Nivel de Confidencialidad: Medio
- Nivel de Autenticidad: Medio
- Nivel de Trazabilidad: Medio

En consecuencia, el adjudicatario se obliga a facilitar a **Madrid Destino** 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. El proveedor del servicio deberá contar con una Certificación de Conformidad expedida por una Entidad Acreditada por la ENAC.

**Las propuestas de los licitadores que no presenten estas certificaciones no serán valoradas.**

- El adjudicatario deberá contar con un centro de operaciones y gestión de incidencias.
- Proporcionar una bolsa de horas de al menos 125 horas para la realización de diversos trabajos que puedan quedar fuera de los servicios anteriormente nombrados tales como:
  - Certificación de instalaciones. En los casos de que sea necesario instalar un nuevo servicio y esta instalación no la realice el personal de la empresa adjudicataria, se podrán solicitar servicios que certifiquen la correcta instalación y documentación de los productos instalados.
  - Migración de servicios. En el caso de ser necesaria la migración de algún servicio externo a la plataforma, se podrán solicitar trabajos contra esta bolsa de horas.



- Otros servicios similares, siempre involucrando perfiles técnicos, siendo estos variados (bases de datos, servidores de aplicaciones, seguridad, etc.)

#### **4.1.3.2. Requisitos mínimos para comunicaciones**

- Servicio de conexión a la red Internet con un ancho de banda mínimo de 250 Mbps. Se deberán detallar las tarifas aplicables en el caso de sobrepasar el ancho de banda de 250 Mbps.
- Operadores: el entorno debe ser multioperador (con presencia mínima acreditada de dos operadores alternativos nacional e internacionales), a través de cuales se dará un nivel de conectividad a MADRID DESTINO balanceada, en alta disponibilidad, redundante y dinámica. En caso de no contar con multioperabilidad, los licitadores deberán proponer alternativas similares que garanticen la continuidad del servicio en lo que respecta a las comunicaciones.
- Servicio de conexión punto a punto o equivalente con un ancho de banda mínimo garantizado de 10 Mbps entre el Centro de Alojamiento y las oficinas de MADRID DESTINO de la calle de los Señores de Luzón 10, para el mantenimiento por parte del personal responsable de MADRID DESTINO.
- Será necesaria la interconexión para el montaje de directorios de nuestra organización (MADRID DESTINO) en alguno/s de los servidores de la plataforma.
- La sala donde estará alojada la plataforma de MADRID DESTINO, dispondrá de dos accesos físicos separados de fibra óptica (Caminos Redundantes).
- La empresa proveedora de los servicios dispondrá de sala de interconexión (Panel de Parcheo) donde están concentradas las terminaciones de red de todos los operadores.
- Comunicaciones del edificio: al objeto de evitar punto único de fallo por rotura física, el edificio que aloje la plataforma de MADRID DESTINO dispondrá al menos de dos acometidas independientes y separadas para los servicios de cableado de Operadores de Comunicaciones.
- Servicio para poder tener acceso mediante VPN a toda la plataforma desde el exterior, con la posibilidad de creación de distintos usuarios y con cliente funcional en Windows y Linux.
- Se requerirá un mínimo de 18 direcciones IP públicas para la disposición de los sistemas requeridos.
- Se requerirá el acceso a una plataforma en la que se pueda analizar el consumo de ancho de banda de la plataforma con estadísticas diarias, mensuales y anuales.

#### **4.1.3.3. Requisitos mínimos para copias de respaldo y recuperación**

- Servicio de copias de respaldo y recuperación para toda la información existente en el almacenamiento compartido y en los discos de sistema de cada servidor, así como las cintas necesarias y su almacenamiento. La periodicidad de las copias de seguridad se acordará con MADRID DESTINO. Se incluirá en este servicio los dispositivos hardware y las licencias de software necesarias (tarjetas de red, agentes, etc.). Se requiere un mínimo de 8 TB, siendo



indispensable el crecimiento de dicho espacio bajo petición de MADRID DESTINO, el posible crecimiento se deberá tarificar.

- Servicio de copias de seguridad y recuperación de las bases de datos existentes (MySQL, PostgreSQL, MongoDB, CouchDB).

#### **4.1.4. Requisitos alojamiento**

##### **4.1.4.1. Requisitos mínimos de la electrónica de red**

El adjudicatario proporcionará todos los dispositivos de red (balanceadores, enrutadores, cortafuegos, conmutadores, switches, hubs, etc.) necesarios para el correcto funcionamiento de la plataforma, teniendo en cuenta que se requiere redundancia para proporcionar una alta disponibilidad.

Los licitadores deberán especificar en sus propuestas la electrónica de red que consideran necesaria teniendo en cuenta los equipos descritos para el alojamiento.

Será obligatorio presentar el número de componentes y los modelos propuestos para el servicio de todos aquellos elementos de electrónica de red objeto de la propuesta. Se consideran así mismo incluidos en la propuesta cuantos cableados sean necesarios para la operación del sistema.

Del mismo modo, se considera parte del servicio la configuración lógica de los aparatos de red que sean parte del servicio, incluyendo gestión de puertos, creación y gestión de VLANes, programación de reglas, etc.

En este sentido MADRID DESTINO no será propietario de ninguno de los elementos de red instalados en la plataforma.

##### **4.1.4.2. Requisitos mínimos del centro de alojamiento**

Son requisitos indispensables que ha de incluir el servicio de gestión de la plataforma los siguientes:

- MADRID DESTINO dispondrá de una consola de administración donde podrá crear/eliminar servidores, ampliar o disminuir los recursos de la solución de hosting, así como de herramientas de monitorización de los servidores. También dispondrá de la posibilidad de crear plantillas modelo de servidor (s.o y software) para darle más agilidad a la creación de los mismos.
- El acceso a la consola anteriormente referida se hará mediante un sistema de doble autenticación.
- Modalidad 24x7 para todos los servicios de gestión de la plataforma. Incluyendo el acceso a los distintos servidores que la conforman (acceso ssh) tanto desde MADRID DESTINO como a través de VPN y a los distintos paneles de gestión de la plataforma (acceso web).
- Alta disponibilidad de protección contra ataques por cortafuegos, gestionado y monitorizado por el personal especializado del Data Center.
- Administración de la plataforma:



- Administración de servicios en la nube. Madrid Destino dispondrá de un panel de administración para poder ampliar o disminuir los recursos de la solución de hosting, así como de herramientas de monitorización de los servidores.
- Administración de los sistemas operativos Linux y Windows.
- Administración de los entornos virtuales (VMWARE).
- Administración de las bases de datos MySQL.
- Administración de los entornos web Apache + Drupal
- Administración del clúster con haproxy y del balanceo de carga.
- Administración DNS's
- Administración de la electrónica de red (balanceadores, firewalls, etc).
- Verificación de la creación de nuevos servidores. Si un nuevo servidor es creado, el adjudicatario deberá verificar su correcta creación (entendiendo una instalación lógica dentro del sistema de gestión del proveedor). La instalación en dichos nuevos servidores del software de monitorización necesario correrá a cargo del proveedor, sin incurrir en un coste adicional.
- Creación de servidores nuevos si así es requerido por MADRID DESTINO.
- Instalación y actualización del software requerido por MADRID DESTINO tanto de los servidores nuevos como en los futuros servidores. Esta actuación puede ser desde un sistema operativo (Ubuntu, Red Hat, CentOS, Windows, etc.) hasta un servicio (ftp, base de datos, etc.). En el caso de que este software requiera licencia, MADRID DESTINO proporcionará la información necesaria para su correcta instalación.
- Monitorización de la plataforma:
  - Caída de servicios
  - Capacidad de almacenamiento insuficiente
  - Detección de intrusión.
  - Etc.

#### **4.1.4.3. Requisitos seguridad**

El servicio de alojamiento, así como las operaciones de mantenimiento y/o soporte a los usuarios o sistemas, deberán 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 los mismos sin autorización de MADRID DESTINO.
- Se requerirá de un sistema de filtrado de IPs por localización geográfica para el acceso a nuestra plataforma.
- Se requerirá un sistema de generación de snapshots automáticas de las máquinas virtuales, de modo que se disponga de una imagen de los últimos tres días (una imagen diaria).
- Se requerirá una plataforma endpoint (EDR + EPP) que proporcione protección contra malware para los sistemas operativos instalados mediante análisis on-access y bajo demanda. En estos momentos la herramienta instalada en la mayoría de los servidores es BitDefender Endpoint Security.
- Se requerirá de un centro de operaciones de seguridad (SOC) con la finalidad de supervisar y gestionar la seguridad de la plataforma.

Deberá incluir los siguientes servicios:

- Soporte normativo ante incidentes.
- Cuadros de mando disponibles de forma online y en tiempo real.
- Análisis forense digital.
- Monitorización de seguridad 24x7.
- Comité mensual para presentar el informe de la actividad.
- Análisis continuo de vulnerabilidades.
- Gestión de incidentes de seguridad, contención y respuesta ante estos. Mantenimiento evolutivo de seguridad.
- Alerta temprana (BAT) e inteligencia (IoC).
- Service Desk de Seguridad.
- Vigilancia de activos digitales.



#### 4.1.4.4. **Gestión de incidencias**

El adjudicatario deberá poner a disposición de MADRID DESTINO un sistema remoto de gestión de incidencias que sirva para gestionar las mismas con los siguientes requisitos mínimos:

- El sistema permitirá la gestión de un flujo de estados personalizado (alta/baja/modificación) para la gestión de las incidencias. A título enunciativo y no exhaustivo se citan los siguientes estados: Alta incidencia, Pendiente de asignar, Pendiente de resolver, Resuelta, Aceptada por el usuario.
- El sistema permitirá asignar a las incidencias los estados (dentro del flujo de estados creado) y transitar por cada uno de ellos, indicando la fecha y hora en la que se realizó cada uno de los tránsitos.
- Cierre de incidencias.
- El sistema generará información estadística sobre el número de incidencias en un periodo de tiempo determinado, incidencias pendientes, incidencias resueltas, etc. (Esta funcionalidad también estará disponible en el módulo de gestión estadística).
- El sistema permitirá medir el tiempo de resolución de incidencias.
- El sistema permitirá documentar la resolución de las incidencias más complejas, permitiendo incluir notas o documentos más elaborados.
- Notificación de estados de incidencia. Los usuarios de MADRID DESTINO que hayan abierto las incidencias recibirán en sus paneles de comunicación las informaciones oportunas que decidan los administradores. Estas notificaciones podrán ser automáticas según por ejemplo, vaya actualizándose el estado de la incidencia. Además, Los administradores podrán comentar las incidencias a fin de aportar información adicional a las mismas.
- Se considerará incidencia **crítica** a las incidencias ajenas a MADRID DESTINO que causen la pérdida de acceso desde el exterior (público en general) a cualquiera de los servidores alojados (ej.: acceso web). El tiempo de resolución máximo deberá ser de 2 horas desde el comienzo de la incidencia.

#### 4.1.5. **Descripción de la plataforma actual**

Se propone una infraestructura 100% virtual, donde todos los servicios tengan por debajo una redundancia hardware implementada por el alojador.

##### 4.1.5.1. **Entornos COM, MOD y PRO**

Cada uno de estos entornos contará con las siguientes capas con uno o varios servidores por cada una de ellas: base de datos, capa de aplicación, balanceadores, buscador Solr y en el caso de MOD también un servidor de mapas.



Se creará una red local para cada entorno, de manera que las comunicaciones de los servidores balanceadores, aplicación y bases de datos no repercutan en el resto de la infraestructura.

Se creará una red local para interconectar los distintos entornos, con el fin de que estos puedan intercambiar información entre ellos.

Debe haber la posibilidad de ampliar memoria y procesador en caliente (con servidor encendido), espacio en disco con servidor apagado.

El entorno COM está en proceso de migración a una tecnología más avanzada, en este caso Drupal 9. Por ello se duplicarán entornos que se detallan a continuación hasta que finalice dicha migración.

### **Servicio CDN**

Se dispone de un servicio CDN en el entorno COM (tanto en Producción como en Preproducción). Este CDN se encarga de servir la parte de estáticos (imágenes, estilos, js). Se sirve a través de subdominios desacoplados del dominio principal. A nivel de tráfico puede alcanzar alcanza un máximo de transferencia de 6TB/mes.

Es posible que durante la duración del contrato este CDN se extienda a otros entornos.

### **Servicio NFS**

Cada entorno dispondrá de servicio NFS, bien con servidores independientes por entorno (como actualmente) o una unidad NFS común a todos los entornos. En cualquier caso, la unidad NFS debe tener alta disponibilidad ya que en ella se va a alojar el código que será accesible por los frontales y es necesario un alto rendimiento, que puede ser dado mediante cabinas de discos con redundancia por RAID y discos Fibre Channel o SSD.

NFS de partida de 100GB por entorno. Posibilidad de ampliar durante la duración del contrato en un 20%.

### **Entornos:**

#### **- COM**

Actualmente 12 servidores con un total de 100 CPUs, 152GB de RAM y 1TB de disco. Toda la plataforma basada en Debian 7.

La distribución de los servidores es la siguiente:

- 2 servidores balanceadores
- 6 servidores para la capa de negocio
- 2 servidores de base de datos
- 1 servidor buscador Solr
- 1 servidor NFS



Actualmente se está implementando una migración del portal a Drupal 9, implicando la creación de nuevos servidores basados en Drupal 9, con una arquitectura similar a la actual, de modo que el número total de servidores y vCPUs, memoria, etc. podrá variar ligeramente del que se describe.

- **MOD**

Actualmente 10 servidores con un total de 82CPUs, 98GB de RAM y 1196GB de disco. Toda la plataforma basada en Debian 7.

La distribución de los servidores es la siguiente:

- 2 servidores balanceadores
- 3 servidores para la capa de negocio
- 2 servidores de base de datos
- 1 servidor buscador Solr.
- 1 servidor de mapas.
- 1 servidor NFS

- **PRO**

Actualmente 9 servidores con un total de 50 CPUs, 82GB de RAM y 966GB de disco. Toda la plataforma basada en Debian 7...

La distribución de los servidores es la siguiente:

- 2 servidores balanceadores
- 3 servidores para la capa de negocio
- 2 servidores de base de datos
- 1 servidor buscador Solr
- 1 servidor NFS

- **Entorno de Preproducción Drupal 7**

12 servidores que sirven de preproducción de las plataformas COM, PRO y MOD: 6 de aplicación, 3 balanceadores, 1 de base de datos, 1 servidor de mapas y 1 servidor NFS. Toda la plataforma basada en Debian 7.

Actualmente, en total 40 CPUs, 84 GB de RAM y 1536 GB disco.



#### - **Entorno de Reproducción D9**

Como se menciona en un punto anterior, actualmente se está llevándolo a cabo una migración a Drupal 9 de la plataforma .COM. Este entorno ya creado es el que da servicio al entorno de pre-producción y Calidad.

5 servidores que servirán de preproducción para el futuro entorno COM basado en Drupal 9. Consta de 2 servidores de aplicación, 1 balanceador, 1 de base de datos y SOLR, 1 servidor NFS.

Con un total de 12 CPUs, 22 GB de RAM y 325 GB de disco.

#### **4.1.5.2. Entorno Centro de Inteligencia Turística**

Actualmente 2 servidores, en total 32 CPUs, 96GB de RAM y 546GB de disco. Un servidor de base de datos basado en CentOS y otro Windows 2008 Server.

#### **4.1.5.3. Otros servidores Cloud de la plataforma de Turismo**

Actualmente también constan 8 servidores que mantienen webs de distinto tipo (campañas de turismo, aplicativos de Madrid Convention Bureau, servicios de las aplicaciones móviles, etc), en total sumarían 30 cpus, 76 GB de RAM y 862 GB de disco. Todos ellos basados en CentOS 6 y 7.

#### **4.1.5.4. Tabla resumen**

En la siguiente tabla se muestra un resumen de servidores y características totales incluidas en la plataforma de turismo en la actualidad:

<b>Característica</b>	<b>Valor</b>
Servidores totales	58
Servidores Linux	57
Servidores Windows	1
vCPU totales	346
RAM total	610 GB
Almacenamiento servidores total	6577 GB
Servicio CDN (Transferencia mensual)	6TB/mes



#### **4.1.5.5. Potencial de crecimiento entorno Cloud**

Durante la duración del servicio, el número de servidores en modo Cloud podrá ir variando en función de las necesidades de MADRID DESTINO. Para su tarificación, se seguirá el modelo indicado en el PCAP.

En el servicio se incluirá la instalación, monitorización, consumos eléctricos, alojamiento, servidores virtuales, integración con servicios SOC, instalación de antivirus, gestión de los servicios instalados y operación.

#### **4.1.6. Procedimiento de migración**

##### **4.1.6.1. Requisitos mínimos de la migración y puesta en producción**

Son requisitos indispensables que ha de incluir el servicio de instalación y paso a operación:

- Será absolutamente necesaria una duplicación de todos los servidores de la plataforma, así como los servicios asociados en las instalaciones del alojador. De forma que convivan con el alojador saliente un mínimo de una semana antes de que se haga el cambio definitivo a la nueva plataforma.
- El proceso de migración de la plataforma actual debe de poder realizarse en un plazo no superior a los 20 días naturales.
- El tiempo máximo en la que los contenidos de los diferentes servicios web no se podrán actualizar será como máximo de 3 días naturales.
- En ningún momento las aplicaciones dejarán de dar el servicio, a excepción del servicio de gestión de contenidos.
- Se requiere una gráfica sobre la propuesta de arquitectura en la que se muestre la disposición lógica de los elementos que compondrán la plataforma, es decir, servidores, electrónica de red, comunicaciones y todos los elementos requeridos para el correcto funcionamiento de la plataforma.
- Para nuevos servidores que se deban instalar se requiere la puesta en producción de los mismos, conjuntamente con los suministradores de los servidores que tenga contratada MADRID DESTINO, según la arquitectura propuesta por el adjudicatario. El plan de direccionamiento se acordará con MADRID DESTINO.
- Una vez finalizada la instalación, el proveedor de alojamiento certificará el óptimo funcionamiento de todos los elementos de la plataforma. A partir de ese momento se hará cargo del soporte, mantenimiento y operación de la misma. Además, proporcionará a MADRID DESTINO toda la documentación referente a la solución implantada.

#### **4.1.7. Perfiles asignados al proyecto**

El adjudicatario deberá prestar el servicio mediante la asignación de recursos. Los mismos deberán estar descritos en la oferta haciendo mención de los servicios gestionados a los que estarán dedicados.

Los perfiles contemplados serán los siguientes:



- Jefe de proyecto
- Consultor Técnico:
  - Técnico de sistemas (base de datos, sistema operativo, servicios de aplicaciones, almacenamiento)
  - Técnico de redes, comunicaciones y seguridad
  - Técnico especialista en Virtualización / Cloud
- Operador

## **5. Lote 2 Servicio de alojamiento en la nube de la plataforma de unificación de las webs culturales (SP23-00240)**

### **5.1.1. Objeto del contrato**

MADRID DESTINO necesita contratar los servicios de alojamiento de un data-center especializado cubriendo los siguientes aspectos:

- Plataforma en cloud para el alojamiento de los servidores.
- Monitorización 24x7.
- Servicios gestionados de administración de los sistemas.
- Backup / Restore.
- Comunicaciones entre cliente y proveedor, así como caudal de salida a Internet.
- Electrónica de red.
- Seguridad (gestión y monitorización antivirus, servicios SOC)
- Ciertas licencias de software que se especifican en este documento y que deben ser incluidas en la propuesta en modo servicio.

El servicio servirá en su mayor parte para albergar las páginas Webs de cultura que gestiona directa o indirectamente Madrid Destino. También están en esta plataforma servicios como la web corporativa y servicios de extranet de Madrid Destino.

La infraestructura donde se da el servicio deberá tener redundancia hardware implementada.

Las Web serán independientes de manera funcional, pero trabajarán bajo una estructura lógica común basada casi en su totalidad en una arquitectura de tres capas (presentación, lógica de negocio y datos) por lo que la infraestructura de servidores virtuales deberá estar agrupada en grupos de servidores, donde también deberán estar dotados de redundancia a nivel de servidor frontal, NFS y backend.



Los servicios se solicitarán bajo demanda y deberán permitir flexibilidad de crecimiento o decrecimiento según las necesidades de Madrid Destino.

El servicio deberá permitir la creación e VPNs tanto para Madrid Destino como para dar acceso a terceros colaboradores de Madrid Destino.

La conexión entre Madrid Destino y el proveedor deberá estar soportada por una línea punto a punto o por un acceso con caudal garantizado de al menos 10 Mbps.

### **5.1.2. Plataforma a alojar**

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

### **5.1.3. Requisitos genéricos**

#### **5.1.3.1. Requisitos mínimos del centro de alojamiento**

Son requisitos indispensables que ha de incluir el centro de alojamiento los siguientes:

- 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 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/m<sup>2</sup>.



- La empresa proveedora de los servicios contará con un centro de operaciones y soporte en modalidad 24x7 con personal propio presencial en dicho centro de operaciones.
- Será requisito mínimo el disponer de técnicos especialistas para la gestión de servicio bajo metodología ITIL con certificación Foundation o similar. El adjudicatario deberá garantizar que al menos 4 de las personas asignadas a la operación de la plataforma poseen dicha certificación.
- Que todas las instalaciones, infraestructuras y equipamientos necesarios para la prestación del servicio de alojamiento se encuentren en España.
- Instalación del software requerido por MADRID DESTINO. Esta instalación puede ser desde un sistema operativo (Ubuntu, Red Hat, CentOS, Windows, etc.) hasta un servicio (ftp, base de datos, etc.). En el caso de que este software requiera licencia, dicho software será proporcionado por MADRID DESTINO. Ciertas licencias de software podrán ser incluidas en modo servicio.
- Instalación de servidores si es requerido por MADRID DESTINO. También se incluirá la instalación y configuración del software básico de monitorización, backup, etc... que sea necesario para dar el servicio.
- Cumplimiento Esquema Nacional de Seguridad:

El adjudicatario deberá cumplir la normativa legal aplicable en materia de seguridad en el marco de los servicios prestados, específicamente, con el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y las guías de apoyo elaboradas por el CCN en este sentido.

La conformidad con lo dispuesto en el ENS se alcanza satisfaciendo los mandatos contenidos en su texto articulado y mediante la adecuada implantación de las medidas de seguridad contempladas en el Anexo II del citado Real Decreto 3/2010, para la siguiente categorización:

- Nivel de Disponibilidad: Medio
- Nivel de Integridad: Medio
- Nivel de Confidencialidad: Medio
- Nivel de Autenticidad: Medio
- Nivel de Trazabilidad: Medio

En consecuencia, el adjudicatario se obliga a facilitar a **Madrid Destino** 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.

El proveedor del servicio deberá contar con una Certificación de Conformidad expedida por una Entidad Acreditada por la ENAC.

- El adjudicatario deberá contar con un centro de operaciones y gestión de incidencias.
- Proporcionar una bolsa de horas de al menos 125 horas para la realización de diversos trabajos que puedan quedar fuera de los servicios anteriormente nombrados tales como:



- Certificación de instalaciones. En los casos de que sea necesario instalar un nuevo servicio y esta instalación no la realice el personal de la empresa adjudicataria, se podrán solicitar servicios que certifiquen la correcta instalación y documentación de los productos instalados.
- Migración de servicios. En el caso de ser necesaria la migración de algún servicio externo a la plataforma, se podrán solicitar trabajos contra esta bolsa de horas.
- Otros servicios similares, siempre involucrando perfiles técnicos, siendo estos variados (bases de datos, servidores de aplicaciones, seguridad, etc.)

#### **5.1.3.2. Requisitos mínimos para comunicaciones**

- Servicio de conexión a la red Internet con un ancho de banda mínimo de 250 Mbps. Se deberán detallar las tarifas aplicables en el caso de sobrepasar el ancho de banda de 250 Mbps.
- Operadores: el entorno debe ser multioperador (con presencia mínima acreditada de dos operadores alternativos nacional e internacionales), a través de cuales se dará un nivel de conectividad a MADRID DESTINO balanceada, en alta disponibilidad, redundante y dinámica. En caso de no contar con multioperabilidad, los licitadores deberán proponer alternativas similares que garanticen la continuidad del servicio en lo que respecta a las comunicaciones.
- Servicio de conexión punto a punto o equivalente con un ancho de banda mínimo garantizado de 10 Mbps entre el Centro de Alojamiento y las oficinas de MADRID DESTINO de la calle de los Señores de Luzón 10, para el mantenimiento por parte del personal responsable de MADRID DESTINO.
- Será necesaria la interconexión para el montaje de directorios de nuestra organización (MADRID DESTINO) en alguno/s de los servidores de la plataforma.
- La sala donde estará alojada la plataforma de MADRID DESTINO, dispondrá de dos accesos físicos separados de fibra óptica (Caminos Redundantes).
- La empresa proveedora de los servicios dispondrá de sala de interconexión (Panel de Parcheo) donde están concentradas las terminaciones de red de todos los operadores.
- Comunicaciones del edificio: al objeto de evitar punto único de fallo por rotura física, el edificio que aloje la plataforma de MADRID DESTINO dispondrá al menos de dos acometidas independientes y separadas para los servicios de cableado de Operadores de Comunicaciones.
- Servicio para poder tener acceso mediante VPN a toda la plataforma desde el exterior, con la posibilidad de creación de distintos usuarios y con cliente funcional en Windows y Linux.
- Servicio VPN para permitir acceso 'site to site' a proveedores y/o servicios externos.
- Se requerirá un mínimo de 18 direcciones IP públicas para la disposición de los sistemas requeridos.



- Se requerirá el acceso a una plataforma en la que se pueda analizar el consumo de ancho de banda de la plataforma con estadísticas diarias, mensuales y anuales.

#### **5.1.3.3. Requisitos mínimos para copias de respaldo y recuperación**

- Servicio de copias de respaldo y recuperación para toda la información existente en el almacenamiento compartido y en los discos de sistema de cada servidor, así como las cintas necesarias y su almacenamiento. La periodicidad de las copias de seguridad se acordará con MADRID DESTINO. Se incluirá en este servicio los dispositivos hardware y las licencias de software necesarias (tarjetas de red, agentes, etc.). Se requiere un mínimo de 8 TB, siendo indispensable el crecimiento de dicho espacio bajo petición de MADRID DESTINO, el posible crecimiento se deberá tarificar.
- Servicio de copias de seguridad y recuperación de las bases de datos existentes (MySQL, PostgreSQL, MongoDB).

#### **5.1.4. Requisitos alojamiento**

##### **5.1.4.1. Requisitos mínimos de la electrónica de red**

El adjudicatario proporcionará todos los dispositivos de red (balanceadores, enrutadores, cortafuegos, conmutadores, switches, etc.) necesarios para el correcto funcionamiento de la plataforma, teniendo en cuenta que se requiere redundancia para proporcionar una alta disponibilidad.

Los licitadores deberán especificar en sus propuestas la electrónica de red que consideran necesaria teniendo en cuenta los equipos descritos para el alojamiento.

Será obligatorio presentar el número de componentes y los modelos propuestos para el servicio de todos aquellos elementos de electrónica de red objeto de la propuesta. Se consideran así mismo incluidos en la propuesta cuantos cableados sean necesarios para la operación del sistema.

Del mismo modo, se considera parte del servicio la configuración lógica de los aparatos de red que sean parte del servicio, incluyendo gestión de puertos, creación y gestión de VLANes, programación de reglas, etc.

Se requerirá también un sistema de prevención de intrusiones (IPS), que analice en tiempo real las conexiones y protocolos para determinar si se está produciendo o se va a producir un incidente, permitiendo el control de acceso a la red.

En este sentido MADRID DESTINO no será propietario de ninguno de los elementos de red instalados en la plataforma.

##### **5.1.4.2. Requisitos mínimos del centro de alojamiento**

Son requisitos indispensables que ha de incluir el servicio de gestión de la plataforma los siguientes:

- MADRID DESTINO dispondrá de una consola de administración donde podrá crear/eliminar servidores, ampliar o disminuir los recursos de la solución de hosting, así como de herramientas de monitorización de los servidores. También dispondrá de la posibilidad de crear plantillas modelo de servidor (s.o y software) para darle más agilidad a la creación de los mismos.



- El acceso a la consola anteriormente referida se hará mediante un sistema de doble autenticación.
- Modalidad 24x7 para todos los servicios de gestión de la plataforma. Incluyendo el acceso a los distintos servidores que la conforman (acceso ssh) tanto desde MADRID DESTINO como a través de VPN y a los distintos paneles de gestión de la plataforma (acceso web).
- Alta disponibilidad de protección contra ataques por cortafuegos, gestionado y monitorizado por el personal especializado del Data Center.
- Administración de la plataforma:
  - Administración de servicios en la nube. Madrid Destino dispondrá de un panel de administración para poder ampliar o disminuir los recursos de la solución de hosting, así como de herramientas de monitorización de los servidores.
  - Administración de los sistemas operativos Linux y Windows.
  - Administración de los entornos virtuales (VMWARE).
  - Administración de las bases de datos MySQL y PostreSQL.
  - Administración de los entornos web nginx + drupal.
  - Administración del clúster con nginx como reverse Proxy y del balanceo de carga.
  - Administración DNS's
  - Administración de la electrónica de red (balanceadores, firewalls, etc).
- Verificación de la creación de nuevos servidores. Si un nuevo servidor es creado, el adjudicatario deberá verificar su correcta creación (entendiendo una instalación lógica dentro del sistema de gestión del proveedor). La instalación en dichos nuevos servidores del software de monitorización necesario correrá a cargo del proveedor, sin incurrir en un coste adicional.
- Creación de servidores nuevos si así es requerido por MADRID DESTINO.
- Instalación y actualización del software requerido por MADRID DESTINO tanto de los servidores nuevos como en los futuros servidores. Esta actuación puede ser desde un sistema operativo (Ubuntu, Red Hat, CentOS, Windows, etc.) hasta un servicio (ftp, base de datos, etc.). En el caso de que este software requiera licencia, MADRID DESTINO proporcionará la información necesaria para su correcta instalación.
- Monitorización de la plataforma:
  - Caída de servicios
  - Capacidad de almacenamiento insuficiente



- Detección de intrusión.
- Etc.

#### **5.1.4.3. Requisitos seguridad**

El servicio de alojamiento, así como las operaciones de mantenimiento y/o soporte a los usuarios o sistemas, deberán 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 los mismos sin autorización de MADRID DESTINO.
- Se requerirá de un sistema de filtrado de IPs por localización geográfica para el acceso a nuestra plataforma.
- Se requerirá una plataforma endpoint (EDR + EPP) que proporcione protección contra malware para los sistemas operativos instalados mediante análisis on-access y bajo demanda. En estos momentos la herramienta instalada en la mayoría de servidores es BitDefender Endpoint Security.
- Se requerirá un sistema de generación de snapshots automáticas de las máquinas virtuales, de modo que se disponga de una imagen de los últimos tres días (una imagen diaria).
- Se requerirá de un centro de operaciones de seguridad (SOC) con la finalidad de supervisar y gestionar la seguridad de la plataforma.

Incluirá los siguientes servicios:

- Soporte normativo ante incidentes.
- Cuadros de mando disponibles de forma online y en tiempo real.
- Análisis forense digital.
- Monitorización de seguridad 24x7.
- Comité mensual para presentar el informe de la actividad.
- Análisis continuo de vulnerabilidades.



- Gestión de incidentes de seguridad, contención y respuesta ante estos. Mantenimiento evolutivo de seguridad.
- Alerta temprana (BAT) e inteligencia (IoC).
- Service Desk de Seguridad.
- Vigilancia de activos digitales.

#### **5.1.4.4. Gestión de incidencias**

El adjudicatario deberá poner a disposición de MADRID DESTINO un sistema remoto de gestión de incidencias que sirva para gestionar las mismas con los siguientes requisitos mínimos:

- El sistema permitirá la gestión de un flujo de estados personalizado (alta/baja/modificación) para la gestión de las incidencias. A título enunciativo y no exhaustivo se citan los siguientes estados: Alta incidencia, Pendiente de asignar, Pendiente de resolver, Resuelta, Aceptada por el usuario.
- El sistema permitirá asignar a las incidencias los estados (dentro del flujo de estados creado) y transitar por cada uno de ellos, indicando la fecha y hora en la que se realizó cada uno de los tránsitos.
- Cierre de incidencias.
- El sistema generará información estadística sobre el número de incidencias en un periodo de tiempo determinado, incidencias pendientes, incidencias resueltas, etc. (Esta funcionalidad también estará disponible en el módulo de gestión estadística).
- El sistema permitirá medir el tiempo de resolución de incidencias.
- El sistema permitirá documentar la resolución de las incidencias más complejas, permitiendo incluir notas o documentos más elaborados.
- Notificación de estados de incidencia. Los usuarios de MADRID DESTINO que hayan abierto las incidencias recibirán en sus paneles de comunicación las informaciones oportunas que decidan los administradores. Estas notificaciones podrán ser automáticas según por ejemplo, vaya actualizándose el estado de la incidencia. Además, Los administradores podrán comentar las incidencias a fin de aportar información adicional a las mismas.
- Se considerará incidencia **crítica** a las incidencias ajenas a MADRID DESTINO que causen la pérdida de acceso desde el exterior (público en general) a los servidores alojados (ej.: acceso web). El tiempo de resolución máximo deberá ser de 4 horas desde el comienzo de la incidencia.

#### **5.1.5. Descripción de la plataforma actual**

Se propone una infraestructura 100% virtual, donde todos los servicios tengan por debajo una redundancia hardware implementada por el alojador.

La plataforma actual se encuentra distribuida por lo que se ha denominado Entornos. Cada Entorno da servicio a un grupo de webs. Cada uno de estos entornos posee entre seis y 10 servidores que dan



servicio a las capas de presentación, aplicación o datos según corresponda. En la actualizada se dispone de 5 entornos basados en este concepto.

Se creará una red local para cada entorno, de manera que las comunicaciones de los servidores frontend, NFS y bases de datos no repercutan en el resto de la infraestructura.

Se creará una red local para interconectar los distintos entornos, con el fin de que estos puedan intercambiar información entre ellos.

### **Servicio NFS**

Cada entorno dispondrá de servicio NFS, bien con servidores independientes por entorno (como actualmente) o una unidad NFS común a todos los entornos. En cualquier caso, la unidad NFS debe tener alta disponibilidad ya que en ella se va a alojar el código que será accesible por los frontales y es necesario un alto rendimiento, que puede ser dado mediante cabinas de discos con redundancia por RAID y discos Fibre Channel o SSD.

NFS de partida de 5 TB para cada entorno con la posibilidad de crecer en tamaño en un 20% durante la duración del servicio.

### **Balanceadores**

Se asignará un Balanceador a cada entorno de servidores. El responsable de este servicio será el alojador, pudiendo permitir por panel de control el que se puedan parametrizar las siguientes funciones:

- Protocolo.
- Puerto en el balanceador.
- Puerto en los servidores.
- Definir servidores que atienden el balanceador.
- Persistencia de sesión de usuario en segundos.
- Tipo de balanceo: Round Robin o Least Connections.
- Balanceo por dominio.

### **Servidores Front - end**

Entre dos y cuatro servidores front-end por entorno (sistema operativo Centos 7 64bits) que servirán todas las peticiones que lleguen al balanceador.

### **Servidores Back - end**

Entre dos y cuatro servidores back-end por entorno (sistema operativo Centos 7 64bits), configurados como maestro-esclavo, que se configurarán con MySQL y que atenderán todas las peticiones que lleguen de los frontales.



#### 5.1.5.1. *Inventario de servidores actuales*

En el momento de la redacción del pliego MADRID DESTINO cuenta con la siguiente plataforma alojada en servicio Cloud que podrá ser distinta que la que exista en el momento de la adjudicación y que deberá de ser migrada:

- Entorno Cultura1. Compuesto por un total de 8 servidores virtuales con un total de 30CPUs, 100GB de memoria y 4968GB de almacenamiento compartido distribuido de la siguiente manera:
  - 2 servidores de 4CPUs y 12GB de memoria.
  - 4 servidores de 4 CPUs y 16GB de memoria.
  - 1 servidor de 2 CPUs y 4GB de memoria.
  - 1 servidor de 4 CPUs y 8GB de memoria.

Todos los servidores están basados en plataformas CentOS y aplicativos OpenSource (Drupal, nginx, Tomcat, MySQL, etc).

También se dispone de un servidor NFS para repositorio de código de 4038 GB.

- Entorno Cultura2. Compuesto por un total de 9 servidores virtuales con un total de 34CPUs, 100GB de memoria y 2824GB de almacenamiento compartido distribuido de la siguiente manera:
  - 3 servidores de 4CPUs y 8GB de memoria.
  - 3 servidores de 4 CPUs y 16GB de memoria.
  - 2 servidores de 4 CPUs y 12GB de memoria.
  - 1 servidor de 2 CPUs y 4GB de memoria.

Todos los servidores están basados en plataformas CentOS y aplicativos OpenSource (Drupal, nginx, Tomcat, MySQL, etc)

También se dispone de un servidor NFS para repositorio de código de 2050 GB.

- Entorno Global. Compuesto por un total de 10 servidores virtuales con un total de 38CPUs, 104GB de memoria y 960GB de almacenamiento compartido distribuido de la siguiente manera:
  - 5 servidores de 4CPUs y 8GB de memoria.
  - 3 servidores de 4 CPUs y 16GB de memoria.
  - 1 servidor de 2 CPUs y 4GB de memoria.
  - 1 servidor de 4 CPUs y 12GB de memoria.



Todos los servidores están basados en plataformas CentOS y aplicativos OpenSource (Drupal, nginx, Tomcat, MySQL, etc).

También se dispone de un servidor NFS para repositorio de código de 250GB.

- Entorno Especiales. Compuesto por un total de 8 servidores virtuales con un total de 30CPUs, 66GB de memoria y 1200GB de almacenamiento compartido distribuido de la siguiente manera:
  - 6 servidores de 4CPUs y 8GB de memoria.
  - 1 servidores de 4 CPUs y 16GB de memoria.
  - 1 servidor de 2 CPUs y 2GB de memoria.

Todos los servidores están basados en plataformas CentOS y aplicativos OpenSource (Drupal, nginx, git, Tomcat, MySQL, etc).

También se dispone de un almacenamiento NFS para repositorio de código de 450GB.

- Entorno Extranet. Compuesto por un total de 2 servidores virtuales Windows con un total de 8CPUs, 16GB de memoria y 1500GB de almacenamiento compartido distribuido de la siguiente manera:
  - 2 servidores de 4CPUs y 8GB de memoria.

Todos los servidores están basados en plataformas Windows y .NET. Las licencias serían parte del servicio.

- Entorno Comunidades. Compuesto por un total de 4 servidores virtuales con un total de 20CPUs, 56GB de memoria y 300GB de almacenamiento compartido distribuido de la siguiente manera:
  - 1 servidor de 4CPUs y 8GB de memoria.
  - 3 servidor de 4CPUs y 16GB de memoria.

Todos los servidores están basados en plataformas CentOS y aplicativos OpenSource (Node.js, Ruby, PostgreSQL, MongoDB, etc)

- Servicio Plesk

Se dispone de un servicio Plesk para el alojamiento y gestión mediante interfaz gráfica dbasado en çplesk. Las características de dicha plataforma serían las siguientes:

Número servidores: **1**  
 Plesk Obsidian **Versión 18.0.46** Actualización 2  
 Sobre **Debian 10.13**

Actualmente el servicio Plesk aloja una única web con las siguientes características:

**Uso del disco** 1647.8 MB  
**Tráfico** 38871.3 MB/mes



**WordPress** 6.0.2

**PHP** 8.0.23

**MariaDB** 10.3.36

#### **5.1.5.1. Tabla resumen**

En la siguiente tabla se muestra un resumen de servidores y características totales incluidas en la plataforma en la actualidad (incluyendo el servidor Plesk):

<b>Característica</b>	<b>Valor</b>
Servidores totales	42
vCPU totales	162
RAM total	446 GB
Almacenamiento servidores total	11952 GB

#### **5.1.5.1. Potencial de crecimiento entorno Cloud**

Durante la duración del servicio, el número de servidores en modo Cloud podrá ir variando en función de las necesidades de MADRID DESTINO. Para su tarificación, se seguirá el modelo indicado en el PCAP.

En el servicio se incluirá la instalación, monitorización, consumos eléctricos, alojamiento, servidores virtuales, gestión de los servicios instalados y operación.

#### **5.1.6. Procedimiento de migración**

##### **5.1.6.1. Requisitos mínimos de la migración y puesta en producción**

Son requisitos indispensables que ha de incluir el servicio de instalación y paso a operación:

- Será absolutamente necesaria una duplicación de todos los servidores de la plataforma, así como los servicios asociados en las instalaciones del alojador. De forma que convivan con el alojador saliente un mínimo de una semana antes de que se haga el cambio definitivo a la nueva plataforma.
- El proceso de migración de la plataforma actual debe de poder realizarse en un plazo no superior a los 20 días naturales.
- El tiempo máximo en la que los contenidos de los diferentes servicios web no se podrán actualizar será como máximo de 3 días naturales.



- En ningún momento las aplicaciones dejarán de dar el servicio, a excepción del servicio de gestión de contenidos.
- Se requiere una gráfica sobre la propuesta de arquitectura en la que se muestre la disposición lógica de los elementos que compondrán la plataforma, es decir, servidores, electrónica de red, comunicaciones y todos los elementos requeridos para el correcto funcionamiento de la plataforma.
- Para nuevos servidores que se deban instalar se requiere la puesta en producción de los mismos, conjuntamente con los suministradores de los servidores que tenga contratada MADRID DESTINO, según la arquitectura propuesta por el adjudicatario. El plan de direccionamiento se acordará con MADRID DESTINO.
- Una vez finalizada la instalación, el proveedor de alojamiento certificará el óptimo funcionamiento de todos los elementos de la plataforma. A partir de ese momento se hará cargo del soporte, mantenimiento y operación de la misma. Además, proporcionará a MADRID DESTINO toda la documentación referente a la solución implantada.

#### **5.1.7. Perfiles asignados al proyecto**

El adjudicatario deberá prestar el servicio mediante la asignación de recursos. Los mismos deberán estar descritos en la oferta haciendo mención de los servicios gestionados a los que estarán dedicados.

Los perfiles contemplados serán los siguientes:

- Jefe de proyecto
- Consultor Técnico:
  - Técnico de sistemas (base de datos, sistema operativo, servicios de aplicaciones, almacenamiento)
  - Técnico de redes, comunicaciones y seguridad
  - Técnico especialista en Virtualización / Cloud
- Operador

#### **6. Seguridad de la información**

El adjudicatario se compromete durante la duración del proyecto a:

- No introducir software microinformático ajeno al Madrid Destino.
- No divulgar las estructuras de carpetas ni los ficheros de información, así como los aplicativos realizados a medida ni la información almacenada en ellos.
- No difundir ni publicar los sistemas de seguridad de la información existentes o previstos.



- No revelar la información obtenida de los sistemas de información de Madrid Destino, ni la documentación que se suministre o la que pudiera tener acceso, con independencia del soporte en que se encuentre.
- Realizar buen uso del o los correos electrónicos de Madrid Destino que les fuesen encomendados.
- Mantener las contraseñas que pudieran conocer en secreto, tanto las propias como las de los sistemas.
- Respetar y promover las medidas de seguridad implantada o por implantar en Madrid Destino.
- No conectarse a otras redes o sistemas que sean ajenos a las propias de Madrid Destino sin el consentimiento previo y por escrito por parte de Madrid Destino.
- Las conexiones externas que deban realizarse por necesidades del servicio se realizarán bien mediante VPN controladas por Madrid Destino, bien fuera de las redes de Madrid Destino.
- No se podrán instalar dispositivos de comunicación del tipo que sean sin el permiso expreso y por escrito de Madrid Destino.
- No se podrá extraer información de los sistemas de Madrid Destino sin el consentimiento expreso de ésta.
- En caso de que el adjudicatario deba instalar equipamiento propio, aunque sea de forma temporal, deberá borrar de forma permanente aquella información que se haya extraído de los sistemas de Madrid Destino cuando se produzca la retirada del equipo.
- Los equipos que se retiren propiedad de Madrid Destino serán formateados. Antes de realizar la retirada de un equipo, ésta deberá ser aceptada por escrito por parte de Madrid Destino.
- El adjudicatario y el personal que éste asigne al proyecto se comprometerá a la no divulgación del sistema de instalaciones de cualquiera de los edificios objetos del contrato.

## **7. RESPONSABLE DEL SERVICIO / SUSTITUTO**

El adjudicatario estará obligado a nombrar un responsable del servicio que será el interlocutor entre el responsable de los servicios de Madrid Destino y entre el personal de la empresa adjudicataria. Asimismo, la empresa adjudicataria deberá designar un sustituto del responsable del servicio. La función del responsable del servicio será actuar como interlocutor con Madrid Destino que garantice que la empresa adjudicataria cumple con sus obligaciones contractuales.

## **8. OBLIGACIONES LABORALES Y SOCIALES**

El adjudicatario está obligado al cumplimiento de la normativa vigente en materia laboral, de seguridad social, de integración social de discapacitados 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, así como de las que se promulguen durante la ejecución del contrato.



La relación del organismo u organismos donde los licitadores podrán obtener información sobre la fiscalidad, y sobre las disposiciones vigentes en materia de protección de empleo, condiciones de trabajo y prevención de riesgos laborales, aplicables a los servicios prestados durante la ejecución del contrato, serán los señalados en el Pliego de Cláusulas Administrativas.

No existirá vinculación laboral alguna entre el personal que se destine a la ejecución del contrato y Madrid Destino, por cuanto aquél queda expresamente sometido al poder direccional y de organización de la empresa adjudicataria en todo ámbito y orden legalmente establecido y siendo, por tanto, ésta la única responsable y obligada al cumplimiento de cuantas disposiciones legales resulten aplicables al caso, en especial en materia de contratación, Seguridad Social, prevención de riesgos laborales y tributaria, por cuanto dicho personal en ningún caso tendrá vinculación jurídico-laboral con Madrid Destino, y ello con independencia de las facultades de Control e Inspección que legal y/o contractualmente corresponden al mismo.

A la extinción de los contratos de servicios, no podrá producirse en ningún caso la consolidación de las personas que hayan realizado los trabajos objeto del contrato como personal de Madrid Destino.

## **9. CLÁUSULAS SOCIALES DE OBLIGADO CUMPLIMIENTO**

Siguiendo instrucciones del decreto publicado el 19 de enero de 2016 del delegado del Área de Gobierno de Economía y Hacienda sobre la incorporación de cláusulas sociales en los contratos celebrados por el Ayuntamiento de Madrid, sus Organismos Autónomos y Entidades del Sector Público Municipal, los licitadores deberán cumplir las siguientes cláusulas:

- Es obligatorio 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.
- Debido a que la mano de obra es una parte fundamental del componente económico del presente procedimiento, se ha tenido en cuenta para la determinación del precio de contrato, el salario base más el complemento de antigüedad establecido en el Estatuto de los Trabajadores ya que el Convenio Colectivo del Sector TIC se encuentra actualmente sin vigencia.
- En toda la documentación, publicidad, imagen o materiales que deban aportar los licitadores para el presente procedimiento 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.
- La empresa 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 pueden 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.
- La empresa adjudicataria deberá acreditar el cumplimiento de estos extremos mediante la documentación que corresponde al desempeño del contrato, el sector TIC.
- La empresa adjudicataria deberá adoptar las medidas oportunas para evitar que de la ejecución del contrato puedan derivarse daños al personal de Madrid Destino, los empleados municipales o a los ciudadanos en general.
- La empresa 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 empresa adjudicataria principal destinado a la ejecución del contrato.
- Para la acreditación del cumplimiento de esta obligación, se exigirá a la empresa adjudicataria al inicio de la ejecución del contrato la presentación de una declaración responsable en la que se señale que las personas trabajadoras destinadas a la ejecución del contrato se encuentran afiliadas y dadas de alta en la Seguridad Social.
- En todo caso, el órgano de contratación podrá solicitar, cuando lo considere oportuno, la aportación de la documentación que acredite el contenido de la declaración responsable.
- Con carácter previo a la finalización del contrato, la empresa adjudicataria deberá presentar un informe relativo al cumplimiento de las obligaciones sociales que le fueran exigibles legal o contractualmente.
- En el desarrollo las webs diseñadas en la ejecución del presente contrato o dirigidas a las personas usuarias o beneficiarias del mismo, serán de preceptivo cumplimiento el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social, aprobado por Real Decreto 1494/2007, de 12 de noviembre, así como los protocolos internacionales de accesibilidad ((W3C y las Web Content Accessibility Guidelines 1.0 y Norma UNE 139803: 2004), que establecen como grado de accesibilidad mínimo obligatorio el nivel AA , aplicable a las páginas de Internet de las Administraciones Públicas (artículos 18, 19 y 20 de la Ley 56/2007, de 28 de Diciembre, de medidas de impulso de la Sociedad de la Información, artículo 14 de la Ley 27/2007, de 23 de Octubre, de Reconocimiento de la Lengua de Signos, la Ley 11/2007, de 22 de Junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y artículos 3, 6 y 12 del Real Decreto 1494/2007, de 12 de noviembre).
- Para la acreditación del cumplimiento de esta obligación los licitadores están obligados a presentar una declaración responsable relativa al cumplimiento de estas obligaciones en materia de accesibilidad. Esta declaración responsable deberá incluirse en el sobre relativo a la documentación técnica, especificándose esta obligación de los licitadores tanto en el pliego de prescripciones técnicas como en el apartado correspondiente a la presentación de la documentación técnica del Anexo I al PCAP.



## 10. CONDICIÓN ESPECIAL DE EJECUCIÓN.

De conformidad con el artículo 202.1 de la Ley de Contratos de Sector Público, al tratarse de un servicio que durante su ejecución implicará cesión de datos, el adjudicatario deberá someterse a la normativa nacional y de la Unión Europea en materia de protección de datos. Esta condición tiene carácter de obligación contractual esencial.

## 11. PROTECCIÓN DE DATOS Y CONFIDENCIALIDAD

### Normativa

De conformidad con la Disposición adicional 25ª de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, los contratos que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD), y la normativa complementaria.

Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento. En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 28 del RGPD. En todo caso, las previsiones de este deberán de constar por escrito.

### Tratamiento de Datos Personales

Para el cumplimiento del objeto de este pliego, el adjudicatario deberá almacenar en su plataforma los datos personales de los cuales MADRID DESTINO es Responsable del Tratamiento (Responsable del Tratamiento) de la manera que se especifica en el Anexo a este pliego, denominado "Tratamiento de Datos Personales".

Ello conlleva que el adjudicatario actúe en calidad de Encargado del Tratamiento y por tanto tiene el deber de cumplir con la normativa vigente en cada momento, tratando y protegiendo debidamente los Datos Personales.

Por tanto, sobre MADRID DESTINO recaen las responsabilidades del Responsable del Tratamiento y sobre el adjudicatario las de Encargado de Tratamiento.

Si el adjudicatario destinase los datos a otra finalidad, los comunicara o los utilizara incumpliendo las estipulaciones del contrato y/o la normativa vigente, será considerado también como Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente, así como, del incumplimiento contrato.

El Anexo "Tratamiento de Datos Personales" describe:

- a) los Datos Personales a proteger,
- b) el tratamiento a realizar,



- c) los sistemas/dispositivos de tratamiento, manuales y automatizados, cuya ubicación y equipamiento podrá estar bajo el control de MADRID DESTINO o bajo el control directo o indirecto del adjudicatario, u otros que hayan sido expresamente autorizados por escrito por MADRID DESTINO, según se especifique en el Anexo
- d) los usuarios o perfiles de usuarios asignados a la ejecución del objeto de este Pliego,
- e) el destino de los datos objeto de tratamiento y
- f) las medidas a implementar por el adjudicatario.

En caso de que como consecuencia de la ejecución del contrato resultara necesario en algún momento la modificación de lo estipulado en el Anexo “Tratamiento de Datos Personales”, el adjudicatario lo requerirá razonadamente y señalará los cambios que solicita. En caso de que MADRID DESTINO estuviese de acuerdo con lo solicitado emitiría un Anexo “Tratamiento de Datos Personales” actualizado, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

#### **Estipulaciones como Encargado de Tratamiento**

De conformidad con lo previsto en el artículo 28 del RGPD, el adjudicatario se obliga a y garantiza el cumplimiento de las siguientes obligaciones, complementadas con lo detallado en el Anexo “Tratamiento de Datos Personales”:

##### **a) Tratamiento conforme a instrucciones de MADRID DESTINO**

Tratar los Datos Personales conforme a las instrucciones documentadas en el presente Pliego o demás documentos contractuales aplicables a la ejecución del contrato y aquellas que, en su caso, reciba de MADRID DESTINO por escrito en cada momento.

El adjudicatario informará inmediatamente a MADRID DESTINO cuando, en su opinión, una instrucción sea contraria a la normativa de protección de Datos Personales aplicable en cada momento.

##### **b) Finalidad de tratamiento**

No utilizar ni aplicar los Datos Personales con una finalidad distinta a la ejecución del objeto del Contrato. En ningún caso podrá utilizar los datos para fines propios.

##### **c) Medidas de seguridad**

Tratar los Datos Personales de conformidad con los criterios de seguridad y el contenido previsto en el artículo 32 del RGPD, así como observar y adoptar las medidas técnicas y organizativas de seguridad necesarias o convenientes para asegurar la confidencialidad, secreto e integridad de los Datos Personales a los que tenga acceso.

En todo caso, deberá implantar mecanismos para:

- a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.



- c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- d) Seudonimizar y cifrar los datos personales, en su caso.

En particular, y sin carácter limitativo, se obliga a aplicar las medidas de protección del nivel de riesgo y seguridad detalladas en el Anexo "Tratamiento de Datos Personales".

**d) Deber de confidencialidad y secreto**

Mantener la más absoluta confidencialidad y secreto sobre los Datos Personales a los que tenga acceso para la ejecución del contrato, así como sobre los que resulten de su tratamiento, cualquiera que sea el soporte en el que se hubieren obtenido. La presente obligación debe observarse incluso después de que finalice la prestación del servicio.

Esta obligación se extiende a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta del adjudicatario, siendo deber del adjudicatario instruir a las personas que de él dependan, de este deber de secreto, y del mantenimiento de dicho deber aún después de la terminación de la prestación del Servicio o de su desvinculación.

**e) Relación de personas autorizadas**

Llevar un listado de personas autorizadas para tratar los Datos Personales objeto de este pliego y garantizar que las mismas se comprometen, de forma expresa y por escrito, a respetar la confidencialidad, y a cumplir con las medidas de seguridad correspondientes, de las que les debe informar convenientemente.

Y mantener a disposición de MADRID DESTINO dicha documentación acreditativa.

**f) Formación**

Garantizar la formación necesaria en materia de protección de Datos Personales de las personas autorizadas a su tratamiento.

**g) Comunicación de datos a terceros**

Salvo que cuente en cada caso con la autorización expresa del Responsable del Tratamiento, no comunicar (ceder) ni difundir los Datos Personales a terceros, ni siquiera para su conservación.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

**h) Delegado de Protección de Datos**

Nombrar Delegado de Protección de Datos, en caso de que sea necesario según el RGPD, y comunicarlo a MADRID DESTINO, también cuando la designación sea voluntaria, así como la identidad y datos de contacto de la(s) persona(s) física(s) designada(s) por el adjudicatario como sus representante(s) a efectos de protección de los Datos Personales (representantes del Encargado de Tratamiento), responsable(s) del cumplimiento de la



regulación del tratamiento de Datos Personales, en las vertientes legales/formales y en las de seguridad.

**i) Destino de los datos**

Una vez finalizada la prestación contractual objeto del presente Pliego, se compromete, según corresponda y se instruya en el Anexo “Tratamiento de Datos Personales”, a devolver o destruir (i) los Datos Personales a los que haya tenido acceso; (ii) los Datos Personales generados por el adjudicatario por causa del tratamiento; y (iii) los soportes y documentos en que cualquiera de estos datos consten, sin conservar copia alguna; salvo que se permita o requiera por ley o por norma de derecho comunitario su conservación, en cuyo caso no procederá la destrucción. El Encargado del Tratamiento podrá, no obstante, conservar los datos durante el tiempo que puedan derivarse responsabilidades de su relación con el Responsable del Tratamiento. En este último caso, los Datos Personales se conservarán bloqueados y por el tiempo mínimo, destruyéndose de forma segura y definitiva al final de dicho plazo.

**j) Transferencias internacionales**

Salvo que se indique otra cosa en el Anexo “Tratamiento de Datos Personales” o se indique así expresamente por MADRID DESTINO, a tratar los Datos Personales dentro del Espacio Económico Europeo u otro espacio considerado por la normativa aplicable como de seguridad equivalente, no tratándolos fuera de este espacio ni directamente ni a través de cualesquiera subcontratistas autorizados conforme a lo establecido en este Pliego o demás documentos contractuales, salvo que esté obligado a ello en virtud del Derecho de la Unión o del Estado miembro que le resulte de aplicación.

En el caso de que por causa de Derecho nacional o de la Unión Europea el adjudicatario se vea obligado a llevar a cabo alguna transferencia internacional de datos, el adjudicatario informará por escrito a MADRID DESTINO de esa exigencia legal, con antelación suficiente a efectuar el tratamiento, y garantizará el cumplimiento de cualesquiera requisitos legales que sean aplicables a MADRID DESTINO, salvo que el Derecho aplicable lo prohíba por razones importantes de interés público.

**k) Notificación de violaciones de la seguridad de los datos**

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 48 horas, y a través de [dpd@madrid-destino.com](mailto:dpd@madrid-destino.com), las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si se dispone de ella se facilitará, como mínimo, la información siguiente:



- a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- e) Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

**l) Asistir al responsable de tratamiento en la respuesta al ejercicio de derechos**

Cuando una persona ejerza un derecho (de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, u otros reconocidos por la normativa aplicable (conjuntamente, los “Derechos”), ante el Encargado del Tratamiento, éste debe comunicarlo a MADRID DESTINO con la mayor prontitud a la dirección de correo electrónico [dpd@madrid-destino.com](mailto:dpd@madrid-destino.com)

La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción del ejercicio de derecho, juntamente, en su caso, con la documentación y otras informaciones que puedan ser relevantes para resolver la solicitud que obre en su poder, e incluyendo la identificación fehaciente de quien ejerce el derecho.

El adjudicatario asistirá a MADRID DESTINO, siempre que sea posible, para que ésta pueda cumplir y dar respuesta a los ejercicios de Derechos.

**m) Colaborar con MADRID DESTINO en el cumplimiento de sus obligaciones como Responsable del Tratamiento**

Colaborar con MADRID DESTINO en el cumplimiento de sus obligaciones en materia de (i) medidas de seguridad, (ii) comunicación y/o notificación de brechas (logradas e intentadas) de medidas de seguridad a las autoridades competentes o los interesados, y (iii) colaborar en la realización de evaluaciones de impacto relativas a la protección de datos personales y consultas previas al respecto a las autoridades competentes; teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga.

Asimismo, pondrá a disposición de MADRID DESTINO, a requerimiento de esta, toda la información necesaria para demostrar el cumplimiento de las obligaciones previstas en



este Pliego y demás documentos contractuales y colaborará en auditoras o en inspecciones llevadas a cabo, en su caso, por la AEPD.

En los casos en que la normativa así lo exija (ver art. 30.5 RGPD), llevar, por escrito, incluso en formato electrónico, y de conformidad con lo previsto en el artículo 30.2 del RGPD un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de la AEPD (Responsable del tratamiento), que contenga, al menos, las circunstancias a que se refiere dicho artículo.

**n) Evidencias de cumplimiento normativa de protección de datos**

Disponer de evidencias que demuestren su cumplimiento de la normativa de protección de Datos Personales y del deber de responsabilidad activa, como, a título de ejemplo, certificados previos sobre el grado de cumplimiento o resultados de auditorías, que habrá de poner a disposición de MADRID DESTINO a requerimiento de esta. Asimismo, durante la vigencia del contrato, pondrá a disposición de MADRID DESTINO toda información, certificaciones y auditorías realizadas en cada momento.

**o) Derecho de información**

Corresponde al Responsable facilitar el derecho de información en el momento de la recogida de datos. En el caso en el que el encargado del tratamiento, en la prestación del servicio efectúe la recogida de datos de carácter personal, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.

La presente cláusula y las obligaciones en ella establecidas, así como el Anexo correspondiente de este pliego relativo al Tratamiento de Datos Personales constituyen el contrato de encargo de tratamiento entre MADRID DESTINO y el adjudicatario a que hace referencia el artículo 28.3 RGPD.

Las obligaciones y prestaciones que aquí se contienen no son retribuíbles de forma distinta de lo previsto en el presente pliego y demás documentos contractuales y tendrán la misma duración que la prestación de Servicio objeto de este pliego y su contrato, prorrogándose en su caso por períodos iguales a éste.

No obstante, a la finalización del contrato, el deber de secreto continuará vigente, sin límite de tiempo, para todas las personas involucradas en la ejecución del contrato.

Para el cumplimiento del objeto de este pliego no se requiere que el adjudicatario acceda a ningún otro Dato Personal responsabilidad de MADRID DESTINO, y por tanto no está autorizado en caso alguno al acceso o tratamiento de otro dato, que no sean los especificados en el Anexo "Tratamiento de Datos Personales".

Si se produjera una incidencia durante la ejecución del contrato que conllevará un acceso accidental o incidental a Datos Personales responsabilidad de MADRID DSTINO no contemplados en el Anexo "Tratamiento de Datos Personales el adjudicatario deberá ponerlo en conocimiento de MADRID DSTINO, en concreto de su Delegado de Protección de Datos a través del buzón [dpd@madrid-destino.com](mailto:dpd@madrid-destino.com), con la mayor diligencia y a más tardar en el plazo de 48 horas.



### **Sub-encargos de tratamiento asociados a Subcontrataciones**

Cuando el pliego permita la subcontratación de actividades objeto del pliego, y en caso de que el adjudicatario pretenda subcontratar con terceros la ejecución del contrato y el subcontratista, si fuera contratado, deba acceder a Datos Personales, el adjudicatario lo pondrá en conocimiento previo de MADRID DESTINO, identificando qué tratamiento de datos personales conlleva, para que MADRID DESTINO decida, en su caso, si otorgar o no su autorización a dicha subcontratación.

En todo caso, para autorizar la contratación, es requisito imprescindible que se cumplan las siguientes condiciones (si bien, aun cumpliéndose las mismas, corresponde a MADRID DESTINO la decisión de si otorgar, o no, dicho consentimiento):

- Que el tratamiento de datos personales por parte del subcontratista se ajuste a la legalidad vigente, lo contemplado en este pliego y a las instrucciones de MADRID DESTINO.
- Que el adjudicatario y la empresa subcontratista formalicen un contrato de encargo de tratamiento de datos en términos no menos restrictivos a los previstos en el presente pliego, el cual será puesto a disposición de MADRID DESTINO a su mera solicitud para verificar su existencia y contenido.
- El adjudicatario informará a MADRID DESTINO de cualquier cambio previsto en la incorporación o sustitución de otros subcontratistas, dando así a la AEPD la oportunidad de otorgar el consentimiento previsto en esta cláusula. La no respuesta de MADRID DESTINO a dicha solicitud por el contratista equivale a oponerse a dichos cambios.

### **Información**

Las Partes únicamente se comunicarán aquellos datos de carácter personal que sean adecuados, pertinentes y no excesivos en relación con las necesidades derivadas del presente Contrato, garantizando que dichos datos sean exactos y puestos al día, obligándose a comunicar a la otra, sin dilación indebida, aquellos que hayan sido rectificadas y/o deban ser cancelados según proceda.

MADRID DESTINO garantiza a los representantes e interlocutores del adjudicatario el tratamiento de sus datos de carácter personal conforme a la legislación vigente y a tal efecto informa que serán incorporados en un fichero titularidad de MADRID DESTINO en los siguientes términos:

**Responsable:** MADRID DESTINO CULTURA TURISMO Y NEGOCIO, S.A., con domicilio en Madrid, calle Conde Duque, 9-11, 28015 Madrid.

**Delegado de Protección de datos:** [dpd@madrid-destino.com](mailto:dpd@madrid-destino.com)

**Finalidades:** Gestionar y cumplir la relación establecida (incluyendo, la gestión del expediente jurídico de contratación, la formalización y archivo de los contratos y escrituras, la gestión de la contabilidad, el cumplimiento de obligaciones impositivas, de facturación, de transparencia y de control)



**Plazo de conservación:** Se limitará al periodo que sea necesario para dar cumplimiento a la relación contractual y durante los plazos de prescripción de las acciones civiles, penales, administrativas o de cualquier otro tipo que pudieran derivarse de la actividad o servicio prestado y del tratamiento de los datos, además de los periodos establecidos en la normativa de archivos y patrimonio documental español.

**Destinatarios:** Agencia Tributaria, Tribunal de Cuentas, Plataforma de Contratación del Estado y demás administraciones públicas, para el cumplimiento de obligaciones de transparencia y control, fiscales, así como, a entidades financieras para la gestión de cobros y pagos y autoridades judiciales. Las obligaciones de transparencia conllevan la publicación en la correspondiente sede electrónica la relación de los contratos suscritos por MADRID DESTINO, con mención de las partes firmantes, su objeto, plazo de duración, modificaciones realizadas, obligados a la realización de las prestaciones y, en su caso, las obligaciones económicas convenidas.

**Legitimación:** Ejecución de un contrato

**Derechos:** El ejercicio de derechos de acceso, rectificación, supresión, portabilidad y limitación u oposición, así como, a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, puede solicitarse mediante e-mail dirigido a [dpd@madrid-destino.com](mailto:dpd@madrid-destino.com), con referencia a "Área Legal" e identificación de la persona solicitante mediante documento oficial.

## 12. SOLICITUD DE INFORMACIÓN

Para solicitar información más detallada sobre este servicio o ampliar información sobre plazo del procedimiento de contratación, las empresas participantes podrán hacerlo a partir de la recogida de este documento a la dirección [rg@esmadrid.com](mailto:rg@esmadrid.com)

Madrid Destino se reserva el derecho de solicitar la ampliación de la información presentada por cada una de las empresas en sus ofertas.

La mera presentación de propuestas implica la aceptación sin reservas de las condiciones establecidas en el presente documento para la ejecución de los trabajos objeto del Contrato.

Por MADRID DESTINO, S.A.

Por el ADJUDICATARIO

Fdo.: Responsable del Contrato

Fdo.: Órgano de Contratación



## ANEXO I “TRATAMIENTO DE DATOS PERSONALES”

### *Descripción general del tratamiento de Datos Personales a efectuar:*

El tratamiento consistirá en los **SERVICIOS DE ALOJAMIENTO DE LAS PLATAFORMAS WEB DE MADRID DESTINO CULTURA TURISMO Y NEGOCIO, S.A.**

El alcance del servicio es el descrito en el Pliego de Prescripciones Técnicas, siendo las webs principales afectada por el servicio las siguientes:

- Lote 1 – Alojamiento plataforma de Turismo:
  - esMADRID.com y web Madrid Convention Bureau.
  - esmadridpro.com (servicios para socios, traveltrade y prensa)
  - Modernización (en especial la base de datos de atenciones y encuestas)
  - explore.esmadrid.com
  - Cupos MCB
  - Cualquier otra web que se aloje en la plataforma durante la prestación del servicio.
- Lote 2 – Alojamiento plataforma de Cultura:
  - medialab-prado.es
  - madrid-destino.com
  - teatrocircoprince.es
  - teatrofernangomez.es
  - documentamadrid.es
  - intermediae.es
  - mataderomadrid.org
  - archivodecreadores.es
  - ciudadistrito.es
  - teatroespanol.es
  - centrocentro.org
  - cinetecamadrid.es
  - naves.mataderomadrid.org
  - Cualquier otra web que se aloje en la plataforma durante la prestación del servicio.

### *Elementos del tratamiento*

El tratamiento de los Datos Personales comprenderá:

- Registro (grabación)
- Conservación (almacenamiento)
- Destrucción (de copias temporales)
- Conservación (en sus sistemas de información)
- Duplicado Copia (copias temporales)
- Copia de seguridad



□ Recuperación

El personal adscrito por la organización adjudicataria, para proporcionar los Servicios establecidos en el Pliego no puede tratar Datos Personales.

En caso de que como consecuencia de la ejecución del contrato resultara necesario en algún momento la modificación de lo estipulado en este Anexo, el adjudicatario lo requerirá razonadamente y señalará los cambios que solicita. En caso de que MADRID DESTINIO estuviese de acuerdo con lo solicitado, MADRID DESTINO emitirá un Anexo actualizado, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

**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 (copias de seguridad, por ejemplo). 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.

**Medidas de seguridad**

Los datos deben protegerse empleando las medidas que un empresario ordenado debe tomar para evitar que dichos datos pierdan su razonable confidencialidad, integridad y disponibilidad.

MADRID DESTINO como empresa integrante del sector público institucional dependiente del Ayuntamiento de Madrid está sujeta al Esquema Nacional de Seguridad (ENS) siéndole de aplicación el Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica.

En la medida en la que los sistemas de información de MADRID DESTINO objeto de tratamiento estén sujetos al Esquema Nacional de Seguridad, las medidas de seguridad a adoptar por la empresa adjudicataria son las recogidas en el Anexo II de Medidas de Seguridad del Real Decreto 3/2010.



En el caso en el que los datos a tratar sean de nivel medio o de nivel alto las medidas de seguridad de nivel medio o alto definidas en el artículo 82 del Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica de Protección de Datos (RLOPD) y demás normativa aplicable vigente en cada momento.

El adjudicatario no podrá no implementar o suprimir dichas medidas mediante el empleo de un análisis de riesgo o evaluación de impacto salvo aprobación expresa de MADRID DESTINO.

A estos efectos, el personal del adjudicatario debe seguir las medidas de seguridad establecidas por MADRID DESTINO, no pudiendo efectuar tratamientos distintos de los definidos por MADRID DESTINO.



## 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 las 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 concurran 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.