MINISTERIO
DE CONSUMO

SECRETARÍA GENERAL DE
CONSUMO Y JUEGO

DIRECCIÓN GENERAL
DE ORDENACIÓN DEL JUEGO

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE ALOJAMIENTO Y PROCESAMIENTO ADMINISTRADO Y GESTIONADO, SEGURIDAD Y MONITORIZACIÓN DE LAS INFRAESTRUCTURAS TECNOLÓGICAS QUE SUSTENTAN Y POSIBILITAN EL EJERCICIO DE COMPETENCIAS ATRIBUIDAS A LA DIRECCIÓN GENERAL DE ORDENACIÓN DEL JUEGO

DIRECCIÓN GENERAL DE ORDENACIÓN DEL JUEGO

(Expediente 202205C02PA0001)

Índice

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

1 ANTECEDENTES

El Ministerio de Consumo fue creado a través del Real Decreto 2/2020, de 12 de enero, por el que se reestructuran los Departamentos ministeriales, y a él corresponde la propuesta y ejecución de las políticas del Gobierno en materia de consumo, protección del consumidor y de juego, que hasta entonces estaban integradas en el Ministerio de Sanidad, Consumo y Bienestar Social, y en el Ministerio de Hacienda.

El Real Decreto 495/2020, de 28 de abril, por el que se desarrolla la estructura orgánica básica del Ministerio de Consumo y se modifica el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales, atribuye a la Dirección General de Ordenación del Juego (en adelante DGOJ), bajo la Secretaría General de Consumo y Juego, las competencias vinculadas a la regulación, autorización, supervisión, coordinación, control y, en su caso, sanción, de las actividades de juego de ámbito estatal.

Así mismo, la Dirección general de Ordenación del Juego asume el objeto, funciones y competencias que la Ley 13/2011, de 27 de mayo, de regulación del juego atribuye a la extinta Comisión Nacional del Juego.

Con tal fin es necesario establecer los sistemas de información que hagan posible el ejercicio de dichas competencias, para lo cual es necesario contar con las infraestructuras TIC que hagan

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

posible el cumplimiento de las mismas. En concreto, desde el momento de la creación de la DGOJ en 2011, ante la falta de recursos tecnológicos propios de infraestructuras y plataformas, se realizaron una serie de contratos apoyados en el AM25/2002 primero, y el AM27/2012 para la contratación de servicios de alojamiento de sistemas de información después, así como diversos contratos de adquisición de las infraestructuras tecnológicas y el software necesario para la correcta prestación de los servicios derivados de las competencias atribuidas a esta Dirección General. En 2017, vía Expediente 62/2017 para la contratación de alojamiento administrado para las aplicaciones informáticas de la DGOJ, dichos contratos se aglutinaron en el contrato vigente de infraestructuras y plataformas tecnológicas. La modalidad de prestación del servicio actual se realiza a través de dos Centros de Proceso de Datos (en adelante CPD) de un **proveedor privado de este tipo de servicios en la modalidad de Hosting Administrado**. Próximo a finalizar, se hace preciso iniciar un nuevo expediente de licitación para la contratación de los mismos.

Se detallan en el presente pliego los aspectos técnicos del nuevo servicio a contratar, con el fin de que cualquier empresa interesada pueda preparar su propuesta de acuerdo con las condiciones necesarias para la prestación del servicio descritas en el presente pliego de prescripciones técnicas.

2 OBJETO Y ALCANCE DEL CONTRATO

El objeto del presente contrato son los servicios de uso, gestión y administración de infraestructuras y plataforma tecnológica de proceso y almacenamiento de datos, monitorización y aseguramiento de la seguridad de los sistemas de información que sustentan y posibilitan el ejercicio de competencias atribuidas a la DGOJ para un periodo de dos años, con posibilidad de prórroga por otros dos en régimen de renovación anual, desde el 4 de mayo de 2022 a 3 de mayo de 2024.

El alcance del contrato podría concluirse por tanto que son los servicios de explotación y gestión de los sistemas y servicios corporativos de proceso de datos de la DGOJ, aseguramiento de la continuidad de los mismos a través de la monitorización y la seguridad de la información, así como la provisión, alojamiento y operación de la plataforma tecnológica en modalidad de hosting de los sistemas corporativos de la DGOJ.

Más concretamente, y con independencia de las condiciones técnicas de ámbito general vinculadas a la provisión del servicio su, los servicios demandados al adjudicatario serán los siguientes:

- Servicio de Almacenamiento administrado.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Servicio de Virtualización de Servidores.
- Servicio de Base de Datos y BI
- Servicio de Balanceo de Carga.
- Servicio de Cortafuegos.
- Servicio de Plataforma Windows y Linux.
- Servicio de Comunicaciones y VPN.
- Servicio de Gestión de Licencias y actualización/soporte.
- Servicio de Respaldo y recuperación de información.
- Servicio de Seguridad de las infraestructuras tecnológicas y la información.
- Servicio de Continuidad de negocio.
- Servicio de Monitorización de los servicios.
- Servicio de Gestión y Seguimiento de los Servicios.
- Servicio de Soporte a los Sistemas de Información de la DGOJ.
- Servicio Avanzado de Soporte Especializado para la BDD ORACLE.

Todas las tareas y servicios indicados en el presente pliego técnico forman parte esencial del servicio contratado a realizar por el adjudicatario. Asimismo se requieren los servicios y tareas de gestión de las plataformas, infraestructura hardware y software que soporta estos servicios y la resolución de peticiones e incidencias sobre los mismos, tal y como se detalla en los apartados de Condiciones Técnicas Generales del servicio y en cada apartado de Condiciones Técnicas Particulares del servicio del presente pliego.

Queda fuera del alcance del contrato cualquier actividad relacionada con desarrollos, asistencia o soporte técnico sobre las aplicaciones de negocio de la DGOJ, a excepción de la asistencia al respecto de compatibilidades con configuraciones relacionadas con los Sistemas Operativos, Sistemas Gestores de Base de Datos (en adelante SGBD), y otro software de base objeto de gestión de este contrato, tal y como se describe en el apartado de Soporte a los Sistemas de Información de la DGOJ, y lo descrito en el apartado de Servicio de Gestión y Seguimiento de los Servicios, así como lo dispuesto en las Condiciones Técnicas Particulares de cada servicio.

3 DESCRIPCIÓN DEL SERVICIO Y DEL ENTORNO ACTUAL

Para una mejor comprensión de los sistemas de información y los servicios considerados en este pliego, a continuación se describe sucintamente cada una de ellos:

3.1 Sistemas de Información Actuales

- **Aplicaciones de cara al ciudadano** (personas físicas y jurídicas – esencialmente, operadores de juego):

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- **Sede electrónica (sede.ordenacionjuego.gob.es) y páginas web públicas de información general de la DGOJ (**www.ordenacionjuego.es, www.jugarbien.es, www.juegoseguro.es y www.juegoilegal.es). Permiten tanto a ciudadanos como a operadores de juego informarse acerca de la actividad de la DGOJ e interactuar con los servicios ofrecidos por la DGOJ para la tramitación de expedientes y consulta de información de carácter general.
- **Servicios web externos.** Para que en modalidad 24x7 los operadores de juego con licencia en el territorio nacional puedan consultar las prohibiciones de acceso al juego (presencia o no en el Registro General de Interdicciones de Acceso al Juego –RGIAJ-), así como verificar los datos de identidad de los jugadores.
- **Servicios web ofrecidos en red SARA:** servicio de consulta de inscripción en el registro de prohibidos, que se ofrece a las CCAA a través del servicio de Intermediación.

- **Aplicaciones internas de la DGOJ:**
  - **Gestión electrónica de trámites competencia de la DGOJ**: aplicación informática que permite al personal gestor de la DGOJ la tramitación de distintos procedimientos administrativos, como pueden ser las autorizaciones, peticiones de licencias, denuncias y gestión del Registro General de Personas Vinculadas a Juego, entre otros.
  - **Sistema de Registro de Operadores,** que consiste en un sistema maestro de datos de los operadores de juego online (nombre, razón social, dirección, contactos, etc.) al que pueden acceder los gestores para consultar cualquier información relacionada con los mismos. Incluye el Registro General de Licencias y el Registro de Personas Vinculadas a Operadores de Juego, así como la información relativas a los expedientes de autorización de juego ocasional, el censo de Operadores Ilegales y el fichero de Entidades Certificadores de Juego.
  - **Gestor de Información de Operadores,** que permite parametrizar los servicios web externos de consulta de prohibiciones de acceso al juego y dar de alta a los operadores en el servicio, introduciendo su certificado e Ips. También permite hacer consultas sobre las peticiones del servicio para resolver incidencias, parametrizar las alarmas del servicio y hacer informes y estadísticas con los datos que almacena.
  - **Gestor de Expedientes Electrónicos,** para cumplir con la normativa relacionada (Esquema Nacional de Interoperabilidad RD 4/2010 y las Normas Técnicas de Interoperabilidad)
  - **Servicios web internos** a consumir por otras aplicaciones de la DG.
  - **Consulta y descarga del fichero de interdicciones de Acceso al Juego.** Acceso por parte de las Comunidades Autónomas a través de la Red SARA para el traslado del fichero a sus correspondientes sistemas de Información así como

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

para realizar las inscripciones, cancelaciones y modificaciones en cumplimiento de los convenios de Integración y Reconocimiento mutuo ente las CCAA y la DGOJ.

- **Relacionadas con la Subdirección General de Inspección:**
  - **Sistema de descarga y validación de ficheros de evidencias de juego.** Constituido por la aplicación NAIPE (basada en el producto comercial Axway 5 Suite), cuyo cometido es la descarga y validación de los ficheros XML reportados por los operadores en sus Sistemas de Control Interno (SCI), y el sistema CENSO, que consiste en un Master Data Management de los usuarios de juego online a nivel nacional.
  - **Plataforma Big Data.** Construida sobre una base de datos columnar de nueva generación, HP Vertica, y se alimenta de los datos procedentes de los registros de juego (Jus) de NAIPE, relativos a las partidas de juego online, los jugadores participantes y los movimientos económicos efectuados durante las mismas.
  - **Sistema de Generación de Informes (SGI).** Sistema de uso interno desarrollado en Internet Information Server para Windows contra la base de datos Oracle, que presenta informes predefinidos y parametrizables.
- **Herramientas de apoyo.** Aplicaciones para la gestión de incidencias y solicitudes, inventario y ciclo de vida del desarrollo de software (GLPI, Jenkins, SONAR, Redmine, etc.)
- **Herramientas software relacionadas con la seguridad.** LDAP (producto WBS Vision Agnitio basado en openLDAP) combinado con y Active Directory Application Mode (ADAM) de Microsoft, aplicación SSO Single Sign-On para el acceso interno a todas las aplicaciones de la casa, y aplicación de gestión de perfiles y usuarios de la red (APSEC)
- **Servicios horizontales.** Adicionalmente, se dispone de los siguientes servicios de bajo nivel, accesibles por más de una aplicación. Algunos de ellos forman parte de sistemas ya mencionados en el anterior párrafo:
  - Bases de datos Oracle.
  - Bases de datos MySql
  - Bases de datos PostgreSQL.
  - Gestor de contenidos, basado en el producto Drupal.
  - Gestor documental, basado en el producto Alfresco
  - Servicio de sistema de ficheros (NFS y CIFS).

- **Appliances de balanceo de carga y seguridad**:
  - Sistemas de balanceo de carga (F5)
  - Cortafuegos perimetral e interno (Checkpoint y Fortigate)
  - Sistemas de prevención y detección de intrusiones (IMPERVA)

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Correlación de eventos de seguridad (OSSIM AlientVault)

3.2 Infraestructura software Actual

Se detalla en este apartado el software comercial que está siendo utilizado en cada uno de los sistemas de información, distinguiendo por un lado los sistemas gestores de bases de datos (o similares) y por otro los demás, que se clasifican en los que usan plataformas Windows y los que se emplean en las plataformas Linux.

3.2.1 Sistemas Gestores de Base de Datos

Los SGBD utilizados son:

- Oracle 12.2 con replicación en el entorno de Producción mediante Active Data Guard (dos parejas de servidores físicos, cada uno en un CPD distinto), en preproducción (una física) y desarrollo (una física).
- MySQL 5.1. Las aplicaciones que hacen uso de este gestor son:
  - Drupal
  - Aplicaciones de software libre de uso generalista en tareas de desarrollo tales como Sonar, Testlink, GLPI, Redmine, TikiWiki, etc.
- PostgreSQL, en este momento es backend de una aplicación específica desplegada en Drupal.
- HP Vertica, para la plataforma de BigData, licenciado para una capacidad máxima de 9 TB medidos en “raw data” (texto plano), en proceso de cambio a licencia perpetua por nodos, ilimitada en cuanto a almacenamiento.

3.2.2 Plataforma Windows

Las plataformas Windows que actualmente usa la DGOJ se utilizan como Directorio Activo, Servidor de Ficheros, DNS, DHCP (dando servicio a los PCs de la sede de la DGOJ sita en c/ Atocha 3), sistema de impresión multifuncional y plataforma DLP. El número aproximado de usuarios es 60 internos y 50 externos, y la Administración es llevada por el área de infraestructuras de la DGOJ. La versión de los servidores Windows es Server 2012, aunque se migrará a 2019 en los próximos meses

3.2.3 Plataformas Linux

La DGOJ dispone de una planta de alrededor de 48 sistemas Linux, típicamente destinados a soportar servidores de aplicaciones (Tomcat), gestores de contenido (Alfresco), gestores web (Drupal), Bases de Datos (MySQL y PostgreSQL) y herramientas de Sistemas (Redmine, Jenkins, Sonar, etc.)

Aunque están administrados por el adjudicatario actual (se ocupa de la administración, mantenimiento, monitorización, parcheo, etc), la DGOJ requiere cierta autonomía para utilizar

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

dichos sistemas y obtener cierta información, como por ejemplo rendimiento, acceso a archivos de logs de las aplicaciones o a ficheros generados por las mismas, etc.

El acceso a las máquinas se realiza a través de autenticación integrada con el LDAP.

Todas las aplicaciones web de la DGOJ están desplegadas sobre sistemas Linux (Red Hat Enterprise Linux, versiones 5, 6 y 7, en proceso de migración a la versión 8). El software utilizado es el siguiente:

- Gestor de contenidos (basado en Drupal 7, en proceso de migración a Drupal 9). Se dispone de una plataforma Drupal bajo la cual existen diversos portales, fundamentalmente con información estática:
    - www.ordenacionjuego.es. Contiene a su vez:
        - el buscador de operadores (http://www.ordenacionjuego.es/es/operadores/buscador) basado en un desarrollo que adquiere los datos de una vista del servidor de Oracle.
        - agenda pública de la DGOJ con visor y buscador de eventos futuros y pasados (http://www.ordenacionjuego.es/es/agenda/buscar)
        - buscador de noticias de la DGOJ (http://www.ordenacionjuego.es/es/actualidad/buscar).
        - área restringida donde usuarios externos acceden a información que la DGOJ les publica en el portal (ordenacionjuego.gob.es/colaboradores)
        - área de noticias de consumo interno, donde un editor publica noticias del mercado del juego y existe un buscador de las noticias publicadas (ordenacionjuego.gob.es/noticias)
        - distintos canales RSS asociados a algunos de las funcionalidades anteriores
    - www.juegoseguro.es
    - www.juegoilegal.es
    - www.jugarbien.es (incorpora un buscador de operadores http://www.jugarbien.es/empresas-del-sector).
    - sede.ordenacionjuego.gob.es (solo la parte estática de la sede electrónica de la DGOJ utiliza Drupal, estando la parte dedicada a la tramitación, registro electrónico, consulta de CSV, … ofrecida por distintas aplicaciones JAVA).
- Gestor documental (basado en Alfresco Enterprise 6.2)
    - La sede electrónica almacena la documentación de los distintos procedimientos, accediendo a este servicio a través de unos servicios web desarrollados a tal efecto.
    - Todos los documentos disponibles en los distintos portales de la DGOJ están albergados en este servicio, existiendo un servicio de comunicación estándar entre este servicio y el gestor de contenidos.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- *La documentación de los distintos proyectos de la DGOJ también está archivada en este gestor documental, a fin de poder dotar a la misma de semántica que facilite su búsqueda y recuperación*

- Servidor de aplicaciones: Apache Tomcat 8.5 sobre Java 1.8
-
- Servidor web: Apache HTTP Server 2.4.
- Software de transferencia y descarga de ficheros: Axway 5 Suite, utilizado en la aplicación NAIPE. Debido al fin del ciclo de vida de esta versión, se abordará en breve el paso a la versión Axway B2Bi, con lo que se puede considerar que para el momento en que se inicie el servicio por parte del nuevo adjudicatario esta migración estará terminada
- Directorio LDAP: WBS Vision Agnitio.
  Arquitectura JEE con frameworks y estándares JFS, JPA, SOAP.

4 CONDICIONES TÉCNICAS DEL SERVICIO A PROPORCIONAR

4.1 CONDICIONES GENERALES

4.1.1 Instalaciones y arquitecturas necesarias para la prestación de servicios

Los servicios se proporcionarán en dos CPD con el objeto de facilitar alta disponibilidad en modo activo-activo.

De forma general se deberá contemplar que tanto los servidores como el resto de equipamiento se encuentre distribuido en cada uno de los CPD, de manera que en caso de desastre en uno de ellos, todos los servicios esenciales que ofrece la DGOJ continuarán siendo ofrecidos sin pérdida de servicio.

Se dispondrá de tres entornos con servicios diferenciados:

- Producción-internet: para publicación de servicios vía internet
- Producción-intranet: accesibles únicamente desde la sede de la DGOJ u organismos alcanzables a través de la red SARA
- Preproducción-pruebas/desarrollo: accesible desde la sede de la DGOJ y en ocasiones desde el exterior vía internet o red SARA

Como se describirá a continuación, cada CPD ofrecerá determinados servicios de TI (almacenamiento, seguridad, balanceo de carga…). La arquitectura propuesta pretende que cada uno de estos servicios pueda prestarse desde un CPD de forma autónoma a desde donde se preste el resto.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Aunque el diseño de la arquitectura requerida es un diseño para soportar un modelo activo-activo, existen ciertos servicios no esenciales en modo 24x7 que no están replicados en los dos CPD (entornos de desarrollo o preproducción, sistema de descarga y validación de ficheros de evidencias de juego, sonda de detección de intrusiones, sistema de correlación de eventos...), siendo únicamente proporcionados a través del conocido como CPD principal. Por ello, la tendencia natural del servicio es que el mismo se entregue desde éste, conmutando al secundario cuando exista algún problema en el primario o las labores de mantenimiento y actualización así lo aconsejen.

Como servicios de carácter general, los relacionados con la electrónica de red, monitorización y backup son ofrecidos de forma transparente, sin tener conocimiento esta Dirección General de los detalles técnicos de implementación.

Para los servicios a prestar se definirán arquitecturas que comprendan:

- Instalaciones físicas donde ubicar las infraestructuras, plataformas tecnológicas y servicios de proceso de datos requeridos así como los servicios auxiliares de gestión de los mismos. Típicamente instalaciones de CPDs principales y centros de gestión, monitorización y control.
- Instalaciones físicas donde ubicar las infraestructuras, plataformas tecnológicas que den soporte de continuidad de negocio y respaldo para aquellos servicios que según este pliego deban contar con Servicio de Continuidad de Negocio. Típicamente instalaciones de CPDs de respaldo así como sus correspondientes centros de gestión, monitorización y control.
- La topología general de las redes y las comunicaciones propias del Servicio de Comunicaciones así como la ubicación de los servidores, cabinas o cualesquiera elementos hardware de infraestructura de las mismas (incluyendo las redes SAN y LAN, las redes VLAN y la red de gestión…), de acuerdo con las políticas de separación física y lógica de entornos, y las políticas propias del Servicio de Continuidad de Negocio. El equipamiento proporcionado será compatible, cuando sea aplicable en función de su naturaleza, con el protocolo IPV6.
- El Software de virtualización, software de base y control del mismo y las infraestructuras físicas en las que se basen los servicios en modalidad de virtualización con la potencia de proceso y memoria necesarias para la provisión correcta de los servicios virtualizados correrán a cargo del adjudicatario.
- El Software de aplicaciones y de ofimática necesario para los servicios auxiliares de gestión del servicio y de las infraestructuras, así como el software de sistemas, tanto de Sistemas Operativos como SGBD, servidores de aplicaciones y servidores web que soporten tales servicios auxiliares.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Todo software de otros servicios comunes tales como software de sistemas de almacenamiento, de copias de seguridad y restauración desde/hacia cinta magnética o similar, de cortafuegos y otros elementos de seguridad, así como el software de sistemas, tanto de Sistemas Operativos como SGBD, servidores de aplicaciones y servidores web que soporten tales servicios comunes.
- El adjudicatario de este contrato deberá proveer una plataforma de monitorización del estado y la gestión de alertas y eventos, que permita conocer en tiempo real el estado de uso y la información principal de los servidores y servicios. Esta plataforma deberá realizar, como mínimo, todos los chequeos y monitorizaciones que se efectúan a día de hoy (*consultar ANEXO III: PLATAFORMA DE MONITORIZACIÓN ACTUAL*).
- La empresa adjudicataria del servicio tendrá la obligación de instalar y mantener actualizado un software de protección antivirus en los servidores que forman parte de todas las plataformas. Este software deberá evitar el contagio de estas máquinas con cualquier tipo de virus, troyanos o malware, por lo que correrá por parte del adjudicatario su instalación y actualización diaria.
- Los aplicativos comerciales utilizados en los servicios de respaldo de información, monitorización y estadísticas, antivirus, etc., dispondrán de soporte comercial oficial y se encontraran en versiones actuales y en las condiciones de operación y soporte definidos por el fabricante o desarrollador.
- La normativa para la implementación de sistemas y especificaciones de seguridad, entornos para aplicaciones y documentación exigible.

Las líneas de comunicación entre el CPD del adjudicatario y la DGOJ serán proporcionadas por el Contrato Único de Comunicaciones. Las líneas se dimensionarán con capacidad suficiente para soportar el tráfico requerido y respetar los niveles de servicio requerido (véase las consideraciones técnicas específicas de los servicios involucrados). Si el adjudicatario no dispone de equipamiento del lote 1 del Contrato Unificado de Comunicaciones de la AGE, debe permitir la instalación del equipamiento correspondiente al mismo, para tener visibilidad de las sedes del Ministerio de Consumo, entre ellas de la propia DGOJ.

Las instalaciones tendrán que cumplir con las siguientes características:

- Alojamiento de equipamiento
  - Gestión y mantenimiento de infraestructuras técnicas de CPD.
  - Control de acceso a las áreas técnicas.
  - Seguridad física perimetral de las salas del CPD.
  - Suministro eléctrico continuado y sistemas automáticos de autogeneración.
  - Clima, control de temperatura y humedad.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Protección antiincendios y medidas adicionales de seguridad
- Cableado eléctrico, de red (LAN) y de datos (SAN).
- Gestión de incidentes, cambios y problemas según especificaciones ITIL.

- Provisión de equipamiento
  - Provisión e instalación de servidores físicos en armarios técnicos
  - Provisión y almacenamiento de servidores virtualizados.
  - Provisión de sistemas de almacenamiento y de salvaguarda de datos.
  - Gestión de los recursos asignados, LAN virtual, disco, etc.
  - Gestión de incidentes, cambios y problemas según especificaciones ITIL, así como sistemas que, de acuerdo con los procedimientos que se establezcan al inicio de la prestación del servicio, permita el seguimiento tanto de las peticiones como de las incidencias abiertas, así como su estado de resolución.
- Provisión de comunicaciones según lo dispuesto en los distintos apartados de Condiciones Técnicas particulares referidas a comunicaciones.

El servicio debe contemplar la evolución de los sistemas de forma que las actualizaciones o incorporación de nuevos sistemas se realicen de forma ágil y formalizada en el contrato del servicio. En este sentido el servicio solicitado debe contemplar la actualización ordinaria y el "hardening" (robustecimiento periódico) de hardware y software (parches, versiones, obsolescencia, vulnerabilidades, etc.), así como un compromiso de renovación tecnológica según lo dispuesto en el apartado Compromiso de Actualización e Innovación Tecnológica. Los equipos hardware provistos por el adjudicatario (switches, routers, etc.) se deben encontrar en todo momento en las condiciones de operación (versiones de firmware, parches, etc.) definidas por el fabricante y en las condiciones de soporte adecuadas para garantizar la alta disponibilidad y seguridad requerida por los servicios de la DGOJ.

Además de la prestación de los servicios mediante la infraestructura y componentes instalados en los dos CPDs indicados, el proveedor adjudicatario podrá dar cumplimiento a los requerimientos solicitados en el presente pliego usando tanto los recursos propios, así como mediante subcontratación, a través de alguna de las posibilidades tecnológicas existentes cubiertas bajo el paradigma de Cloud Computing, o computación en la nube, en cuanto al acceso a los recursos computacionales (como redes, servidores, almacenamiento, aplicaciones, y servicios), siempre que se cumplan al menos los requerimientos mínimos exigidos en el presente pliego técnico, así como la legislación vigente, con especial incidencia en cuestiones de seguridad y protección de datos por la propia naturaleza de las soluciones de Cloud. En ese sentido, los datos no podrán salir del espacio económico europeo y deberá consignarse la ubicación de los centros de datos utilizados así como el propósito con el fin de evaluar la necesidad de realizar la correspondiente notificación a la Agencia Española de Protección de Datos si así fuera necesario.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Adicionalmente, cualquier servicio no contemplado inicialmente en esta modalidad de servicios en la nube, será susceptible de ser migrado durante la ejecución del contrato, previo análisis, evaluación y autorización por parte del proveedor y de la DGOJ. Por otra parte, durante el tiempo de ejecución del contrato, la DGOJ podrá realizar la contratación de servicios en la nube para cubrir necesidades hasta ahora no detectadas, para lo cual se requerirá que el adjudicatario proporcione los servicios necesarios para proporcionar esa interconexión de manera fiable y segura.

Las actividades a realizar por el adjudicatario en el ámbito de infraestructura y arquitectura serán:

- Colaboración con la DGOJ en la definición de las arquitecturas, aportando sus conocimientos tecnológicos y de negocio. Esta colaboración se concretará en propuestas de mejora o innovación tecnológica tal como se indica en el apartado de Compromiso de Actualización e Innovación Tecnológica.
- Homologación de nuevos productos y tecnologías, entendida como la verificación de que un nuevo producto a incorporar es acorde con el resto de productos y tecnologías existentes, tal como se indica en el apartado de Compromiso de Actualización e Innovación Tecnológica.
- Implementación de sistemas (infraestructuras, productos, componentes, tecnologías, aplicaciones, etc.) conforme a la arquitectura definida.
- Mantenimiento de la documentación de arquitecturas, como parte de la actividad de documentación de los servicios.
- Colaboración para el diagnóstico de causas de incidencias.
- Resolución de incidencias en sus distintas criticidades, problemas, cambios y peticiones independientemente de que se notifiquen desde las diferentes unidades de la DGOJ o se detecten y tramiten desde los propios sistemas del adjudicatario en cuanto a monitorización, gestión y control de los servicios.
- Escalado, en su caso, de incidencias, problemas y peticiones a otros grupos de soporte.
- Colaboración en las máquinas administradas por la DGOJ y coordinación en todo caso para instalación de software de aplicación o puestas en producción de proyectos de desarrollo de aplicaciones que requieran actuaciones en hardware y/o software de los sistemas.
- Generación, publicación y gestión de conocimiento útil interno al servicio.
- Formación interna continuada al propio servicio.
- Elaboración de documentación, informes y procedimientos, según lo detallado en cada apartado del presente pliego.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Cumplimiento de requisitos de calidad definidos por la DGOJ.
- Establecimiento de alarmas y sistemas de monitorización y registro automático de incidencias, según lo establecido en el presente pliego.

Para cumplir con la legislación nacional y comunitaria sobre los datos de juego online, ambos CPD deben encontrarse en territorio español.

4.1.2 Ubicación de las Instalaciones e Infraestructuras

El apartado 5.1.14 de la Resolución de 6 de octubre de 2014, de la Dirección General de Ordenación del Juego, por la que se aprueba la disposición por la que se desarrollan las especificaciones técnicas de juego, trazabilidad y seguridad que deben cumplir los sistemas técnicos de juego de carácter no reservado objeto de licencias otorgadas, requiere que el sistema de control interno de cada operador esté ubicado en España. Por consiguiente, en consonancia con dicho requerimiento, **los Centros de Procesos de datos en cuyas infraestructuras se almacenarán sus datos, objeto de la presente contratación, deberán estar ubicados en territorio Español.**

Sin menoscabo de dicho requerimiento mínimo, las decisiones relativas a la ubicación física de las infraestructuras corresponderán al adjudicatario, el cual determinará la ubicación basándose en principios de seguridad de la información, disponibilidad y rendimiento de los sistemas.

En general se seguirá el siguiente esquema:

- Infraestructura para aplicaciones en producción y otros entornos de aplicaciones: residirán en centros bajo gestión del adjudicatario, con las condiciones de seguridad, identificación y acceso que se establezcan.
- Infraestructura para respaldo: Se ubicará en centros bajo gestión del adjudicatario, distintos de los de producción, siguiendo las mejores prácticas en cuanto a distancia de los centros de producción, comunicaciones, accesibilidad, seguridad, etc.

El adjudicatario dispondrá de un Centro de Respaldo ubicado a una distancia suficiente del Centro de Proceso de Datos de Producción según las mejores prácticas, de manera que se minimicen los riesgos de desastres que puedan afectar a ambos centros al objeto de garantizar la continuidad del negocio en caso de eventos que pudieran afectar a la misma área metropolitana.

Al mismo tiempo, la distancia entre ambos centros también ha de cumplir con las limitaciones operacionales Data Center TO Data Center (DC2DC), con el fin de asegurar los rendimientos deseados de latencia, de manera que **el tiempo medio de comunicación entre dos máquinas físicas ubicadas en distinto Centro de Respaldo sea inferior a 0,75 ms, así como que se realizará a través de una conexión DWDM entre ambos centros con un ancho de caudal de al menos 1 Gbps**. El cumplimiento de este requerimiento de tiempo de latencia de conexión entre dos

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

máquinas físicas **se considera parte esencial del contrato y, por tanto, su incumplimiento es motivo de exclusión**.

4.1.3 Catálogo de Elementos Constituyentes de los Servicios

Para constituir los servicios detallados en el objeto y alcance del presente pliego, el adjudicatario deberá tener actualizado un catálogo de componentes que constituyen el contrato teniendo en cuenta:

- Servicios auxiliares que considere necesario para la correcta prestación de los servicios requeridos por la DGOJ.
- Elementos y agrupaciones mínimas que el adjudicatario considere para la prestación de los servicios requeridos por la DGOJ reflejando:
    - Elementos ofrecidos por el adjudicatario mediante los que se constituirán los servicios.
    - Agrupaciones estandarizadas de elementos que constituirán un servicio concreto.
- Unidades de medida de los elementos con costes asociados, lo que permitirá calcular los costes asociados a cada servicio.

Los costes asociados a las unidades de medida de todos los elementos y agrupaciones de elementos, constituyen el coste total de los servicios prestados.

4.1.4 Gestión de Activos

Con carácter general, las principales obligaciones del adjudicatario en relación a la gestión de activos asociados a cada uno de los servicios son:

- Proponer un método para la adquisición y/o transferencia de los activos de la DGOJ y/o de terceros que estén prestando el servicio actual.
- Identificar el equipamiento puesto a disposición de la DGOJ (dedicado o compartido), independientemente de su ubicación.
- Mantener un Inventario actualizado de los activos en servicio. El adjudicatario mantendrá actualizada en todo momento la información de arquitectura de red, inventario y configuración del entorno.
- Velar porque los activos en servicio sean de primeras marcas del mercado que cumplan con los requisitos exigidos para cada servicio en los distintos apartados de Condiciones Particulares.
- Proponer y ejecutar un Plan de renovación del equipamiento, a aprobar por la DGOJ, según lo dispuesto en el apartado de Compromiso de Actualización e Innovación Tecnológica.
- Realizar el servicio de mantenimiento de los equipos durante la vigencia del contrato, durante las Ventanas de Mantenimiento acordadas en función del ANS de cada servicio.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Para los productos de software aportados por el adjudicatario al servicio, disponer obligatoriamente de las licencias correspondientes compatibles con los productos y desarrollos de la DGOJ, homologadas para cada uno de los servicios, realizándose un proceso de actualización tecnológica plasmado en planes de actualización y de verificación de compatibilidad funcional con los productos y desarrollos de la DGOJ, tal como se indica en el apartado de Compromiso de Actualización e Innovación Tecnológica.

4.1.5 Tareas generales de administración y gestión

Como norma general, el adjudicatario realizará las siguientes tareas para todos los servicios:

a) Tareas de monitorización, operación y administración de infraestructuras. Todas las necesarias sobre infraestructuras, sean éstas de naturaleza hardware, software, de sistemas o de comunicaciones, para que los usuarios de la DGOJ puedan desarrollar con normalidad aquellas actividades que dependan del uso de los servicios o aplicaciones corporativas soportadas por los servicios requeridos. Como mínimo, se deberán cubrir los elementos y monitorizaciones descritos en el ANEXO III: PLATAFORMA DE MONITORIZACIÓN ACTUAL.

b) Gestión de la configuración y el mantenimiento de los equipos en horario 24x7 (en los de máxima criticidad) durante todo el plazo de vigencia del contrato, para que su disponibilidad y rendimiento cumplan los Acuerdos de Nivel de Servicio (ANS) requeridos, así como la documentación asociada a dichas tareas (CMDB, esquemas de conectividad de red, etc.). Puede consultarse la relación de servicios/componentes y criticidades en el apartado del presente pliego *de las condiciones generales asociadas al Horario del servicio y criticidades*. La DGOJ tendrá acceso a toda la información de configuración y acceso de todos los elementos del entorno.

c) Actualización de productos comerciales. Previa aprobación de la DGOJ, se instalarán los parches necesarios que permitan alcanzar un óptimo nivel de seguridad y rendimiento en las plataformas. En los entornos de producción, las operaciones de actualización se realizarán de forma general en los horarios de baja utilización del servicio, previa autorización por parte de la DGOJ.

d) Realización de las actuaciones en los equipos físicos definidas por el fabricante como responsabilidad de cliente, por ejemplo: cambios de baterías estándar.

e) Tareas de administración para los sistemas operativos de los servidores objeto de la licitación: la DGOJ se reserva el control del usuario administrador de los servidores linux de base de datos, así como de los servidores Windows y, en general, la de los entornos de desarrollo. No obstante, se podrá solicitar al adjudicatario la realización de tareas como aplicación de parches, instalación y configuración de herramientas y opciones del sistema operativo en cualquiera de éstos. De forma adicional, se podrá solicitar, de manera consensuada y para actuaciones puntuales, permisos de administración en

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

cualquiera de las máquinas. Será necesario proporcionar acceso a las consolas de virtualización para revisión de inventario, acceso al sistema operativo de las máquinas virtuales, etc. En consonancia con el crecimiento previsto de recursos, **se estima que el número de máquinas puede verse incrementado en la misma cantidad, un 15% anual**. Todo ello sin menoscabo de otras tareas a realizar por el adjudicatario en relación a estos servidores administrados por la DGOJ, así como el resto de servidores de la plataforma, como la puesta a disposición de parches, monitorización, backup, etc, tal y como se refleja en los servicios asociados a lo largo del presente pliego.

Se presentan a continuación los servidores a administrar por una u otra parte; aunque se puede observar una cierta dispersión en los sistemas Linux en cuanto a versiones, lo previsible es que antes de la entrada en servicio de la presente licitación todos los servidores linux que lo admitan hayan sido migrados a la versión 8 de RHEL:

Sistema Operativo	**Máquinas**	**Administradas por adjudicatario**
Red Hat Linux 5	1	0
Red Hat Linux 6	37	33
Red Hat Linux 7	8	7
Red Hat Linux 8	3	3
Windows Server 2012	8	0
Windows Sever 2016	5	0
Windows Server 2019	2	0
Resto (appliances)	7	0
TOTAL	**71**	**43**

f) Tareas de Seguridad en el acceso a Internet. Referida a la accesibilidad, disponibilidad y fiabilidad de la información de los sistemas a través de Internet y de acuerdo a las políticas generales de seguridad de la DGOJ. Estas actividades estarán coordinadas con la DGOJ, y deberán incluir:

- Colaboración en la definición de políticas y procedimientos de seguridad que apliquen al acceso a Internet por parte de sistemas, conforme a la política de seguridad que se establezca y a la legislación y a las normativas vigentes.
- Creación de reglas de acceso de la solución de proxy.
- Creación de reglas de acceso, gestión de las DMZ y de la alta disponibilidad del cortafuegos. Se desea detalle de la solución de cortafuegos así como que sea compatible con las reglas de tipo SNORT que la DGOJ recibe periódicamente del Centro Criptológico Nacional (CCN).
- Chequeo periódico de los sistemas de seguridad a fin de detectar y prevenir posibles vulnerabilidades en los sistemas.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- El adjudicatario ha de incluir la realización de un análisis de intrusión anual desde el exterior (Internet) a los sistemas de información publicados por la DGOJ.
- Apoyo en la realización de las revisiones y auditorías que se establezcan.

g) Control de acceso y registros:

- Registro y análisis periódicos de accesos conforme a la normativa definida.

h) Cumplimiento de legislación, normativa y políticas. Realizar, de forma coordinada con la Unidad de Seguridad TIC de la DGOJ, las actividades necesarias para garantizar el cumplimiento de cualquier legislación aplicable, incluyendo la Ley Orgánica de Protección de Datos, el Esquema Nacional de Seguridad, normativa y recomendaciones del CCN y de las políticas, normas y procedimientos de seguridad definidas por la DGOJ.

i) Administración de seguridad englobará, como mínimo, las siguientes actividades:

- Identificación segura de usuarios previa a la realización de tareas de administración.
- Distribución y mantenimiento de los antivirus, antispam y parches de seguridad para todas las máquinas, servidores e infraestructuras.
- Cumplimiento de los estándares de seguridad marcados por la legislación vigente y la propia DGOJ.

j) Licencias de software. El adjudicatario se encargará de gestionar la adquisición para el mantenimiento de licencias (salvo algunas excepciones detalladas en el apartado correspondiente de las condiciones técnicas particulares). Si la situación lo requiere, hará uso del soporte y garantías que estas licencias cubren y gestionará las actualizaciones de versión y aplicación de parches de forma transparente para la DGOJ. El adjudicatario deberá mantener información del servicio que permita comprobar que se dispone de las licencias de software requeridas para su prestación independientemente de que los productos sean proporcionados por el adjudicatario o hayan sido proporcionadas por la DGOJ para su instalación en las infraestructuras gestionadas por el adjudicatario. Esta información se conservará durante todo el período del contrato y será auditable.

k) Servicios de pase a producción. Las actualizaciones de nuevas funcionalidades en cualquiera de las plataformas descritas en este pliego siempre se llevarán a cabo en horarios en los que el servicio se vea menos afectado – periodos de mínimo tráfico – pudiendo producirse de madrugada o durante los fines de semana. Durante estas subidas a producción se contará con la asistencia técnica que se precise por parte del equipo humano ofertado para este contrato.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Las aplicaciones desarrolladas por la DGOJ y que se ejecutan en los servidores TOMCAT son aplicaciones auto-contenidas, por lo que las labores de despliegue de una nueva versión se basan en una posible modificación del fichero de configuración (IPs de acceso a la BD…), el manejo del balanceador de carga para hacer un despliegue sin pérdida de servicio y la actualización física del fichero instalado en el servidor de aplicaciones.

l) Gestión del Almacenamiento SAN. Incluye la gestión de las cabinas con operaciones de creación y gestión de unidades lógicas (LUNs), asignación a servidores, cambios de tamaño, generación de clones y snapshots, actualización de software y firmware, y monitorización del estado y la ocupación, así como la gestión de switches SAN.

m) Análisis de logs de sistemas y de aplicativos de cara a la mejora de los procesos de supervisión y monitorización del sistema (mantenimiento proactivo).

n) Optimización de la configuración con posterioridad al análisis de los logs señalados en el punto anterior y especialmente cuando vaya dirigida a soportar cargas de trabajo excepcionales en periodos puntales.

o) Redacción, gestión y mantenimiento de la documentación:

- Dado que la administración general quedará en manos del adjudicatario, será necesario documentar el entorno, los procedimientos de operación, las operaciones de cambio programadas, etc., de forma que la DGOJ conozca en todo momento el estado de los equipos que le dan servicio. A su vez, se diseñarán procedimientos a seguir en el caso de realizar operaciones sobre cualquiera de los elementos, de forma que la DGOJ esté informada de las actuaciones a realizar, su motivo, el plan de contingencia, etc.
- Documentación del servicio. Los informes al respecto de disponibilidad y rendimiento, así como de estado de cumplimiento de los ANS, se proporcionará mensualmente para cada ámbito del servicio objeto del contrato.

p) Otras tareas contempladas a lo largo del presente pliego tales como:

- Resolución de incidencias, problemas y peticiones de nivel de administración, y escalado a otros grupos de soporte.
- Gestión de servidores virtuales y físicos
- Instalación y migración de servidores, software base (p.ej. sistemas operativos)
- Instalación y gestión de servidores web y de aplicaciones
- Administración y configuración del software base.
- Administración del middleware tipo gestores de aplicaciones, tomcat, drupal, alfresco, etc, así como la gestión de alarmas que aseguren el correcto funcionamiento de la BBDD.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Instalación y administración de colas de impresión.
- "Tuning" o ajuste fino de los sistemas.
- Análisis de la calidad de servicio ofrecida.
- Planificación, coordinación y mejora del rendimiento del servicio.
- Resolución de incidencias, consultas y peticiones escaladas por las distintas unidades de la DGOJ.
- Soporte a proyectos corporativos que involucren a los sistemas objeto de este pliego.
- Gestión de la capacidad para estimar y planificar los recursos (potencia de proceso, espacio en disco, etc.)
- Mantenimiento preventivo, evolutivo y correctivo de servidores.
- Instalación de certificados electrónicos de servidores y componentes tales como los balanceadores F5.
- Actividades de gestión de las copias de respaldo y recuperación.

4.1.6 Relaciones entre servicios

Corresponde al adjudicatario establecer mecanismos de coordinación e implantación de mejores prácticas (ISO 20000, ITIL, etc.) que agilicen la relación entre los servicios, con la supervisión de la DGOJ, evitando la necesidad de arbitraje o control excesivo por parte de la DGOJ.

El adjudicatario, deberá tener actualizado en todo momento el **Documento de Relaciones de Dependencia entre activos y servicios** asociados al presente pliego que determinará las relaciones entre servicios y activos, lo que dependerá de la solución y la modalidad de prestación ofertado.

El licitador, respecto cada servicio, deberá asegurar:

- El control y coordinación de las actividades del servicio.
- La coordinación con el resto de servicios y con la DGOJ conforme al modelo de relación que se establezca.
- La gestión de las actividades del servicio: planificación general, control económico, control de la documentación técnica, operativa y administrativa, información de seguimiento, medición de indicadores y niveles de servicio, análisis de riesgos y ejecución de planes de acción derivados, planes de mejora de los servicios e innovación.
- La gestión de los Recursos Humanos (asignación, formación, retención...).

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- El aseguramiento del cumplimiento de las políticas, normativa, procedimientos e instrucciones de la DGOJ aplicables.

4.1.7 Horario del servicio y criticidades

Dado que la DGOJ ha de ofrecer determinados servicios en modo 24x7, se definen las siguientes criticidades:

Tipo 1	Tipo 2
Servicios y Sistemas que dan soporte a los Servicios Web, la Sede electrónica y los portales web de la DGOJ	Resto de servicios y Sistemas de la DGOJ

Servicio	Tipo	Horario
Servicio de almacenamiento	1	24x7
Servicio de virtualización de servidores	1	24x7
Servicio de balanceo	1	24x7
Servicio de cortafuegos	1	24x7
Servicio de plataforma Windows y LDAP	1	24x7
Servicio de comunicaciones	1	24x7
Servicio de comunicaciones internas y gestión de direccionamiento interno asignado a los servidores	1	24x7
Servicio de respaldo y recuperación de la información	1	24x7
Sistema de prevención de intrusión (IPS)	1	24x7
Gestor Documental Alfresco	1	24x7
Sistema de descarga y validación de ficheros de evidencias de juego	1	24x7
Gestor de contenidos Drupal	1	24x7
Aplicaciones de cara al ciudadano, operadores de juego y otros organismos públicos	1	24x7
Bases de datos Oracle, MySQL y PostgreSQL	1	24x7
Correlación de eventos	2	13x5
Sonda de detección de intrusión (IDS)	2	13x5
Aplicaciones internas	2	13x5
Plataforma Big Data	2	13x5

Puntualmente y por periodos previamente acordados con el adjudicatario, se puede solicitar que alguno de los servicios descritos con anterioridad pase de criticidad de tipo 2 a tipo 1, con

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

el fin de asegurar el servicio en determinados periodos de actividad crítica de la DGOJ, como puede ser el uso de la sede electrónica en periodos de concesión de licencias.

El horario de los servicios no críticos y la atención a incidencias, peticiones o cambios se realizará de acuerdo con la siguiente tabla:

<table>
<tr><th>Entorno</th><th>Detección y resolución de Incidencias</th><th>Peticiones</th><th>Cambios</th></tr>
<tr><td>Producción</td><td>24 X 7</td><td rowspan="3">Laborables y festivos locales de lunes a viernes de 08:00 a 21:00 horas</td><td rowspan="3">Laborables y festivos locales de lunes a viernes de 08:00 a 21:00 horas</td></tr>
<tr><td>Pre-Producción</td><td rowspan="2">Laborables y festivos locales de lunes a viernes de 08:00 a 21:00 horas</td></tr>
<tr><td>Desarrollo</td></tr>
</table>

Podrán planificarse paradas de sistemas por necesidades específicas de mantenimiento fuera de este horario de servicio. Estas paradas deberán ser aprobadas por la DGOJ.

Atención continuada para servicios de alta criticidad

Se requerirá un servicio de retén (soporte de segundo nivel) fuera del horario estándar del servicio, que reciba las incidencias y realice las actuaciones necesarias para reponer el servicio de acuerdo con el ANS establecido al efecto en cada uno de los apartados de Condiciones Técnicas Particulares de cada servicio.

4.1.8 Acceso al CPD y salas de trabajo

El personal funcionario o con relación contractual de servicios con la DGOJ que se determine específicamente, dispondrá de acceso con restricciones y previo aviso al CPD en horario 24x7.

4.1.9 Transferencia Tecnológica

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete a facilitar en todo momento a las personas designadas por la Administración a tales efectos la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrolla el servicio, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

La empresa adjudicataria deberá entregar una propuesta de Plan de Formación para el personal técnico de la DGOJ responsable de la plataforma tecnológica y del seguimiento de la ejecución del contrato.

El adjudicatario al finalizar el contrato deberá devolver la documentación relativa al proyecto, así como entregar cualquier otra generada durante el desarrollo del mismo. La propiedad intelectual o industrial de los productos resultantes del contrato se regulará conforme a lo dispuesto en el artículo 308 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.

4.1.10 Compromiso de actualización e innovación tecnológica

A lo largo de la vida del Contrato se hace necesario, tal y como se ha venido indicando a lo largo del presente apartado de Condiciones Técnicas Generales del Servicio, una actualización tecnológica de las infraestructuras hardware y software a medida que el ciclo de vida de los productos que soportan los servicios contratados evolucione en cuanto a versiones estables, abandono de versiones obsoletas, actualizaciones menores de seguridad o bugs (parches), actualizaciones mayores e introducción de innovaciones que favorezcan la calidad de los servicios contratados en cualquiera de sus dimensiones de rendimiento técnico o económico, bien sea en cuanto a mejora del cumplimiento de los Acuerdos de Nivel de Servicio o en cuanto a la reducción de Costes Unitarios de los Servicios.
A fin de garantizar el correcto funcionamiento de los servicios basados en licencias de productos software, se requiere:

- Acceso a todas la versiones soportadas de todos los productos incluidos, tanto en dígitos mayores (major releáse upgrade) como menores (minor release).

- Acceso a todos los parches de producto generados por el fabricante.

- Disponibilidad de los Paquetes de Soporte que genera el fabricante.

- Disponibilidad de los paquetes de mejora de productos.

- Resolución de problemas a través de apertura de incidencias en centros de soporte o servicios equivalentes.

- Acceso a la base de datos de conocimiento de los distintos productos sobre errores de software y formas de evitarlos si las hubiera.

El suministro del mantenimiento de licencias permitirá disponer del suministro de cualquier versión posterior durante la ejecución del contrato.

Se exige por tanto al adjudicatario la elaboración de un Plan de Actualización e Innovación Tecnológica, revisable anualmente. Dicho Plan debe incluir:

- Una hoja de ruta de cambios de actualización o innovación tecnológica previstos en los distintos elementos hardware y software de cada servicio, indicando plazos de realización.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Se entiende que la justificación de algunos de los plazos de realización puede estar directamente condicionada por el ciclo de vida de vigencia de mantenimiento del software comercial utilizado en la prestación de los servicios, por lo que se debe incluir tanto en el Plan inicial como en las revisiones anuales, los Roadmap de evolución de todos los productos de los fabricantes implicados en la prestación del servicio indicando las fechas límite de funcionamiento o soporte de sus productos.

- El impacto previsto de la aplicación de dichos cambios en el propio servicio o en otros servicios objeto de este contrato, así como en los desarrollos, aplicaciones y productos de la DGOJ desplegados sobre los servicios objeto de actualización o innovación tecnológica.

  Ejemplo: El Impacto ante actualizaciones de versión de Apache Tomcat de 6 a 8, sería la Verificación del funcionamiento de Aplicaciones Web propiedad de la DGOJ desplegados sobre dicha versión de servidor de aplicaciones.

- El impacto negativo previsto en caso de no realizarse la actualización o innovación tecnológica en el plazo propuesto.

Se deberán contemplar nuevas dotaciones, renovaciones de equipamiento y actualizaciones de versiones de software de manera que se garanticen los niveles de servicio y de acuerdo a la planificación de entrada/salida de aplicaciones en producción.

La DGOJ verificará y aprobará el plan.

4.1.10.1 Planes de mejora

Uno de los mecanismos de garantía y mejora de la calidad de los servicios serán los planes de mejora. Estos planes se elaborarán anualmente para cada servicio a partir del análisis de distintos indicadores y encuestas. En base al análisis realizado, se establecerán los objetivos de mejora para cada servicio y se realizará un seguimiento de los planes para verificar el cumplimiento de los mismos.

4.1.10.2 Revisiones y auditorias de los servicios

La DGOJ planificará y realizará revisiones y auditorías sobre todos los aspectos relevantes de actividad de cada servicio. Estas auditorías podrán ser ejecutadas por la DGOJ o auditores independientes y darán lugar a informes de anomalías y recomendaciones.

La resolución de las anomalías y recomendaciones detectadas estará incluida en el alcance de los servicios objeto de este pliego. Así, el adjudicatario deberá presentar planes de actuación para su subsanación. El incumplimiento de estos planes podrá dar lugar a penalizaciones.

4.1.10.3 Innovación

Anualmente, el adjudicatario propondrá métodos concretos para implementar la innovación técnica y metodológica dentro de cada servicio. Estos métodos incluirán la elaboración de

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

propuestas para la realización de proyectos de innovación en el ámbito de la planificación anual de proyectos tecnológicos de la DGOJ.

4.1.11 Servicios avanzados de soporte Windows, Drupal y Alfresco

La DGOJ estima necesario contar con un soporte especializado de las plataformas Windows y de los servidores web (Drupal 7 en proceso de migración a 9) y gestor de contenidos (Alfresco 6.2) al objeto de posibles migraciones, soporte, resolución de incidencias y optimización de dichos servicios existentes en la organización.

- Soporte Proactivo en cuanto a asesoramiento, migraciones, y revisión, definición y optimización de la arquitectura de los distintos servicios.

- Soporte Reactivo en cuanto a la atención y resolución de casos de soporte, incidencias o fallas de las plataformas incluidas en este servicio.

El Responsable Técnico de Infraestructuras del proveedor, contará con el apoyo de los perfiles técnicos avanzados o consultores en las distintas herramientas. Cuando así se requiera, se integrará a tiempo parcial en el Equipo de Trabajo de la DGOJ para su intervención de forma proactiva o reactiva.

De esta manera, todas las peticiones de soporte proactivo o reactivo serían canalizadas a través del Responsable Técnico de Infraestructuras del proveedor para la DGOJ.

Dichos perfiles se encargarán de coordinar internamente con los fabricantes las peticiones de soporte a los mismos y coordinar sus trabajos con la DGOJ.

Además, se encargará de gestionar todo lo necesario en posibles crisis, o incidentes, así como elaborará los informes requeridos por la DGOJ.

Se estima necesaria una dedicación de 192 horas de perfil consultor al año (16 horas al mes) a dedicar, según los requerimientos y la planificación que se consensue con la DGOJ, en una o varias de las distintas herramientas. El coste de este servicio queda incluido en el concepto de mensualidad.

4.2 CONDICIONES TÉCNICAS PARTICULARES DEL SERVICIO

4.2.1 Servicio de Almacenamiento Administrado

Se definen las siguientes tipologías de disco, que se emplearán en el resto del documento:

1) Disco NAS de alto rendimiento: capaz de soportar 1200 IOPS/TB con una latencia máxima de 5 ms
2) Disco NAS de rendimiento medio: capaz de soportar 400 IOPS/TB con una latencia máxima de 26 ms

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

3) Disco NAS de bajo rendimiento: capaz de soportar 80 IOPS/TB con una latencia máxima de 50ms
4) Disco SAN de alto rendimiento: capaz de soportar 4000 IOPS/TB con una latencia máxima de 3 ms
5) Disco SAN de rendimiento medio: capaz de soportar 1500 IOPS/TB con una latencia máxima de 8 ms

El adjudicatario proporcionará el servicio de almacenamiento que actualmente se está ofreciendo a la DGOJ, desde las cabinas del adjudicatario actual a través de NAS (NFS/CIFS) o SAN, en los términos y parámetros actuales, o mejorados de rendimiento, calidad, disponibilidad y fiabilidad.

El servicio de almacenamiento debe ofrecerse de forma transparente, por lo el adjudicatario deberá asumir el control, operación, administración y adquisición de las licencias correspondientes, así como todo lo que pudiera necesitarse en relación con el resto de servicios en lo que a la correcta prestación del servicio de almacenamiento se refiere. El volumen actual asignado a datos existente, categorizado según las grandes agrupaciones de servicios, puede consultarse en el ANEXO I: PLATAFORMA TECNOLÓGICA ACTUAL. Se expresa a continuación el mínimo que debe ser ofertado, teniendo en cuenta el crecimiento previsto sobre lo actualmente asignado hasta que entre en vigor el servicio con el nuevo adjudicatario:

Uso	Acceso	Categoría	Capacidad	Snapshot	% CPD primario
Staging base de datos	NAS	Disco NAS de alto rendimiento	35 TB	20%	3%
Carpetas compartidas	NAS	Disco NAS de rendimiento medio	26 TB	20%	100%
Replicación carpetas compartidas	NAS	Disco NAS de bajo rendimiento	32 TB	20%	0%
Máquinas virtuales	SAN	Disco SAN de rendimiento medio	20 TB	n/a	90%
Máquinas virtuales	SAN	Disco NAS de alto rendimiento	3.2 TB	n/a	100%
Bases de datos	SAN	Disco SAN de alto rendimiento	90 TB	n/a	50%

El objetivo del almacenamiento NAS para el staging de la copia de seguridad de las distintas bases de datos de Oracle, está orientado para permitir una mayor velocidad de recuperación en caso de desastre. Al estar ofrecido por red, se facilita también la recuperación en un entorno alternativo

El sistema de ficheros accedido en modo NAS (NFS/CIFS) deberá necesariamente contar con mecanismos de alta disponibilidad que permitan recuperar el servicio en el centro de standby

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

con un RPO inferior a 10 segundos y un RTO inferior a 10 minutos. Actualmente se realiza una copia en el centro de respaldo en modo asíncrono.

Para facilitar recuperaciones rápidas de ficheros o rutas individuales, el almacenamiento proporcionado en modo NAS deberá contar con un sistema de *snapshot* o imágenes fijas, que se deben ir tomando con las siguientes periodicidades en la propia unidad, siendo visibles y accesibles:

- Horaria, cada hora entre las 9 y las 21 horas, siendo necesario conservar 60 de estas copias
- Diaria a las 0:00, siendo necesario conservar 7
- Semanalmente, los sábados a la 01:00, siendo necesario conservar 2

La unidad sobre la que se replican los datos deberá generar los siguientes *snapshot* sobre la propia unidad de copia:

- Diario a las 0:00, siendo necesario conservar 31 de estas copias
- Semanal los sábados a las 01:00, siendo necesario conservar 8
- Mensual a las 0:30 del día 1 del mes, siendo necesario conservar 2

El espacio reservado para estas copias es del 20% de la capacidad asignada. Se podrá proponer un sistema alternativo que permita una mayor granularidad o una mayor retención, pero el espacio adicional que se necesite reservar no puede ser imputado contra la capacidad de las unidades, que se han dimensionado teniendo en cuenta ese 20%

Las máquinas virtuales deberá estar soportadas por discos proporcionados desde este servicio de almacenamiento, con los tamaños y calidades expresados en el apartado *de condiciones técnicas particulares asociadas al Servicio de virtualización de servidores.*

Un factor crítico es que las cabinas de almacenamiento deberán disponer de mecanismos que le permitan soportar la caída de discos sin que afecte a la integridad de la información contenida, de cara a cumplir con la disponibilidad estipulada en el Acuerdo de Nivel del servicio correspondiente. Este objetivo se conseguirá a través de la configuración RAID o tecnología equivalente que resulte más conveniente para la satisfacción del ANS.

El sistema de almacenamiento debe poder permitir la gestión "en caliente", tanto intercambio de discos como aumento o disminución de volúmenes. Debe ser posible la creación flexible de volúmenes sin necesidad de asignar discos físicos concretos a cada volumen (Thin Provisioning).

Es requerimiento indispensable que se disponga de un sistema de monitorización y gestión avanzada, externo y complementario a las herramientas de gestión de la cabina, accesible por la DGOJ en modo consulta, puesto que a la hora de solicitar acciones de gestión de

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

almacenamiento es necesario poder comprobar de manera ágil y rápida el estado actual, así como el rendimiento o ratio de utilización de los distintos elementos.

El adjudicatario deberá proporcionar informes mensuales, reports, grados de ocupación y gestión de las unidades lógicas de almacenamiento.

En el caso de los servicios NAS que se ofrezcan simultáneamente por CIFS y por NFS debe ser posible establecer permisos desde los servidores Windows y Linux, respectivamente, de manera completa e independiente. Los permisos establecidos sobre las unidades accedidas en modo CIFS se establecerán para usuarios y grupos del Directorio Activo, y los establecidos para el mismo recurso accedido por NFS se establecerán para usuarios y grupos de los ficheros de configuración *passwd* y *group* de la máquina en la que se establezcan, y dichos permisos deben coexistir de manera independiente. Si fuera necesaria la adquisición de una licencia para dar cumplimiento a este requisito, ésta deberá ser proporcionada por el adjudicatario.

La capacidad de almacenamiento total que actualmente se está ofreciendo, podrá alcanzar un incremento de hasta el 15% anual, a petición de la DGOJ, sin que ello suponga variación alguna del importe del mismo.

4.2.2 Servicio de Virtualización de Servidores

Es cometido del adjudicatario proveer el servicio de virtualización que actualmente dispone la DGOJ, dimensionando adecuadamente las granjas de servidores para alojar todas las máquinas virtuales, y proporcionando al menos los siguientes recursos, suficientes para los actualmente disponibles más el incremento esperable durante la tramitación de esta licitación*:* 1200 GB de RAM, 285 vCPUs y 18 TB de disco, del cual 3.2 TB deben ser obligatoriamente SAN de alto rendimiento y el resto, SAN de rendimiento medio.

Desde el punto de vista del sistema operativo empleado en cada sistema de información, se distinguen dos tipos:

- Sistemas de Directorio Activo y servicios asociados, como DHCP, DNS, etc. (12 máquinas)
- Sistemas de información de arquitectura Web o bases de datos, basados en sistema operativo Linux Server (47 máquinas)

Ambos entornos se ejecutan, en su totalidad, en modo virtualizado para conseguir un óptimo aprovechamiento de los recursos hardware, una mayor disponibilidad y una mejor tolerancia a fallos.

Si la gestión de los servicios (F5 virtual, SIEM, etc.) necesita la creación de máquinas virtuales en la infraestructura virtual de la DGOJ, éstas no computarán de ninguna manera en los recursos del organismo.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

El servicio de virtualización debe ofrecerse de forma transparente, así que el adjudicatario deberá asumir el control, operación, administración y adquisición de las licencias correspondientes.

Se necesita disponer en este servicio de un mecanismo de recuperación de desastres de forma que si un centro cae totalmente o existe una incidencia en la cabina de almacenamiento los servidores virtualizados se puedan levantar en el centro de respaldo en un tiempo de alrededor de 60 minutos (RTO) y con una pérdida de datos y actividad de la máquina inferior a 10 segundos (RPO). El mecanismo existente en este momento consiste en la replicación de determinadas máquinas entre CPD, pudiendo estimarse que se deben provisionar un máximo de 15 máquinas en este mecanismo de replicación.

La solución técnica propuesta y ejecutada por el adjudicatario deberá ofrecer periódicamente un informe actualizado de utilización de las máquinas virtuales o se deberá permitir el acceso a una consola donde se puede consultar esta información.

La planta de servidores administrados podrá alcanzar un incremento de hasta el 15% anual de servidores virtuales o de cualquiera de los parámetros que los definen -VCPU, memoria, disco-, durante el período de vigencia del contrato, sin que ello suponga variación alguna del importe del mismo. No se computarán aquellos servidores o recursos que se creen con el objeto de realizar pruebas de rendimiento o de aplicación y cuya permanencia en servicio sea inferior al mes, pudiendo disponer de un máximo de cualquiera de estos valores:

- 4 servidores
- 16 vCPU
- 128 GB de RAM.

La configuración típica de los servidores virtuales será la comprendida en los siguientes parámetros:

- vCPU: 1, 2, 4, 8 o 16
- GB de RAM: 4, 8, 16, 32, 64, 128

4.2.3 Servicio de Base de Datos y BI

Se separan estos dos servicios por sus características peculiares y necesidad de definición detallada y exacta de los requisitos:

Oracle

El sistema de licenciamiento de Oracle se basa en el número de procesadores (cores) en el que se ejecuta la base de datos. Por tanto, hay varias maneras de proporcionar este servicio sin incurrir en incumplimiento del acuerdo de licencia:

- Servidores físicos con el número exacto de cores
- Servidores físicos que admitan particionamiento de recursos

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Servidores físicos que usen el sistema de virtualización de Oracle (anteriormente OVM, actualmente KVM por fin de soporte del anterior), que permite hacer "pinning" de cores a las máquinas virtuales, obligando a que se ejecuten sólo en el número de cores licenciados.

En todo caso, es requisito que estos cores soporten la tecnología "multithread", puesto que para la base de datos aparecerán dos procesadores lógicos, uno para cada thread del core. Otra configuración no puede ser admitida, a fin de proteger la inversión en licencias de la DGOJ.

A modo de información, los servidores de base de datos están actualmente definidos usando la tercera opción, con el producto OVM; quiere esto decir que es imprescindible la migración al producto soportado, KVM, para lo que el adjudicatario deberá proporcionar las máquinas virtuales sobre dicho producto, si es que opta por esta opción.

Asimismo, la versión actual del sistema operativo de las máquinas virtuales de base de datos así definida es la 6.10 de Red Hat Enterprise Linux, por lo que se deberá también migrar también a una versión soportada por el software de base de datos Oracle de dicho sistema operativo u otro similar, siempre que el adjudicatario cuente con soporte oficial para el mismo.

Es muy importante resaltar que, si se opta por un entorno de virtualización para proporcionar este servicio, éste debe respetar los requisitos recién expresados. Si no se toma esta precaución y se usa otro hipervisor, Oracle puede presumire que la base de datos se ejecuta en todos los procesadores de la máquina física, y reclamará licenciamiento por todos. Los técnicos de la DGOJ pueden asistir al adjudicatario en esta tarea, o éste puede hacer uso del soporte avanzado que se solicita con la intermediación de dichos técnicos. En ningún caso admitirá la DGOJ responsabilidad patrimonial alguna porque el adjudicatario ignore este hecho.

El dimensionamiento necesario es el siguiente:

Entorno	**CPD**	**Rol**	**CPU**	**Memoria (GB)**
Gestión	Primario	OEM	4	15
Desarrollo	Standby	Única	8	80
Preproducción	Primario	Standby	8	16
Preproducción	Standby	Primaria	8	64
Producción	Primario	Primaria 1	16	96
Producción	Primario	Primaria 2	20	409
Producción	Standby	Standby 1	16	96
Producción	Standby	Standby 2	20	192

Este dimensionamiento tiene carácter de mínimo en cuanto a la memoria y de exacto en cuanto a los procesadores, porque en otro caso se estaría incumpliendo el licenciamiento, como se ha reiterado.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

En las bases de datos del entorno de producción y preproducción se replica la información entre los CPD, utilizando la característica Oracle Active Data Guard u Oracle Data Guard, según el uso de las distintas instancias.

Las instancias del entorno de desarrollo están en el CPD primario y no se encuentran replicadas.

HP Vertica

En el CPD primario están instalados dos clústers de servidores físicos de base de datos, para los entornos de preproducción y producción de la plataforma de Big Data (BD) de la DGOJ, con tecnología HP Vertica.

El entorno de producción no se encuentra replicado (no se requiere alta disponibilidad), pero sí que se realiza back-up, para recuperación de la información que contienen en caso de contingencia.

Además, existen dos servidores virtuales para los servicios de ETL de la plataforma de Big Data, en el CPD primario.

Por las características del producto, éste debe ser ejecutado sobre un cluster de servidores idéntidos, con una línea de comunicación interna de 10 G, debiendo proporcionarse las máquinas con dos tarjetas de red de esta velocidad conectadas a dos switches distintos, para proporcionar redundancia; asimismo, estos nodos deben contar con almacenamiento local, no se admitirá que sea disco SAN asignado desde las cabinas

A modo de orientación, estas son las características de los servidores que ejecutan los servicios de ambos entornos. Las características se deben considerar mínimas en este caso, es admisible ofertar equipos de superior capacidad en cualquiera de sus parámetros:

- Entorno de bases de datos de Producción: 4 unidades HP DL380
    - Procesador: E5-2640v3 Intel Xeon 2 x 8 core Intel Xeon (2.6 GHz)
    - Memoria RAM: 128 GB
    - Discos: 48TB raw disk basado en 8 TB SATA HD (SAS1: 1TB y SAS2: 16TB en RAID 10). (NOTA: Se detalla el almacenamiento local porque se hace uso intensivo de él dentro del clúster).
    - NIC: 4x1Gb y 2x10Gb
- Entorno de bases de datos de Preproducción: 2 unidades HP DL380
    - Procesador: E5-2637v3 Intel Xeon 2 x 4 core Intel Xeon (3.5 GHz)
    - Memoria RAM: 64 GB
    - Disco: 12TB raw disk basado en 2 TB SATA HD (SAS1: 1TB y SAS2: 4TB en RAID 10). (NOTA: Se detalla el almacenamiento local porque se hace uso intensivo de él dentro del clúster).
    - NIC: 4x1Gb y 2x10Gb

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Se hace constar que estos servidores disponen de una versión de sistema operativo RHEL 6.10, que está cerca de finalizar su ciclo de soporte. Por tanto, **la solución propuesta por el adjudicatario deberá incluir un plan de migración a servidores de iguales o superiores características físicas con sistema operativo de la última versión compatible con Vertica**.

4.2.4 Servicio de Balanceo de Carga

El servicio de balanceo debe ofrecerse de forma transparente, de forma que el adjudicatario deberá asumir el control, operación, administración, monitorización, mantenimiento y actualización, para lo que deberá contar con el soporte oficial correspondiente. La DGOJ deberá contar con los correspondientes permisos de visualización del estado de los equipos.

El servicio de balanceo de carga se presta actualmente mediante un cluster de balanceadores f5 de BigIP, consistente en hardware dedicado en exclusividad para la DGOJ y se desea mantener la misma modalidad dedicada. Además, se debe provisionar un appliance virtual con la misma tecnología y versión que los mismos, para definir los servicios virtuales de los entornos de preproducción y desarrollo, con el fin de probar la aplicación de parches y nuevas versiones del firmware de los balanceadores.

En cada CPD hay un balanceador, trabajando ambos en alta disponibilidad en modo activo-pasivo, y realizando el balanceo de la carga hacia los servidores correspondientes, independientemente de su ubicación física.

Sobre las características comunes de un balanceador se quiere volver a hacer hincapié en la necesidad de cumplimiento de las siguientes funcionalidades:

- Terminador de túneles SSL de sesiones seguras
- Un mismo string publicado en varios dominios
- Control de string de forma que sean sólo visibles determinados string para determinados rangos de IPs
- Dejar pasar la IP del cliente remoto al servidor web correspondiente (entrada sin NAT)
- Poder manejar la petición de certificados al cliente remoto y pasar el mismo en la cabecera http al servidor web correspondiente
- Permitir conexiones salientes desde los servidores a los que da servicio entrante, pudiendo enmascarar la dirección IP utilizando una específica para estas conexiones, aunque esto también lo puede realizar algún otro elemento de la arquitectura propuesta (NAT de salida)
- De forma añadida, se requiere la inclusión de software específico que permita la segmentación de entornos.

En el caso de que el adjudicatario final fuese empresa distinta al actual, se entiende que el traspaso de configuraciones y equipos se podrá realizar de un adjudicatario a otro dentro de la fase de transición definida dentro de las fases de prestación del servicio del presente pliego. Se

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

hace notar, a este prespecto, que la configuración existente tiene una complejidad alta, por lo que los equipos que se oferten deben ser capaces de definir reglas complejas.

Durante la vigencia de la presente licitación no se prevé la expiración del soporte de ninguno de los elementos de balanceo

4.2.5 Servicio de Cortafuegos

Como servicio a ofrecer de forma transparente, el adjudicatario deberá asumir el control, operación, administración, monitorización, mantenimiento y actualización, para lo que deberá contar con el soporte oficial correspondiente. La DGOJ deberá contar con los correspondientes permisos de visualización del estado de equipos.

La arquitectura de seguridad actual utiliza dos niveles de cortafuegos de diferente fabricante configurados por parejas en alta disponibilidad en modo activo-pasivo. En cada CPD hay uno de los equipos de la pareja. Esta arquitectura debe ser respectada por los licitadores.

Es necesario recordar que la seguridad es un elemento esencial en la construcción de los sistemas de información de la DGOJ, ya que cualquier fuga de información puede resultar en una pérdida de credibilidad de las funciones inspectoras y regulatorias de la DGOJ, haciendo peligrar su propia existencia como órgano.

Características mínimas de los cortafuegos:

- De conexión hacia el exterior
    - Alta disponibilidad 24x7 mediante réplica de dispositivos
- De conexión con la LAN interna
    - Alta disponibilidad 24x7 mediante réplica de dispositivos
- De separación para el entorno de las consolas de gestión disponibles para la DGOJ
- Separación de otros entornos (opcionales, y dependiendo del entorno a securizar puede que sea necesario alta disponibilidad 24x7)

Adicionalmente se dispone, como medio de protección de la red local de la sede de la DGOJ sita en c\ Atocha, de dos cortafuegos en alta disponibilidad que deberán ser administrados por el adjudicatario, incluyendo el soporte técnico y escalado con el fabricante, en las mismas condiciones y con las mismas responsabilidades que los instalados en los CPD

Se deberá mantener la utilización del proxy integrado en el cortafuegos interno para acceso a internet de determinados servidores y de los usuarios del Ministerio de Consumo, incluidos los de la DGOJ, puesto que en este momento la entidad no dispone de otra salida a Internet. No obstante, se podrá proponer como mejora la disposición de un servicio de proxy en la nube para la navegación de los usuarios.

Durante la vigencia de la presente licitación no se prevé la expiración del soporte de ninguno de los elementos relacionados en este apartado

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

4.2.6 Servicio de Plataforma Windows

Tal y como ya se ha adelantado en la descripción del entorno actual, y más concretamente en el apartado *3.2.2 Plataforma Windows*, se requiere disponer de al menos las mismas plataformas Windows que actualmente usa la DGOJ para su uso, al menos, como Directorio Activo, Servidor de Ficheros, DNS, DHCP (utilizado por los PCs de la red de Atocha) y sistema de impresión multifuncional. El número aproximado de usuarios es de 200 internos y 100 externos, y la administración es realizada por el área de infraestructuras de la DGOJ. La versión de los servidores Windows existentes es Server 2012, en proceso de migración a la versión 2019.

El adjudicatario deberá proporcionar informe de auditoría semestral de análisis y comparación del estado del sistema de archivos compartidos en red vía herramienta o sistema dedicado que permita aportar dicha información en cuanto a volumen disponible y ocupado, tipos de archivos almacenados por usuario, usuario con más uso de espacio, etc, así como que permita crear alertas de uso de los archivos, como por ejemplo copia masiva de archivos desde o al servidor, acciones realizadas fuera de cierto horario, etc….

Además del servicio del suministro de licencias en modo SPLA (Service Provider License Agreement) por parte del proveedor tal y como se está prestando el servicio actualmente, se requiere establecer un "***Servicio de soporte especializado de Windows"*** *según lo descrito en el apartado de condiciones técnicas generales*.

4.2.7 Servicio de Plataforma Linux

El adjudicatario queda obligado a proporcionar licenciamiento Linux, preferiblemente Red Hat Enterprise Linux, versión 8. En el caso de presentar propuesta de un sistema operativo alternativo, debe presentar un estudio que justifique que la alternativa está soportada por todas las herramientas software que se describen a lo largo del presente pliego (Vertica, Oracle, Alfresco, Drupal, etc.)

Debe asimismo presentar prueba de que ha contratado un servicio de soporte para resolución de incidencias, consultas y servicio de suscripción para actualizaciones de funcionalidad y seguridad.

El número de licencias a provisionar debe ser igual o superior al número de máquinas linux que se relacionan en el presente pliego, y se deben tener previstas las correspondientes al incremento anual máximo del 15%.

4.2.8 Servicio de Comunicaciones y VPN

Desde cada CPD se tendrá acceso a todas las redes necesarias:

- Red de la DGOJ (*Atocha*), el servicio está soportado por el lote 1 del Contrato Unificado de Comunicaciones de la AGE.
- Red SARA a través de la red del Ministerio de Consumo.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Internet. El servicio es soportado por el lote 3 del Contrato Unificado de Comunicaciones de la AGE.

Si el adjudicatario no dispone de equipamiento del lote 1 del Contrato Unificado de Comunicaciones de la AGE, debe permitir la instalación del mismo en sus CPD, para tener visibilidad de las sedes del Ministerio de Consumo, entre ellas de la propia DGOJ.

El acceso a Internet se proporciona dentro del Contrato Unificado de Comunicaciones de la AGE, por lo que el futuro proveedor no tendría que suministrarlo. Sin embargo, deberá permitir la instalación de los elementos de comunicación correspondientes al lote 3 de CORA, si no dispone de ellos o si los responsables del contrato unificado lo considerasen necesario.

Los equipos de ambos CPD deberán ser visibles entre sí mediante extensión de distintas VLANs, de manera que serán accesibles independientemente de su ubicación física, la latencia entre máquinas ubicadas en dos CPD distintos no puede ser superior a 0,75 ms. En el CPD secundario existirán al menos una VLAN privadas de muy altas prestaciones de caudal (10 Gbps), dedicadas a la plataforma de Big Data.

Existirá un servicio VPN SSL para el acceso remoto del personal interno y de diferentes grupos de desarrolladores a los servidores y aplicaciones de la DGOJ. La autenticación se realizará por medio del LDAP de la DGOJ y se establecerán medidas de control de tráfico IP para evitar accesos a sistemas no autorizados. Previo a la conexión, se realizará un chequeo del equipo cliente para comprobar el cumplimiento de determinados parámetros de seguridad (comprobación de actualización de antivirus y sus firmas, entre otros) y solicitará doble factor de autenticación.

Adicionalmente, este servicio será compatible con dispositivos móviles Android o iOS, permitiendo acceder a servicios internos de la DGOJ vía terminales móviles.

Se debe permitir al menos la conexión de 200 usuarios, con una concurrencia del 100%

Como ya se ha manifestado, el adjudicatario deberá proveer al menos las siguientes líneas y caudal de comunicaciones no cubiertas por el Contrato Unificado de Comunicaciones, además de las VLAN que se describen a continuación:

Descripción	Acceso	Caudal
Conexión entre CPDs		1 Gpbs
Conexión VLAN de la plataforma Big Data (CPD 2) Producción y Pruebas		Dual 10 Gbps

Los diferentes entornos estarán segmentados e interconectados mediante cortafuegos. Existirán diferentes niveles de protección en función de la exposición de los servidores y de la funcionalidad que facilitan.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Se proporcionará una eficiente gestión y supervisión del direccionamiento interno asignado al Ministerio de Consumo en el plan de direccionamiento de la AGE. El Adjudicatario proporcionará todos los elementos y electrónica de red necesaria para dar soporte a todos los servicios exigidos en este pliego y propondrá un sistema de gestión del direccionamiento de IP privadas asignadas a los servicios internos. Esta gestión deberá permitir conocer y mantener actualizada la relación de IP's, con las URL's, servicios, puertos y servidores asociados. También se incluirá las IP's de todos los elementos de comunicación que intervengan en la red de comunicación interna.

Se mantendrá un registro que contendrá el rango completo de direccionamiento interno, y se conservará el rango de direccionamiento indicado, así como el caudal y la topología de redes virtuales existentes, sin menoscabo de que pudieran solicitarse la creación/eliminación de alguna por cuestiones técnicas o de seguridad. A efectos de documentación, se reproducen las principales VLAN de servicio actualmente definidas en los CPD:

Descripción
Web Services y web PRE a fw internos
Web Services y web PRO a fw internos
Web Services y web PRE a balanceadores
Web Services y web PRO a balanceadores
FW internos a DC y LDAP
FW internos a BB.DD.
Red interna servidores BBDD Oracle
Red interna servidores BBDD Vertica (10 Gbps)

El registro recogerá si la IP está libre y si está asignada su utilización: asociada a un interfaz, a un servidor, servicio interno con su url y puerto...etc. Es obligación del adjudicatario mantener el registro de direccionamiento privado.

Cualquier solicitud o actuación (por ejemplo un nuevo servidor) que afecte al contenido de este registro deberá reflejarse en el mismo. La operación a realizar, así como la actualización, no deberá exceder el plazo de 5 días.

El Adjudicatario entregará una copia de este registro cuando el personal de Infraestructuras de la DGOJ se lo solicite. En todo caso formará parte de la documentación que el adjudicatario deberá entregar.

Respecto a la plataforma de Big Data, los servidores Big Data necesitan un rendimiento de red elevado, por usar una arquitectura distribuida, por lo que es requisito que su interfaz de interconexión esté conectada a al menos 10Gbps. Para conseguir alta disponibilidad, será necesario que cada equipo se conecte a dos switches diferentes por puertos de 10Gbps.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

También destacar que las redes de gestión, monitorización y back-up de los equipos, se ofrecen por interfaces distintas a la de servicio, y su definición, mantenimiento y gestión corresponde al adjudicatario por entero.

Los técnicos del adjudicatario colaborarán en la resolución de cualquier incidencia de comunicaciones internas que afecte al acceso de los servicios del CPD independientemente de que la causa sea imputable al Adjudicatario.

4.2.9 Servicio de Gestión de Licencias y Actualización/Soporte

Hasta la fecha de aprobación del presente pliego, la DGOJ dispone de las siguientes licencias que el nuevo adjudicatario deberá asumir a nivel de adquisición para su renovación durante el periodo de vigencia del contrato:

- WBS Vision Agnitio.
- Axway Synchrony (en su versión 5, "Axway Suite 5"), auque lo previsible es que antes de la entrada en funcionamiento del servicio se haya migrado al producto Axway B2Bi, por fin del cliclo de vida del producto actual
- Licencias Oracle para los entornos de la DGOJ.
- HP Vertica (está en proceso de adquisición una licencia por nodo sin límite de espacio)
- Para el resto de productos tales como sistemas operativos Red Hat/Debian y Windows, Alfresco, Drupal, etc, tanto la licencia de uso necesarias como la renovación corren a cargo del adjudicatario.

Las licencias necesarias para la correcta provisión del servicio y que no sean proporcionadas por la DGOJ, deberán ser adquiridas por el adjudicatario. Estas deberán tener como día de entrada en vigor justamente el día de entrada en vigor del presente contrato. Las licencias que se adquieran o renueven deberán cubrir la totalidad del período de ejecución del contrato. Aun cuando se irán referenciando a lo largo del presente servicio las fechas de fin de mantenimiento de las licencias propiedad de la DGOJ, recomendamos la consulta del ANEXO II: SOPORTE Y MANTENIMIENTO DE HARDWARE Y SOFTWARE.

En los casos de Axway, Oracle y HP Vertica, el adjudicatario deberá gestionar la renovación de las licencias y soporte asociado, de forma que éstas serán propiedad de la DGOJ. En los restantes casos, las licencias podrán adquirirse a nombre del proveedor.

Cabe destacar que debido a la evolución tecnológica de los productos software, todos los productos y versiones indicados podrán ser modificados a lo largo de la vida del contrato, tal y como se refleja en el apartado "*Compromiso de actualización e innovación tecnológica*".

A continuación se pasa a exponer los detalles específicos de cada plataforma.

Axway 5 Suite

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

El adjudicatario tendrá que renovar las licencias de este producto, que actualmente obran en poder de la DGOJ, en modalidad máquina virtual, con las siguientes características:

	PRODUCCIÓN		Preproducción		Desarrollo		Fecha fin de mantenimiento
	CPUs	Núcleos	CPUs	Núcleos	CPUs	Núcleos	
Synchrony Integrator	2	4	2	4	1	2	30/04/2019
Synchrony Gateway	1	2	1	2	1	2	30/04/2019
Synchrony Sentinel	1	2	1	2	0	0	30/04/2019

El proveedor no tendrá que hacer uso del servicio de soporte de las mismas, tarea que correrá a cargo del equipo de desarrollo de la aplicación NAIPE.

Open LDAP/WBS Vision Agnitio

El adjudicatario, deberá proporcionar los mecanismos de alta disponibilidad activo-activo con copias para la replicación, así como los mecanismos de acceso a soporte que considere oportunos para resolver incidencias relacionadas con el funcionamiento de los módulos instalados así como que renovar las licencias de este producto a contar a partir del 30 de abril de 2022 y por el periodo de vigencia del contrato, en modalidad estándar o aquella que ofrezca un soporte con las siguientes características:

- Canal de alta de ticket: correo, web, teléfono
- Asistencia remota o telefónica
- 2 Contactos autorizados
- Tiempos máximos de respuesta:
    - Incidencia grave: 8 horas laborables
    - Incidencia media: día siguiente laborable
    - Incidencia leve o consulta: 2 días laborables
- Horarios de recepción telefónica, asistencia remota por teléfono, y asistencia presencial:
    - De Septiembre a Diciembre y de Enero a Junio: L-J 8:30-14, 15-18; V: 8:30-15
    - En Julio y Agosto, LMXJV 8:30-15
- Requerimientos técnicos
    - Modelo hardware: 40/50/100/200/300/Virtual
    - Número de productos: 2
    - HA/Balanceo: Si
    - Usuarios base: 5.000
    - Módulo Identity Management
    - Módulo Report Services

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Número de casos/consultas incluidos: 10
- Número de incidencias de producto (bugs) incluidos: ilimitadas
- Mantenimiento hardware appliance: Soporte in-situ, con sustitución de piezas y mano de obra
- Soporte reactivo y proactivo (no evolutivo)

Oracle

- La administración, gestión y actualización de la base de datos Oracle se realiza por personal de la DGOJ.
- No obstante, el adjudicatario deberá configurar los módulos de monitorización correspondientes asociados a una operación 24x7, aun cuando las alarmas de dichos sistemas sean atendidas por personal de la DGOJ y del adjudicatario según el responsable asociado a su solución.
- Adicionalmente, y en la línea de posibilitar ofrecer soluciones de servicios de base de datos en modo SAAS, en el caso de que se aborde por parte del adjudicatario dicha estrategia de consolidación, el mismo deberá hacerse cargo de la adquisición y renovación, y por el plazo de ejecución del contrato, de las licencias asociadas de este software, teniendo en cuenta que necesitará de la aprobación de la DGOJ en el caso de que dichas operaciones supongan la desaparición del soporte de las actuales licencias.

La DGOJ dispone de las siguientes licencias, que deberán ser renovadas por el adjudicatario:

PRODUCTO	***CSI***				***Fecha fin mantenimiento***
	18851592	19218468	19753410	20355012	
	Licencias	Licencias	Licencias	Licencias	
Advanced Security - Named User Plus Perpetual	50	50	100		30/04/2019
Advanced Security - Processor Perpetual	4	4			30/04/2019
Database Vault - Named User Plus Perpetual	50	50	100		30/04/2019
Database Vault - Processor Perpetual	4	4			30/04/2019
Oracle Database Enterprise Edition - Named User Plus Perpetual	50	150	200		30/04/2019
Oracle Database Enterprise Edition - Processor Perpetual	4	4			30/04/2019

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Partitioning - Named User Plus Perpetual		100	100		30/04/2019
Tuning Pack - Named User Plus Perpetual		200			30/04/2019
Tuning Pack - Processor Perpetual		8			30/04/2019
Diagnostics Pack - Named User Plus Perpetual		200			30/04/2019
Diagnostics Pack - Processor Perpetual		8			30/04/2019
Oracle Active Data Guard				4	30/04/2019

NOTA: las licencias basadas en usuarios son las correspondientes a las labores dedicadas a sistemas de bases de datos de inspección.

Alfresco

El adjudicatario deberá proporcionar los mecanismos de alta disponibilidad, que al menos serán activo-pasivo con copias para la replicación fuera de línea, así como los mecanismos de acceso a soporte que considere oportunos para resolver incidencias relacionadas con el funcionamiento de los módulos instalados.

MySQL

El adjudicatario deberá proporcionar los mecanismos de alta disponibilidad, que al menos serán activo-activo en modo lectura y activo-pasivo en escritura, así como los mecanismos de acceso a soporte que considere oportunos para resolver incidencias relacionadas con el funcionamiento de los módulos instalados.

PostgreSQL

El adjudicatario deberá proporcionar los mecanismos de alta disponibilidad, que al menos serán activo-activo en modo lectura y activo-pasivo en escritura, así como los mecanismos de acceso a soporte que considere oportunos para resolver incidencias relacionadas con el funcionamiento de los módulos instalados.

Drupal

El adjudicatario deberá proporcionar los mecanismos de acceso a soporte que considere oportunos para resolver incidencias relacionadas con el funcionamiento de los módulos instalados.

HP Vertica:

La licencia actual, en modalidad Express para volumen de información no superior a 5 TB, proporciona soporte durante un año a partir de la fecha de su adjudicación, la cual a día de hoy se considera vigente hasta el 1 de julio de 2018. *La DGOJ se está planteando su migración a lo largo de este año 2017 o comienzos del 2018 a una solución basada en la versión Premium del producto.*

El soporte que incluye la licencia en proceso de adquisición por parte de la DGOJ incluye las siguientes características:

- Debe permitir el uso de la misma licencia para ilimitados sistemas de prueba y desarrollo y sin que el espacio ocupado en dichos entornos compute para el cálculo del espacio ocupado en el entorno productivo. El espacio máximo que se puede ocupar en los mencionados entornos de desarrollo y prueba deberá poder ser, como mínimo, la cantidad máxima licenciada para el entorno productivo (5 TB, en el caso actual)
- Cualquier incidencia del producto HPE Vertica será responsabilidad del fabricante. Asimismo el fabricante será el responsable de la creación de cualquier parche que solucione cualquier bug o que mejore cualquier proceso.
- Servicios comprendidos en el soporte actual:
    - **Software Support Online:** Acceso a SSO 24x7, incluyendo acceso a actualizaciones de producto, acceso a una extensa base de datos de conocimiento que incluye información sobre síntomas conocidos y soluciones propuestas, especificaciones y literatura técnica.
    - **Advanced self-solve:** después del primer registro de un caso, recibirá una respuesta sobre ello. Dispone de diversos parámetros de búsqueda que permiten que esta búsqueda sea flexible. Cada intento de búsqueda será almacenado en su histórico de casos para permitir una mejor detección de problemas.
    - **Access to technical resources:** Se puede acceder mediante SSO o por teléfono.
    - **Support delivery languages:** Soporte principalmente en inglés, aunque en algún caso pueden prestarse en muchos otros idiomas. Todo dependerá en todo caso de la disponibilidad de conocimiento y recursos.
    - **Escalation management:** procedimientos formales para facilitar la resolución de problemas de software complejos.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- **Software updates:** arreglo de bugs, patches y la generación de nuevas Major Versions and Minor Versions.
- **Patches**: en cuanto hay nuevas versiones disponibles, éstas se publican a SSO para facilidad de acceso.
- **Named callers:** un número ilimitado de usuarios pueden registrar casos a través de SSO o por teléfono.

Los tiempos de respuesta objetivo del servicio de soporte, que son los propios de la versión Enterprise Standard y aplicarían también a esta licencia Express, deberían ser los siguientes:

- Nivel 1 (caída del sistema productivo): de lunes a domingo, 24x7, los 365 días del año
- Niveles 2 (fallo de funcionalidad/característica importante), 3 (fallo de funcionalidad/característica menor) y 4 (problema menor, solicitud de documentación, información, solicitud de evolución, etc.): Soporte disponible 9x5 entre 8 a.m. y 5 p.m. en días laborables locales, excluyendo días festivos y fiestas locales. Los tiempos de respuesta para avisos realizados fuera de la ventana de cobertura aplicarán al siguiente día laborable.

El proveedor del servicio se responsabilizará de la actualización del software y su administración física y lógica (administración del clúster, configuración del software, gestión de usuarios, monitorización mediante módulos específicos del producto), haciendo uso del soporte que proporcionan las licencias adquiridas por la DGOJ durante el presente año 2017 y renovadas por él adjudicatario al vencimiento de estas en julio de 2018.

<u>Appliances de balanceo y seguridad</u>

El adjudicatario tendrá que renovar las siguientes licencias, cuya adquisición y gestión está llevando el actual proveedor del servicio, para que puedan dar soporte a partir del día de entrada en vigor del contrato hasta el fin del plazo de ejecución del mismo.

Concepto	Fin Soporte
Powerpath EMS	28/02/2018
IP Replicator	28/02/2018
Checkpoint	28/02/2018
Checkpoint Atocha	28/02/2018
Fortigate	28/02/2018
F5	28/02/2018
Alien Vault	28/02/2018

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

IMPERVA	28/02/2018

Plataformas Windows:

- La administración de los equipos con sistema operativo Windows, se realiza por personal de la DGOJ, por lo que no se considerará como un servicio a incluir en la oferta. Sí se deberá contemplar el soporte de las licencias necesarias para su ejecución, el back-up de dichos servidores y la instalación de los agentes necesarios para back-up, monitorización, etc.

Plataformas Linux:

- La administración y actualización del software de base detallado en el apartado "*Plataformas Linux*", con excepción de los dos últimos ítems (WBS Vision Agnitio y la arquitectura JEE con frameworks y estándares JFS/JPA/SOAP), será responsabilidad del proveedor del servicio.

4.2.10 Servicio de Respaldo y recuperación de la información

El documento ofertado por el adjudicatario con la política de respaldo de la información a aplicar para su aprobación por la DGOJ, deberá ser considerado como un documento vivo, susceptible de evolucionar durante la ejecución del contrato, y deberá contemplar como mínimo los siguientes aspectos:

- Relación de todos los elementos sobre los que haya que realizar copias de seguridad.
- Periodicidad y tipo de copia para cada uno de los elementos antes citados.
- Soportes a utilizar en cada caso.
- Lugares de almacenamiento de las copias y plazos de reciclado.
- Pruebas de verificación y condiciones para su realización.
- Procedimientos de actuación frente a incidentes.
- En los casos pertinentes, cifrado de las copias de seguridad.
- Procesos de salvaguarda de la información fuera del CPD origen del mismo utilizando el otro CPD.

Una vez estudiada la propuesta de política de respaldo de la información, en el momento del establecimiento del servicio, se redactará una estrategia de realización de copias de seguridad y de recuperación, y se desarrollará un procedimiento automático de acuerdo con dicha estrategia, para conseguir un funcionamiento seguro de las bases de datos y una garantía de recuperación pronta y completa ante fallos.

Como mínimo, la política de respaldo deberá incluir:

- Copia de seguridad incremental diaria de los servidores con retención de 1 semana
- Un back-up completo semanal con periodo de retención de 4 semana
- Un back-up completo mensual con periodo de retención de 4 meses, que se debe ejecutar la primera semana del mes
- En estos momentos, la copia de seguridad de los servidores virtuales y de los físicos que dan soporte a los servicios de base de datos (Oracle y Vertica) se realizan por agente, y la de los sistemas de ficheros compartidos por CIFS/NFS por protocolo NDMP. Se pueden admitir alternativas a estas técnicas si la DGOJ las estima adecuadas (backup de máquinas virtuales por snapshot, por ejemplo), tras analizar que se consiga la misma granularidad y nivel de retención, o superior, que con las tecnología que se aplican en este momento.
- Se deberán almacenar los logs de registros de actividad y control de acceso de elementos principales tales como balanceadores, cortafuegos, sondas, servidores web y de aplicaciones, Directorio Activo, etc. Si la DGOJ decide almacenarlos en alguna de sus unidades de servicio, para un mayor control y facilidad de explotación, el espacio asignado a estos registros no se computará a efecto del espacio solicitado y sus ampliaciones del 15% anual
- Implantación de las políticas de cumplimiento de normativas a las unidades de copia de seguridad (LOPD hasta grado 2, seguridad, control de acceso, etc)

La empresa adjudicataria tendrá la responsabilidad de aplicar la política de respaldo acordada y de comprobar el correcto funcionamiento del proceso en su conjunto.

Adicionalmente, podrán existir peticiones puntuales de copias de seguridad de elementos que requieran políticas de retención específicas.

El proveedor ofrecerá sistemas de back-up local al CPD para cada uno de los servidores alojados en él, así como para los servicios de ficheros alojados en la cabina principal (NFS/CIFS) La tecnología actual de respaldo es:

- Software: Veritas Netbackup
- Respaldo en plataformas basadas en disco

Aunque no es requisito, sí es valorable el que sea posible recuperar en el otro CPD un backup realizado en uno de ellos

Para la DGOJ es imprescindible la recuperación de cualquier transacción que haya tenido lugar por parte de un usuario en cualquiera de las bases de datos (Oracle, MySQL o PostgreSQL–para las instancias de Drupal y Alfresco-) que componen las diferentes plataformas. Por esta razón, los procedimientos y sistemas de back-up de las bases de datos deberán garantizar que, en caso de incidencia, se puedan recuperar todos los datos almacenados hasta el mismo momento de producirse la incidencia, mediante la activación del modo “archivelog” de las bases de datos u otro procedimiento similar.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

El software de base de datos HP Vertica cuenta con su propio sistema de generación de ficheros de back-up, los cuales entraran en el flujo ordinario de gestión de back-up del adjudicatario desde el momento en que son generados, con la política y periodicidad que se establezca finalmente.

En el caso de las máquinas virtuales se establecerán medidas para poder recuperar desde una máquina virtual completa hasta un fichero concreto de la misma, utilizando los mecanismos que el adjudicatario disponga.

Deberán establecerse los mecanismos necesarios para que las máquinas virtuales no replicadas del CPD 1 al CPD 2 (o viceversa) y aquellas en funcionamiento en modo activo-pasivo sean replicadas en el CPD 2 para su posible puesta en producción en caso de necesidad debido a imposibilidad de entrega de servicio en el CPD 1 (y viceversa, en el caso de máquinas virtuales no replicadas que dan servicio desde el CPD 2)

Se establecerán dos categorías, según el entorno del que se trate:

- Producción: se replicará la máquina minimizando las tareas de intervención en su recuperación, como máximo en un plazo de 2 días. Esto afecta a 12 máquinas:
    - 4 máquinas que comportan la infraestructura de la aplicación NAIPE
    - versionado, integración continua y control de calidad del código de los desarrollos
    - herramientas de gestión y monitorización de la base de datos Oracle
    - ejecución de procesos ETL de la plataforma de Big Data
    - laboratorio de manipulación de datos.
    - base de datos MySQL (master y slave, siendo replicada el master del CPD 1 al CPD 2 y el slave en sentido contrario)
    - base de datos PostgreSQL (master y slave, siendo replicada el master del CPD 1 al CPD 2 y el slave en sentido contrario)
    - LDAP/WBS Vision Agnitio (master y slave, siendo replicada el master del CPD 1 al CPD 2 y el slave en sentido contrario)

  Dada la complejidad para determinar las modificaciones que se realizan en estas máquinas (tanto de información de negocio como de sistema operativo, estas últimas menos usuales), se puede entender que una copia semanal de las mismas sería el mínimo necesario, no siendo necesario guardar copias anteriores a la última realizada.

- Pre-producción y desarrollo: se pueden recuperar en el otro CPD, implicando tareas de intervención y contando con un plazo de recuperación máximo de una semana máximo. Estas máquinas no sufren cambios de forma habitual, por lo que una copia mensual sería suficiente. En total se trata de 8 máquinas en el entorno de desarrollo y 15 del entorno de pre-producción.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Además, el adjudicatario deberá, una vez iniciada la ejecución del servicio redefinir las necesidades de monitorización de la actividad en colaboración con la Administración de Sistemas de la DGOJ, así como prever las necesidades de capacidad y escalabilidad del sistema en colaboración con el mismo área responsable. Adicionalmente, deberán realizarse copias periódicas de recuperación de datos planificadas con la DGOJ.

Las licencias incluidas en la oferta del software necesario para el necesario funcionamiento del servicio indicado de respaldo y recuperación de información correrán a cargo del adjudicatario.

En consonancia con el crecimiento esperado para el resto de servicios, el espacio ocupado por estas copias de seguridad puede ser incrementado hasta en un 15% anual sin coste para la DGOJ.

4.2.11 Servicio de Seguridad de las infraestructuras tecnológicas y de la información

Al objeto de dar unos servicios al ciudadano seguros, que protejan los datos personales, su intimidad, la integridad de la información, que eviten ataques, y que garanticen el cumplimiento de la normativa vigente en materia de seguridad TIC, el adjudicatario deberá cumplir una serie de requisitos en materia de seguridad en distintas áreas TIC relacionadas con los diferentes servicios pedidos en el presente pliego. Se exige que el adjudicatario ofrezca unos servicios de seguridad de carácter horizontal a todos los demás servicios exigidos en este pliego, y en particular que se articule en las áreas contempladas en el presente apartado.

El adjudicatario, su solución y todo el personal que intervenga en la prestación contractual, quedan obligados a aplicar las medidas necesarias para el cumplimiento de la normativa vigente de Protección de Datos de Carácter Personal.

Para ello el adjudicatario, como **Responsable del Tratamiento**, implantará las medidas de seguridad exigidas en dicha normativa, manteniendo las evidencias de su cumplimiento a disposición de la DGOJ, y prestando los servicios adjudicados con las condiciones necesarias de seguridad, física, lógica y de las comunicaciones.

El adjudicatario se compromete a tomar las medidas necesarias para dar cumplimiento a los requisitos derivados del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, así como asumir las responsabilidades y obligaciones establecidas en la política de seguridad del Ministerio de Consumo y los controles y salvaguardas de seguridad que se deriven de la categorización de los sistemas y servicios vinculados al objeto de la prestación contratada.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Para ello el adjudicatario, como **Responsable de Sistemas, y Administrador de Seguridad** en lo que exclusivamente se refiere a las infraestructuras, plataforma tecnológica y servicios de proceso de datos, como gestor técnico y propietario de las mismas para ofrecer los servicios solicitados en el presente pliego, implantará las medidas de seguridad exigidas en dichas Leyes y normas de desarrollo, manteniendo las evidencias de su cumplimiento a disposición de la DGOJ.

Serán requisitos mínimos todos los que se exponen en el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Para ello, se aplicarán todas las medidas de seguridad de nivel BÁSICO y MEDIO y algunas de nivel ALTO que se establecen en el Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema nacional de Seguridad en el ámbito de la administración electrónica. En la línea de la aplicación del mismo, la DGOJ cuenta con un Plan de Seguridad que deberá ser ejecutado y aplicado. Dicho Plan será un elemento vivo, susceptible de evolucionar durante la ejecución del contrato por parte de trabajos externos a este contrato. La documentación aportada podrá estructurarse siguiendo los apartados presentes en la guía CCN-STIC 808 de verificación del cumplimiento de las medidas de seguridad presentes en el ENS.

Adicionalmente, **los servicios proporcionados por el adjudicatario deberán cumplir al menos con el Tier III de la norma Telecommunications Infrastructure Standard for Data Centers (TIA-942).**

4.2.11.1 Administración de la Seguridad de los Sistemas

Este servicio asume la administración y operación de la infraestructura de seguridad de todos los componentes y servicios prestados a la DGOJ, y por lo tanto, el adjudicatario deberá.

a) Gestionar la política de seguridad de los dispositivos.
b) Gestionar las versiones de software de los dispositivos.
c) Aplicar parches.
d) Gestionar configuraciones.
e) Gestionar y optimizar las opciones de seguridad:
    - Para realizar la configuración segura de los sistemas operativos, debe realizarse siguiendo las guías del fabricante del software o guías de otras organizaciones expertas.
    - Desactivación de servicios innecesarios: el principio de mínimo privilegio establece que todo aquello que no sea estrictamente necesario debe ser desactivado, para reducir posibles puntos de fallo.
    - La configuración de seguridad de los sistemas operativos y de las aplicaciones debe realizarse siempre que éstas no interfieran el funcionamiento correcto de los mismos.
f) Uso de software de seguridad para el sistema:

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Se instalará software específico de seguridad, como **sistemas de detección de intrusiones** a nivel de equipo (HIDS, Host IntrusionDetectionSystem).
- Se instalarán **antivirus** en los servidores corporativos.

g) Entendimiento, control y optimización de las configuraciones de los equipos correspondientes a la infraestructura de seguridad gestionada desde el SOC, incluyendo el proceso de control de cambios en dichas configuraciones al objeto de mejorar el rendimiento de los equipos en materia de seguridad.

h) Gestión y atención a los requerimientos de la DGOJ, en cuanto a solicitud de cambios sobre la infraestructura de seguridad gestionada desde el SOC, informes y atención de incidente, así como consultas con relación al estado de la seguridad

Las licencias de los productos software de seguridad necesarios para la correcta prestación del servicio serán a cargo del adjudicatario, así como sus actualizaciones y mantenimiento, tanto en lo que se refiere a gestión, como a sistemas de actualización de parches, antivirus y sistemas de detección de intrusiones.

Del mismo modo correrá a cargo del adjudicatario cualesquiera plataformas y software de base, incluyendo Sistemas operativos que resultasen necesarios para la correcta operación de los servicios de seguridad exigidos.

El coste de la instalación, las licencias necesarias para la instalación, configuración y actualización de los servicios y de los equipos necesarios que forman parte de la solución técnica demandadas en este pliego por la DGOJ, serán a cargo del adjudicatario.

4.2.11.2 Servicio de correlación de eventos de seguridad

Para poder identificar situaciones que pongan en peligro la seguridad de los sistemas y servicios prestados a la DGOJ, y para poder establecer una trazabilidad en el control de acceso, conocer quién ha hecho qué, cuándo y con qué resultado, será necesario que los elementos que componen el Sistema de Seguridad Perimetral así como otros sistemas considerados de importancia vital, generen registros (logs) como mínimo de las operaciones que deseamos monitorizar y que puedan ser almacenados durante el tiempo que se considere oportuno para su posterior gestión y análisis por parte del Responsable de Seguridad de la DGOJ.

Por lo tanto, será responsabilidad del adjudicatario la de contar con un sistema de administración de información y eventos de seguridad centralizado (SIEM por sus siglas en ingles) que permita realizar la correlación de logs y/o análisis forense al objeto de analizar posibles errores y caídas de servicio de las aplicaciones y desarrollos de la DGOJ con finalidad de alertar sobre actividad sospechosa detectada en las zonas descritas en la arquitectura de seguridad, así como contar con un registro de las bitácoras de seguridad de los diferentes dispositivos monitorizados. Más concretamente, tal y como ya se ha comentado a lo largo del pliego y puede consultarse en los anexos, la DGOJ cuenta con el sistema OSSIM Alienvault (Open

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Source Security Information Manager), aunque a lo largo de la ejecución del servicio actual se han detectado carencias a nivel de capacidad, rendimiento y funcionalidad que aconsejan su sustitución, por lo que se tendrán en cuenta las propuestas de mejora en este sentido.

4.2.11.2.1 Funcionalidad requerida del servicio

Dentro de las funcionalidades mínimas del servicio se identifican:

a) Recopilación de todos los logs de los sistemas involucrados.
b) Para cada Sistema incluir los logs tanto de Aplicación, y del Servidor de Aplicación y/o Servidor Web, en su caso, así como del Sistema.
c) Respecto a la actividad del Sistema, se entiende que se recogerá información sobre el estado de los recursos del Sistema.
d) Se indicaran por parte de la DGOJ que indicadores de logs serán registrados
e) Establecer unos permisos de acceso a los logs con independencia de los permisos existentes en el sistema que los ha generado.
f) Evitar que puedan ser alterados o eliminados.
g) Poder realizar búsquedas en dichos logs.
h) Poder ver lo que ha ido ocurriendo como una secuencia de registros.
i) Generar alarmas cuando se identifiquen sucesos fuera de lo común o no autorizados gracias a la correlación de eventos (observando lo que ocurre en varios sistemas como un todo y no con la visión parcial que cada sistema tiene).

Tal y como ya se ha mencionado, se identifican como sistemas objeto de este servicio:

- Los sistemas de protección del perímetro como son;
  - Balanceador de Carga
  - Cortafuegos de entrada a la DMZ de la DGOJ
  - Directorio Activo
- Así como todos los servidores considerados de importancia vital asociados a las Plataformas para Aplicaciones Web que la DGOJ utiliza en el ejercicio de sus competencias, ya sean estas plataformas externas o internas, las cuales aportan los servicios que presta la DGOJ de cara a los ciudadanos, así como las aplicaciones corporativas y de inspección del mercado del juego online.

4.2.11.2.2 Requisitos para la Gestión Centralizada de los registros de eventos de seguridad (logs)

A continuación, se describe los requerimientos funcionales y no funcionales para la gestión centralizada de los eventos de seguridad.

Requerimientos funcionales:

- Los registros de eventos (logs) deberán consolidarse en un punto central, para su conservación durante el período que indique la DGOJ sin menoscabo que los

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

diferentes sistemas de origen de los logs, mantengan estos durante el tiempo limitado que considere el adjudicatario. Actualmente la DGOJ cuenta con un sistema centralizado que sólo está dimensionado para trabajar stand-alone, por lo que existe una única instancia en el CPD primario y recolecta los logs de todos los sistemas operativos, balanceadores, cortafuegos, e ips para su posterior correlación y tratamiento. El sistema existente, y que el adjudicatario deberá gestionar, administrar y mantener es OSSIM *Alienvault*

- Será necesario garantizar que los registros de logs, para su correlación, deban tener por lo menos; la identificación del sistema que lo generó, marca de tiempo y detalles del evento para su trazabilidad.
- Debe existir un proceso de reducción de datos para el proceso de correlación eficiente.
- Las marcas de tiempo de los registros de eventos deben estar sincronizadas e incluir por lo menos la fecha y hora en la que se generó.
- Los registros de eventos {logs) deben tener algún mecanismo de identificación del sistema o tecnología de información que los generó para efectos de su utilización como evidencia digital.

Requerimientos no funcionales:

- Se debe utilizar un método de transporte confidencial.
- Se debe utilizar algún mecanismo de autenticación con respecto al sistema que los generó.
- Se debe asegurar que no se perdió, ni cambió ningún dato en los registros de eventos para su uso como evidencia digital.
- Se debe verificar que el sistema esté en un correcto estado de funcionamiento en el momento en que se generan o modifican los registros.
- Los registros de eventos de seguridad, deben poder ser consultados en el futuro y en el presente.

4.2.11.3 Monitorización de la Seguridad

4.2.11.3.1 Monitorización de eventos de seguridad

Este servicio supervisará el estado de los activos de la DGOJ y generará las alertas correspondientes en caso de eventos que puedan afectar a la seguridad de la información. Sus principales funciones serán.

a) Detección y recolección de evidencias de las incidencias maliciosas o no que ocurran en la infraestructura de la DGOJ y que puedan poner el peligro la seguridad de la información.
b) Discernir entre falsos positivos o negativos analizando las diferentes alertas detectadas.
c) Recolectar los eventos de seguridad de diferentes fuentes de información mediante sondas locales.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

d) Procesar y correlar los eventos recolectados en tiempo real para detectar sucesos relevantes en la infraestructura gestionada que puedan ser indicativas de un ataque y emitir las alertas oportunas.
e) Integrar fuentes de información procedentes de múltiples dispositivos y fabricantes.
f) Adaptar las sondas de recolección a nuevas fuentes de información no previstas inicialmente, tanto en el método de recolección como en el formato mismo de la información.
g) Integrar esta información en el esquema de monitorización de la información procedente de la plataforma de monitorización actualmente operativa en la DGOJ o en sistemas similares.
h) Almacenar y resguardar los eventos recolectados durante un amplio rango de tiempo para, en caso de necesidad, realizar un análisis forense y obtener datos relativos al origen, destino y traza de los incidentes de seguridad.
i) Utilizar canales de comunicación seguros con cifrado de datos y verificación de origen y destino.
j) Disponer de canales de comunicación alternativos a la conexión a Internet de la DGOJ (fuera de banda) y de mecanismos de conmutación automática de uno a otro en caso de indisponibilidad del acceso principal. Disponibilidad del servicio en 24x7.

4.2.11.3.2 Sistemas IPS

Al igual que los cortafuegos y balanceadores, se dispone de una pareja de IPS en modo activo-pasivo, cada uno de ellos en un CPD. La funcionalidad deseada para estos equipos es la siguiente:

- Web Application Firewall - WAF
    - Seguridad en las aplicaciones
    - Servicio de reputación de IPs maliciosas, redes TOR, redes de phishing, botnets y proxies anónimos actualizado cada hora, conteniendo además actualizaciones de geolocalización
    - Algoritmo de aprendizaje web que:
        - Aprenda por URL
        - Aprenda de todos los orígenes
        - Aprender elementos HTML y XML, además de SQL gracias a la integración con las funcionalidades de base de datos
        - Aprender de entornos de preproducción mediante un dispositivo y que dicho aprendizaje se aplique en producción, pese a ser otro dispositivo distinto
    - Capaz de capturar usuarios web autenticados por certificado, formulario web, kerberos y NTLM
    - Políticas de seguridad multi-capa completamente customizables y sencillas, incluyendo criterios de firmas, aprendizaje, por país y por hora entre otras
    - Protección contra web scrapping, bruteforcing y fraude digital
    - Actualización de firmas de ataque con un máximo de 20 días

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Tiempo de recuperación 2 horas

- Firewall de base de datos – DBM
  - Seguridad en el acceso y transferencia de datos a y desde las bases de datos
  - No es necesaria la alta disponibilidad siempre que el fallo del equipo no impida proporcionar servicio
  - Aprendizaje de peticiones SQL por usuario o grupos de usuario
  - Capaz de bloquear ataques SQL como descubrimiento de SSID, modificaciones de protocolo y otros comportamientos anómalos
  - Capacidad de guardar la información de forma segura, no dejando datos sensibles en los servidores de base de datos
  - Monitorización del trafico SQL desde los dispositivos hardware colocados en red, siendo la instalación de agentes en las bases de datos totalmente secundario y únicamente para monitorización de trafico local
  - Monitorización y securización siempre en tiempo real
  - No debe necesitarse activar ninguna traza ni auditoría interna de la propia base de datos
  - Despliegue en modo sniffer o modo bridge
  - Debe ser posible analizar el tráfico SQL incluso si se encriptan las comunicaciones entre los servidores de aplicación y los equipos de usuarios y la base de datos
  - Tiempo de recuperación 2 horas
- Cortafuegos de Sistemas de ficheros
  - Monitorización del tráfico en red, no debe ser necesario la instalación de ningún agente en los servidores de recursos compartidos
  - Monitorización en tiempo real
  - Capacidad de descubrimiento de datos sensibles mediante nombre, extensión y path
  - Políticas de seguridad con opción de alertar y/o bloquear, con capacidad de bloquear ataques contra los ficheros sensibles
  - Despliegue en modo sniffer o modo bridge

El control, operación, administración, monitorización, mantenimiento y actualización de los sistemas IPS correrá a cuenta del adjudicatario, para lo que deberá contar con el soporte oficial correspondiente.

4.2.11.3.3 Incorporación de herramientas de monitorización de terceros

La DGOJ tiene firmado un acuerdo con el CCN-CERT por el que está suscrito al Sistema de Alerta Temprana para la detección rápida de incidentes y anomalías dentro del ámbito de la administración, que permite realizar acciones preventivas, correctivas y de contención.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

La DGOJ monitoriza la información de seguridad relevante del tráfico entrante en sus sistemas a través de Internet por medio de una Sonda para recoger estos eventos. El adjudicatario deberá por tanto conectar el sistema de monitorización de la DGOJ (la sonda del CCN_CERT) en el punto más apropiado de la red al objeto de analizar el tráfico hacia los sistemas de la DGOJ con el fin de enviar los eventos de seguridad a un sistema central ubicado en el CCN-CERT que realiza una correlación entre los distintos eventos y dominios.

Las características técnicas de este servicio requieren del despliegue de la sonda que deberá ser realizado del siguiente modo:

i. Se estudiará junto al adjudicatario la arquitectura de red existente, y se elegirá la mejor forma de integración para que cauce el menor impacto.
ii. La conexión entre la sonda y el sistema central se realizará siempre de forma segura, a través de distintas opciones disponibles (VPN, SSL, etc). Estas conexiones podrán realizarse de forma directa (a través de una salida dedicada hacia Internet, ej. ADSL) o indirecta (a través de los corta fuegos del contratista).
iii. La sonda será gestionada totalmente por el personal de la DGOJ CCN-CERT.
iv. La sonda vigilará el tráfico de salida a Internet, no entrando en el tráfico interno del contratista.

Se requerirá por parte del contratista que habilite en sus instalaciones un espacio para el equipo que hará la función de sonda con las siguientes características:

a) Un espacio para enracar un equipo de 1 U.
b) Varias tomas de red Ethernet 1GH (mínimo 4).
c) Dos conexiones a red eléctrica para las fuentes redundantes.
d) Replicación del tráfico entrante al CPD1 en el equipo.

4.2.11.4 Gestión de la Seguridad

Como regla general se cumplirá con lo establecido en el Esquema Nacional de Seguridad, según el RD 3/2010 de 8 de enero, siendo de cumplimiento imprescindible su aplicación a los activos de información relacionados con la Sede Electrónica de la DGOJ, así como aquellos derivados de la información aportada por los operadores de juego online en cumplimiento de la normativa vigente.

La DGOJ proporcionará al adjudicatario una relación de los activos de información incluidos en las prestaciones del servicio.

La DGOJ determinará la criticidad de los activos de información Objeto de ser soportados por los servicios y activos contemplados en este contrato, asignando los niveles de seguridad que, según establece el RD 3/2010, obligan a disponer de las medidas de seguridad correspondientes, las cuales el adjudicatario deberá implementar en sus instalaciones y de las cuales dispondrá de las evidencias necesarias para una auditoría o control rutinario.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

4.2.11.4.1 Gestión de incidencias

Un aspecto particularmente importante de la Gestión de la Seguridad es el la respuesta del adjudicatario frente a los diferentes incidentes de seguridad que puedan producirse sobre los sistemas de información objeto del contrato, para lo que se dispondrá de un proceso integral para hacer frente a los mismos, incluyendo:

a) Clasificar y priorizar las diferentes alertas generadas por el proceso de Monitorización.
b) Contener o neutralizar los ataques detectados de acuerdo con los procedimientos establecidos por la DGOJ
c) Procedimiento de reporte de incidentes, detallando el escalado de la notificación, utilizando canales seguros de comunicación para el intercambio de información de forma que garanticen la confidencialidad, integridad y origen legítimo de las notificaciones.
d) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
e) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
f) Procedimientos para informar a las partes interesadas, internas y externas.
g) De forma general establecer procedimientos para:
   - Prevenir para que no se repita el incidente.
   - Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
   - Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidencias.

4.2.11.4.2 Oficina Técnica de Seguridad

Como parte de los servicios de seguridad se requiere la monitorización de los elementos que conforman la solución integral de seguridad implantada, con el fin de verificar el estado de cada uno de los elementos que lo soportan y tomar las acciones necesarias en caso de presentarse uno o más eventos que supongan una amenaza.

El servicio debe ser prestado desde un Centro de Operaciones dedicado a la Seguridad Informática (SOC), el cual debe estar dentro del territorio nacional formada por personal del equipo de seguridad del adjudicatario. El objetivo de este Centro será el de supervisar, gestionar y monitorizar de forma remota los servicios y configuraciones de seguridad, con el fin de proteger los servicios de información residentes en los servidores y appliance de uso específico.

Los servicios a realizar por parte de esta oficina de seguridad, o SOC, serán al menos los siguientes:

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

a) Mantener una visualización en línea desde un punto remoto de todos los equipos de seguridad lógica necesaria para prestar los servicios, observando sus funciones principales, rendimiento, bitácoras, alarmas, eventos e informes para conservar su mejor funcionamiento y rendimiento en un esquema 7x24.
b) Coordinación y respuesta ante incidentes de seguridad. Notificación, seguimiento y respuesta ante incidentes de seguridad que le hayan sido notificados o que hayan sido detectados por sus propios dispositivos de seguridad, dentro del ámbito de los servicios prestados a la DGOJ.
c) Tener la proactividad necesaria para evitar ataques e incidentes de seguridad, detectar dichos ataques y coordinar con e la DGOJ las actividades de contención correspondientes.
d) Establecer procesos y procedimientos para mantener los niveles de servicio que la DGOJ requiere, y que se concretan en los Acuerdos de Nivel de Servicio que se detallarán más adelante.
e) Análisis de intrusión anual desde Internet a los servicios publicados por la DGOJ (Pentesting Manual).
f) Herramienta de pentesting persistente y automático para los servicios que determine la DGOJ entre los publicados.
g) Ataque anual simulado de phishing contra los usuarios de la DGOJ.
h) Chequeos periódicos de los sistemas internos.
i) Detección de comportamientos anómalos en base al tráfico desplegado en la red mediante chequeos periódicos externos al objeto de detectar las vulnerabilidades presentes en los procesos de autentificación o autorización, así como la falta de cifrado en el transporte de la información.
j) Gestión y evolución del Sistema de Gestión de Seguridad de la Información (SGSI).
k) Seguimiento del cumplimiento en materia de la LOPD.
l) Asesoramiento y elaboración de informes.
m) Revisión del análisis de insuficiencias de los sistemas (Cumplimiento del E.N.S. y del R.D. 1720/2007)
n) Revisión de la declaración de aplicabilidad.
o) Revisión del plan de mejora de la seguridad inicial.
p) Revisión del grado de implantación del plan de mejora de la seguridad aprobado, en su caso.
q) Revisión de métricas e indicadores inicialmente definidos.
r) Jornada de formación de "refresco" y concienciación a los roles y personas involucradas.

La Oficina de Seguridad realizará labores de asesoramiento sobre cualquier tema relacionado con seguridad que se le pueda plantear, así como de elaboración de informes.

Además, el adjudicatario del presente concurso quedará obligado, por motivos de seguridad con la DGOJ, al cumplimiento de las siguientes acciones o permisos:

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

a) A informar con diligencia a la DGOJ de cualquier incidencia en la solución (o en el personal que forma parte de la misma) y que pueda suponer un riesgo para la seguridad los servicios o para los objetivos del mismo.
b) A la elaboración de un informe detallado por motivo de una incidencia que pueda afectar la seguridad o los objetivos los servicios siempre que la DGOJ se lo solicite.
c) A permitir y facilitar que la DGOJ realice controles (auditorías o inspecciones) durante el período de vigencia de la adjudicación.
d) A permitir y facilitar que la DGOJ instale en los equipos de los servicios aplicativos que permitan verificar los acuerdos de nivel de servicio.
e) A proporcionar a la DGOJ la información o documentación que se le solicite y sea relativa a la adjudicación y durante el período de vigencia de la misma.
f) A cumplir los requisitos de la DGOJ para la entrega segura de los datos al finalizar el proyecto.
g) A la finalización del contrato se devolverá a la DGOJ toda la información utilizada y la que se genere durante el proceso, eliminándose toda la que hubiera en poder del adjudicatario.

El coste de la instalación, las licencias necesarias para la instalación, configuración y actualización de los servicios y de los equipos necesarios que forman parte de la solución técnica demandadas en este pliego por la DGOJ, serán a cargo del licitador.

4.2.11.4.2.1 Marco metodológico del SOC

El SOC deberá contar con las siguientes capacidades para la correcta operación del servicio:

- Debe operar con una metodología propia, que deberá estar alineada y armonizada con marcos de referencia y estándares como ITIL, ISO 27001, CERT de Carnegie Mellon, prácticas del SANS Institute, entre otras. Dicho marco debe estar debidamente documentado y deberá acreditarse mediante la aportación de modelos de los procedimientos, guías y plantillas que constituirán posteriormente los elementos fundamentales para la prestación del servicio con los niveles de calidad requeridos.
- Dicha metodología debe estar probada en proyectos reales, de ámbito nacional o internacional, del Centro de Operaciones de Seguridad
- Se deberá disponer de informes de seguimiento del servicio emitidos con periodicidad mensual.
- Debe estar dotado de una estructura funcional con al menos las siguientes áreas:
  - Operaciones
  - Soporte
  - Procesos
  - SLAs
  - Calidad
  - Tiger Team

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Se deberá disponer de Indicadores y Métricas de evaluación concretas para cada uno de los procesos del SOC, así como Acuerdos de Nivel de Servicio (ANS) específicos y consensuados, que permitan realizar la evaluación permanente de la calidad del servicio prestado, así como el establecimiento de procesos de mejora continua.

4.2.11.4.2.2 Infraestructura Tecnológica

El SOC deberá contar con las siguientes capacidades para la correcta operación del servicio:

- Un sistema de Service Desk que sea compatible con ITIL. Dicha compatibilidad deberá ser demostrada y validada en al menos 10 procesos por alguna organización externa que sea referencia para validación ITIL
- Un módulo de manejo de incidentes de seguridad integrado con el sistema de Service Desk.
- Un módulo de CMDB (Configuration Management Data Base) integrado con el sistema de Service Desk.
- Un módulo de evaluación de la calidad en el servicio a clientes integrado con el sistema de Service Desk.
- Un módulo para la monitorización y cálculo de los Niveles de Servicio.
- Un portal para alta, baja y cambios en tickets levantados por el cliente que tenga la capacidad de ser accedido vía Web.
- Un portal de informes en el cual se puedan consultar todos los informes referentes a la operación de sus clientes, el cual debe ser accesible vía Web.
- Existencia de controles de acceso físico al SOC (biométricos, CCTV con capacidad de grabación, etc).
- Un área especial para realizar sesiones de análisis de problemas de incidentes de seguridad, sin afectar a la operación del SOC. Esta área debe contar con pantallas de tamaño adecuado que permitan monitorizar cualquier consola del SOC por un equipo de trabajo para la resolución de dichos incidentes de seguridad.

4.2.11.4.3 Entregables de seguridad después de la adjudicación

Durante los tres primeros meses de prestación del servicio, el adjudicatario estará obligado a acordar con el DGOJ un calendario para la entrega de la siguiente documentación de seguridad:

- La documentación y desarrollo de procedimientos debidamente probados y estandarizados para la realización de las tareas de la gestión de configuración, actualización y mantenimiento.
- La documentación adecuada de todos y cada uno de los cambios que se llevan a cabo para la gestión de configuración, actualización y mantenimiento.
- Plan de Recuperación ante incidentes.
- Política de Copias de Seguridad y Restauración.
- Evidencias del borrado de configuración obsoletas.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Documentación del licitador relativa a su Organización de la seguridad : El adjudicatario deberá entregar el documento de la "Política de seguridad" institucional, la organización de la seguridad implantada en sus instalaciones, detallando las medidas de seguridad y el equipo responsable de la seguridad de los sistemas de información de la DGOJ objeto de esta licitación, con la definición detallada de las funciones, deberes y responsabilidades de los diferentes roles los servicios con sus asignaciones y Plan de formación de los integrantes de dicho equipo.
- Informe del Análisis de Riesgos en formato a definir por la DGOJ. En este documento se deberán contemplar los aspectos siguientes:
    - Identificación de los activos del sistema.
    - Identificación las amenazas más probables
    - Identificación las salvaguardas que protegen dichas amenazas.
    - Identificación los riesgos residuales.
    - Como parte del Análisis de Riesgos se deberá disponer de un diagrama de las dependencias entre activos, de forma particular de los que se encuentran incluidos en la Sede Electrónica de la DGOJ, en aplicaciones corporativas relacionadas con tramitación electrónica de procedimientos, y aquellos relacionados con la función de investigación e inspección realizada por la DGOJ. Dicho diagrama estará a disposición de la DGOJ para su análisis.
- Procedimientos de seguridad.
- Registro y resolución de todas las incidencias de seguridad sobre los sistemas de información de la DGOJ.
- Registros de "logs" de los incidentes de seguridad que permita su trazabilidad.
- Informe de todas las incidencias de seguridad y su resolución, ocurridas a lo largo del proyecto.
- Mecanismos de gestión y protección de registros de actividad e información para auditorías (trazabilidad) y monitorización.
- Informes de las auditorías que serán realizadas por entidades acreditadas, externas al adjudicatario. El adjudicatario propondrá varias entidades auditoras y la DGOJ seleccionará la entidad que considere más idónea. Los gastos de esta auditoría estarán incluidos en el precio de licitación.
- Normativa de seguridad en cuanto al uso correcto e indebido de equipos, servicios e instalaciones.
- Registro de la gestión de equipamiento, soportes, etc.
- Entregar una planificación de hitos, relativos a la seguridad, en todas las fases del ciclo de vida de la solución dada. Este entregable tiene que incluir, entre otros: hitos de diseño; pruebas de seguridad; posibles auditorías de seguridad, de cumplimiento de estándares de seguridad, tests de penetración, análisis de vulnerabilidades, hacking ético.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Informe de resultados de los planes de pruebas de seguridad.
- Informe de resultados de los planes de pruebas de integración.
- Información sobre los mecanismos de auditoría (pistas de auditoría).

La DGOJ podrá solicitar al adjudicatario más documentación relacionada con los requisitos de seguridad exigidos en los pliegos de licitación.

4.2.12 Servicio de Continuidad del Negocio

El objeto mínimo del presente servicio consiste en el diseño, e implantación de una solución que garantice la continuidad de los servicios prestados por la DGOJ en producción en caso de alguna contingencia que afecte a la disponibilidad de los mismos en el centro de procesamiento de datos principal (CPD1). Actualmente, se está llevando a cabo un proyecto de revisión y adecuación del Sistema de Gestión de Continuidad de Negocio (SGCN) cuya finalización se estima a mediados de marzo de 2022 y que conlleva la pertinente elaboración del plan de continuidad de negocio (PCN), y su respectiva implantación junto con los procedimientos asociados.

En relación a los trabajos de mantenimiento del Sistema de Gestión, el adjudicatario llevará a cabo las siguientes actuaciones:

- Revisión de los procesos y servicios de DGOJ, en cuanto a funciones, activos dependientes e interdependencias entre activos.
- Revisión de AR y BIA.
- Revisión de las estrategias de continuidad de negocio y escenarios de contingencia.
- Revisión de Plan de gestión de Crisis (respuesta, comunicación, respuesta legal, emergencia y procedimientos de recuperación y vuelta a la normalidad).
- Soporte a pruebas.
- Formación de refresco a los roles involucrados.

Como ya se ha indicado a lo largo del presente pliego, la DGOJ presenta actualmente un modelo de continuidad del negocio fundamentado en sincronización de información y servicios hacia un Centro de Respaldo (CPD2), que dispondrá de todos los elementos de comunicaciones e infraestructuras hardware y software básicos y auxiliares necesarios para la prestación de los servicios objeto de continuidad de negocio.

La solución de respaldo que propuesta por el adjudicatario deberá observar los siguientes requisitos a nivel de recuperación operativa de los servicios en caso de desastre en un centro diferente del utilizado en la explotación:

- El adjudicatario dispondrá de un Centro de Respaldo ubicado a una distancia suficiente del Centro de Proceso de Datos de Producción según las mejores prácticas, de manera que se minimicen los riesgos de desastres que puedan afectar a ambos centros.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Al mismo tiempo la distancia entre ambos centros también ha de cumplir con las limitaciones operacionales Data Center TO Data Center (DC2DC) de replicación síncrona de datos entre Centros de Proceso de Datos.
- **La DGOJ considera el requisito en distancia máxima a cumplir en 160 kilómetros y en 15 kilómetros la distancia mínima entre los centros de proceso de datos del adjudicatario (CPDs) para los rendimientos deseados y la replicación síncrona DC2DC**.

El Centro de Respaldo dispondrá, para dar servicio en situaciones de desastre en el plazo de tiempo definido, de la siguiente infraestructura:

- Servidores necesarios para alojar las aplicaciones que se definan en el Plan de Contingencia.
- Las capacidades de almacenamiento en disco y de salvaguarda de datos compatibles con los sistemas del Centro de Proceso de Datos de Producción.
- Las líneas de comunicaciones entre el Centro de Proceso de Datos de Producción, el Centro de Respaldo y las instalaciones de la DGOJ.

Así como las necesarias infraestructuras para los servicios auxiliares adicionales necesarios para el correcto funcionamiento de todos los servicios objeto de Continuidad de Negocio.

En cuanto a los Sistemas de Almacenamiento, objeto también de Continuidad de Negocio, proporcionarán el Almacenamiento necesario para todos los datos de Producción.

El adjudicatario llevará a cabo las tareas de gestión de los sistemas correspondientes a la infraestructura existente en el Centro de Respaldo y garantizará la infraestructura mínima necesaria para dar soporte a la operativa diaria del centro de proceso de datos principal tal y como se ha puesto de manifiesto a lo largo del presente pliego.

El adjudicatario deberá ejecutar pruebas anuales de continuidad de negocio de acuerdo con el detalle especificado en el alcance de este servicio. A este respecto, el adjudicatario deberá realizar una prueba total y tres parciales de los servicios principales tales como Firewall, balanceadores, Gestor Documental, Servicio de Virtualización, Almacenamiento, etc. Dentro de las pruebas de contingencia se incluirá la recuperación de información contenida en los back-ups realizados.

Así mismo, el adjudicatario deberá asegurarse de que todas las personas involucradas en la prestación del servicio estén preparadas y tengan total conocimiento de las implicaciones que conlleva dicho servicio. A este respecto, el adjudicatario deberá tener actualizado como mínimo:

- Los procedimientos de actuación incluidos en el Plan de Continuidad de Negocio cuando este esté elaborado.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- El Plan de Recuperación ante Desastres en caso de que surjan necesidades de cambio debido al resultado de las pruebas de continuidad.
- La infraestructura hardware y software del Centro de Respaldo de manera que el plan este vigente en todo momento.
- La información de cada elemento del servicio: ubicación o estado actual, posibles incidencias a las que esté expuesto, elementos relacionados a los que pueda repercutir la incidencia, descripción de actividades a realizar para maximizar la seguridad.
- La organización de contingencia, así como las responsabilidades y funciones de cada una de las unidades y equipos que la componen.

La metodología para cada una de estas actividades tendrá que estar siempre alineada con las mejores prácticas de los estándares internacionalmente reconocidos.

4.2.13 Servicio de Monitorización de los Servicios

El adjudicatario deberá proveer de una plataforma de monitorización adecuada para la recolección de los diferentes eventos de todos los elementos que conforman los sistemas de información de la DGOJ, teniendo en cuenta los diferentes entornos, aplicaciones y sistemas operativos.

Como mínimo se deberá ofrecer el servicio de monitorización de todos los elementos, atributos y parámetros que están siendo monitorizados actualmente (consultar ANEXO III: PLATAFORMA DE MONITORIZACIÓN ACTUAL) a la periodicidad que se está llevando a cabo, facilitar la visualización gráfica de la información de monitorización, así como la realización de acciones en base a valores críticos de los elementos objeto de la monitorización.

El adjudicatario propondrá su propia herramienta de gestión de alarmas en la que, adicionalmente a las funcionalidades requeridas, se permitirá el envío de correos o alertas móviles a las direcciones de correo o terminales móviles propias de la DGOJ.

La empresa adjudicataria del contrato proporcionará una solución, ya sea una consola en las instalaciones de la DGOJ o un acceso remoto on-line, para que la DGOJ tenga acceso a los datos que se estén monitorizando en tiempo real, y a datos históricos que permitan evaluar la evolución de los diferentes parámetros de los servidores que integran las plataformas descritas en este pliego. La empresa adjudicataria formará al personal que designe la DGOJ en la herramienta que se utilice para este fin.

Deberá proporcionarse alta disponibilidad en todos los elementos de monitorización, indicando el adjudicatario elementos hardware y software que utilizará, así como el sistema y las políticas que se establecerán para el enriquecimiento a lo largo de la prestación del servicio de las políticas inicialmente establecidas.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Se entiende que en caso de que los servicios pasen a operar en respaldo, existirá un servicio de monitorización bajo la nueva situación de explotación de los servicios, por lo que la monitorización es objeto de inclusión en los planes destinados a garantizar la Continuidad del Negocio del Servicio, cumpliendo lo dispuesto en el apartado de Continuidad del Negocio.

La monitorización de la disponibilidad de los servicios y aplicaciones se realizará tanto desde la red interna de la DGOJ y del adjudicatario, como desde un punto externo a la misma, a través de Internet, para replicar el acceso de los usuarios a los sistemas de información de la DGOJ.

El licitador debe proporcionar el almacenamiento suficiente para almacenar los registros de los eventos de monitorización y seguridad (SIEM), tanto los existentes en este momento en los sistemas del adjudicatario actual, que en este momento se pueden estimar en 2 TB, como los que se vayan generando a lo largo del contrato, **sin que este espacio compute dentro de los distintos grupos de almacenamiento solicitados en el apartado de "*Servicio de Almacenamiento Administrado*".**

Además de tener la capacidad suficiente para poder soportar todos los servicios con la carga actual descrita, se deberá hacer una provisión adicional para el crecimiento en el período de vigencia del contrato y sus posibles prórrogas.

4.2.14 Servicio de Gestión y Seguimiento de los Servicios

4.2.14.1 Modelo de Gobierno para la gestión del servicio

El Modelo de Gobierno y Relación propuesto por el adjudicatario para la prestación y gestión de los Servicios exigidos en el pliego, deberá tener en cuenta los siguientes aspectos.

El modelo de Gobierno y Relación deberá definir los distintos actores del Adjudicatario, de la DGOJ y otros proveedores de servicios, que intervienen en la prestación y gestión de los Servicios.

Dichos actores formarán parte de un Órgano de Gobierno para la Gestión de Proyecto que cubra todos los aspectos de este Contrato.

La Administración aportará varios actores:

- El Responsable de Infraestructuras y Sistemas que hará de Coordinador Técnico. Si este lo considera necesario:
- Responsable del Servicio de Comunicaciones.
- Responsable del Servicio de Directorio Activo.
- Responsable de Seguridad, como interlocutor con la Unidad de Seguridad TIC del Departamento, por la especial importancia de este Servicio de Seguridad exigido en el pliego.
- Las Áreas de Desarrollo.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

El Adjudicatario también aportará varios actores, y dispondrá de los adecuados profesionales, arquitectos de sistemas, administradores y técnicos de sistemas, técnicos de seguridad, administradores de bases de datos, técnicos de comunicaciones, etc... Como mínimo aportará para el gobierno del servicio:

- Responsable del Servicio.
- Personal técnico del adjudicatario que realice tanto las tareas generales de administración y gestión definidas en este pliego como las tareas específicas asociadas a cada servicio detalladas en cada apartado de Condiciones Técnicas particulares de este pliego.

El Responsable del Servicio será representante permanente del adjudicatario ante el equipo de Gestión del Servicio la DGOJ, para lo cual deberá tener la dedicación adecuada.

Este representante actuará junto con el Coordinador Técnico la DGOJ, y se coordinará en un Órgano de Gestión del Proyecto con el resto de responsables operativos y proveedores de servicios, con el objetivo de proporcionar respuestas tempranas a cualquier tipo de incidencia para la que se requiera la toma de acciones correctivas o preventivas en el ámbito de servicios dentro del marco de este contrato.

Para la correcta prestación de los servicios exigidos en el pliego y el correcto desempeño de las tareas asociadas a cada uno de ellos, se exige la participación, sin coste adicional, de cualesquiera otros miembros del personal del adjudicatario cuando sea necesaria su asistencia a la hora de cumplir tanto con las Tareas generales de administración y gestión del apartado de Condiciones Técnicas generales, como con las Tareas específicas asociadas de cada apartado de Condiciones Técnicas Particulares de cada Servicio de este pliego.

Adicionalmente, para la realización de dichas tareas, y con el objeto de resolver peticiones, incidencias y cambios, puede ser necesario involucrar a terceras partes, como proveedores de servicios de mantenimiento, soporte de los fabricantes de los equipos utilizados por el adjudicatario, etc, por lo que el Modelo incluirá a dichos actores.

El modelo de Gobierno deberá regir las relaciones entre todos los actores mencionados.

Será objetivo del Órgano de Gestión del Proyecto proporcionar respuestas tempranas a cualquier tipo de incidencia para la que se requiera la toma de acciones correctivas o preventivas en el ámbito de servicios dentro del marco de este contrato.

El Modelo de Gobierno contemplará las actuaciones, participantes y relaciones entre ellos teniendo en cuenta el modelo de referencia ITIL y los procesos detallados en el siguiente apartado.

El Modelo de Gobierno y Relación incluirá los flujos de actuaciones de todos los procesos ITIL detallados (P.ej. Gestión de las Incidencias) de forma personalizada para la DGOJ teniendo en cuenta los diferentes Servicios definidos en este pliego y el detalle de tareas a realizar, Peticiones, Incidencias, Cambios y Configuraciones, detallados tanto en el apartado

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

de Condiciones Técnicas Generales del Servicio, como en cada apartado de Condiciones Técnicas Particulares de cada Servicio de este pliego.

El personal del adjudicatario asignado a la prestación del servicio deberá ubicarse en un centro de operaciones del adjudicatario, salvo que para el correcto desarrollo del servicio existan razones, como por ejemplo incidencias, que justifiquen suficientemente realizar la actividad en las dependencias de la DGOJ.

El adjudicatario deberá comunicar a la DGOJ la ubicación de dicho centro de operaciones en el que se desarrollarán las actividades contratadas.

4.2.14.2 Servicio de gestión de incidencias y peticiones

El adjudicatario deberá proporcionar a la DGOJ una herramienta de gestión de incidencias y peticiones que permita a ésta la verificación del cumplimiento de los Acuerdos de Nivel de Servicio establecidos en el contrato sobre la resolución de incidencias y peticiones.

La herramienta deberá permitir tanto la realización de peticiones de servicio y su seguimiento, como el seguimiento de las incidencias producidas en las plataformas objeto del servicio, a fin de verificar su resolución en tiempo y forma, y monitorizar su tiempo de resolución efectivo.

Además, deberá hacer posible el tratamiento de cada una de las plataformas consideradas de manera independiente, estableciendo canales de interacción y reporte vía correo electrónico y SMS con usuarios y grupos de usuarios personalizados para cada una de ellas. Dicha personalización contemplará tanto el control de qué usuarios pueden realizar peticiones referentes a una plataforma en concreto, como el de aquellos usuarios susceptibles de recibir información acerca de las intervenciones realizadas en cada una de las plataformas consideradas.

4.2.14.3 Plataforma de estadísticas e informes

El adjudicatario deberá proveer de una plataforma de estadísticas e informes adecuada para la recolección de los diferentes ficheros de log de los servidores web y de aplicaciones utilizados en los distintos sistemas de información de la DGOJ, teniendo en cuenta los diferentes entornos, aplicaciones y sistemas operativos.

En los informes deberán figurar al menos los siguientes datos: nº diario y total mensual de visitas a la página de inicio, impactos totales (hits) diario y máximo mensual, visitantes nuevos y recurrentes, páginas servidas, nº máximo de usuarios concurrentes por día y mes, total errores por servidor, tiempo de respuesta de la URL, páginas más/menos visitadas, direcciones IP de origen, origen geográfico de los accesos, plataformas y exploradores utilizados, dispositivos móviles, robots y spider, franjas horarias diarias y semanales.

La empresa adjudicataria formará al personal de la DGOJ en la herramienta o solución propuesta que permita acceder a las estadísticas y la generación de informes básicos y a demanda, así

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

como datos históricos que permitan evaluar la evolución del negocio en las distintas plataformas descritas en este pliego. Los datos deberán conservarse al menos 12 meses en la plataforma.

4.2.14.4 Informes del nivel de prestación de los servicios

Mensualmente, la empresa adjudicataria deberá elaborar un informe de estado de los servicios que detalle, al menos, los siguientes puntos:

- Cumplimiento de los ANS.
- Cualesquiera incidencias y peticiones abiertas, su estado, tiempo de resolución y operaciones llevadas a cabo para solucionarlas.
- Arquitectura de comunicaciones de los servicios.
- Gráficas de monitorización de los servicios obtenidas de la plataforma de monitorización explicando las anomalías detectadas si las hubiera.
- Niveles de disponibilidad de las plataformas.
- Niveles de utilización de las plataformas y de los diferentes elementos que las constituyen, tanto nativos como virtualizados.
- Niveles y evolución del espacio libre y ocupado en las cabinas de almacenamiento.
- Recomendaciones para la mejora del servicio.
- Uso de ancho de banda total y por aplicaciones
- Operaciones de respaldo de información: realizadas, exitosas y capacidad ocupada global y por equipo.

Estos informes serán presentados a la DGOJ dentro de los 2 primeros días de cada mes.

La información contenida deberá ser suficiente para comprobar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) considerados y para el cálculo de las penalizaciones aplicables. En cualquier caso, los informes deberán indicar el incumplimiento de los Acuerdos de Nivel de Servicio (ANS) considerados siempre que éstos se hayan producido.

En todo caso, el número de informes y su contenido, se irá modificando con la evolución de la explotación de los sistemas, ajustándose en cada momento a los requerimientos de la DGOJ.

Para cada incidencia surgida durante la prestación del servicio que produzca impacto en cualquiera de los diferentes servicios, se remitirá un informe de la misma en las 24h siguientes a su detección que incluya la información detallada de la misma, y si es posible las causas y las acciones para su resolución, así como las acciones de mejora para evitar su reproducción, en su caso.

A modo orientativo, se presenta adjunto al presente pliego un extracto de los informes de seguimiento mensuales que el presente adjudicatario está realizando, sin menoscabo de cierta información incluida en los mismos que no se aporta por cuestiones de seguridad.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

4.2.15 Servicio de Soporte a los Sistemas de Información de la DGOJ

4.2.15.1 Soporte a los sistemas de información Existentes

Aunque ya se ha puesto de manifiesto a lo largo del presente pliego, es un servicio de Plataformas que soportan los desarrollos, aplicaciones y productos de la DGOJ reflejados a alto nivel en el apartado "*3.1 Sistemas de Información Actuales*", tanto en entorno productivo como pre productivo o en fase de desarrollo.

Las principales plataformas de aplicaciones a las que se les deberá dar soporte por medio de los distintos servicios contemplados en el presente pliego, con unas u otras necesidades de disponibilidad o criticidad, tal y como se pone de manifiesto en el apartado de las condiciones generales "*Horario del Servicio y Criticidades*"

- Servicio de publicación web
- Servicio de plataformas para aplicaciones internas o corporativas.
- Servicio de Plataformas para aplicaciones de cara al ciudadano, operadores de juego y otros organismos públicos.
- Sistema de descarga y validación de ficheros de evidencias de juego.
- Servicio de plataformas de análisis y explotación de datos (BI).

Tal y como se ha podido ver a lo largo del pliego, a excepción de la plataforma de análisis y explotación de datos, el resto de plataformas basadas en web están soportadas por servidores de aplicaciones Tomcat sobre plataforma Linux y BDD Oracle.

Por otro lado, la plataforma con la que cuenta la DGOJ para el análisis diferenciado de los sistemas de explotación, orientado a la SG de Inspección (plataformas de análisis y explotación de datos), con entorno de pruebas y producción, está montada sobre un cluster del producto HP Vertica, que gestionará y mantendrá el adjudicatario. La extracción de datos a esta plataforma se hace con la herramienta de software libre Talend, y la explotación con el cliente de software libre Squirrel.

4.2.15.2 Soporte a sistemas de información adicionales

Con independencia de los sistemas de información objeto del servicio señalados en el apartado 3.1, el adjudicatario podrá ser requerido para dar soporte cualquier sistema adicional cuyo desarrollo y puesta en marcha se produzca durante la ejecución del contrato y siempre que estén basados en tecnologías similares a las ya utilizadas, sin que ello suponga incremento alguno del importe del mismo.

En cualquier caso, tanto para sistemas existentes como adicionales, la evolución tecnológica de las plataformas y servicios objeto del contrato podrá conllevar la migración y/o actualización tanto de los aplicativos, como de los productos de software de base sobre los que éstas operan. Estos procesos de migración y actualización podrán requerir la habilitación temporal de servidores físicos y/o virtuales adicionales que permitan establecer los entornos de prueba

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

necesarios para validar las estrategias de migración y/o actualización establecidas por la DGOJ. Dichos recursos hardware adicionales correrán por cuenta de la DGOJ, siendo ésta la que determine sus parámetros de explotación y configuración, quedando por cuenta del adjudicatario la explotación de dichos servidores durante el periodo requerido.

4.2.15.3 Apoyo Técnico y Consultoría al Área de Desarrollo de la DGOJ

Se desea un servicio de apoyo técnico y consultoría por parte del adjudicatario, gestor de las plataformas y servicios exigidos en este pliego, para su implicación, con los especialistas necesarios, en el análisis de peticiones e incidencias que la DGOJ pueda plantear al respecto de todos los sistemas, servicios y plataformas, relacionadas con el rendimiento de las aplicaciones de la DGOJ.

Se trata de un servicio de apoyo técnico por lo que se prestará en función de la naturaleza de las peticiones e incidencias, de acuerdo al apartado de Modelo de Gobierno y de Relación y al apartado de Servicio de Gestión de Incidencias y Peticiones.

Respecto a los sistemas e infraestructuras que soportan las aplicaciones corporativas de la DGOJ, con el fin de garantizar su disponibilidad y rendimiento, se realizará en caso de petición por parte de la DGOJ:

- Soporte para la provisión de infraestructura para proyectos de desarrollo y para nuevas aplicaciones en producción.
- Apoyo técnico al servicio de Mantenimiento de Aplicaciones para la resolución de incidencias.
- Soporte a los equipos de desarrollo de Aplicaciones para la resolución de incidencias, escaladas desde el CAU.
- Soporte para la resolución de incidencias del entorno de producción o explotación. Asesoramiento en la elaboración de los procedimientos que regulen la relación entre el Área de desarrollo y de infraestructuras.
- Control del deterioro en el rendimiento de las aplicaciones y generación de informes.
- Generación de informes de problemas y discriminación de incidencias versus problemas.
- Apoyo técnico al equipo de desarrollo desde las fases iniciales, para facilitar las implantaciones de los proyectos.
- Asesoramiento en la definición de Planes de Contingencias.
- Apoyo técnico en la implementación de nuevas versiones tanto de desarrollos a medida realizados para la DGOJ, como de productos comerciales
- Gestión y puesta en producción de aplicaciones y cambios de versión de aplicaciones y servicios, asegurando que se cumplen todas las condiciones necesarias en cuanto a estabilidad, documentación de despliegue, automatización, etc (capacidad, verificación de

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

procesos, control del resultado de las pruebas de lanzamiento, necesidades de backup y monitorización, etc.).

- Asegurar la disponibilidad de los servicios.
- Generación, Publicación y Gestión de Conocimiento útil interno al servicio
- Gestión de peticiones de la DGOJ relacionadas con la explotación de las aplicaciones (accesos de usuarios a aplicaciones, ejecución de procesos especiales en producción,...).
- Diagnóstico y resolución de incidencias.
- Establecimiento de alarmas y sistemas de monitorización y registro automático de incidencias.
- Análisis de incidencias, determinación de problemas y planes de acción para su solución.
- Provisión y asesoramiento en la definición de la infraestructura (hardware, software de sistemas y entornos) necesaria para la ejecución de proyectos de desarrollo.
- Actualización de versiones de software de aplicación. Incluye su homologación y la provisión de la infraestructura necesaria.
- Para proyectos de desarrollo que impliquen la incorporación de nuevo software de aplicaciones, análisis y homologación del software propuesto.
- Gestión de la configuración entre entornos, garantizando la sincronización conforme a las normas de la DGOJ.
- Apoyo técnico al servicio de Mantenimiento de Aplicaciones en la determinación de las causas de incidencias ocurridas en las aplicaciones. El objetivo de esta actividad es evitar imprecisiones a la hora de determinar las causas de incidencias de forma que permita atribuir correcta y rápidamente qué servicios tiene la responsabilidad de la resolución del fallo.
- Resolución de las incidencias que tengan su causa en la infraestructura que soporta las aplicaciones.
- Asesoramiento al servicio de Desarrollo y Mantenimiento de Aplicaciones en el control del deterioro en el rendimiento de las aplicaciones, generación de informes y estudio de mejoras.
- Elaboración de documentación, informes y procedimientos.
- Cumplimiento de requisitos de calidad definidos por la DGOJ.

Estas peticiones al respecto de este servicio descritas, tendrán el tratamiento de incidencia en lo que al servicio afectado respecta, por lo que aplicará, en su caso, el ANS del servicio afectado.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Cabe destacar que cuando se trate de un estudio o análisis de un problema, los plazos a considerar serán mayores.

4.2.16 Servicio Avanzado de Soporte Especializado para la base de datos Oracle

El presente servicio adicional consiste en ofrecer servicios avanzados de soporte especializado, de carácter reactivo, proactivo y correctivo, de soporte para la puesta en marcha de proyectos de consolidación y homogeneización de infraestructuras asociadas a este contrato, así como asesoría tecnológica y control de calidad específica.

Deberán ser proporcionados directamente por el fabricante de la tecnología, cubriendo la totalidad del período de ejecución del contrato. Como mínimo tendrán como objeto los entornos de producción de las bases de datos CNJRIAJ e INSPROD, aunque los de carácter reactivo deberán cubrir también los entornos de desarrollo y pruebas.

En ningún caso el uso de este servicio exonerará al adjudicatario del cumplimiento de los ANS.

Los servicios se describen a continuación:

- Apoyo de segundo nivel 8x5 de incidencias críticas o de prioridad 1.
- Monitorización, investigación y análisis de las incidencias críticas, de cara a conseguir la máxima disponibilidad del gestor de base de datos. Estudios detallados sobre el origen de las incidencias, revisión de patch-sets y recomendaciones, consultas versiones y/o parámetros de base de datos, buenas prácticas, acceso a Product Support y seguimiento de Service Requests.
- Monitorización de incidencias no críticas
- Contacto directo con la línea de desarrollo de producto de Oracle, con los siguientes objetivos:
    - Inclusión en las nuevas versiones del producto de soluciones a bugs o problemas encontrados en el software gestor de base de datos, o a necesidades específicas de negocio existentes en la DGOJ.
    - Aprovechamiento de la experiencia del fabricante con otros clientes a nivel mundial con la misma versión de producto, plataforma y arquitectura existentes en la DGOJ.
- Alertas proactivas (informaciones y recomendaciones técnicas preventivas-proactivas muy precisas generadas por Oracle en la red de conocimiento interno)
- Asesoramiento proactivo y preventivo del hardware y software Oracle. El equipo técnico de Oracle proporcionará de forma preventiva información técnica relativa al entorno hardware y software: alertas e incidencias, consultas sobre configuración y procedimientos, nuevas versiones y parches, soluciones temporales y recomendaciones técnicas específicas, etc. Reporte de los principales parámetros de gestión del servicio, y seguimiento de la evolución del software de bases de datos.

- Asesoramiento y apoyo en la administración y explotación del entorno de producción con el objetivo de proporcionar el mejor nivel de disponibilidad, rendimiento, seguridad, gestión de incidencias y gestión de cambios, y al mismo tiempo descartar la aparición de problemas debidos a malas prácticas.
- Asistencia en recuperación de sistemas con software Oracle. Análisis post-incidente de causa raíz del problema e informe con recomendaciones, extracción de datos de la base de datos caída, reproducción de problemas genéricos, creación de test case y asistencia en work-arounds.
- Apoyo y asesoramiento en la instalación de nuevas versiones de los productos adquiridos por la DGOJ (por ejemplo, DataBase Vault, Enterprise Manager…), detectando las posibilidades de los mismos y la alineación con los procesos de negocio, colaborando en la evolución y validación técnica de los mismos y desarrollando las funcionalidades que sean necesarias para cumplir con los objetivos funcionales de la DGOJ.
- Apoyo y asesoramiento en migraciones. Estudio de toma de requisitos y diseño, planificación de actividades (apoyo o ejecución íntegra de la migración), elaboración de informe y presentación.
- Comprensión e interiorización de los objetivos de negocio de la DGOJ, para alinear las funcionalidades del software de base de datos con los mismos y, en caso de ser existir gaps, solventarlos a través de actualizaciones del software.
- Revisiones de los entornos de base de datos (CNJRIAJ / INSPROD) en términos de:
    - Rendimiento. Informes de actividad del sistema, tiempos de respuesta del software, análisis de eficiencia, shared pool y/o sentencias.
    - Configuración. Información de sistemas, configuración Oracle, información de red, documentación.
- Planificación y ejecución de la instalación de las nuevas versiones a ser implantadas en la DGOJ. Transferencia de conocimiento vía sesiones técnicas teórico-prácticas personalizadas por cada una de las nuevas funcionalidades a ser implantadas en la DGOJ, o bien sobre productos o tecnologías Oracle.
- Asistencias planificadas fuera de horario. Soporte presencial y/o remoto fuera del horario del Servicio (un paso a Producción, una actualización de versión, instalación de parches, etc.) proporcionando asistencia en el caso de surgir algún problema o incidencia.
- Soporte al backup y recovery de datos.
- Revisión de la seguridad de la base de datos, tanto en lo relativo a la utilización de la misma por las aplicaciones y usuarios finales, como por los administradores, detectando las carencias de los productos instalados y promoviendo el desarrollo de funcionalidades que superen dichas deficiencias.
- Ejecución de pruebas de alta disponibilidad. Estudio inicial y diseño, planificación de actividades, ejecución de pruebas, elaboración de informe y presentación.

dgoj.dgeneral@ordenacionjueg.gob.es

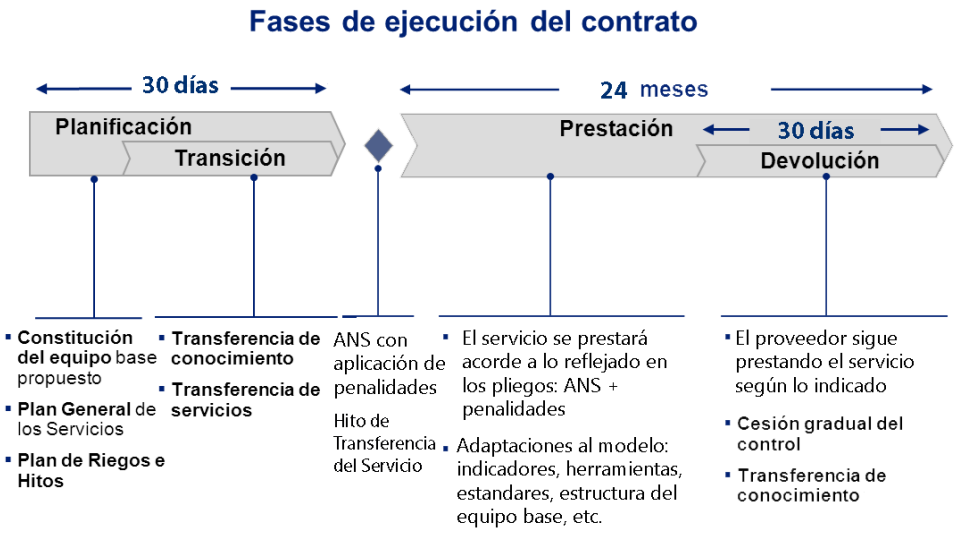
C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Nombramiento de un Gestor del Servicio por parte del fabricante Oracle (Technical Account Manager), responsable técnico del servicio, supervisión, asignación de recursos y correcta ejecución de todo el servicio. Ayudará a construir y mantener la relación con las personas clave, tanto del contrato como de la DGOJ, responsables de la gestión y soporte, para asegurarse de que cada elemento del soporte prestado por el adjudicatario se ajuste a los requerimientos de los usuarios. Además, será el encargado de involucrar los recursos más adecuados en cada momento para cubrir las necesidades de soporte. Como apoyo a este TAM, tanto los medios personales adscritos a este contrato como el personal de la DGOJ tendrán asignado un equipo de soporte y podrá acceder a un centro de respuesta Oracle en horario 8x5.
- Refuerzo de Especialistas. Jornadas de Ingenieros Técnicos Senior especialistas en tecnologías y productos Oracle como recursos de apoyo para el mantenimiento de los entornos, análisis, implantación de proyectos o auditorías.

5 FASES DE LA PRESTACIÓN DEL SERVICIO

Siguiendo la metodología de la DGOJ, la prestación del Servicio se dividirá en varias fases o etapas:

- Planificación
- Transición
- Hito de transferencia del servicio
- Prestación del servicio
- Devolución del servicio.



dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

5.1 Fase de planificación

La fase de planificación será única, simultánea para todos los servicios y en algunos momentos solapada con la transferencia del servicio. Los objetivos asociados a esta fase inicial son los siguientes:

- **Organización y constitución** del equipo de trabajo base propuesto.
- Desarrollo del **Plan General** de los servicios. La DGOJ tendrá la capacidad de aprobar o modificar la fecha de inicio, duración y contenido de cada una de las fases, para garantizar la consecución de la transferencia completa en los plazos y condiciones deseadas.
- Definición del **Plan de Riesgos**, incluyendo la identificación de riesgos principales y las acciones asociadas, con especial foco en la garantía de la continuidad en la resolución de incidencias y peticiones (principalmente las críticas).
- Elaboración de un **Plan de Hitos** principales, incluyendo fechas y requisitos para que se produzcan.

Con referencia a la fase posterior de **Transición** el adjudicatario desarrollará un **Plan de la Transición** del servicio y conocimiento. Dicho plan de transición deberá contemplar al menos las siguientes actividades y contenidos:

- Detalle de las actividades a realizar por los equipos de trabajo y cronograma asociado.
- Identificación y recopilación de la documentación necesaria (documentación de los sistemas y aplicaciones, documentación técnica, procedimientos de actuación, etc.) para la asunción del servicio[1]
- Identificación de los riesgos específicos a la fase de transición, con especial énfasis en las tareas iniciadas o previstas en el momento en el que el adjudicatario asume el servicio.
- Definición de los hitos principales de la transición incluyendo fechas y requisitos para que se produzcan.
- Identificación de las actividades de comunicación y formación necesarias para garantizar la fase de transición.

En esta documentación, además de identificar todas las actividades a llevar a cabo con las fechas de inicio y fin de cada una de ellas, se incluirán los criterios aplicables de aceptabilidad y

[1] *En aquellos casos en los que no exista documentación previa necesaria para prestar el servicio, el adjudicatario entrante deberá planificar, de acuerdo con la DGOJ, y ejecutar su elaboración, sin coste adicional*.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

cualquier otro detalle adicional que se estime pertinente. Adicionalmente, los documentos propuestos tendrán que ser aprobados por la DGOJ previamente a su ejecución.
En cualquier caso, se espera la participación activa del adjudicatario para garantizar la correcta alineación de las planificaciones. La DGOJ podrá identificar dependencias y condicionantes que el adjudicatario deberá respetar.
Una vez exista un plan definitivo de Transición acordado, las fechas de transferencia serán inamovibles, salvo que la DGOJ requiera una nueva planificación del plan definitivo de Transición.

5.2 Fase de transición

5.2.1 Transferencia del conocimiento

Mientras continúa la fase de planificación, y después de que la DGOJ apruebe el plan general diseñado que permitirá al nuevo adjudicatario tomar el control efectivo de los servicios de forma gradual pero sin pérdida de servicio, podrá iniciarse la fase de Transferencia del conocimiento.

El objetivo de esta fase es el traspaso de los elementos básicos e imprescindibles para la prestación del servicio, entre el adjudicatario saliente y el entrante. Durante la misma, el adjudicatario saliente sigue prestando servicio a la DGOJ, por lo que su disponibilidad será limitada, y el adjudicatario entrante ejecuta el plan definitivo de Transición con todas las actividades que le permitan prepararse para asumir el servicio.

La forma de transferir el conocimiento entre el adjudicatario saliente y el entrante será aplicando la técnica del solapamiento. Esta técnica consiste en que el personal del adjudicatario entrante, una vez conoce de manera básica, los procedimientos de trabajo, los sistemas, la infraestructura tecnológica y las herramientas existentes a través del estudio de los documentos que los describen con el objeto de conocer el detalle práctico el uso de las herramientas y sistemas, así como la aplicación práctica de los procedimientos.

La situación actual tiene las ventajas de una avanzada homogeneización de entornos, estandarización de versiones y un elevado grado de virtualización, lo que facilita la transición a nuevos sistemas o plataformas. Cada servicio tendrá que pasar en mayor o menor medida por una fase de transición en la que se adaptará el servicio a las nuevas soluciones técnicas de prestación. A lo largo del presente pliego se detallan los condicionantes técnicos al respecto de productos o versiones para los que las aplicaciones de la DGOJ están adaptadas.

En muchos casos la dependencia de las distintas aplicaciones a esas condiciones tecnológicas es tal que no se puede variar sin que suponga una adaptación y desarrollo sobre dichas aplicaciones. La DGOJ no asumirá los costes de adaptación que se deriven de transformaciones de servicio no solicitadas explícitamente, y por tanto, los cambios propuestos en la arquitectura de los CPD que impacten negativamente en las aplicaciones conllevarán que el adjudicatario asuma los costes de modificación de las aplicaciones.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Durante esta fase, la gestión del servicio sigue siendo del adjudicatario saliente, por lo que las actividades se desarrollarán teniendo en cuenta la prioridad del servicio sobre cualquier otra circunstancia.

Esta fase durará 30 días naturales como mínimo (incluyendo la fase de planificación) y todo el personal que participe en esta etapa deberá firmar el preceptivo acuerdo de confidencialidad sobre la información que se reciba.

Todos los intercambios formales realizados entre el adjudicatario saliente y entrante, deberán quedar documentados y aceptados por ambos adjudicatarios (entrante y saliente), de manera formal y fehaciente.

El adjudicatario del contrato tiene la obligación de documentar todas las actividades realizadas durante del proceso de transición y entregar esa documentación a la DGOJ cuando termine el proceso de transición. Para la correcta certificación de esta fase, se solicitara al adjudicatario el Estado del Arte de los Servicios correspondientes a este pliego. Dicho producto implicará al menos las siguientes actividades mínimas:

- Mediciones sobre uso, comportamiento y requerimientos de los servicios que permitan ajustar los valores iniciales estimados para el Acuerdo de Nivel de Servicio (ANS), y los mecanismos de control de los mismos.
- Elaborar la documentación de gestión necesaria (procedimientos, manual de calidad, ANS, matriz detallada de responsabilidades, plan de trabajo para el cumplimiento del ANS, etc).

Todos los servicios deberán estar plenamente operativos al finalizar esta fase, por lo que es esencial que el adjudicatario acredite el cumplimiento del plan definitivo de Transición y estar en disposición de realizar el servicio según lo dispuesto en el presente pliego previamente a la formalización del contrato, o al hito de transferencia del servicio.

5.2.2 Transferencia de servicios

La transferencia de servicios entre adjudicatarios (entrante y saliente) deberá ser llevada a cabo por adjudicatario entrante, quien contará con la información aportada por el adjudicatario actual.

Es requisito imprescindible que las condiciones de realización de los trabajos transferencia garanticen la continuidad en el servicio, considerando que las plataformas y los servicios objeto de este contrato son las utilizadas por los usuarios finales de las mismas, tanto internos como externos a la organización. Para garantizar la continuidad, será necesario acordar la planificación de todo el proceso de migración con los responsables del Centro de Servicios en el que se encuentran actualmente alojadas las aplicaciones informáticas, estableciendo los periodos de solape mínimos entre el funcionamiento de los CPD´s entrante y saliente.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

La transferencia del servicio finaliza con el hito de Transferencia del Servicio del adjudicatario saliente al entrante, cuya fecha estará definida en el plan definitivo de Transición aprobado por la DGOJ. El adjudicatario entrante se compromete a cumplir con dicha fecha de finalización de la Transición.

La adjudicación del contrato a un adjudicatario distinto del actual no supondrá un impacto en los servicios de la DGOJ. Durante el periodo de transferencia y para garantizar la continuidad de los servicios, el nuevo adjudicatario podrá recurrir al adjudicatario actual asumiendo el coste del servicio. En todo caso la DGOJ abonará los servicios al nuevo adjudicatario desde la fecha de formalización del contrato.

Uno de los elementos más importantes de este punto es la transferencia de las copias de seguridad (de máquinas realizadas via agente y de una serie de snapshots elegidos por la DGOJ para las unidades protegidas mediante esta técnica), así como de todos los logs de los elementos de seguridad almacenados en el SIEM, y de los servidores que la DGOJ considere necesarios.

5.2.3 Hito de transferencia del servicio

Se trata del hito culminante de la Transición. Antes de que pueda ocurrir este hito, el adjudicatario entrante deberá haber realizado las siguientes tareas:

- Ejecución de todas las actividades planificadas en relación a este hito en el plan definitivo de Transición.
- Registro documental de todas las entregas habidas entre adjudicatarios o entre la DGOJ y el adjudicatario entrante.
- Registro documental de todos los hechos significativos de la Transición.
- Presentación de la base de datos de conocimiento de la operativa del equipo de trabajo.

Al final de la fase de Desarrollo de la Transferencia, se procederá a ejecutar el hito de transferencia del servicio, que marcará el inicio de la fase de prestación del servicio y, por lo tanto, la finalización de la prestación del servicio por el adjudicatario saliente.

A su vez, el adjudicatario entrante recibirá, si no lo ha hecho en momentos anteriores, todas las peticiones de servicio y trabajos inacabados. El adjudicatario entrante es responsable de atender la lista de tareas y trabajos que estén iniciados o pendientes de inicio, en el momento en que asuma el servicio. Esto incluye, de manera expresa, la resolución de incidencias que no hayan podido ser resueltas por el adjudicatario saliente, antes del hito de Transferencia del servicio.

El cumplimiento del hito de transferencia del servicio, deberá quedar formalmente documentado mediante actas y deberá ser aceptado tanto por parte del adjudicatario entrante, como por parte de la DGOJ.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Este hito se corresponde con el periodo de vigencia del contrato actual, cuya fecha de finalización es el 30 de abril de 2022 o cualquier fecha anterior.

Tan pronto como el adjudicatario entrante adquiera el servicio se entrará en la fase de prestación del servicio.

5.3 Fase de prestación del servicio

La fase de prestación del servicio comenzará tras el cumplimiento del hito de transferencia del servicio.

Desde este momento, el adjudicatario entrante es responsable de ofrecer los servicios que se detallan en este pliego, y finalizará formalmente con la fase de devolución del servicio el 30 de abril de 2024, sin menoscabo de una posible prórroga del contrato. En particular cabe destacar que asume:

- Cumplimiento con la totalidad de los Acuerdos de nivel de servicio desde el comienzo de la prestación del servicio el 1 de mayo de 2022.
- Mantenimiento de la documentación de los servicios objeto de la transferencia. La documentación deberá ser actualizada ante cualquier modificación del servicio, así como generar la nueva documentación que se estime necesaria.
- Seguimiento de los procesos y procedimientos operacionales y de soporte, según lo indicado en el presente pliego.
- Cumplimiento de todas las tareas de seguimiento del servicio, incluyendo la presentación de los informes acordados.
- Todo el resto de las tareas identificadas en el presente pliego.

5.4 Fase de devolución del servicio

En todos los casos, mientras continúa la fase de prestación del servicio, existirá una fase de devolución del servicio para garantizar la transferencia del conocimiento adquirido o generado, así como los activos adquiridos durante la prestación del servicio por parte del adjudicatario hacia la DGOJ, o hacia el adjudicatario que la DGOJ designe, sin que ello repercuta en una pérdida del control o del nivel de calidad del servicio.

En caso de cese o finalización de contrato, el adjudicatario estará obligado a devolver el control de los servicios objeto del contrato, simultaneándose los trabajos de devolución con los de prestación del servicio, sin coste adicional.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

El servicio deberá seguir prestándose, pero adicionalmente habrá que realizar las actividades propias de la reversión del servicio. Durante esta fase, la DGOJ reducirá el número de cambios e intervenciones al mínimo posible, para reducir la complejidad de la gestión del servicio, en estas circunstancias.

Al inicio de la fase de devolución del servicio, el adjudicatario hará una evaluación y planificación de todas las actividades necesarias. Dicho traspaso se realizará con una duración mínima de 30 días naturales desde la notificación del inicio de esta fase.

El adjudicatario deberá realizar el proceso de transición de salida o devolución del servicio, asegurando que se mantienen correctamente, durante el traspaso, el control de servicios y deberá colaborar activamente con la DGOJ y con el futuro adjudicatario durante este proceso, para facilitar la transferencia del conocimiento y los servicios.

El compromiso de devolución del servicio del adjudicatario a la DGOJ incluye:

- El adjudicatario deberá hacer entrega a la DGOJ de una versión actualizada de toda la documentación e información manejada para la prestación del servicio antes de la finalización del contrato.
- Traspaso a la DGOJ de la propiedad de los activos del adjudicatario susceptibles de ser transferidos.
- Traspaso de la información de la DGOJ alojada en infraestructura del adjudicatario a los sistemas que determine la DGOJ. Entre esta información, las copias de seguridad (de máquinas realizadas via agente y de una serie de snapshots elegidos por la DGOJ para las unidades protegidas mediante esta técnica), así como de todos los logs de los elementos de seguridad almacenados en el SIEM, y de los servidores que la DGOJ considere necesarios.
- Traspaso de contratos de terceros y titularidad de licencias según el caso atendiendo a la solicitud y conformidad de la DGOJ.
- Traspaso del conocimiento de los recursos del adjudicatario a los recursos designados por la DGOJ según el caso.
- Traspaso de la documentación del servicio a la DGOJ.

En el coste de la devolución del servicio deberá contemplarse la transmisión de la propiedad de todas las herramientas desarrolladas por el contratista de forma exclusiva para la prestación de los servicios. La DGOJ se reserva el derecho de aceptar la transmisión del total de las herramientas pudiendo elegir las que sean de su interés. En caso de solicitar la transmisión de la propiedad de un número menor de herramientas del total ofertado se procederá a valorar las elegidas y reajustar el coste del servicio.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

6 MEDICIÓN DE LOS NIVELES DE PRESTACIÓN DEL SERVICIO

El presente PPT establece el conjunto de Acuerdos de Nivel de Servicio (ANS), que serán objeto de seguimiento mensual y el nivel de cumplimiento de los mismos como umbral de calidad de servicio.

Se entiende por ANS el nivel de prestación del servicio exigido al contratista para cada uno de los indicadores.

El principal objetivo del ANS es establecer parámetros medibles que permitan a la DGOJ, como contratante del servicio, y al adjudicatario, controlar la calidad de los servicios prestados, tanto de manera puntual como en su evolución en el tiempo.

El adjudicatario proporcionará la información necesaria para el seguimiento del ANS establecido mediante los correspondientes informes de seguimiento, y garantizará el mantenimiento de históricos de actividad durante todo el período de vigencia del contrato.

La información será objetiva y obtenida preferentemente a través de los registros elaborados con las herramientas de gestión. Tanto las herramientas de gestión como la forma de extracción de la información serán aprobadas por la DGOJ.

El contratista presentará mensualmente el informe correspondiente a la medición del ANS; dicha información deberá ser obtenida mediante los procedimientos y mecanismos establecidos por la DGOJ, que se reserva el derecho de contrastar la información facilitada.

El incumplimiento de los valores comprometidos en el ANS supondrá la aplicación de penalidades previstas en el pliego de cláusulas administrativas.

El ANS inicialmente definido será de aplicación desde el momento en que el adjudicatario comience a prestar el servicio.

A fin de mejorar la calidad del servicio prestado, el ANS recogido en el presente apartado, estará orientado a la mejora continua.

El ANS descrito establece los valores mínimos exigidos al adjudicatario del contrato. Cualquier modificación que pueda sufrir a lo largo de la vigencia del contrato, siempre a través de los procedimientos y Reuniones de Seguimiento establecidas, serán en pro de una mejora en la calidad del servicio.

En los indicadores definidos se establece el Nivel de Servicio mínimo exigido para los servicios objeto de este contrato. Los niveles de servicio por debajo de este umbral estarán sujetos a penalidades especiales que se calcularán conforme al procedimiento descrito en el pliego de

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

cláusulas administrativas particulares. El cumplimiento de los niveles de servicio se revisará mensualmente en las Reuniones de Seguimiento del Contrato

Los indicadores de calidad y sus acuerdos de nivel de servicio pueden verse modificados siempre y cuando se produzcan eventos y circunstancias ajenas al contratista y que afectan a los trabajos a desarrollar

- **Incidencias críticas, de carácter masivo o de afección de servicios críticos**: En caso de producirse una Incidencia crítica de carácter masivo, cuya causa origen sea ajena al servicio prestado por el adjudicatario (como la caída general de alguna de las aplicaciones o servicios relevantes), y que por su impacto en el servicio incremente en un 30% la demanda media anual de servicio diaria y por tanto afecte de forma negativa al cumplimiento de los ANS's, se analizarán los días afectados por la incidencia concreta de forma independiente. Este análisis permitirá verificar si el incumplimiento del nivel de servicio está ocasionado por esta causa.
- **Condiciones anormales de prestación del servicio:** En caso de producirse problemas de rendimiento o dimensionamiento de la infraestructura, sistemas de información, etc. propiedad de la DGOJ, que soportan la gestión del servicio objeto del contrato y que de forma clara perjudiquen el normal desempeño del servicio prestado por el adjudicatario, se analizará la circunstancia de forma independiente. Este análisis permitirá verificar si el incumplimiento del nivel de servicio está ocasionado por esta causa.

Aun cuando se detallan a continuación cada uno de los indicadores propuestos, se presenta a continuación una tabla resumen de los mismos:

Acuerdos de nivel de servicio					
Indicador		**Descripción**	**Nivel del Servicio**	**Incumplimiento Nivel del Servicio**	
				Leve	**Grave**
I_1	***Disponibilidad de los SS.II de la DGOJ***	Tiempo de disponibilidad de los sistemas de información considerados críticos y de disponibilidad 24x7 de la DGJO.	≥ 95%	< 95% y ≥ 90%	< 90%
I_2	***Disponibilidad de los servicios***	Tiempo de disponibilidad de los sistemas de los servicios no	≥ 95%	< 95% y ≥ 90%	< 90%

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Acuerdos de nivel de servicio					
Indicador		**Descripción**	**Nivel del Servicio**	**Incumplimiento Nivel del Servicio**	
				Leve	**Grave**
		considerados básicos para la ejecución de los sistemas de información, tales como monitorización, gestión y seguimiento de los servicios, Seguridad, etc			
I_3	***Notificación de incidencias, e informes asociados.***	Se notificará a la DGOJ las alarmas detectadas y las acciones correctoras realizadas para solucionarlas, así como toda la información de análisis que se considere relevante asociada a la incidencia detectada.	≤ 1 día y 100% de alarmas existentes analizadas y acciones correctoras asociadas.	> 1 día y ≤ 2 días o < 100% y ≥ 95% de alarmas existentes	> 2 días o > 95% de alarmas existentes
I_4	***Tiempo de entrega de informes mensuales de seguimiento del servicio o datos solicitados.***	Tiempo entrega informes de seguimiento del servicio, o tiempo de entrega de informes o datos solicitados por la DGOJ sobre la fecha estimada de entrega.	Informes periódicos ≤ 2º Jornada laboral tras el plazo de entrega estimado. Datos ≤ 4º Jornada laboral tras la petición de datos.	Inf_periódicos > 2 días Datos > 4 días	Inf_periódicos > 3 días Datos > 6 días
I_5	***Cumplimiento de plazos de entrega de encargos de trabajo Planificados***	Indicador para la detección de desviaciones en la consecución de los plazos de los hitos y entregables previstos en las planificaciones, tales como los servicios adicionales o las mejoras de almacenamiento por ejemplo.	Desviación ≤ 25%.	Desviación > 25%.	Desviación > 35%.
I_6	***Tiempo de resolución de problemas e incidencias***	Indicador del nivel de resolución de incidencias en función del tiempo	Críticas ≤ 2 horas Importante ≤ 4 horas	Críticas > 2 hs Importante > 4 hs Básica > 36 hs	Críticas > 4 hs Importante > 6 hs

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Acuerdos de nivel de servicio					
Indicador		**Descripción**	**Nivel del Servicio**	**Incumplimiento Nivel del Servicio**	
				Leve	**Grave**
		de resolución dedicado en función de la criticidad de la misma. Se entiende por tiempo de resolución el tiempo transcurrido desde que se detecta el problema o incidencia hasta que se da por solucionado.	Básica ≤ 36 horas		Básica > 40 hs
I_7	***Tiempo de respuesta para cambios solicitados por la DGOJ.***	Este indicador mide el tiempo de respuesta transcurrido entre la realización de la petición de cambio y la asignación de la misma a un técnico para su resolución en función de si dicho cambios es considerado de tipo básico, importante o crítico.	Críticas ≤ 0,5 horas Importante ≤ 1 hora Básica ≤ 2 horas	Críticas > 0,5 hs Importante ≤ 1 h Básica > 2 hs	Críticas > 0,5 hs Importante ≤ 1 h Básica > 2 hs
I_8	***Tiempo máximo de ejecución de cambios solicitados por la DGOJ.***	Este indicador mide el tiempo máximo transcurrido desde que se realiza la petición de cambio hasta se indica como realizada/verificada en función de si dicho cambios es considerado de tipo básico, importante o crítico.	Críticas ≤ 4 horas Importante ≤ 24 horas Básica ≤ 48 horas	Críticas > 4 hs Importante > 24 hs Básica > 48 hs	Críticas > 8 hs Importante > 48 hs Básica > 72 hs
I_9	***Realización de Copias de seguridad***	Indicador que mide el tanto por ciento de éxito de las copias de seguridad realizadas a lo largo del fin de semana.	= 100% copias de segurdad completadas en un fin de semana	< 100%	< 95%

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Acuerdos de nivel de servicio					
Indicador		**Descripción**	**Nivel del Servicio**	**Incumplimiento Nivel del Servicio**	
				Leve	**Grave**
I_10	***Tiempo de respuesta ante recuperación de datos (restores)***	Mide el tiempo transcurrido desde la petición de recuperación de datos, en función de su criticidad, hasta el comienzo de la operación de recuperación.	Críticos ≤ 2 horas resto ≤ 10 horas	Críticos > 2 hs resto > 10 hs	Críticos > 4 hs resto > 15 hs
I_11	***Tiempo de respuesta ante recuperación de máquinas virtuales no replicadas en CPD espejo***	Mide el tiempo que se tarda en levantar una máquina virtual cuando esta no está replicada en el otro CPD, diferenciandose entre calidad del servicio según la prioridad de la máquina.	*Máquinas Prioritarias* ≤ 2 días Resto ≤ 7 días	*Prioritarias* > 2 días Resto > 7 días	*Prioritarias* > 3 días Resto > 9 días
I_12	***Perfiles asignados durante la ejecución***	Mide la experiencia de los perfiles existentes durante la ejecución en relación a los perfiles ofertados	Experiencia de los perfiles profesionales adscritos a la ejecución del contrato ≥ Experiencia de los perfiles profesionales ofertados	Experiencia del perfil profesional inferior a la ofertada en el momento de la licitación	Experiencia del perfil profesional inferior a la ofertada en más de un producto o materia o certificaciones inferiores

6.1 ANS 1 - Disponibilidad de los sistemas de información de la DGOJ

Mide el porcentaje de tiempo en que los sistemas de información de la DGOJ (hardware, software y comunicaciones) están operativos de forma que los usuarios puedan acceder a todos los servicios que estos proporcionan con el tiempo de respuesta adecuado.

La falta de disponibilidad se determina por la imposibilidad de acceder o de usar de forma razonable los servicios principales de cada sistema de información, plataforma o componente por parte de un usuario interno o externo.

Un fallo en un elemento que se encuentra redundado y que no interrumpe el servicio no se considera incumplimiento.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

En el cálculo de la disponibilidad no se contabilizará el tiempo dedicado a las ventanas de mantenimiento planificado, siempre que hayan sido notificadas previamente a la DGOJ, ni tampoco aquellas paradas que lo sean a petición de la DGOJ, como por ejemplo, por cambios de la plataforma tecnológica.

En el informe mensual se detallará el % de disponibilidad mensual, y anual, desglosando el % de caídas y el % de indisposición por causas planificadas.

Este acuerdo de nivel de servicio se contabilizará para cada uno de los sistemas de información indicados.

El objetivo mínimo será del 95% anual y mensual.

La contabilización se verá afectada por un coeficiente en función del horario en que produzca, es decir, un incumplimiento de nivel de servicio en horario de 7:00 a 15:00 se considerará más grave que en horario, por ejemplo de 21:00 a 7:00.

Horario	**Coeficiente**	
Laborable	Tipo 1	Tipo 2
7:00 a 15:00	4	4
15:00 a 21:00	4	3
21:00 a 7:00	4	1
Festivo 0:00 a 24:00	4	1

6.2 ANS 2 - Disponibilidad de los servicios

Mide el porcentaje de tiempo en que las plataformas ofertadas por el adjudicatario para los servicios de monitorización, estadísticas e informes y gestión de incidencias están operativas y realizando sus funciones correspondientes para cada sistema de información de la DGOJ.

El objetivo mínimo será del 95% anual y mensual para cada uno de los servicios.

6.3 ANS 3- Notificación de incidencias, e informes asociados

Se notificará a la DGOJ las alarmas detectadas y las acciones correctoras realizadas para solucionarlas.

El objetivo será del 100% de comunicación de alarmas y las acciones correctoras antes de 24 horas. En caso, de que dada su complejidad e importancia sea necesario realizar un informe de la incidencia ocurrida, este informe se remitirá en un máximo de 48 h.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

6.4 ANS 4- Tiempo de entrega de informes mensuales de seguimiento del servicio o datos solicitados

El objetivo del presente indicador es garantizar la adecuada gestión de los informes de seguimiento periódicos que se establezcan, tales como el informe de seguimiento mensual, así como la solicitud de informes o datos solicitados por la DGOJ en relación a la prestación del servicio, de forma que la tramitación de los mismos se realice de forma ágil y correcta en el menor tiempo posible, ajustándose siempre a los procedimientos definidos por la DGOJ.

Los informes periódicos se entregarán a la DGOJ con un máximo de 2 días a partir de la finalización de la fecha de entrega estimada. Los informes o datos relacionados con el servicio pedidos por la DGOJ y no considerados periódicos, se entregarán con un plazo máximo de 4 días.

6.5 ANS 5 – Cumplimiento de plazos de entrega de encargos de trabajo Planificados

El objetivo del indicador es conseguir que se cumplan los plazos de los hitos y entregables previstos en las planificaciones aprobadas por la DGOJ en cuanto a actuaciones a realizar por parte del proveedor del servicio.

El fin último es la detección de desviaciones en la consecución de los plazos de los hitos y entregables previstos en las planificaciones, tales como los servicios adicionales o las mejoras de almacenamiento por ejemplo.

Se requiere cumplir la planificación de los hitos y entregables y la eventual desviación sea ≤ 25%, siendo la métrica de medida:

$$\left(\frac{Número\ días\ reales}{Número\ de\ días\ planificados} - 1\right) * 100$$

Por necesidades del servicio, cambios de prioridades, o similar, es posible que sea necesario reajustar la planificación a lo largo del proyecto. Las nuevas fechas se deberán volver a proponer por parte del proveedor y aprobar por parte de la DGOJ.

6.6 ANS 6 – Tiempo de resolución de problemas e incidencias

El objetivo del indicador es conseguir la mejora de la calidad de servicio, que redundará en el aumento de la satisfacción del usuario. Indicador del nivel de resolución de incidencias en función del tiempo de resolución dedicado en función de la criticidad de la misma. Se entiende por tiempo de resolución el tiempo transcurrido desde que se detecta el problema o incidencia hasta que se da por solucionado.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Se distinguirá entre críticos (parada total), importantes (parada parcial) y básicos (no afecta al servicio).

- El tiempo máximo de resolución de un problema o incidencia crítica será de 2 horas.
- El tiempo máximo de resolución de un problema o incidencia importante será de 4 horas.
- El tiempo máximo de resolución de un problema o incidencia básica será de 36 horas.

La medición se contabilizará para cada problema, no por valores medios.

El tiempo que transcurra entre la decisión de la solución y su implantación, debido a la planificación de ésta en horarios de baja actividad, no contará como tiempo de resolución. En función de la complejidad de la incidencia y especialmente si precisa de la colaboración de terceros (por ejemplo: soporte de fabricante) podrá valorarse por la DGOJ la excepción al cumplimiento de este ANS.

6.7 ANS 7 - Tiempo de respuesta para cambios solicitados por la DGOJ

Se distinguirá entre tipos de cambios básicos, importantes y críticos.

- Se entiende por tiempo de respuesta al tiempo transcurrido entre la realización de la petición de cambio y la asignación de la misma a un técnico para su resolución.

Los tiempos máximo objetivo se recogen en la siguiente tabla

Tipo de cambio	Tiempo de respuesta
Básico	2 horas
Importante	1 horas
Crítico	0.5 horas

El tiempo se contabilizará para cada cambio no por valores medios.

6.8 ANS 8 - Tiempo máximo de ejecución de cambios solicitados por la DGOJ

Se distinguirá entre tipos de cambios básicos, importantes y críticos.

- Se entiende por tiempo máximo de ejecución al tiempo transcurrido desde que se realiza la petición de cambio hasta se indica como realizada/verificada.

Los tiempos máximo objetivo se recogen en la siguiente tabla

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Tipo de cambio	Tiempo Max de Ejecución
Básico	48 horas
Importante	24 horas
Crítico	4 horas

El tiempo se contabilizará para cada cambio no por valores medios.

6.9 ANS 9 - Realización de Copias de seguridad

Se incluirá en el informe el nº de operaciones realizadas y su % de éxito.

El adjudicatario definirá la ventana máxima en la que se deben realizar las operaciones de cada tipo de copia de seguridad en caso de fallo o error de las tareas planificadas.

El objetivo es que finalice con éxito el 100% de las copias de seguridad de tipo "completo" durante un tiempo máximo de un fin de semana.

6.10 ANS 10 - Tiempo de respuesta ante recuperación de datos (restores)

Se distinguirá entre datos críticos y no críticos.

Se contabilizará el tiempo transcurrido desde la petición hasta el comienzo de la operación de recuperación.

El tiempo máximo para recuperación de una copia de respaldo crítico será de 2 horas. El tiempo máximo para recuperación de una copia de respaldo no crítico será de 10 horas.

6.11 ANS 11 - Tiempo de respuesta ante recuperación de máquinas virtuales no replicadas en CPD espejo

Se distinguirá entre máquinas prioritarias (2 días para su puesta en producción en el CPD espejo) y no prioritarias (7 días para su puesta en producción en el CPD espejo).

Se contabilizará el tiempo transcurrido desde la petición hasta el comienzo de la operación de recuperación.

6.12 ANS 12 - Perfiles asignados durante la ejecución

Indicador para la comprobación de que los requisitos de los perfiles profesionales adscritos a la ejecución del contrato son, como mínimo, iguales a los ofertados y tomados en consideración para la adjudicación del contrato al objeto de garantizar el cumplimiento de los requisitos de los perfiles profesionales durante la ejecución del del mismo.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Se comprobará que la experiencia y certificaciones de los perfiles profesionales adscritos a la ejecución del contrato sea mayor o igual que la experiencia y certificaciones de los perfiles profesionales ofertados cuando se produzca algún cambio en los perfiles profesionales adscritos a la ejecución del contrato. En caso de incumplimiento, la revisión del nivel del servicio se realizará con periodicidad quincenal hasta la subsanación del error..

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

ANEXO I. PLATAFORMA TECNOLÓGICA ACTUAL

Dado el periodo temporal existente entre la aprobación del presente pliego y el tiempo de adjudicación del mismo, así como las necesidades cambiantes del órgano gestor, el inventario asociado a los distintos equipos hardware, comunicaciones y volumetrías reflejados en el presente anexo pueden sufrir variaciones, por los distintos licitadores deberán solicitar para la correcta estimación de sus ofertas, los datos actualizados a fecha de inicio del proceso.

Cabe destacar que, asociado al presente pliego, a modo de complemento del ANEXO II, se aporta una tabla descriptiva en formato Excel con los componentes existentes actualmente en la DGOJ, uso que se le da, relación con componente en alta disponibilidad en su caso, CPD en el que reside, etc.

1 Inventario de Equipos

1.1 Servidores

Se proporcionan los datos en el momento de redactar este documento, pero se está en proceso de actualización de las versiones de RedHat a la 8, por falta de soporte de las anteriores. Se puede esperar que el proceso esté terminado para el inicio del servicio. El 85% de las máquinas se encuentran en el CPD primario

Sistema Operativo	**Máquinas**
Red Hat Linux 5	1
Red Hat Linux 6	37
Red Hat Linux 7	8
Red Hat Linux 8	3
Windows Server 2012	8
Windows Sever 2016	5
Windows Server 2019	2
Resto (appliances)	7
TOTAL	**71**

Se resume en la siguiente tabla el total de recursos aproximados en el momento de redactar este documento.

Tipo de recurso	Cantidad	% CPD primario
VCPU	262	82%

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

vMemoria	1075 GB	85%
Disco de rendimiento medio	14 TB	90%
Disco alto rendimiento	3.2 TB	100%

El coste de mantenimiento de los equipos físicos y de la plataforma de virtualización, correrá de cuenta del contratista, siendo el periodo anual y comenzando y terminando con el servicio contratado.

1.2 Backup

Datos actuales de volumen de backup que deberá prestarse sobre las cabinas del adjudicatario:

Concepto	**Espacio en TB**
Espacio ocupado en Backup	35
Espacio diario	3
Espacio semanal adicional staging bbdd	4

1.3 Comunicaciones y seguridad

Es responsabilidad del adjudicatario garantizar las siguientes calidades de servicio:

Descripción	Acceso	Caudal
Conexión entre CPDs		1 Gpbs
Conexión VLAN de la plataforma Big Data (CPD primario) Producción y Pruebas		Dual 10 Gbps

El resto de conexiones (comunicación con la DGOJ de los CPD, con el resto de sedes del Ministerio, de red SARA y salida a Internet) están cubiertas por el Contrato Unificado de Comunicaciones (CUC) gestionado por la Secretaría General de Administración Digital (SGAD) y no son objeto de este contrato.

En cuanto a los elementos de seguridad existentes, se deben proporcionar los siguientes por parte del adjudicatario, a excepción del IDS que es la sonda LUCIA del CCN. Los firewall perimetrales deben ser de distinto fabricante que el firewall interno.

Concepto	**CPD 1**	**CPD 2**
Firewall perimetral	1	1
Firewall interno	1	1
IDS	1	
IPS/WAF	1	1
Balanceadores	1	1

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Firewall perimetral sede DGOJ (2)	n/a	n/a

El coste de mantenimiento de los equipos de seguridad y licencias de software, correrá de cuenta del contratista, siendo el periodo anual y comenzando y terminando con el servicio contratado.

2 Volumetría

2.1 Almacenamiento

Datos aproximados en TB

Uso	Acceso	Categoría	Capacidad	Snapshot	% CPD primario
Staging base de datos	NAS	Disco NAS de alto rendimiento	32 TB	20%	3%
Carpetas compartidas	NAS	Disco NAS de rendimiento medio	24 TB	20%	100%
Replicación carpetas compartidas	NAS	Disco NAS de bajo rendimiento	29 TB	20%	0%
Máquinas virtuales	SAN	Disco SAN de rendimiento medio	14 TB	n/a	90%
Máquinas virtuales	SAN	Disco NAS de alto rendimiento	3.2 TB	n/a	100%
Bases de datos	SAN	Disco SAN de alto rendimiento	85 TB	n/a	50%

2.2 Bases de datos

En la siguiente tabla se pueden obtener una idea de la dimensión de las bases de datos de la DGOJ, a fecha de enero de 2022:

	Interdictos	Inspección
Tablas de usuario	***1.739***	**5.322**
Registros tablas de usuario	**585.510.394**	**256.915.946.294**
Tabla con mayor número de registros	**82.363.053**	**34.383.125.532**
Esquemas de usuario	***72***	**92**
Tablas sistema	***2.068***	**2.850**

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Registros tablas sistema	**51.014.579**	**162.294.406**
Total Tablas	***3.807***	**8.172**
Total Registros	**636.524.973**	**257.078.240.700**
Tamaño de la base de datos *Real* *Asignado*	 **3,589 TB** **3,815 TB**	 **27,189 TB** **31,006 TB**

2.3 Datos tratados diariamente por las aplicaciones de Inspección

Descripción	**Cantidad**
Número de ficheros procesados al día (media)	35.000 ficheros al día
Tamaño de ficheros comprimidos (en MB) al día (media)	120 MB de datos comprimidos al día
Incidencia en base de datos. Crecimiento de base de datos (en GB) al día (media)	12 GB al día (tablas e índices).

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

ANEXO II. SOPORTE Y MANTENIMIENTO DE HARDWARE Y SOFTWARE

1 Soporte hardware

La DGOJ no tiene en propiedad hardware alguno, por lo que el adjudicatario no proveerá servicio de housing. La renovación tecnológica, durante la ejecución del contrato, del conjunto de elementos hardware en los que se sustenta la prestación del servicio, serán asumidos por riesgo y ventura del adjudicatario.

2 Soporte software

Actualmente, la DGOJ se encuentra en proceso de cambio y actualización de paradigma de licenciamiento de ciertas herramientas y soluciones tecnológicas contempladas en los servicios objeto del presente contrato, por lo que el licenciamiento y el soporte no deberá ser asumido por el adjudicatario, mientras que la provisión de equipamiento hardware, así como el resto de servicios asociados si. Las soluciones que licenciará y mantendrá soporte la DGOJ son:

- Vertica: La DGOJ cambiará el modo de licenciamiento a perpetuo basado en nodos y vinculado a dicha adquisición contratará el soporte por la duración del presente contrato.
- Axway: Ante la futura perdida de soporte de la solución existente, la DGOJ cambiara y migrará la solución actual al modelo de suscripción de la versión B2Bi del citado producto. Como ocurriera en el caso anterior, la DGOJ licitará el modelo de suscripción por una duración igual a la ejecución del presente contrato.
- ORACLE: La DGOJ se encuentra en proceso de adquisición de nuevas licencias y su mantenimiento asociado por el mismo periodo de duración que la ejecución del presente contrato. **No así el mantenimiento de las licencias actuales y el servicio avanzado de soporte del producto, que deberán ser soportadas por el adjudicatario, así como la contratación del citado servicio avanzado.**

El conjunto de software a proveer/renovar por parte del adjudicatario será:

PRODUCTO	**CPUs/Users**	**Cores**	**CPUs/Users**	**Cores**	**CPUs/Users**	**Cores**	**CPUs/Users**	**Cores**	***Fecha fin mantenimiento (último día del mismo)***
	Identificadores o entornos		identificadores o entornos		identificadores o entornos		identificadores o entornos		
ORACLE	**CSI 18851592**		**CSI 19218468**		**CSI 19753410**		**CSI 20355012**		
Advanced Security - Named User Plus Perpetual	50	n.a.	50	n.a.	100	n.a.			30/04/2022

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

Advanced Security - Processor Perpetual	4		4						30/04/2022
Database Vault - Named User Plus Perpetual	50	n.a.	50	n.a.	100	n.a.			30/04/2022
Database Vault - Processor Perpetual	4		4						v
Oracle Database Enterprise Edition - Named User Plus Perpetual	50	n.a.	150	n.a.	200	n.a.			v
Oracle Database Enterprise Edition - Processor Perpetual	4		4						30/04/2022
Partitioning - Named User Plus Perpetual			100	n.a.	100	n.a.			30/04/2022
Tuning Pack - Named User Plus Perpetual			200	n.a.					30/04/2022
Tuning Pack - Processor Perpetual			8						30/04/2022
Diagnostics Pack - Named User Plus Perpetual			200	n.a.					30/04/2022
Diagnostics Pack - Processor Perpetual			8						30/04/2022
Oracle Active Data Guard							4		30/04/2022
WBS Agnitio	Ilimitado		ilimitado						30/04/2022
Alfresco Enterprise 6.2	Ilimitado		Ilimitado						30/04/2022

ANEXO III. PLATAFORMA DE MONITORIZACIÓN ACTUAL

La plataforma actual de monitorización se describe a continuación:

- **Monitorización de procesos y componentes en servidores administrados por el proveedor (a grandes rasgos, todas las máquinas virtuales).** Para cada servidor de la DGOJ, se ejecuta periódicamente un conjunto de módulos destinados a recolectar información de métricas técnicas relevantes para la calidad del servicio. Dicha información se centraliza en una herramienta para su representación gráfica y para el envío de alarmas ("warning" y "critical") al sobrepasarse los umbrales o condiciones establecidas para cada módulo. Los módulos se ejecutan periódicamente, tienen asociados textos descriptivos con instrucciones adicionales a seguir para la gestión de las incidencias asociadas (normalmente relativas a escalados a otros grupos técnicos, al envío de correos a determinados destinatarios o a la aplicación de restricciones horarias). En la mayoría de los módulos no está cumplimentado al no necesitar instrucciones adicionales. También hay un timeout asociado a la ejecución del módulo, expresado en segundos. Para la gran mayoría de módulos el valor está establecido a 0 (sin timeout). Todos estos parámetros deben ser configurables. La DGOJ indicará los servidores en los que debe implementarse cada módulo.

  Como módulos estándar se deberá disponer de:
  - Chequeo del sistema de ficheros (NFS): comprobación del montaje, lectura y escritura de los NFS
  - Comprobación de la escritura del NFS en los directorios /documentospro, /ficherosxmlpro, /gesdoc, /var/www/html, con sus diferentes variaciones por entorno (por ejemplo, existen /documentospre y /documentosdes)
  - Chequeos de accesos a DNS desde diferentes servidores a www.google.com y al DNS de Atocha.
  - Chequeo de loops (o número de vueltas por CPU) para verificar el rendimiento del nodo, utilizando histórico y estadísticas
  - Chequeo de Macrolan (comprueba la conexión contra una IP de la Macrolan de cliente)
  - Chequeo de conectividad, conexiones establecidas por puerto 1523 de la base de datos de Oracle
  - Chequeo de robo de CPU
  - Comprobación de porcentaje de espacio libre en disco (/mydb, /mydb/backup, /mydb/log) para los servidores de MySQL y rutas equivalentes en PostgreSQL
  - Chequeo de disponibilidad de Cron, NTP, SSH, Syslog (comprobación si el servicio está activo o no)

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Comprobación de que la interfaz eth0 negocia a fullduplex, su velocidad de negocio, el valor de la velocidad de negocio entrante y la de negocio saliente.
- Chequeo de % de CPU libre
- Chequeo de carga media ("load average", o número de procesos) en los últimos 15 minutos, últimos 5 minutos y último minuto
- Chequeo de número de procesos activos o en ejecución
- Chequeos de % de espacio utilizado de determinados puntos de montaje (a indicar por la DGOJ)
- Chequeo de % de memoria RAM sin usar, % de memoria RAM usada, y memoria RAM total.
- Chequeo de % de memoria SWAP sin usar, % y cantidad de memoria SWAP usada, y cantidad de memoria SWAP total.
- consumo de memoria virtual Java
- ancho de banda de Internet consumido y de salida a Internet
- nº de conexiones de red y nº de conexiones en el servidor de aplicaciones

- Como módulos específicos se tiene:
  - Chequeo de estado de los servicios de Alfresco, Apache, Axway, JBoss, Squash, Tomcat6, Tomcat8-cfx, Tomcat8-des, Tomcat8-plt.
  - Chequeo de los procesos activos de Axway.
  - Chequeo de la descarga de un PDF con Alfresco, desde Apache
  - Comprobación de que la conexión con el Gateway de servicio es correcta
  - Chequeo de conexiones TCP:
    - contra los servidores de base de datos de Oracle
    - contra el servicio de validación de certificados de la FNMT (ocspap.cert.fnmt.es) usando el puerto 80
    - contra el servicio de sellado de tiempo de @firma a través de la Red SARA (tsafirma.redsara.es) usando el puerto 8443
  - Comprobación desde el servidor de aplicaciones de la sede (APSE) y desde Apache de que el servicio Alfresco se encuentra activo
  - Comprobación URL de Alfresco y Share desde el propio nodo por gestión
  - Estadisticas de Alfresco (SoapUI)
  - Monitorización de desconexiones de BBDD para detectar incidencias por corte de comunicaciones con las bases de datos de Oracle. Consiste en buscar la cadena "cerrada: La conexi" en los ficheros de log del Tomcat de la aplicación de gestor de solicitudes. Si en la última media hora apareciera dicha cadena en 10 o más ocasiones se deberá enviar correo al buzón usual de incidencias de la DGOJ, reiniciar el Tomcat en cuestión y truncar el log.
  - Chequeo de conexiones activas de MySQL
  - Chequeo de número de sockets de MySQL establecidos por el puerto de 3306, dando como resultado "critical" en caso de tener 0 conexiones/sockets;

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

"warning" entre 50 y 100 conexiones pues puede suceder que no esté cerrando las conexiones correctamente; "normal" entre 1 y 50 conexiones. Son umbrales consolidados por la experiencia, ya que actualmente tiene entre 15 y 20 conexiones establecidas, pero puede haber excepciones.

- Los chequeos para PostgreSQL se definirán con posterioridad a la implantancción de la plataforma de monitorización, dado que el proyecto es reciente y no se dispone de experiencia en la gestión de esta plataforma
- Chequeo de timestamp del agente utilizado para medir la sincronización NTP entre agente y servidor (diferencia de tiempos entre agente y servidor NTP inferior a un determinado valor)
- Chequeo del estado de índices de SOLR (indexador de Alfresco). Su cometido es verificar que la indexación está funcionando correctamente en el componente SOLR de Alfresco
- Chequeo de login en la aplicación de SSO. Consistirá en logarse en el SSO corporativo (con un usuario de prueba), obtener las cookies, visualizar el listado, pinchar en la aplicación "Consulta de usuarios en el Directorio", que se abra una nueva pestaña y acceder a esa aplicación.
- Tiempo_sonda_SoapUI. Esta monitorización verifica el correcto funcionamiento de Alfresco (crear carpeta, salvar documento de 2Mb, borrar carpeta y documento). Técnicamente recoge el valor de tiempo que tarda en ejecutarse el paso de getFolderidByPath en la sonda SoapUi. Envía alarma cuando la duración completa del test supera los 15 segundos.
- Comprobación de URLs de los aplicativos mediante test.jsp o el framework de la DGOJ (se proporcionará la lista de URLs).
- Chequeo del estado del servicio LDAP.

- **Monitorización de procesos y componentes en servidores administrados por la DGOJ (a grandes rasgos, los servidores de base de datos).** Consiste en la creación de alarmas en base a la ocurrencia de determinados eventos. Las sondas que verifican la ocurrencia de dichos eventos se lanzan periódicamente, variando la periodicidad según la verificación de que se trate (periodicidad que deberá ser configurable). Dichas alarmas se enviarán en forma de correo electrónico con destinatarios los enumerados en una lista de personal de la DGOJ. También se gestiona el envío de un único correo diario de alarma por entorno (PRO y DESA/PRE) con el resumen de los chequeos realizados en los servidores del entorno, así como el detalle de las veces que se ha producido una "lentitud" o "error". Adicionalmente, el resultado de las monitorizaciones se puede chequear mediante un interfaz gráfico, y también se puede modificar la configuración de las mismas. Los ficheros de log que sirven de base a los reportes deberán borrarse en el momento adecuado para no ocupar espacio necesario para los demás sistemas. Las monitorizaciones que se deberán cubrir son:

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- **Monitorización de recursos.** Las validaciones se ejecutan cada 5 segundos, y se envía un correo electrónico a las direcciones especificadas en la validación cuando se verifique la condición de advertencia ("warning") o crítico ("critical"), al sobrepasarse los umbrales establecidos. Mientras se mantenga la condición de advertencia o crítico se mantendrá el envío de correo electrónico, hasta completar un total de 5 envíos (el inicial más 4 repeticiones) momento a parir del cual se dejará de enviar correos aunque continúe vigente la condición de advertencia o crítico. Tipología de monitorizaciones:
  - Uso de CPU
  - Llenado de sistemas de ficheros:
    - Sistemas Linux de Oracle (/, /Oracle/product/oradata y /var). Responden a la situación de llenado del sistema de ficheros de Oracle y la consiguiente parada de la base de datos, en el sentido de estar levantada pero sin poder aplicar más transacciones ni proporcionar nuevas conexiones hasta que libere espacio para archivado.
    - Sistemas Linux del cluster BI (/sasdata/DDS en el servidor de Data Management).
    - C: en sistemas Windows.
  - Ocupación de Swap
  - Ocupación de Memoria
  - Verificación de:
    - Procesos en ejecución (cron, sshd, syslog, xinetd…). Se envía alarma si el proceso no está activo.
    - Servicios en ejecución (EventLog, LanManServer, W32Time). Se envía alarma si el servicio no está activo.
  - Chequeo de conectividad con direcciones IP. Se envía alarma si la IP no está accesible (la DGOJ indicará las IPs a monitorizar)

- **Chequeo del rendimiento de CPU:** se medirá el rendimiento del conjunto de CPUs (ejecutando un programa de benchmarking, 1secbench, que durante un segundo se ejecuta en todas las CPU a la vez con máxima prioridad teórica como "nice -20") y se dividirá por el número total de CPU. Si el valor es inferior a 200 (valor deducido de la experiencia) se genera la correspondiente alarma por "lentitud", obteniendo una medida de degradación del rendimiento.

- **Chequeo de conectividad y rendimiento con direcciones IPs:** Para la IP de su servidor de base de datos pareja de Data Guard se ejecutará un ping con un bloque de 8 KB y 5 repeticiones. Si la duración del mandato es superior a 5 s o el porcentaje de paquetes perdidos es superior al 20% se generará la correspondiente alarma de "lentitud". Si el mandato ha finalizado en "error" (lo

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

que incluye el caso de pérdida del 100% de paquetes) se generará la correspondiente alarma de "fallo". Solo se aplica a los servidores de base de datos que forman parte de un Data Guard.

- **Chequeo de acceso y rendimiento a sistemas de ficheros (NFS):** Para cada sistema de ficheros NFS verifica que es posible escribir y borra un fichero de 8 Mb. Si la duración del mandato es superior a 5 segundos se generará la correspondiente alarma de "lentitud". Si el mandato ha finalizado en "error" se generará la correspondiente alarma de "fallo".

- Monitorización hardware de los servidores físicos, con aviso al proveedor para que trate la incidencia directamente con el soporte de hardware que tenga contratado. Los envíos de correo se hacen desde el servidor SNMP implícito en las tarjetas ILO.

- **Chequeos de salud y reglas de correlación sobre los servidores que soportan los cortafuegos perimetrales e internos, balanceadores, IPS y OSSIM Alienvault.** Se realizarán chequeos de salud periódicos de los distintos componentes, y mediante reglas se hará una correlación de los resultados obtenidos para generar alertas de seguridad en el software de correlación. Cada chequeo de salud lleva asociados un umbral para categorizar el resultado como "warning" y otro para categorizarlo como "critical".

  Como chequeos de salud que se están realizando, tenemos los siguientes:
  - Cortafuegos perimetral:
    - Estado del servicio SNMP del máster de Checkpoint de la arquitectura pasivo/activo.
    - Tiempo que ha pasado desde el último reinicio el sistema.
    - Uso de memoria principal (RAM).
    - Uso de los buffers de memoria.
    - Espacio libre en disco.
    - Memoria disponible en 32bits y 64 bits
    - Número de procesos de la máquina.
    - Número de conexiones SNMP.
    - Porcentaje de uso de la memoria SWAP.
    - Comprobación de los métodos de sincronización.
    - Para cada una de las interfaces eth1, eth2, eth3.1635, eth3, Mgmt:
      - Comprobación de que la interfaz esté funcionando.
      - Comprobación de que el número de paquetes descartados en la interfaz no pasa de un umbral establecido

- Comprobación de que el número de errores en la interfaz no pasa de un umbral de riesgo
- Comprobación del número de interfaces activas en ese momento.
- Chequeo auxiliar de OPSVIEW que habilita los chequeos de las interfaces.

- Cortafuegos interno:
  - Estado de la interfaz
  - Tiempo desde el ultimo reinicio
  - Comprobación cuando se ha producido un balanceo.
  - Comprobación de la disponibilidad del acceso vía HTTPS y SSH
  - Para cada uno de los dos nodos:
    - Número de sesiones establecidas concurrentemente en el nodo
    - Comprobación de que la CPU no esté muy cargada en el nodo
    - Comprobación de que no existe un exceso de memoria principal (RAM) utilizada en el nodo.
- Balanceador:
  - Comprobación de que funcionan las interfaces 1.1, 1.2, 1.3, 1.4, mgmt
  - Estado del máster de Checkpoint de la arquitectura pasivo/activo.
  - Tiempo que ha pasado desde el último reinicio del sistema.
  - Comprobación de que no sobrepase el nivel de carga de CPU especificado medio en 1, 5 y 15 minutos.
  - Comprobación de nivel de carga de la memoria RAM y SWAP.
  - Comprobación del espacio ocupado de la memoria SWAP.
  - Comprobación de que el número de procesos se encuentra entre un umbral mínimo y máximo establecido.
  - Comprobación del número de interfaces activas en ese momento.
  - Comprobación de las conexiones activas que tiene abiertas en un momento determinado el balanceador.
  - Chequeo auxiliar de OPSVIEW que habilita los chequeos de las interfaces.
- IPS:
  - Tiempo desde el último reinicio.
  - Comprobación de que no sobrepasa el nivel de carga de CPU especificado medio en 1, 5 y 15 minutos.
  - Comprobación de que el nivel de carga de la memoria RAM y SWAP no sobrepasa los umbrales.
  - Número de procesos de la máquina.
  - Comprobación de que el número de procesos de cron, monit, rsyslog, snmp y ssh estén en el rango del umbral.
  - Comprobación de memoria usada en la partición / y /var
  - Comprobación del número de conexiones TCP activas.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Comprobación del número de interfaces activas en ese momento.
- Comprobación de que la interfaz 1 y 2 están funcionando.

- OSSIM Alienvault:
  - Relacionados con con la administración de eventos de seguridad (correlación de logs)
    - Comprobación de si existe un tiempo anómalo sin alarmas en el correlador.
    - Comprobación de que el número de procesos de las siguientes tipologías estén en el rango del umbral correspondiente:
      - Procesos activos de la base de datos de Alienvault (mysqld)
      - agente de Alienvault (agent),
      - interfaz gráfica de Alienvault (apache)
      - framework de Alienvault (framework)
      - monitor que aseguran que los procesos se levanten (monit)
      - recepción de logs en el correlador (rsyslog)
      - servidor del correlador (server)
      - snort eth24 y snort eth30
    - Comprueba que el número de procesos total no sobrepase el umbral (runaway processes)
    - Comprueba que la memoria no sobrepase el nivel de carga de memoria especificado medio en 1, 5 y 15 minutos.
    - Carga de memoria de la máquina.
    - Carga de la memoria swap (encolamiento de procesos).
    - Uso de las particiones /, /usr, /var
    - Chequeo auxiliar de OPSVIEW que habilita los chequeos de las interfaces.
    - Comprobación de que las distintas interfaces están activas
    - Para las distintas interfaces eth0, eth1, eth2, eth3, eth4, eth5, io:
      - Comprobación de que la interfaz está funcionando
      - Comprobación de que el número de paquetes descartados en la interfaz no pasa de un umbral establecido.
      - Comprobación de que el número de errores en la interfaz no pasa de un umbral de riesgo.
    - Reinicio automático si se sobrepasan la carga del SWAP el 50% y RAM 80%
    - Comprobación de que está funcionando el agente SyMoN.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Comprobación de correcta recepción de logs de Checkpoint, balanceador F5 (134 y 217), WAF Imperva, enviados con syslog y directorio activo (snare)

Como reglas de correlación, se han de ofrecer las siguientes directivas:

- Tecnología FW (cortafuegos)
  - Conexiones de un usuario no esperado a VPN.
  - Múltiples intentos de autenticación sobre la VPN con un mismo usuario desde varias direcciones IP o desde la misma IP
  - Múltiples intentos de autenticación sobre la VPN (distintos usuarios) desde una misma IP.
  - Múltiples intentos de autenticación fallidos sobre la VPN con un acceso exitoso a la plataforma desde una misma dirección IP.
  - Intento de descubrimiento de puertos desde un mismo host.
  - Múltiples conexiones sobre diversos puertos desde una misma dirección IP sobre una IP concreta.
  - Intento de descubrimiento de equipos en la red corporativa desde mismo host.
  - Virus que hagan gran cantidad de conexiones de host interno a webs listadas en baja reputación, o de hosts internos a una web listada en baja reputación.
  - Host interno infectado que hagan gran cantidad de conexiones a host publico o públicos (no webs) listado en baja reputación.
  - Gran cantidad de conexiones desde un host a un puerto de una misma máquina
  - Host que realiza peticiones DNS a servidores públicos.
  - Host que realiza peticiones DNS a servidores públicos de baja reputación.
  - Múltiples peticiones NTP entre servidores internos
  - Intentos de autenticación sobre el servicio VPN.
  - Cambios en el FW por un usuario.
  - Conexiones sobre puertos de propagación de malware.
  - Múltiples intentos de autenticación.
  - Multitud de bloqueos en el FW.
  - Peticiones a host públicos sobre el servicio DNS.
  - Peticiones a host públicos de baja reputación sobre el servicio DNS.
  - Host realizando conexiones sobre muchos puertos distintos de una máquina corporativa.
  - Escaneo de servicios desde un host externo a otro interno en poco tiempo.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- Conexiones de un host sobre múltiples máquinas en poco lapso de tiempo.
- Conexiones desde un host corporativo hasta los servicios http y https de múltiples hosts maliciosos.
- Conexiones desde un host corporativo hasta servicios https y https de un host público malicioso.
- Conexiones desde un host corporativo hasta servicios que no sean http y https de múltiples hosts maliciosos.
- Conexiones desde un host corporativo hasta servicios que no sean http y https de un host público malicioso.
- Conexiones de un equipo a un puerto concreto de múltiples máquinas en poco tiempo.
- Conexiones de un equipo sobre servicio DNS de múltiples equipos.
- Conexiones de un equipo sobre servicio DNS de múltiples equipos maliciosos.
- Conexiones a puertos sospechosos de virus.
- Equipo y usuario que deshabilita un virtual domain.
- Detección de multitud de conexiones de un mismo usuario sobre varias máquinas sin respuesta.
- Detección de fallos en un sistema de balanceo.
- Conexiones de un host sobre múltiples servicios de otro host.

o Tecnología IDS (detección de intrusiones)

- Búsqueda de consultas erróneas sobre usuarios en BBDD.
- Detección de un host no autorizado realizando conexiones a otros hosts.
- Detección de conexiones sobre un servicio no autorizado.
- Ataque de fuerza bruta desde un host interno.
- Ataque de fuerza bruta desde un host externo.
- Detección de bloqueo del IPS.
- Uso de diversas aplicaciones desde un host a otro.
- Intentos de login desde un mismo host con más de 5 usuarios distintos.
- Detección de varios eventos de seguridad diferentes desde una misma máquina.
- Detección de un mayor número de eventos de seguridad diferentes desde una misma máquina.
- Detección de varios eventos de seguridad desde una web calificada por Imperva como maliciosa.
- Múltiples eventos web (not found, SQLi, XSS, etc)
- Detección de transferencia de contraseñas sin cifrar.
- Detección de vulnerabilidades en:
    - la red del cliente, gestionada por DGOJ.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- la red del cliente, gestionada por el proveedor.
- la red del cliente.

- Detección de múltiples eventos distintos de seguridad leves/graves desde un host sobre un host/múltiples hosts.
- Detección de inyecciones de código desde un host sobre una web corporativa.
- Detección de ataques contra servicios de correo corporativo.
- Detección de una gran cantidad de peticiones por segundo al DNS con el mismo origen, que podría tumbar el servicio.
- Detección de inyección de código desde un host externo sobre un servidor web corporativo.
- Detección de escaneo de puertos de hosts corporativos desde un host interno o externo.
- Detecta múltiples conexiones sobre el servicio TELNET de una máquina corporativa.
- Detección de intentos fallidos de autenticación sobre servicio NetBIOS desde un host sobre una o varias máquinas.
- Detección de múltiples intentos de autenticación sobre servicios FTP desde un host interno o externo.
- Detección de múltiples intentos de autenticación sobre servicios FTP desde un host externo.

- **Monitorización de conmutaciones del balanceador F5.** Envío de correo a una lista de destinatarios cada vez que se detecte la conmutación del balanceador de un nodo al otro. Posibilidad de configurarlo en modo “preempt” para que el servicio vuelva al nodo “activo” tan pronto como sea posible.

- **Monitorización de las comunicaciones extensión de la LAN** (p.ej. la comunicación entre el CPD1 y el CPD2; no solo caudal y acceso, sino también que las conexiones que se abren entre ambos no sufren cortes). Se enviará un correo en caso de que se produzca algún tipo de corte.

- **Monitorización del servicio de acceso remoto por VPN-SSL.**

- **Monitorización del tiempo de acceso a los recursos de ficheros en red.** Generación y gestión de las oportunas alarmas

- **Monitorización de certificados.** La DGOJ dispone de un proceso de verificación de la caducidad de los certificados de entidades externas utilizados por las aplicaciones de la DGOJ para requerir servicios de intermediación, de firma y de marcas de tiempo. Este proceso de lanza periódicamente sobre la totalidad de los certificados,

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

independientemente de la máquina donde se utilicen y consolidad en un único log la información de los certificados y su fecha de caducidad, con un mensaje de advertencia sobre aquellos que están próximos a caducar. La plataforma de monitorización del adjudicatario deberá recopilar esta información a través de un agente y emitirá las alertas correspondientes.

- **Monitorización específica de base de datos:**

    - **Instancias levantadas de base de datos**
    - **Monitorización de llenado de tablespaces de instancias de Oracle.** Debido al gran volumen de información que se carga diariamente en la base de datos que soporta la aplicación NAIPE, es frecuente que los tablespaces se queden rápidamente sin espacio, con la consiguiente pérdida de transacciones cuando se da esta situación. Una alerta que avise del pronto llenado de alguno de los tablespaces (p.ej. cuando se supere determinado umbral) es de mucha utilidad para que el personal encargado pueda anticiparse al llenado y extenderlo convenientemente.
    - **Monitorización del porcentaje de espacio ocupado en la base de datos HP Vertica** (% sobre la capacidad permitida por la licencia adquirida).
    - **Monitorización de rendimiento de la base de datos y acceso a la infraestructura SAN.** Consistiría en la ejecución de una consulta simple (tipo "count") para detectar posibles problemas en base de datos y acceso a los discos SAN que la soportan.
    - **Monitorización de las consultas más pesadas, esperas a recursos, bloqueos**.
    - **Monitorización de los procesos de negocio significativos de la DGOJ ejecutados en los servidores de base de datos.** Se han definido una serie de procesos de negocio batch, que escriben en un fichero de log (en formato syslog) mensajes estandarizados con su fecha de inicio y fecha de fin, cada vez que tiene lugar su ejecución. El script de monitorización lee dicha información, y verifica si los procesos han finalizado correctamente. En caso negativo, genera la correspondiente alarma y envía un correo a una lista de destinatarios. Los procesos de negocio son:
        - ALARMAS_DIARIAS_SVJ : Proceso diario de alarmas de control del uso de los operadores de juego del servicio de verificación de jugadores.
        - CARGA_BBDD_INSPECCION_DIARIO : Proceso diario de carga de datos a la base de datos de inspección de los datos de GOPER (jugadores consultados, peticiones de verificarCambiosRGIAJ, datos de la tabla de cambios rgiaj, menores, cacheo de menores) y de RGIAJ y RPVO.
        - CARGA_CACHEO_MENORES: Proceso diario que carga la tabla de posibles menores para ser posteriormente tratados por el proceso de comprobación de menores.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

- COMPROBACIONES_SVJ : Proceso semanal que realiza una serie de comprobaciones sobre los accesos el servicio de verificación de jugadores (operadores que han llamado a la operación de baja y/o realizado peticiones de verificación de identidad enviando número de soporte) y relación de los operadores que están exentos de alguna de las alarmas
- ESTADISTICAS_DIARIAS_SVJ: Proceso diario de estadísticas de peticiones al servicio web de verificación de jugadores y de los jugadores consultados.
- PROCESO_MENORES: Proceso diario que consulta al SCSP para comprobar posibles menores.
- SYSLOG_OSSIM_APSEC: Proceso que lee los logs generados por el correlador de eventos y extrae los eventos que son de interés para la aplicación de gestión de perfiles y usuarios.
- ETL_LOG_CENTRAL de la Plataforma de Big Data: es un fichero de log generado por los procesos de carga desde NAIPE a HP Vertica, con los datos de todos los procesos de ETL en ejecución o ejecutados. Se encuentra en la máquina virtual donde reside el proceso ETL de la Plataforma de Big Data.
- Salvo el último proceso, que incumbe a HP Vertica y se sitúa en la máquina virtual que ejecuta la ETL, los demás procesos se generan desde la base de datos de Oracle.

- **Operaciones de back-up exitosas y fallidas,** incluyendo información de tipo, hora de comienzo, hora de fin y tamaño de la cantidad de la que se ha hecho back-up. Ocupación de espacio de back-up.

- **Monitorización de las páginas o subpáginas Web públicas de la DGOJ mediante un sistema dual (haciendo uso de dos herramientas):** con esta orientación se pueden detectar incidencias en situaciones excepcionales de fallo de una de las herramientas, y asimismo mejora la sensibilidad de la detección de incidencias al no coincidir los instantes en que ambas herramientas ejecutan sus monitorizaciones. Según el origen de lanzamiento de las sondas, distinguimos:

    - **Desde ubicaciones nacionales:** Desde varias ubicaciones distribuidas por el territorio nacional, un conjunto de sondas de negocio (llamadas a las URL de la DGOJ accesibles desde Internet) son lanzadas desde una herramienta de monitorización cada cierto período de tiempo. En el caso de que la ejecución de una sonda determinada falle para todas las ubicaciones a la vez, se producirá el envío de la correspondiente alarma al Command Center del proveedor para que

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

éste gestione, con todos los grupos técnicos necesarios, su priorización, diagnóstico, notificación y resolución en el menor plazo posible.

- **Desde ubicaciones pertenecientes a otros países.** Desde varias ubicaciones distribuidas por el mundo, se lanzan sondas consistentes en llamadas a las URL públicas de la DGOJ desde una herramienta de monitorización cada cierto período de tiempo. Desde agentes de dicho servicio se ejecuta cada 1' (en caso de monitorizaciones sencillas y descarga de ficheros) o cada 5' (en caso de monitorizaciones basadas en navegaciones complejas, que quizás no puedan efectuar acceso con certificado). Si se produce un fallo en la ejecución de una determinada sonda, la herramienta reintenta la monitorización desde otra ubicación. En caso de fallar una monitorización durante 3 minutos (monitorizaciones sencillas y descarga de ficheros) o durante 5' (monitorizaciones basadas en navegaciones complejas), se producirá el envío de la correspondiente alarma al centro del control para que éste gestione, con todos los grupos técnicos necesarios, su priorización, diagnóstico, notificación y resolución en el menor plazo posible.

Existen varias categorías de monitorización, clasificados según su complejidad:

- Monitorización sencilla de páginas Web, verificando simplemente que es posible acceder a la página en cuestión.
- Monitorización de secuencias de acciones contra páginas Web, realizando una navegación, más o menos compleja, que simule el comportamiento de consultas realizadas por los usuarios. En algunos casos, será necesaria la autenticación mediante certificado electrónico o usuario/contraseña (para lo cual se hará uso de un usuario de tipo "pruebas")
- Monitorización de descarga de ficheros desde una página Web.

La DGOJ indicará al proveedor las páginas/subpáginas Web a monitorizar. Se enviará un SMS a una lista de destinatarios de la DGOJ en caso de incidentes de una cierta severidad en adelante.

También se deberá monitorizar:

- el número de visitas a las páginas públicas en Internet
- tiempos de respuesta y tiempos de carga de las páginas web y de sus contenidos.

- **Monitorización de aplicaciones internas de la DGOJ y servicios web**:
  - **Estado**: las aplicaciones de la DGOJ están diseñadas de tal forma que presentan accesible una URL que recopila la información necesaria para conocer el estado de la aplicación y de los componentes de los que hace uso. La plataforma de

monitorización del adjudicatario deberá recopilar esta información a través de un agente que sondeará las URLs de cada aplicación de la casa y mostrarla gráficamente.

- **Rendimiento y degradación del servicio:** Se trataría de sondas que accederían a las aplicaciones críticas de la casa y realizarían una navegación como usuario gestor (p.ej. acceder al gestor de solicitudes, elegir una solicitud y abrirla; o abrir el gestor de expedientes, seleccionar un documento y abrirlo). Si tardara más de un número determinado de segundos, se generaría una alerta, porque significaría que hay algún problema con el rendimiento. En resumen, este apartado consiste en sondas que detecten y midan la posible degradación en el rendimiento de las aplicaciones internas.
- **Monitorización de servicios web externos de la DGOJ.** Se dispone de un servicio web propio de la DGOJ para verificar el estado de los servicios web externos de la DGOJ, que son especialmente críticos: si no se recupera en cinco minutos, y sobre todo si fallan los dos servidores a la vez, los operadores de juego y jugadores en plataformas on-line acusan el impacto de no poder desarrollar actividad de juego. La DGOJ considera imprescindible poder contar con esta monitorización desde herramientas distintas para aumentar la fiabilidad en la detección de situaciones anómalas.

  Monitorización de aplicaciones web y servicios web internos de la DGOJ. Se dispone de un servicio web propio de la DGOJ para verificar el estado de las aplicaciones interno y de los servicios web internos de la DGOJ, así como de los recursos utilizados por los mismos (BBDD, sistemas de ficheros, ldap …). Este servicio web se invoca periódicamente y se lanza las alertas correspondientes. El servicio tiene capacidad para analizar la situación de aplicaciones que ruedan en dos nodos estableciendo distintos niveles de alerta según falle uno de los dos nodos o los dos.

dgoj.dgeneral@ordenacionjueg.gob.es

C/ ATOCHA 3
28012 - Madrid
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36