Pliego de prescripciones técnicas para la contratación de un «SERVICIO DE UN CENTRO DE CONTINGENCIA»

ÍNDICE

1. Objeto del contrato

El objeto del contrato es la prestación al Consejo de Seguridad Nuclear (en adelante CSN) de un servicio de un centro de contingencia (en adelante CCON) que albergue los datos y servicios críticos del CSN y permita la continuidad de las actividades del organismo en caso de pérdida o indisponibilidad de su centro de proceso de datos principal, conforme a las prescripciones de este pliego.

2. Descripción de las prestaciones

2.1. Alcance

Los servicios solicitados en este pliego incluyen la **provisión, puesta en servicio, explotación, gestión, monitorización, mantenimiento, pruebas y activaciones** de todos los elementos constituyentes del CCON, incluyendo el equipamiento, los programas, las líneas de comunicaciones, el soporte técnico y los demás servicios descritos en este pliego, así como su documentación, garantizando en todo momento su plena operatividad. Las condiciones señaladas en el presente pliego deberán mantenerse durante todo el período de vigencia del contrato.

2.2. Servicios críticos del CSN

Se consideran críticos, entre otros, los servicios siguientes:

- El correo electrónico, tanto interno como externo, el acceso *http* al correo, y el correo para dispositivos móviles.
- Los servicios de ficheros, tanto de archivos corporativos o de usuarios como los de las aplicaciones corporativas.
- Las aplicaciones «web» corporativas.
- Las aplicaciones «web» en Internet, incluyendo el «back office» y el acceso a las bases de datos en el CCON.
- El sistema documental.
- La Intranet corporativa.
- Los servicios básicos del dominio, el directorio activo, etc.

En el **Anexo** se ofrece la descripción de estos servicios y de la plataforma tecnológica del CSN a respaldar en el CCON. Por razones de confidencialidad, el Anexo se facilitará previa petición formal del licitador dirigida al Servicio de Contratación y Convenios del CSN.

2.3. Configuración del centro de contingencia

2.3.1. Centro de servicios gestionados

El servicio de un centro de contingencia se prestará en un centro de servicios gestionados del adjudicatario donde este proveerá una infraestructura, tanto de equipos como de programas,

para el centro de contingencia del CSN. El centro de servicios gestionados del licitador deberá cumplir los requisitos técnicos de TIER III o superior.

El centro de servicios gestionados deberá encontrarse en territorio nacional. Los licitadores deberán indicar en sus memorias técnicas la ubicación del centro de datos desde el que se prestará el servicio. Los datos, aplicaciones y servicios del CCON del CSN deberán albergarse exclusivamente en dicho centro. En ningún caso se admitirá la utilización de una infraestructura de terceros o externa a aquel, salvo para operaciones de copia de seguridad, siempre que el adjudicatario sea titular y responsable de esta infraestructura, opere bajo su directo y exclusivo control y se encuentre en territorio nacional.

El CSN dispone de datos críticos amparados por la LOPD que se albergarán en el CCON. Los licitadores deberán contar con los medios que les permitan cumplir la normativa de protección de datos.

Las memorias técnicas describirán detalladamente el centro de servicios gestionados del licitador destinado a prestar este servicio.

2.3.2. Infraestructura del centro de contingencia

El adjudicatario proporcionará una infraestructura de hardware y software para el CCON del CSN en su centro de servicios gestionados. La infraestructura propuesta deberá ser adecuada y suficiente para satisfacer plenamente los requisitos expresados en este pliego, siempre de acuerdo con las mejores prácticas del mercado, y deberá basarse en la infraestructura y las tecnologías existentes en el CSN descritas en el Anexo.

El adjudicatario proporcionará asimismo la infraestructura de hardware y software adicional que sea necesario instalar en los equipos, los sistemas o el CPD del CSN para que la solución propuesta sea completamente operativa.

Los servidores que el CSN tenga ya virtualizados o que sean susceptibles de ser virtualizados podrán replicarse y activarse en el CCON en plataformas virtuales, siempre y cuando ambas plataformas de virtualización sean compatibles. La plataforma de virtualización propuesta deberá estar dimensionada suficientemente para permitir el crecimiento del número máquinas virtuales replicadas y el aumento de sus recursos.

Los servidores que deban ser respaldados físicamente lo serán por servidores compatibles con ellos al menos a nivel de sistema operativo, y dispondrán de una configuración de hardware suficiente para, en caso de contingencia, garantizar un funcionamiento fluido de las aplicaciones de negocio del CSN para el número mínimo de usuarios al que hace referencia del apartado 2.4.2. Se admiten servidores INTEL-LINUX, UNIX o SOLARIS para soportar la base de datos.

La infraestructura de servidores físicos o virtuales estará dedicada al CCON del CSN, y será monitorizada de forma continua para detectar y resolver, de forma proactiva, fallos en los componentes.

2.3.3. Licencias de software

El adjudicatario proporcionará todas las licencias de los sistemas operativos y demás productos de software necesarios para la puesta en marcha y el correcto funcionamiento de infraestructura de la plataforma de contingencia, así como su mantenimiento.

Las licencias de los sistemas operativos y demás productos, dependiendo de la solución (VMWare, Windows, Exchange, EMC, etc.), y sus contratos de mantenimiento, están incluidas en el alcance del contrato. Las licencias de EMC y Exchange deberán ser nominativas del CSN. El adjudicatario será responsable de la instalación, configuración, mantenimiento y actualización de estos programas, de forma coordinada con el CSN.

No obstante lo anterior, el CSN proporcionará las licencias del RDBMS Oracle Database Enterprise Edition (DBEE), del servidor de aplicaciones «web» Oracle Web Logic (WLS) y del gestor documental Oracle WebCenter Content (WCC, antiguo UCM), todas ellas para un procesador. El adjudicatario también deberá correr con la instalación y configuración de este software, así como con su actualización.

2.3.4. Líneas de comunicaciones

El adjudicatario proporcionará las líneas de comunicaciones necesarias para la solución y, en particular, las siguientes:

1) Una línea de comunicaciones que interconecte el CPD principal del CSN y el CCON que permita la réplica de los datos en una configuración Activo-Pasivo, según el esquema de la Figura 1. Dicha línea deberá estar gestionada y monitorizada por el prestador del servicio. Las comunicaciones por esta línea deberán ser cifradas. Se valorará el caudal de esta línea de comunicaciones.

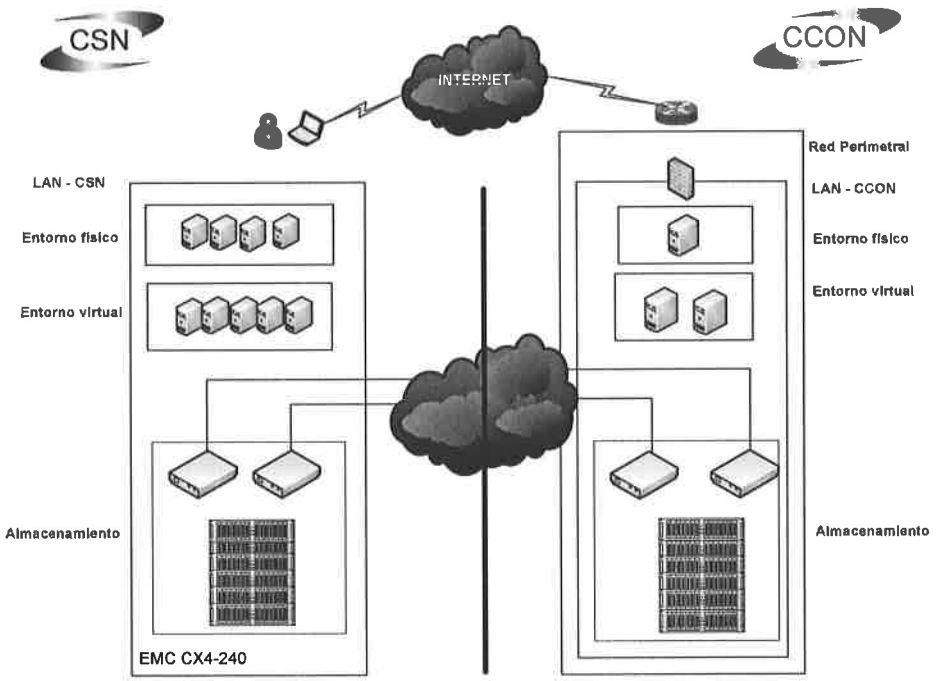

Fig. 1. Esquema básico

2) Una línea de comunicaciones segura de un caudal mínimo garantizado de 4 MB desde el CCON hasta el portal de Internet y sede electrónica del CSN, donde residen sus

aplicaciones corporativas en Internet. El portal del CSN se encuentra alojado en las instalaciones y en los sistemas de un proveedor de servicios de alojamiento «web».

El CCON se comunicará con el centro de contingencia de la Sala de Emergencias del CSN (SALEM-2), instalada en el cuartel general de la Unidad Militar de Emergencias en Torrejón de Ardoz (Madrid), mediante una línea de comunicaciones proporcionada por un proveedor de servicios de comunicaciones en el marco de otro contrato. El adjudicatario facilitará la instalación y alojamiento en su centro de servicios gestionados del equipamiento necesario para habilitar este enlace y prestará el soporte necesario para el encaminamiento de las comunicaciones entre la red del CCON y la SALEM-2.

2.3.5. Red local

La red de área local que interconecte los equipos que configuren la infraestructura del CCON del CSN deberá tener una calidad mínima de 1 GB. Deberán definirse en ella, al menos, cuatro VLAN: usuarios finales, Internet, DMZ, servidores y gestión del CSN.

El adjudicatario facilitará direccionamiento público accesible por Internet y direccionamiento privado para la red del CCON, que podrá ser simétrico al CPD primario.

Los equipos de comunicaciones utilizados no tendrán por qué ser dedicados al CSN.

2.3.6. DNS

El adjudicatario deberá proveer un DNS externo que dé servicio los servidores y servicios del CCON en caso de activación. Correrá a su cargo la configuración del DNS del CCON.

2.3.7. Solución de replica

Las soluciones proporcionadas por el adjudicatario para la réplica de datos, bases de datos, correo, servidores, etc., deberán estar basadas en herramientas automatizadas de soluciones comerciales solventes y contrastadas de las plataformas utilizadas en el CSN (EMC, Oracle, VMWare y Microsoft).

Las memorias técnicas deberán describir detalladamente la solución de réplica adoptada entre las cabinas de almacenamiento (equipos, programas, procedimientos de sincronización y re-sincronización para cada tecnología, monitorización de las réplicas de máquinas y datos, actuaciones previstas en caso de error, etc.), así como las adoptadas, en su caso, para servicios o programas concretos.

La licencia de uso de réplica de datos que forme parte de la solución ofertada contemplará una capacidad mínima de 6 TB. El número de servidores, LUN, instancias de bases de datos, etc., a respaldar no estará limitado.

La solución de réplica propuesta deberá satisfacer los requisitos expresados en el apartado 2.4.3 y los ANS definidos en el apartado 4 de este pliego.

Se valorará la calidad de la solución de réplica propuesta.

2.3.8. Solución de correo

El CSN dispone de dos salidas a Internet, una a través de Red Iris, a través de la cual recibe servicio de DNS y correo electrónico, y otra a través de un proveedor de servicios de acceso a

Internet, teniendo implantada una solución «multihoming» para evitar la pérdida de alguno de los servicios en caso de indisponibilidad de uno de los accesos a Internet.

La solución técnica propuesta deberá estar diseñada para evitar la pérdida de correos del CSN en caso de activación real o de pruebas del CCON. El licitador describirá con detalle la solución propuesta. Adicionalmente, la solución deberá contemplar la prestación de un servicio antivirus y «antispam» para el correo entrante y saliente tanto del CSN como del CCON. Este servicio se dimensionará para un mínimo de 1000 buzones de correo.

2.3.9. Despliegue de las aplicaciones de negocio

El CSN será responsable del despliegue inicial de las aplicaciones de negocio y de cualquier cambio en su configuración que surja posteriormente.

Entra dentro del alcance del contrato los servicios profesionales que la empresa adjudicataria deberá disponer para prestar soporte a los técnicos del CSN en las operaciones de despliegue y pruebas de las aplicaciones de negocio.

2.3.10. Valoración global de la solución

Las memorias técnicas describirán detalladamente el equipamiento propuesto: número de equipos, marca, modelo y configuración; software empleado; cabina de almacenamiento de datos, etc. Asimismo describirán detalladamente la topología de red y sus características; equipos de red, dedicados o compartidos; medidas de seguridad, monitorización, servicios y demás elementos de la solución ofertada, etc.

La solución ofertada deberá ser completa, y alcanzará tanto a los elementos a instalar en el centro de servicios gestionados del licitador como en el CPD y las instalaciones del CSN. En ningún caso la solución ofertada obligará al CSN a ampliar sus sistemas o adquirir programas. Será a cargo del adjudicatario la provisión de cualquier elemento no previsto o no incluido en su oferta que sea necesario para que la solución propuesta funcione correctamente, o la sustitución de aquellos elementos que, habiéndolo sido, sean inadecuados.

Se valorará la calidad de la solución propuesta.

2.4. Activación del centro de contingencia

2.4.1. Activación del centro de contingencia

El servicio comprenderá la eventual activación del CCON y su mantenimiento durante el tiempo en que la activación se mantenga, así como las pruebas de activación periódicas para verificar su plena operatividad.

La indisponibilidad total o parcial del CPD principal del CSN que dé lugar a una activación real del CCON podrá deberse tanto a catástrofes naturales, siniestros, sabotajes, actos terroristas, etc., como a intervenciones en aquél de cualquier naturaleza que causen indisponibilidad de los servicios. Se considerará la posibilidad de que haya más de una contingencia anual dentro del alcance del contrato.

En caso de contingencia que dé lugar a la activación real del CCON, éste permanecerá activado durante el tiempo máximo continuo de uso al que se refiere el apartado 2.4.3. Si, por cualquier causa, la duración de la activación hubiere de superar el tiempo máximo continuo de uso

ofertado, el adjudicatario se comprometerá a seguir prestando servicio hasta el cese de la contingencia. En tal caso, el CSN y el adjudicatario acordarán, con la debida antelación, la solución a aplicar. Las ofertas deberán detallar el coste adicional, por día, de funcionamiento del CCON en estas condiciones.

La activación del CCON se efectuará a petición del CSN, por medio de una notificación de emergencia, y podrá conllevar operaciones de tipo manual y automáticas (centro frío). La notificación se efectuará siguiendo el procedimiento y por los canales previamente establecidos entre el adjudicatario y el CSN. El adjudicatario deberá disponer de atención telefónica de 24x7, todos los días del año para la activación del CCON.

El adjudicatario deberá poner en marcha los procedimientos de activación del CCON en un plazo máximo de **30 minutos** contados a partir de la notificación de emergencia. Se valorarán tiempos menores.

El adjudicatario deberá asignar los recursos técnicos y humanos necesarios para la puesta en marcha del CCON como centro de producción del CSN en el plazo a que se refiere el apartado 2.4.3.

En caso de activación del CCON, el adjudicatario activará la línea de comunicación entre el «web hosting» del CSN y el CCON. El CSN correrá con la reconfiguración de las comunicaciones en el «web hosting» de forma que las aplicaciones de los servicios al ciudadano puedan utilizar la base de datos del CCON en lugar de la del CPD principal.

Una vez activado el CCON, la empresa adjudicataria deberá garantizar la seguridad de su funcionamiento mediante los procedimientos habituales establecidos al efecto: cortafuegos, «antispam», protección antivirus, etc. Asimismo, el adjudicatario deberá asegurar la integridad de los datos que sean modificados durante la activación del CCON con sistemas de copia de seguridad. Correrá a cargo del CSN la administración de las aplicaciones de negocio.

Mientras dure el período de activación, el servicio incluirá la realización por el adjudicatario de copias de seguridad cifradas de los datos albergados en el CCON, que serán debidamente custodiadas, y todo el soporte en la operación y la técnica de sistemas necesaria para su adecuado funcionamiento.

El fin de la contingencia será notificado por el CSN según el procedimiento que se defina.

2.4.2. Acceso al CCON

En caso de activación del CCON, el adjudicatario proporcionará al CSN un punto de acceso seguro en Internet con un caudal suficiente para dar servicio de acceso al CCON, de forma simultánea, a 100 usuarios como mínimo, con posibilidad de ampliación bajo demanda. Se valorará el ancho de banda ofertado del canal de acceso para usuarios.

No se deberá limitar el número de usuarios que pueda acceder al CCON: cualquier usuario del CSN podrá ser un usuario potencial del CCON. Para ello deberán habilitarse procedimientos de sincronización de altas y bajas de usuarios entre el CSN y CCON. El CCON deberá de contar con los mecanismos de autenticación en la red para todos los usuarios del CSN.

El adjudicatario deberá suministrar, en su caso, el cliente de RPV a instalar en los equipos que vayan a conectarse al CCON, y facilitar un servicio de soporte al que podrán dirigirse los usuarios del CCON para resolver incidencias y problemas de conexión al mismo.

Asimismo, en caso de activación del CCON, el adjudicatario pondrá a disposición del CSN al menos dos puestos de trabajo en sus instalaciones, en Madrid, para que puedan ser utilizados por los técnicos del CSN.

2.4.3. Parámetros de servicio del CCON

El tiempo máximo aceptable para el CSN de inoperatividad de los servicios y sistemas críticos descritos en apartado 2.2 es de un día, por lo que se establece un objetivo de tiempo de recuperación (RTO) máximo de **24 horas**, dentro del cual todos los servicios descritos como críticos deberán estar disponibles. La puesta en marcha de estos servicios podrá ser escalonada. Se valorarán las mejoras ofrecidas.

Una vez declarada la emergencia y activado el CCON, éste permanecerá activado durante un tiempo máximo continuo de uso de, al menos, **60 días naturales**, tiempo estimado factible para recuperar el CPD principal. Se valorarán las mejoras ofrecidas.

Se establece una pérdida de datos objetivo (RPO) máxima de **1 hora.** Se valorarán las mejoras ofrecidas.

Los procedimientos de activación y mantenimiento del CCON y de réplica de datos se ajustarán a estos parámetros.

2.4.4. Levantamiento del CPD principal del CSN

Queda fuera del alcance de este contrato el levantamiento del CPD principal del CSN tras de la contingencia que haya dado lugar a la activación del CCON.

La recuperación de los datos del CPD principal a partir de los datos del CCON será responsabilidad del CSN con la colaboración de los técnicos de la empresa adjudicataria.

2.5. Servicios complementarios

2.5.1. Monitorización

El servicio comprenderá la monitorización proactiva de todos los elementos constituyentes de la plataforma del CCON para garantizar su correcto funcionamiento y su completa disponibilidad. Se preverá el envío al CSN de mensajes informativos diarios y alarmas que informen sobre el correcto estado del servicio o adviertan sobre cualquier error, fallo o indisponibilidad de las líneas de comunicaciones, equipamiento, servidores, etc. Las alarmas darán lugar a la inmediata actuación del adjudicatario para la resolución del problema y la restauración de los servicios.

El servicio comprenderá asimismo la monitorización de la réplica de datos de forma que se detecten incidencias en la replicación, tanto por problemas en los equipos como por la pérdida de la línea u otras causas. El prestador del servicio deberá llevar a cabo de forma proactiva los procedimientos necesarios para la resincronización de los datos en el menor tiempo posible.

2.5.2. Servicios profesionales

El servicio incluirá la prestación de todos los servicios profesionales, tanto en el CCON como en el CSN, que sean necesarios para:

- el despliegue y la puesta en marcha de la solución;

- el soporte operativo en el mantenimiento y evolución de la misma;
- el soporte en el despliegue, administración y mantenimiento de las aplicaciones de negocio, y
- el soporte y asistencia en la recuperación del CPD principal.

2.5.3. Documentación

El servicio comprenderá la elaboración, entrega y actualización de toda la documentación del proyecto; en particular, los procedimientos de activación, mantenimiento y vuelta atrás, y la salvaguarda de las configuraciones, así como los demás documentos y procedimientos citados en este pliego.

El adjudicatario, a instancia del CSN o por propia iniciativa, pondrá al día los procedimientos y demás documentación del CCON cuando se produzca algún cambio que lo requiera, en particular, tras la realización de pruebas de activación.

El adjudicatario se compromete a elaborar, facilitar y actualizar esta documentación, que deberá ser aprobada por el CSN.

2.5.4. Renovación tecnológica

El adjudicatario deberá asegurar la renovación tecnológica que garantice la compatibilidad de los recursos contratados en el CCON ante posibles cambios tecnológicos del CSN que alteren sus requerimientos de respaldo. La solución propuesta por el adjudicatario no deberá limitar la necesaria evolución del CPD del CSN.

Formará parte del servicio el soporte técnico y las actuaciones necesarias en el CCON para que las plataformas del CCON y del CSN mantengan su uniformidad. Entre estas tareas se incluirán la instalación de parches y la actualización de las versiones del software de la plataforma. Su ejecución se coordinará entre el CSN y el adjudicatario.

En particular, se prevé que durante la ejecución del contrato podrían aplicarse actualizaciones menores de VMWare en la plataforma de virtualización, actualizarse los sistemas operativos de varios servidores, y actualizarse a la versión 11 de Oracle WebCenter Content, además de aplicarse actualizaciones y parches de seguridad en los diferentes sistemas.

Los procedimientos a elaborar por el adjudicatario deberán contemplar la gestión de implantación de los cambios en el CPD principal en el CCON.

2.6. Pruebas

El CCON deberá ser probado al menos dos veces al año, con una duración mínima de dos días por prueba, de forma que permita garantizar su operatividad en cualquier momento, y del modo que interfiera lo menos posible en el entorno de producción del CPD principal. El CSN podrá solicitar la repetición de las pruebas en las que no se consiga levantar el CCON en el tiempo de activación comprometido. Excepcionalmente, las pruebas podrán llevarse a cabo en fin de semana.

El licitador deberá incluir en su propuesta la planificación y elaboración de planes de pruebas. El calendario de pruebas será acordado entre el CSN y la empresa adjudicataria; no obstante, las ofertas deberán incluir la posibilidad de realizar simulacros de emergencias sin previo aviso.

Al finalizar una prueba el adjudicatario elaborará un informe técnico con los resultados de la misma que se remitirá al CSN para su conocimiento y eventual toma de decisiones. La experiencia obtenida en las pruebas dará lugar a introducción de los cambios procedentes en los procedimientos, en la documentación y, en caso necesario, en la arquitectura del CCON, en cualquiera de sus equipos o en las configuraciones de estos.

El proveedor facilitará un periodo de prueba inicial para permitir al CSN probar el correcto funcionamiento del CCON y sus procedimientos. El tiempo de esta prueba inicial queda supeditado a la correcta valoración del servicio.

2.7. Gestión del servicio

En condiciones de no activación, y según se defina en los procedimientos de gestión de la solución, los técnicos del CSN deberán tener una vía de acceso remota y segura, que no interfiera con el funcionamiento normal de la red y los servicios del CSN, para poder llevar a cabo operaciones de administración sobre las aplicaciones de negocio.

En condiciones de no activación, el adjudicatario notificará al CSN con al menos 48 horas de antelación, siguiendo el procedimiento establecido, las interrupciones por paradas de mantenimiento programado de la plataforma del CCON del CSN. Asimismo deberá notificar al CSN las indisponibilidades del servicio por fallos o averías en el menor tiempo posible, y la recuperación del servicio. En particular se prestará especial atención al control de la correcta replicación de los datos.

El proveedor del servicio facilitará al CSN informes mensuales sobre la disponibilidad y la situación del servicio, incidencias producidas, soluciones aplicadas y tareas realizadas.

Se preverán reuniones de seguimiento con periodicidad, al menos, trimestral entre el prestador del servicio y el CSN.

Las solicitudes del CSN para intervenciones de los técnicos del proveedor se efectuarán por el cauce acordado y deberán ser atendidas en un plazo no superior a las 24 horas del siguiente día laborable.

2.8. Seguridad

2.8.1. Aspectos generales

Las medidas de seguridad de los servicios prestados por el adjudicatario deberán adecuarse a las políticas y normativas en materia de seguridad del CSN en cada momento, considerando que estas políticas irán evolucionando y mejorando con carácter continuo. El adjudicatario deberá cumplir, por tanto, con los requisitos mínimos establecidos en materia de seguridad señalados en el presente pliego, y deberá tener capacidad para adaptarse a las posibles modificaciones y nuevas exigencias de seguridad que se planteen durante la vigencia del contrato. El adjudicatario deberá contar con certificaciones ENS en sus servicios.

2.8.2. *Sistema de gestión*

El adjudicatario, desde el inicio de la prestación del servicio, deberá disponer de un sistema de gestión conforme al modelo ISO 27001, que permita gestionar la seguridad del servicio mediando un proceso repetitivo, aplicando el ciclo de mejora continua basado en el modelo PDCA (planificar, actuar, verificar y hacer).

2.8.3. *Seguridad del centro de servicios gestionados*

En cualquier momento de la ejecución del contrato, el CSN se reserva la facultad de realizar evaluaciones de la seguridad de las instalaciones y sistemas del adjudicatario, así como, también, de auditar los registros que sean relevantes al servicio objeto del presente contrato, debiendo el adjudicatario prestar la colaboración necesaria para tal fin.

2.8.4. *Seguridad del CCON*

La solución ofertada deberá contemplar los elementos de seguridad necesarios para aislar la red destinada al CCON del CSN de cualquier otro entorno, y protegerla frente a intrusiones o ataques malintencionados. El equipamiento de red, los sistemas, infraestructuras, etc., que soporten los servicios prestados al CSN, deben estar perfectamente aislados a nivel operativo (físico y lógico) de cualquier sistema ajeno, de forma que se impida que un cliente pueda acceder a la gestión de los equipos que soportan el servicio del CSN, salvo en los puntos de interconexión debidamente controlados y autorizados individualmente por el CSN.

El adjudicatario debe analizar el servicio prestado, y en caso de detectar patrones sospechosos en materia de seguridad que pudieran suponer mal uso, anomalías, intrusiones u otras amenazas, adoptar de inmediato las medidas oportunas para su corrección. Asimismo, el adjudicatario alertará al CSN en caso de sospechar o detectar la intrusión o presencia interna en los sistemas o equipamientos destinados al servicio del CSN de virus, troyanos o cualquier anomalía que pudiera afectar a la seguridad de la información.

El adjudicatario tiene expresamente prohibido revelar, transmitir o hacer público cualquier detalle o información relativa a la estructura, ubicación, configuración y uso de las infraestructuras y servicios que preste al CSN. En ningún caso informará de la situación, presente o futura, de cualquier servicio o incidencia, a ninguna persona que no se encuentre autorizada e identificada como interlocutor válido por el director del proyecto del CSN.

En este mismo sentido, el adjudicatario tiene la obligación de no comunicar a ninguna persona u organización que no esté identificada y autorizada por director del proyecto del CSN como interlocutor válido para el manejo de este tipo de información, las credenciales de acceso a servicios, sistemas o equipamientos.

2.8.5. *Análisis de riesgos*

El adjudicatario deberá realizar un análisis de riesgos de los activos y servicios relacionados con el servicio contratado mediante el uso de la metodología MAGERIT y el sistema informático PILAR, que determinará los controles de seguridad a aplicar según las normas del anexo II del Esquema Nacional de Seguridad (RD 3/2010). El Análisis de Gestión de Riesgos deberá ser realizado transcurridos doce meses desde el inicio de la fase de prestación inicial del servicio, debiéndose entregar dicho análisis al comité de seguimiento del contrato.

2.8.6. Seguridad de los datos

Los datos del CSN confiados en el CCON, en ningún caso podrán ser utilizados con fin distinto al establecido en este pliego. Una vez cumplida la prestación contractual, el prestador del servicio deberá destruir cualquier copia, tanto principal como de respaldo, de los datos del CSN.

El prestador del servicio, como responsable del tratamiento, no podrá subcontratar con terceros parte de los servicios de custodia, administración, alojamiento de los datos, sin el consentimiento del CSN.

2.8.7. Cumplimiento de la LOPD

El CSN cuenta con ficheros con datos de carácter personal amparados por la LOPD con niveles de protección 1, 2 y 3, que serán custodiados en el CCON. Conforme a la LOPD y su reglamento, el proveedor del servicio tendrá el carácter de encargado del tratamiento, mientras que el CSN mantendrá el carácter de responsable de los ficheros. En cuanto que encargado del tratamiento, el adjudicatario operará siguiendo las instrucciones del CSN como responsable del fichero. Ambos procederán a suscribir el correspondiente Convenio de Protección de Datos requerido por la LOPD y a elaborar el Documento de Seguridad de los ficheros del CSN amparados por la LOPD albergados en el CCON, que será incorporado al Documento de Seguridad del CSN.

El adjudicatario aportará al CSN las pruebas documentales que le aseguren, como responsable de los ficheros, el correcto cumplimiento de las medidas que la normativa de protección de datos establece. En particular, el adjudicatario deberá aceptar las auditorias anuales que la ley prescribe que se realicen en el CSN y en CCON, y facilitar al CSN información sobre su política de seguridad y las auditorías de seguridad que lleve a cabo en sus instalaciones.

El CCON deberá encontrarse ubicado en territorio español para que, entre otras razones, la salida de datos de carácter personal no dé lugar a una transferencia internacional de datos.

3. Implantación del servicio

La empresa adjudicataria diseñará un plan de implantación que incluya:

- La elaboración de la arquitectura y diseño detallados de la solución.
- La provisión, instalación y configuración de la infraestructura física y virtual a nivel hardware y software, así como todos los componentes de seguridad, direccionamiento de red, firewall, routers, etc., tanto en el CCON como en el CSN.
- La habilitación de las líneas de comunicaciones entre el CCON y el CPD principal del CSN, y el CCON y el proveedor de servicios de alojamiento «web».
- El despliegue de las aplicaciones corporativas del CSN. La instalación se llevará a cabo conjuntamente con los técnicos del CSN.
- La definición de los todos los procedimientos técnicos del CCON.
- La configuración y pruebas de la réplica de datos entre el CCON y el CPD del CSN. La copia inicial de datos y la sincronización entre las cabinas de almacenamiento. La monitorización de la réplica de datos.

- La habilitación de las comunicaciones para acceder al CCON.
- La definición y realización de la prueba inicial.
- La puesta en producción y la atención 24x7 para la declaración de emergencias.
- La definición y realización de las pruebas anuales.
- La gestión del servicio y de los cambios en la configuración. El mantenimiento y actualización de la plataforma del CCON. El soporte al CSN en la gestión de las aplicaciones
- La asistencia en la ejecución de los procedimientos acordados en caso de una contingencia.

El plazo máximo de implantación será de **tres meses** a partir de la formalización del contrato. Transcurrido ese plazo se procederá a la realización de las pruebas iniciales, cuya correcta valoración supondrá la entrada en servicio del CCON.

4. Compromisos de nivel de servicio

Para la prestación del servicio, el acuerdo de nivel de servicio se definirá a partir de las referencias siguientes:

Respecto del centro de servicios gestionados:

- ANS 1: Disponibilidad del centro de prestación del servicio: **99'90 %**

  Calculado como el porcentaje de tiempo total de disponibilidad dividido por el tiempo total transcurrido, medido en un periodo cualquiera de doce meses a partir de la fecha de inicio del servicio. En este tiempo de disponibilidad se incluyen las paradas programadas.

- ANS 2: Disponibilidad del acceso a Internet del centro de prestación del servicio del proveedor: **99'90 %**

  Calculado como el porcentaje de tiempo total de disponibilidad del acceso a Internet dividido por el tiempo total transcurrido, medido en un periodo cualquiera de doce meses a partir de la fecha de inicio del servicio. En este tiempo de disponibilidad se incluyen las paradas programadas.

Respecto de los parámetros de servicio:

- ANS 3: Tiempo máximo para la activación del centro de contingencia (RTO): **24 horas**.

  Medido desde la notificación de emergencia por parte del CSN hasta la entrega del último entorno definido en el protocolo de activación de contingencia, incluyendo las tareas que deba emprender el proveedor para el redireccionamiento de las comunicaciones con el «Web Hosting» y la asignación del caudal necesario en al acceso por Internet al CCON del CSN para actuar como centro productivo.

  Están excluidas las indisponibilidades de las aplicaciones de negocio que sean imputables al CSN.

- ANS 4: Tiempo máximo de pérdida de datos (RPO): **1 hora.**

  Medido como tiempo máximo de interrupción de la sincronización de datos entre el CPD principal del CSN y el CCON.

- ANS 5: Tiempo de declaración de situación de emergencias: **30 minutos.**

  Se mide desde la recepción de la notificación de emergencia por parte del CSN al adjudicatario hasta la respuesta de éste aceptando la activación del CCON y estimando el tiempo de puesta en marcha, según los procedimientos, incluyendo la confirmación de la notificación.

- ANS 6: Disponibilidad de la línea de comunicaciones para la réplica de datos: **99'90 %**

  Calculado como el porcentaje de tiempo total de disponibilidad de la línea de réplica de datos dividido por el tiempo total transcurrido, medido en un periodo cualquiera de doce meses a partir de la fecha de inicio del servicio. En este tiempo de disponibilidad se incluyen las paradas programadas.

- ANS 7: Tiempo de respuesta a solicitudes de intervención de los técnicos del proveedor en el CCON: **24 horas del siguiente día laborable.**

  Calculado como el tiempo desde que se cursa la solicitud hasta que el proveedor responde asignando los recursos necesarios para dar respuesta a la solicitud.

5. Planificación y organización

Por parte del CSN, el director de proyecto será el jefe de área de sistemas y comunicaciones. Sus funciones en relación con el alcance del presente pliego serán las de velar por el cumplimiento de los trabajos exigidos y ofertados y emitir las certificaciones de recepción de los mismos. El director de proyecto podrá delegar sus funciones en otra persona; asimismo, podrá incorporar al proyecto durante su realización a las personas que estime necesarias para verificar y evaluar todas las actuaciones a su cargo.

El adjudicatario nombrará un responsable del servicio o coordinador técnico que servirá en todo momento de interlocutor con el CSN y tendrá a su cargo las siguientes funciones:

- Acordar y supervisar la planificación de los trabajos de implantación inicial y de las pruebas iniciales.
- Supervisar la gestión del servicio en operación normal, incluyendo los cambios de la configuración en el software base y en las aplicaciones de negocio.
- Supervisar la activación del CCON ante una emergencia.
- Planificar y supervisar las pruebas anuales.
- Enviar los informes periódicos y de pruebas.
- Asistir a las reuniones de seguimiento donde se analice el desarrollo del servicio.

6. Causas de resolución del contrato

Además de las causas de resolución previstas en el pliego de condiciones administrativas particulares y en la normativa general aplicable, podrán ser causas de resolución del contrato las siguientes:

- El incumplimiento del plazo de implantación del CCON
- El incumplimiento reiterado del RTO pactado, puesto de manifiesto en la prueba inicial de implantación y en las pruebas de activación.
- El incumplimiento del RPO pactado, puesto de manifiesto en reiterados errores o interrupciones de la sincronización de datos.
- El incumplimiento reiterado de los compromisos de disponibilidad del apartado 5 de este pliego.

7. Seguridad y confidencialidad de la información

Las empresas licitadoras manifestaran en sus ofertas su compromiso a tratar de forma confidencial y reservada la información recibida, así como, en el caso de resultar adjudicatarias, la derivada de la ejecución del contrato, que no podrá ser objeto de difusión, publicación o de utilización para fines distintos de los establecidos en este pliego.

En particular, el adjudicatario queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre los datos de carácter personal, que no podrá utilizar con fines distintos a los que figuran en este pliego ni tampoco ceder a otros, ni siquiera a efectos de conservación.

Para garantizar la confidencialidad de los datos de carácter personal, las firmas licitadoras se comprometerán a prestar sus servicios con absoluto respeto a la Ley Orgánica de Protección de Datos de Carácter Personal y a su normativa de desarrollo.

8. Transferencia tecnológica

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

El adjudicatario se comprometerá a facilitar la transferencia del conocimiento a un eventual nuevo adjudicatario, al término del contrato.