

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 1 de 22
		CSN/STI/PRC/17/046

Pliego de prescripciones técnicas
«SERVICIO DE UN CENTRO DE CONTINGENCIA»

 CONSEJO DE SEGURIDAD NUCLEAR Subdirección de Tecnologías de la Información	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 2 de 22
		CSN/STI/PRC/17/046

ÍNDICE

1. Objeto del contrato	4
2. Descripción de las prestaciones	4
2.1. Aspectos generales	4
2.2. Servicios críticos del CSN.....	4
2.3. Configuración del centro de contingencia	5
2.3.1. Centro de servicios gestionados	5
2.3.2. Infraestructura del centro de contingencia: servidores y sistema de almacenamiento	5
2.3.3. Licencias de software	6
2.3.4. Líneas de comunicaciones	6
2.3.5. Red local	7
2.3.6. Seguridad	8
2.3.7. Solución de DNS	8
2.3.8. Solución de réplica de datos.....	8
2.3.9. Solución de correo y servicio de filtrado y limpieza de correo	8
2.3.10. Despliegue de las aplicaciones de negocio	9
2.3.11. Mantenimiento de la infraestructura	9
2.3.12. Plenitud de la configuración	9
2.3.13. Valoración de la configuración del centro de contingencia	9
2.4. Mantenimiento y activación del centro de contingencia	10
2.4.1. Activación del centro de contingencia	10
2.4.2. Acceso al CCON	11
2.4.3. Parámetros de servicio del CCON	11
2.4.4. Levantamiento del CPD principal del CSN.....	11
2.5. Servicios complementarios	12
2.5.1. Monitorización proactiva	12
2.5.2. Servicios profesionales	12
2.5.3. Documentación.....	12
2.5.4. Actualización tecnológica.....	13
2.6. Pruebas	13
2.6.1. Prueba inicial de activación	13
2.6.2. Pruebas ordinarias.....	13

 CONSEJO DE SEGURIDAD NUCLEAR Subdirección de Tecnologías de la Información	Pliego de prescripciones técnicas «<i>Servicio de un Centro de Contingencia</i>»	Página 3 de 22
		CSN/STI/PRC/17/046

2.7.	Gestión del servicio en condiciones de no activación	14
2.8.	Seguridad	14
2.8.1.	Aspectos generales	14
2.8.2.	Sistema de gestión	14
2.8.3.	Seguridad del centro de servicios gestionados	14
2.8.4.	Análisis de riesgos.....	15
2.8.5.	Ficheros amparados por la LOPD.....	15
3.	Implantación e inicio del servicio.....	16
4.	Compromisos de nivel de servicio.....	16
5.	Planificación y organización.....	17
6.	Otras prescripciones y condiciones generales	17
6.1.	Propiedad intelectual	17
6.2.	Transferencia tecnológica.....	17
6.3.	Confidencialidad de la información	18
6.4.	Seguridad de la información	19
6.5.	Cumplimiento de la normativa de protección de datos.....	21
6.6.	Plan de seguridad y confidencialidad.....	21
7.	Reglas especiales respecto del personal laboral de la empresa contratista.....	21

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 4 de 22
		CSN/STI/PRC/17/046

1. Objeto del contrato

El objeto del contrato es la prestación al Consejo de Seguridad Nuclear (CSN) de un **Servicio de un centro de contingencia** (CCON) que permita la continuidad de sus actividades en caso de pérdida o indisponibilidad total o parcial de su centro de proceso de datos principal.

2. Descripción de las prestaciones

2.1. Aspectos generales

El CSN dispone en su sede de un centro de proceso de datos (CPD) que alberga los sistemas informáticos y de comunicaciones con los que se prestan los servicios TIC del organismo. Si bien el CPD y los sistemas instalados en ellos cuentan con políticas y procedimientos de seguridad y cierto grado de redundancia, el CSN precisa contar con un centro de datos alternativo en el que se repliquen y alberguen los servicios que considera críticos, para posibilitar la continuidad de sus actividades en caso de pérdida o indisponibilidad total o parcial de su CPD.

El CSN desea, pues, contratar un servicio de un centro de contingencia en las instalaciones del prestador del servicio, en el cual se repliquen y alberguen sus datos y servicios críticos, que pueda ser inmediatamente activado en caso necesario.

El servicio de un centro de contingencia (en adelante CCON) ha de ser un **servicio totalmente gestionado** que contemple:

- La provisión, instalación, configuración, puesta en servicio y explotación, en las instalaciones del adjudicatario, de todos los elementos constituyentes del centro de contingencia del CSN incluyendo, sin ánimo exhaustivo, el equipamiento, los programas, las soluciones de réplica de datos, las líneas de comunicaciones, las soluciones de seguridad, el direccionamiento público necesario, el servicio de limpieza de correo y el servicio de DNS.
- La prestación de los servicios de monitorización, mantenimiento, administración y gestión ordinaria del servicio y de su infraestructura; la generación de las réplicas; los servicios de copia de seguridad; la realización de pruebas de activación del CCON; la activación real del CCON, en caso necesario; la elaboración y actualización de la documentación y de los procedimientos de uso del servicio; el soporte técnico y los demás servicios descritos en este documento.

El CCON deberá poder ser activado en todo momento ante el acaecimiento de cualquier circunstancia que dé lugar a la indisponibilidad del CPD del CSN. El prestador del servicio habrá de garantizar la plena operatividad y disponibilidad del servicio en modo 24 x 7.

Las condiciones del servicio que se describen en el presente documento deberán mantenerse durante toda la vigencia del contrato y, adicionalmente, durante todo el tiempo de servicios comprometido en el caso de activación del CCON

2.2. Servicios críticos del CSN

El CSN considera críticos, entre otros, los servicios siguientes:

- El correo electrónico corporativo interno y externo, el acceso *http* al correo y el acceso al correo desde dispositivos móviles.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 5 de 22
		CSN/STI/PRC/17/046

- Los servicios de ficheros implementados sobre sus servidores y sistemas de almacenamiento corporativos.
- Las bases de datos Oracle corporativas.
- La Intranet corporativa.
- Las aplicaciones *web* corporativas.
- Las aplicaciones *web* de la Sede Electrónica del CSN en Internet, incluyendo el *back office* y el acceso a las bases de datos en el CCON.
- El sistema documental.
- Los servicios de directorio activo, DNS, impresión y demás servicios básicos del dominio.

En un **Anexo** a este documento se describen estos servicios y la plataforma tecnológica del CSN a respaldar en el CCON. Por razones de confidencialidad, el Anexo se facilitará previa petición formal del licitador dirigida a la Subdirección de Tecnologías de la Información del CSN.

2.3. Configuración del centro de contingencia

2.3.1. Centro de servicios gestionados

El servicio se prestará desde un centro de servicios gestionados propiedad del adjudicatario, donde este proveerá la infraestructura necesaria para el CCON del CSN.

El centro de servicios gestionados del licitador deberá poseer la certificación TIER III o superior y deberá encontrarse en territorio nacional, siendo ambos requisitos imprescindibles

Los datos, aplicaciones y servicios del CCON del CSN deberán albergarse exclusivamente en dicho centro. Se admitirá el uso de una infraestructura externa sólo para llevar a cabo en ella operaciones de copias de seguridad cifradas, siempre que el adjudicatario sea titular y responsable de esa infraestructura, opere bajo su directo y exclusivo control, cuente con medidas de seguridad adecuadas y se encuentre en territorio nacional. En ningún caso se admitirá la utilización de una infraestructura de terceros.

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 en calidad de encargados del tratamiento y estar en situación de suscribir el correspondiente acuerdo con el CSN.

Los licitadores deberán describir detalladamente en sus memorias técnicas la ubicación concreta del centro de servicios gestionados desde el que prestaría el servicio, sus certificaciones, tecnologías, medidas de seguridad y demás características, y los compromisos concretos asumidos en relación con el alojamiento y la gestión de la infraestructura del CCON del CSN.

2.3.2. Infraestructura del centro de contingencia: servidores y sistema de almacenamiento

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.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 6 de 22
		CSN/STI/PRC/17/046

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.

Ambas infraestructuras serán independientes del hardware existente en el CSN y deberán adaptarse a la infraestructura y tecnologías existentes en el CSN, descritas en el Anexo.

Los servidores que el CSN tenga ya virtualizados o sean susceptibles de serlo podrán replicarse y activarse en el CCON en plataformas virtuales, siempre y cuando ambas plataformas de virtualización sean totalmente compatibles. La plataforma de virtualización propuesta deberá permitir el crecimiento del número máquinas virtuales replicadas y el aumento de los recursos asignados a las mismas.

Los servidores que deban ser respaldados físicamente lo serán por servidores compatibles con ellos, al menos en lo que respecta al sistema operativo, versión y nivel de parcheado, 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 por el adjudicatario de forma continua para detectar y resolver, de manera inmediata y proactiva, los fallos o averías que se produzcan.

2.3.3. Licencias de software

El adjudicatario proporcionará las licencias de los sistemas operativos y de los demás productos de software necesarios para la puesta en marcha y el funcionamiento de infraestructura de la plataforma de contingencia, así como su mantenimiento. Las licencias de los sistemas operativos y demás productos (VMWare, Windows, Exchange, etc.) y sus contratos de mantenimiento, están incluidas en el alcance del contrato. Las licencias de Exchange deberán ser nominativas del CSN. El adjudicatario será responsable de la instalación, reinstalación, 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 WebLogic (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 todo este software, así como con su actualización de forma coordinada con el CSN.

2.3.4. Líneas de comunicaciones

El adjudicatario proporcionará las líneas de comunicaciones necesarias para la solución y, al menos, las siguientes:

- 1) **Línea nº 1.** Una línea de comunicaciones segura, de un caudal mínimo de 100 Mbps, entre 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.

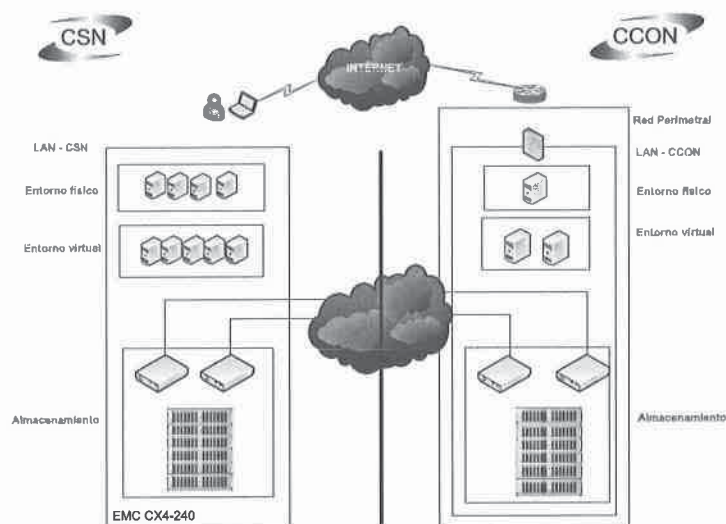


Fig. 1. Esquema básico

- 2) **Línea nº 2.** Una línea de comunicaciones segura de un caudal mínimo garantizado de, al menos, 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 licitador deberá tener en cuenta que el proveedor de servicio de alojamiento del portal de Internet del CSN puede cambiar durante la vigencia del contrato, en cuyo caso deberá prever, a su cargo, el traslado de la línea a un eventual nuevo proveedor.

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 (**Línea nº 3**) proporcionada por un proveedor de servicios de comunicaciones, en el marco de otro contrato. El adjudicatario deberá facilitar la instalación y alojamiento en su centro de servicios gestionados del equipamiento necesario para habilitar este enlace, y prestar el soporte necesario para el encaminamiento de las comunicaciones entre las redes del CCON y de 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 ser al menos Gigabit Ethernet. Deberán definirse en ella, al menos, cuatro VLANs: 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, pero el adjudicatario deberá garantizar totalmente la seguridad y el aislamiento del CCON del CSN.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 8 de 22
		CSN/STI/PRC/17/046

2.3.6. Seguridad

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 y demás infraestructuras 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.

La infraestructura del CCON deberá estar protegida por una doble barrera de cortafuegos de dos fabricantes diferentes, ambas con servicios de seguridad activados (UTM), para garantizar la seguridad de caso de fallos, «bugs», etc., en el equipo de uno de los fabricantes. La barrera interna deberá estar dedicada al CCON del CSN.

El adjudicatario deberá 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.

2.3.7. Solución de DNS

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

2.3.8. Solución de réplica de datos

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 (Oracle, VMWare y Microsoft). Dichas soluciones deben ser independientes del hardware existente en el CSN.

La capacidad de réplica no estará limitada. Tampoco estará limitado el número de servidores, LUNes, instancias de bases de datos, ficheros, etc., que el CSN necesite respaldar.

Los licitadores describirán clara y detalladamente en sus memorias técnicas la solución de réplica general propuesta: equipos, programas, procedimientos de sincronización y re-sincronización, procedimientos de monitorización de las réplicas de datos y servidores, procedimientos de actuación en caso de errores, etc., así como las propuestas, en su caso, para servicios o programas concretos.

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.

2.3.9. Solución de correo y servicio de filtrado y limpieza de correo

El CSN dispone de dos salidas a Internet, una a través de Red Iris, a través de la cual recibe servicios de DNS, y otra a través de un proveedor de servicios de acceso a Internet. La solución

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 9 de 22
		CSN/STI/PRC/17/046

técnica propuesta para la gestión del correo deberá evitar cualquier pérdida de correos del CSN en caso de activación, real o en pruebas, del CCON.

Adicionalmente, el adjudicatario prestará un servicio de filtrado y limpieza de correo, tanto entrante como saliente. Este servicio se prestará de forma continua, con independencia del estado de activación del CCON, aplicándose pues tanto al correo entrante o saliente del CSN en condiciones de no activación del CCON, como al correo entrante o saliente del CCON en caso de activación. El servicio se dimensionará para un mínimo de 1000 buzones de correo.

El licitador describirá con detalle las soluciones propuestas para la gestión del correo y para el filtrado y limpieza del correo entrante y saliente.

2.3.10. 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.

No obstante, la empresa adjudicataria deberá prestar el soporte necesario a los técnicos del CSN en las operaciones de despliegue y prueba de las aplicaciones de negocio.

2.3.11. Mantenimiento de la infraestructura

EL CCON del CSN deberá encontrarse siempre en perfecto estado operativo las 24 horas, los siete días de la semana, y en disposición de ser activado ante cualquier eventualidad.

El adjudicatario deberá llevar a cabo las actuaciones necesarias para el aseguramiento de la plena disponibilidad del CCON, incluyendo las contempladas en los apartados 2.4, 2.5, 2.6 y 2.7.

2.3.12. Plenitud de la configuración

La solución ofertada deberá ser completa, lo que alcanzará a los elementos a instalar tanto en el centro de servicios gestionados del licitador como en el CPD y las instalaciones del CSN. Será a cargo del adjudicatario la provisión de cualquier elemento inadecuado o 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.

La solución y la infraestructura ofertadas:

- Deberán adaptarse a la infraestructura y a las tecnologías existentes en el CSN.
- No requerirán que el CSN amplíe sus sistemas o altere sus configuraciones, o adquiera otros productos.
- Serán independientes del hardware.
- No limitarán o condicionarán de ningún modo la evolución tecnológica de los sistemas del CSN.

2.3.13. Valoración de la configuración del centro de contingencia

Los licitadores describirán clara y detalladamente en sus memorias técnicas la configuración del centro de contingencia ofrecido, pormenorizando los diferentes componentes de la solución a los que se refieren los apartados anteriores.

Se valorará la configuración del centro de contingencia.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 10 de 22
		CSN/STI/PRC/17/046

2.4. Mantenimiento y activación del centro de contingencia

2.4.1. Activación del centro de contingencia

El servicio incluirá la eventual activación real del CCON, en caso necesario, y su mantenimiento durante el tiempo en que la activación se mantenga, así como las pruebas de activación periódicas previstas en este documento para verificar su plena disponibilidad y operatividad y el cumplimiento de los compromisos de nivel de servicio asumidos por el licitador.

El CCON se activará en caso de indisponibilidad total o parcial del CPD principal del CSN o de cualquiera de sus servicios críticos. La activación del CCON podrá deberse tanto a catástrofes naturales, siniestros, averías graves, sabotajes, ciberataques, actos terroristas, etc., como a incidencias o intervenciones técnicas o de cualquier naturaleza que causen indisponibilidad de los servicios. El licitador deberá tener en cuenta la posibilidad de que puedan producirse varias contingencias durante la vigencia del contrato.

En caso de producirse una contingencia que dé lugar a la activación real del CCON, éste permanecerá activado durante el tiempo necesario para la recuperación del CPD principal o el tiempo máximo continuo de uso al que se refiere el apartado 2.4.3. El tiempo máximo continuo de uso continuo comprometido por el adjudicatario se mantendrá incluso en el caso de que la vigencia del contrato finalizare durante su transcurso, siempre que la activación fuera solicitada por el CSN durante la vigencia del contrato.

Si, por cualquier causa, la duración de la activación hubiere de superar el tiempo máximo continuo de uso al que se refiere el apartado 2.4.3 o el ofrecido por el adjudicatario, éste se comprometerá a seguir prestando el 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 económicas (sobre 3) 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 24 x 7, 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.

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 sitio de alojamiento del portal de Internet del CSN y el CCON. El CSN correrá con la reconfiguración de las comunicaciones en el sitio de alojamiento del portal, 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

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 11 de 22
		CSN/STI/PRC/17/046

de los datos que sean modificados durante la activación del CCON con sistemas de copia de seguridad. El CSN se hará cargo de 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 y del resto de la infraestructura, que serán debidamente custodiadas, así como la prestación de 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 real del CCON, el adjudicatario proporcionará al CSN un punto de acceso seguro en Internet con un caudal idóneo y suficiente para dar servicio de acceso al CCON, de forma fluida y simultánea, a 100 usuarios como mínimo, con posibilidad de ampliación bajo demanda. Las memorias técnicas indicarán el caudal ofrecido para este acceso.

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 propios 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 reducciones de tiempo 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 ampliaciones de tiempo ofrecidas.

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

Se exigirá el cumplimiento de estos parámetros en la prestación del servicio y, en su caso, los de las eventuales mejoras de tiempo asumidas por el licitador.

Los procedimientos de mantenimiento y activación del CCON y de réplica de datos, que deberá elaborar el adjudicatario, 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.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 12 de 22
		CSN/STI/PRC/17/046

La recuperación de los datos del CPD principal a partir de los datos del CCON será responsabilidad del CSN. No obstante, la empresa adjudicataria deberá colaborar con los técnicos del CSN en la eventual recuperación de su CPD principal, incluso en el caso de que la vigencia del contrato haya terminado.

2.5. Servicios complementarios

2.5.1. Monitorización proactiva

El servicio comprenderá la monitorización proactiva por el adjudicatario en modo 24 x 7 de todos los elementos constituyentes de la plataforma del CCON para garantizar su correcto funcionamiento y su completa disponibilidad.

El adjudicatario habilitará el envío al CSN de mensajes informativos diarios y alarmas que informen tanto sobre el correcto estado del servicio como sobre cualquier error, fallo o indisponibilidad de las líneas de comunicaciones, equipamiento, servidores, programas, aplicaciones, 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 por el adjudicatario de la réplica de datos de forma que se detecten las incidencias en la replicación originadas tanto por problemas en los equipos como por la pérdida de la línea u otras causas. En caso de incidencia, el prestador del servicio deberá llevar a cabo, de forma proactiva y sin dilación, los procedimientos necesarios para la resincronización en el menor tiempo posible.

2.5.2. Servicios profesionales

El servicio incluirá la prestación a cargo del adjudicatario de todos los servicios profesionales descritos en este documento, tanto en el CCON como en el CSN, y, en todo caso, los que sean necesarios para:

- El despliegue y la puesta en marcha de la solución.
- El soporte operativo en el mantenimiento y evolución de la plataforma y en el aseguramiento de su disponibilidad y plena operatividad.
- El soporte en el despliegue, administración y mantenimiento de las aplicaciones de negocio.
- El soporte operativo y la técnica de sistemas necesaria en caso de activación del CCON.
- El soporte y asistencia en la recuperación del CPD principal.

2.5.3. Documentación

El servicio comprenderá la elaboración, mantenimiento y actualización por el adjudicatario de toda la documentación del proyecto. En particular, los procedimientos de mantenimiento de la infraestructura del CCON, activación del CCON, operación del CCON activado, los procesos de vuelta atrás, la documentación y salvaguarda de las configuraciones y los demás documentos y procedimientos citados en este pliego.

El adjudicatario pondrá al día los procedimientos y demás documentación del CCON cuando se requiera algún cambio en alguno de ellos; en particular, tras la realización de modificaciones o actualizaciones de la plataforma del CCON o cuando, tras la realización de pruebas de activación, sea necesario mejorar o actualizar los procedimientos de mantenimiento y activación del CCON.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 13 de 22
		CSN/STI/PRC/17/046

El adjudicatario se compromete a elaborar, actualizar y facilitar toda esta documentación al CSN, que deberá aprobarla.

2.5.4. Actualización tecnológica

Estará comprendido dentro de alcance del servicio la prestación del soporte técnico y la ejecución de las actuaciones necesarias para que las plataformas del CCON y del CSN mantengan su uniformidad. Entre estas tareas se incluirá 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.

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

2.6. Pruebas

2.6.1. Prueba inicial de activación

Dentro del primer mes de servicio se llevará a cabo una prueba inicial de activación del CCON para comprobar el correcto funcionamiento del servicio implantado. En caso de no resultar exitosa, se llevará a cabo una segunda prueba dentro de los diez días siguientes. Si esta segunda prueba no resultara exitosa, el CSN podrá aplicar las penalizaciones previstas, pudiendo además ser causa de resolución del contrato. Para considerar exitosa la prueba, la activación deberá ser completa y alcanzarse en el tiempo máximo para la activación a que se haya comprometido el adjudicatario (apartado 2.4.3).

Las pruebas iniciales no tendrán la consideración de pruebas ordinarias.

2.6.2. Pruebas ordinarias

El CCON deberá ser probado cuatro veces al año.

Las pruebas tendrán una duración mínima de dos días y se realizarán de forma que permitan comprobar la operatividad y accesibilidad del CCON, el cumplimiento de los compromisos de activación asumidos por el adjudicatario y el correcto funcionamiento de todos los servicios del CSN replicados en el CCON.

El CSN podrá solicitar la repetición de las pruebas en las que no se consiga activar completamente el CCON en el tiempo máximo de activación al que el adjudicatario se haya comprometido.

Las pruebas se llevarán a cabo en días de oficina y de modo que se interfiera lo menos posible en el entorno de producción del CPD principal del CSN. Excepcionalmente, a petición del CSN, 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.

Tras de cada 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

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 14 de 22
		CSN/STI/PRC/17/046

los procedimientos, en la documentación y, en caso necesario, en la arquitectura del CCON o en cualquiera de sus equipos, programas o configuraciones.

2.7. Gestión del servicio en condiciones de no activación

El adjudicatario notificará al CSN con al menos 48 horas de antelación, siguiendo el procedimiento establecido, las interrupciones del servicio por paradas de mantenimiento programado de la plataforma del CCON o de cualquiera de sus componentes, y las previsiones necesarias para la recuperación de la plena operatividad del CCON.

El adjudicatario notificará de inmediato al CSN las indisponibilidades del servicio por fallos o averías y, en particular, los fallos de la correcta replicación de datos y la recuperación del servicio.

Los técnicos del CSN deberán tener una vía de acceso remota y segura al CCON 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.

Las solicitudes del CSN para llevar a cabo actuaciones intervenciones sobre la infraestructura del CCON o cualesquiera otras se efectuarán por el cauce acordado y deberán ser atendidas en un plazo no superior a las 24 horas del siguiente día laborable.

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 del servicio con periodicidad, al menos, trimestral entre el adjudicatario y el CSN.

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 de forma continua. El adjudicatario deberá cumplir, por tanto, con los requisitos mínimos establecidos en materia de seguridad señalados en el presente documento, y deberá tener capacidad para adaptarse a las posibles modificaciones y nuevas exigencias de seguridad que se planteen durante la vigencia del contrato.

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, la de auditar los registros que sean relevantes para el servicio, debiendo el adjudicatario prestar la colaboración necesaria para tal fin.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 15 de 22
		CSN/STI/PRC/17/046

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.

De igual modo, 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.

2.8.4. 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. Este análisis de riesgos se repetirá veinticuatro meses después, en caso de prórroga del contrato.

2.8.5. Ficheros amparados por 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 tanto que encargado del tratamiento, el proveedor del servicio no podrá subcontratar con terceros parte de los servicios de custodia, administración, alojamiento de los datos, sin el consentimiento del CSN, y actuará siempre 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 auditorías 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.

Las anteriores prescripciones se entienden sin perjuicio del cumplimiento por el licitador de las prescripciones generales recogidas en el apartado 6 de este pliego y, en particular, en el subapartado 6.5 *Cumplimiento de la normativa de protección de datos*.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 16 de 22 CSN/STI/PRC/17/046
---	--	--

3. Implantación e inicio del servicio

La empresa licitadora aportará en su memoria técnica un Plan de implantación del servicio que contemple, entre otros aspectos:

- La arquitectura y el diseño detallado de la solución.
- La provisión, instalación, configuración y puesta en marcha de la infraestructura física y lógica en el CSN y en el CCON.
- La provisión y 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».
- La provisión, configuración y habilitación de los elementos de seguridad de la red y de los servicios de correo y DNS.
- La habilitación, configuración y habilitación de la réplica de datos entre el CCON y el CPD del CSN. La copia inicial de datos, la sincronización de los datos y la monitorización de los procesos de réplica de datos.
- El despliegue de las aplicaciones corporativas del CSN. La instalación se llevará a cabo conjuntamente con los técnicos del CSN.
- La habilitación de las comunicaciones para acceder al CCON.
- La definición y realización de la prueba de activación inicial.
- La definición de todos los procedimientos técnicos del CCON y, en particular, los relativos a la activación del CCON, la gestión del servicio, el mantenimiento y actualización de la plataforma y el soporte al CSN.

El servicio se iniciará el **8 de enero de 2018**. El licitador deberá garantizar que en dicha fecha el servicio se encuentre totalmente implantado, en funcionamiento y entregado al CSN.

Se valorará el plan de implantación propuesto.

4. Compromisos de nivel de servicio

Se establecen los siguientes compromisos de nivel de servicio mínimos:

- **ANS 1: Tiempo máximo para la activación del centro de contingencia (RTO): 24 horas.**

Medido desde la petición de activación 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. Se excluyen las indisponibilidades de las aplicaciones de negocio que sean imputables al CSN.

- **ANS 2: 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 3: 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.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 17 de 22
		CSN/STI/PRC/17/046

- **ANS 4: 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 5: 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 del servicio, una vez asignados los recursos necesarios, inicia las actuaciones de cumplimiento de 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 y 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. Otras prescripciones y condiciones generales

6.1. Propiedad intelectual

Los derechos de propiedad intelectual relacionados con el trabajo realizado en la prestación de este servicio pertenecerán al CSN. Cualquier producto o subproducto derivado del mismo no podrá ser utilizado para otros fines fuera del ámbito que le corresponda, sin permiso expreso por escrito del poseedor de la propiedad intelectual.

6.2. 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.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 18 de 22
		CSN/STI/PRC/17/046

6.3. Confidencialidad de la información

Las empresas licitadoras manifestaran en sus memorias técnicas su compromiso a tratar de forma confidencial y reservada la información y la documentación recibidas, 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.

La empresa adjudicataria y, en particular, los miembros del equipo de trabajo que preste el servicio al CSN, guardarán secreto profesional sobre todas las informaciones, documentos y asuntos a los que tengan acceso o conocimiento durante la vigencia del contrato, quedando obligados a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución. Esta obligación no se limitara al tiempo de ejecución del correspondiente contrato, sino que deberá ser respetada aun después de su cumplimiento o resolución.

Cualquier información relacionada con el objeto del contrato, sea cual fuere su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), en cualquier forma o soporte (verbal, escrita, grabada o en cualquier otro medio), que pudiera ser facilitada por el CSN o por cualquier tercero que tenga relaciones contractuales con el organismo, será considerada como "*Información Confidencial*"

La empresa adjudicataria y su equipo de trabajo se obligan pues a:

- Guardar la *Información Confidencial*, bien sea escrita, grabada o en cualquier otro soporte, separada de cualquier otra información de la que pudiera disponer el equipo de trabajo.
- Utilizar o transmitir la *Información Confidencial* exclusivamente para los fines del objeto del contrato.
- No realizar copia de la *Información Confidencial* sin el previo consentimiento escrito del CSN, excepto aquellas copias que sean necesitadas por el equipo de trabajo para su estudio interno.
- Proteger la *Información Confidencial* del acceso a la misma por personas no autorizadas.
- Restringir el acceso a la *Información Confidencial* únicamente a aquellas personas que necesiten conocerla para los fines del objeto del contrato, y asegurarse de que dichas personas conocen las obligaciones que les resultan aplicables en virtud de lo establecido en el presente pliego.
- No facilitar *Información Confidencial* a tercero alguno sin el previo consentimiento escrito del CSN, y responsabilizarse de que, en caso de haber obtenido dicha autorización, dicho tercero firma un compromiso de confidencialidad en términos equivalentes a los contenidos en el presente pliego.

Cualquier publicidad o información a los medios de comunicación referida a la simple existencia del contrato o su contenido, deberá ser previamente aprobada por escrito por el CSN.

A la finalización del servicio, la empresa adjudicataria procederá a destruir o a devolver al CSN toda la *Información Confidencial*, bien sea escrita, grabada o en cualquier otro soporte en que pudiera encontrarse recogida.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 19 de 22
		CSN/STI/PRC/17/046

6.4. Seguridad de la información

El adjudicatario se obliga a cumplir la normativa legal aplicable en materia de seguridad de la información en el marco de los servicios prestados.

Con carácter general deberá prestar especial atención a la observancia de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la anterior; el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y el Real Decreto 951/2015, de 23 de octubre, de modificación del anterior.

La prestación del servicio quedará sujeta a la *Política de seguridad en el ámbito de los sistemas de información del Consejo de Seguridad Nuclear* y demás documentos de seguridad derivados de la misma. El adjudicatario y su equipo de trabajo quedan pues obligados al cumplimiento de todas las normas de seguridad del CSN y, en particular:

- A no registrar datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por el RD 1720/2007 respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. (Artículo 9.2. LOPD).
- A no realizar pruebas con datos de carácter personal.
- A no transferir ningún tipo de datos, de carácter personal o no, de documentación o código fuente de los sistemas de información del CSN a soportes de almacenamiento extraíbles sin el expreso consentimiento del CSN.
- A no extraer del CSN ningún tipo de información mediante redes de comunicaciones o servicios de almacenamiento externos al CSN, como los disponibles en el “Cloud Computing”, o a las propias instalaciones del contratista.
- A notificar cualquier incidencia de seguridad al responsable de Seguridad del CSN según los procedimientos de seguridad del organismo.
- A disponer en sus equipos de un sistema de protección antivirus, actualizado periódicamente y de forma automática, que deberá utilizarse sobre cualquier fichero, soporte y software antes de que cualquiera de éstos resida o se instale en los sistemas de información del CSN. La frecuencia de actualización será como mínimo semanal.
- A no compartir las cuentas de correo asignadas de forma personal ni desviar de forma automática el correo a cuentas particulares o propias de la empresa adjudicataria.

El equipo de trabajo será informado y concienciado por el personal del CSN en los aspectos de seguridad del organismo y cada miembro deberá firmar el reconocimiento de la formación recibida en materia de seguridad. El jefe de proyecto del adjudicatario será el responsable del cumplimiento de las medidas de seguridad por parte del equipo de trabajo.

Cuando el adjudicatario acceda de forma remota a infraestructuras del CSN se compromete a:

- Custodiar debidamente la información de acceso que le facilite el CSN para la conexión durante el periodo de vigencia del contrato, y a destruirla extinguido el mismo.
- No habilitar ni utilizar las funciones de las aplicaciones o sistemas operativos que permitan guardar o recordar las credenciales de acceso de forma automática.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 20 de 22
		CSN/STI/PRC/17/046

- Mantener convenientemente aisladas, lógica y físicamente, las infraestructuras del adjudicatario que se utilicen para acceder a la red corporativa del CSN. Entre cada red, subred o servicio de comunicaciones se implantarán cortafuegos (firewalls) que deberán estar configurados con la política del menor privilegio, bloqueando o denegando cualquier tipo de tráfico no autorizado o innecesario para la prestación del servicio. De la misma forma se permitirán únicamente los puertos, protocolos o servicios autorizados por el CSN. Cualquier puerto, protocolo o servicio no especificado como autorizado se denegará por defecto.

En el marco de la ejecución del contrato, y respecto a los sistemas de información objeto del mismo, las siguientes actividades están específicamente prohibidas:

- La utilización de los sistemas de información para la realización de actividades ilícitas o no autorizadas, como la comunicación, distribución o cesión de datos, medios u otros contenidos a los que se tenga acceso en virtud de la ejecución de los trabajos y, especialmente, los que estén protegidos por disposiciones de carácter legislativo o normativo.
- La instalación no autorizada de software, la modificación de las configuraciones o la conexión a redes.
- La modificación no autorizada del sistema de información o del software instalado, o el uso del sistema distinto al de su propósito.
- La sobrecarga, prueba, o desactivación de los mecanismos de seguridad y las redes, así como la monitorización de redes o teclados.
- La reubicación física y los cambios de configuración de los sistemas de información o de sus redes de comunicación.
- La instalación de dispositivos o sistemas ajenos al desarrollo del contrato sin autorización previa, tales como dispositivos USB, soportes externos, ordenadores portátiles, puntos de acceso inalámbricos o PDA's.
- La posesión, distribución, cesión, revelación o alteración de cualquier información sin el consentimiento expreso del propietario de la misma.
- Compartir cuentas e identificadores personales (incluyendo contraseñas y PINs) o permitir el uso de mecanismos de acceso, sean locales o remoto a usuarios no autorizados.
- Inutilizar o suprimir cualquier elemento de seguridad o protección o la información que generen.

El adjudicatario adquirirá el compromiso de ser auditado por personal autorizado por el CSN, en cualquier momento del desarrollo del contrato, con el fin de verificar la seguridad implementada, comprobando que se cumplen las recomendaciones de protección y las medidas de seguridad de la distinta normativa, en función de las condiciones de aplicación en cada caso.

Asimismo, el CSN se reserva la posibilidad de monitorizar la actividad del equipo de trabajo.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 21 de 22
		CSN/STI/PRC/17/046

6.5. Cumplimiento de la normativa de protección de datos

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 en sus memorias técnicas a prestar sus servicios con absoluto respeto a la Ley Orgánica de Protección de Datos de Carácter Personal y a su normativa de desarrollo, suscribiendo, en su caso, el oportuno contrato de confidencialidad.

La prestación de los servicios descritos en este contrato puede dar lugar a posibles accesos administrativos sobre ficheros con datos de carácter personal residentes en bases de datos Oracle de los que es titular el CSN. Siendo así, y en cumplimiento de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), el adjudicatario y el CSN acuerdan lo siguiente:

- 1) Que el adjudicatario solo llevará a cabo tratamientos de los ficheros de datos de carácter personal siguiendo las instrucciones del CSN y a los únicos y exclusivos efectos de prestar los servicios incluidos en este contrato.
- 2) Que el adjudicatario no aplicará o utilizará los ficheros de datos de carácter personal con fines distintos a la prestación de los servicios objeto de este contrato.
- 3) Que el adjudicatario no extraerá del CSN, comunicará ni cederá los datos incluidos en estos ficheros o los propios ficheros, ni siquiera con fines de salvaguarda o conservación.
- 4) Que el adjudicatario deberá de cumplir, con respecto a los ficheros de datos de carácter personal, la medidas de seguridad descritas en la *Política de seguridad en el ámbito de los sistemas de información del Consejo de Seguridad Nuclear* y demás documentos de seguridad derivados de la misma, así como todas aquellas medidas que sean necesarias para cumplir lo dispuesto en el artículo 9 de la LOPD y el Reglamento 994/1999, de 11 de junio, que lo desarrolla.

6.6. Plan de seguridad y confidencialidad

El licitador incluirá en su memoria técnica un plan de seguridad y confidencialidad de no más de seis páginas de extensión en el que describirá las previsiones, compromisos y actuaciones adicionales que prevea llevar a cabo durante la ejecución del contrato para garantizar la confidencialidad y seguridad de la información y el cumplimiento de la LOPD.

7. Reglas especiales respecto del personal laboral de la empresa contratista

1.- Corresponde exclusivamente a la empresa contratista la selección del personal que, reuniendo los requisitos exigidos en los pliegos, formará parte del equipo de trabajo adscrito a la ejecución del contrato, sin perjuicio de la verificación por parte del Consejo de Seguridad Nuclear del cumplimiento de aquellos requisitos.

La empresa contratista procurará que exista estabilidad en el equipo de trabajo, y que las variaciones en su composición sean puntuales y obedezcan a razones justificadas, en orden a no alterar el buen funcionamiento del servicio informando en todo momento al Consejo.

	Pliego de prescripciones técnicas «Servicio de un Centro de Contingencia»	Página 22 de 22
		CSN/STI/PRC/17/046

2.- La empresa contratista asume la obligación de ejercer de modo real, efectivo y continuo, sobre el personal integrante del equipo de trabajo encargado de la ejecución del contrato, el poder de dirección inherente a todo empresario. En particular, asumirá la negociación y pago de los salarios, la concesión de permisos, licencias y vacaciones, la sustituciones de los trabajadores en casos de baja o ausencia, las obligaciones legales en materia de Seguridad Social, incluido el abono de cotizaciones y el pago de prestaciones, cuando proceda, las obligaciones legales en materia de prevención de riesgos laborales, el ejercicio de la potestad disciplinaria, así como cuantos derechos y obligaciones se deriven de la relación contractual entre empleado y empleador.

3.- La empresa contratista velará especialmente por qué los trabajadores adscritos a la ejecución del contrato desarrollen su actividad sin extralimitarse en las funciones desempeñadas respecto de la actividad delimitada en los pliegos como objeto del contrato.

4.- Siendo el objeto del contrato la prestación de un servicio de un centro de contingencia cuya efectividad requiere disponer de acceso y actuar directamente sobre los sistemas que han de replicarse en aquél, se autoriza a la empresa adjudicataria a prestar sus servicios en las dependencias del Consejo. En este caso, al personal de la empresa contratista se le podrán asignar espacios de trabajo diferenciados del que ocupan los empleados públicos siempre que lo permita la disponibilidad de espacios. Corresponde también a la empresa contratista velar por el cumplimiento de esta obligación.

5.- La empresa contratista deberá designar al menos un coordinador técnico integrado en su propia plantilla, que tendrá entre sus obligaciones las siguientes:

a) Actuar como interlocutor de la empresa contratista frente al Consejo, canalizando la comunicación entre la empresa contratista y el personal integrante del equipo de trabajo adscrito al contrato, de un lado, y la "entidad contratante", de otro lado, en todo lo relativo a las cuestiones derivadas de la ejecución del contrato.

b) Distribuir el trabajo entre el personal encargado de la ejecución del contrato, e impartir a dichos trabajadores las órdenes e instrucciones de trabajo que sean necesarias en relación con la prestación del servicio contratado.

c) Supervisar el correcto desempeño por parte del personal integrante del equipo de trabajo de las funciones que tienen encomendadas, así como controlar la asistencia de dicho personal al puesto de trabajo.

d) Organizar el régimen de vacaciones del personal adscrito a la ejecución del contrato, debiendo a tal efecto coordinarse adecuadamente la empresa contratista con el Consejo de Seguridad Nuclear, a efectos de no alterar el buen funcionamiento del servicio.

e) Informar al Consejo acerca de las variaciones, ocasionales o permanentes, en la composición del equipo de trabajo adscrito a la ejecución del contrato sin perjuicio de las demás obligaciones que se establecen, tanto en el contrato como en los Pliegos de Cláusulas Administrativas y de Prescripciones Técnicas.

	ANEXO	Página 1 de 4
		27-abril-2017

ANEXO

Descripción de los servicios críticos y de la plataforma tecnológica actual del CSN

Correo

Actualmente el CSN cuenta con una infraestructura de correo MS Exchange 2013 compuesta por los siguientes elementos: un grupo de disponibilidad Windows DAG, con dos servidores virtuales locales, con los roles de MAILBOX Server (Servidor de Buzones) y Acceso de Cliente, con unos 800 buzones y un almacenamiento de 120 GB, y tres servidores virtuales remotos con los roles, también, de Servidor de Buzones y Acceso de Cliente, uno situado en la Unidad Militar de Emergencias (UME) y dos en el actual prestador del servicio de un centro de contingencias.

La publicación del dominio de correo del CSN, @csn.es, la realiza RedIRIS, quién proporciona también conexión a Internet.

Como «front-end» de correo se dispone de dos equipos específicos Cisco IronPort.

Se dispone también de correo por Internet (webmail) a través de un servidor físico Windows ForeFront TMG instalado en un Windows Server 2008 R2.

Servicio de ficheros

Actualmente el CSN cuenta con dos servidores virtuales Windows 2012 y Windows 2008, dedicados a servidores de ficheros departamentales y personales. El espacio de almacenamiento utilizado a día de hoy es de 2,5 TB y 600 GB respectivamente. Estos servidores virtuales tienen asignadas cada uno 2 CPU y 1 CPU y una memoria de 6 GB y 4 GB respectivamente.

Se desea también a corto plazo replicar la información de otros 2 servidores de ficheros Windows 2008, con una ocupación aproximada de 1 TB.

Se prevé convertir todos o algunos de estos servidores en unidades NAS durante el tiempo de vigencia del contrato.

Aplicaciones corporativas

El CSN cuenta con un servidor de aplicaciones web Oracle WebLogic 10g sobre dos máquinas virtuales de 4 CPU y 8 GB de memoria con LINUX Red Hat v.4, que soporta todas las aplicaciones corporativas del CSN, unas 83. Existe intención de actualizar este servidor de aplicaciones durante la vigencia del contrato.

Estas aplicaciones utilizan la base de datos corporativa del CSN (ORACLE 11g), con una ocupación en disco de unos 250 GB.

	ANEXO	Página 2 de 4
		27-abril-2017

Aplicaciones web en Internet

El CSN cuenta con un punto de presencia en Internet alojado en las instalaciones de un proveedor externo de alojamiento web, en el que reside tanto su sitio web corporativo, www.csn.es, como sus aplicaciones de *Administración Electrónica*, utilizando estas últimas la base de datos corporativa del CSN a través de una línea dedicada.

En caso de pérdida del CPD principal del CSN, estas aplicaciones deberán seguir funcionando con la base de datos del centro de contingencia a través de una conexión segura.

Sistema documental

El CSN cuenta con un sistema documental con unos cuatrocientos mil documentos, sobre el gestor documental Oracle WebCenter Content (WCC, antiguo UCM), instalado en dos máquinas virtuales con RedHat Enterprise Linux 6, una con 4 CPU , 8 GB de RAM y 2 TB de discos y otra con 2 CPU, 4 GB de RAM y 150 GB de discos.

Intranet corporativa

La Intranet corporativa está montada, como una aplicación web más, en Oracle WebLogic (WLS) y los contenidos en un servidor virtual RedHat Linux Enterprise v. 5.6, con 4 CPU y 8 GB de RAM con Oracle WebCenter Content 11. Hay todavía una parte estática que reside en un servidor Windows 2012 Server (1 CPU y 4 GB de memoria) con IIS, con un almacenamiento de unos 700 Gbytes de contenidos estáticos.

Almacenamiento

El CSN dispone de un sistema de almacenamiento masivo SAN EMC VNX 5400, con una capacidad total de 80 TB brutos.

Los discos de la cabina VNX están jerarquizados en 64 TB brutos en un pool de discos SAS y NL-SAS de un rendimiento de 6Gbss, que soportan las bases de datos, los servidores virtuales y los documentos recientes, y en otro pool de discos NL-SAS de 16 TB brutos destinado a servidores de ficheros NAS, más una Flash Caché de 188 GB.

Servidores

Los servicios del CSN están soportados por un sistema de virtualización VMWare 5.5 sobre cuatro servidores *blades* HP BL460c G6 y dos servidores *blades* HP BL 460c GEN8 en un chasis HP C-7000, conectados al sistema de almacenamiento.

El VirtualCenter está montado en una máquina virtual con vCenter Server Appliance 5.5.

Actualmente hay 83 servidores virtuales, de los cuales 12 se consideran críticos en este momento. Los servidores son Windows 2012 Server, Windows 2008 y Linux Red Hat v. 4 y 6, principalmente.

	ANEXO	Página 3 de 4
		27-abril-2017

Base de datos

La base de datos es Oracle 11g sobre un clúster de Oracle RAC One soportado por dos servidores Sun Enterprise M-3000 con 8 CPU SPARC9 a 2860 MHz y 32 GB de RAM cada uno.

La configuración de la base de datos, los ficheros del sistema (archives, redo log, etc.) y los ficheros de datos residen en LUNs del sistema de almacenamiento (SAN).

Actualmente existen cinco instancias que se consideran críticas.

Comunicaciones

Actualmente existe una línea dedicada entre las instalaciones del proveedor del servicio de alojamiento web donde residen las aplicaciones de los servicios al ciudadano (*Administración Electrónica*) y el CPD del CSN.

Autenticación

La red LAN del CSN es una red Windows que utiliza el directorio activo de Windows como medio de autenticación de usuarios en la red. El CSN cuenta con dos controladores de dominio (CD) con DNS secundarios en dos servidores físicos Windows 2012 Standard. Se cuenta con un solo dominio para toda la organización. El nivel funcional del dominio es Windows 2008.

Replicación de datos y equipos en el centro de contingencia

Actualmente el CSN dispone de un servicio de un centro de contingencia que cuenta con un servidor físico de base de datos con sistema operativo Solaris 9, un servidor virtual Windows como controlador de dominio, dos servidores virtuales Windows para los servicios de correo y otros 13 servidores virtuales Windows y Linux para diferentes propósitos. Estos servidores virtuales se replican al Centro de Contingencia a través del software de réplica Zerto.

Las cinco instancias críticas de base de datos se replican a la máquina Solaris mencionada a través del software DataGuard de Oracle. La replicación de los datos de correo electrónico se efectúa por medio de las herramientas propias de Exchange, grupo de disponibilidad Windows DAG.

Durante el tiempo de vigencia del contrato se prevé que sea necesario aumentar el número de servidores replicados, así como el volumen de la información replicada.

Ficheros del CSN amparados por la LOPD

El CSN tiene inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos un total de 19 ficheros con los niveles de seguridad y tipo de tratamiento siguientes:

Nombre del fichero	Nivel de seguridad	Tipo de tratamiento
Denuncias y notificaciones	Alto	Automatizado
Acción Social	Alto	Mixto
Banco Dosimétrico	Alto	Automatizado
Carnés radiológicos	Básico	Automatizado
Control de acceso físico	Básico	Automatizado
Datos médicos	Alto	No automatizado
Destinatarios de publicaciones	Básico	Automatizado
Empresas externas	Básico	Mixto
Fichero de licencias	Básico	Automatizado
Fichero de personal	Básico	Automatizado
Gestión de carnés radiológicos de los trabajadores del CSN	Alto	No automatizado
Homologación de cursos	Básico	Automatizado
Imágenes institucionales	Básico	Mixto
Registro	Básico	Automatizado
Tasas	Medio	Mixto
Usuarios de servicios telemáticos	Básico	Mixto
Videovigilancia	Básico	Automatizado
Visitantes del Centro de Información	Básico	Automatizado
Expedientes jurídicos	Medio	Automatizado

La información de la mayoría de estos ficheros y de las aplicaciones que la utilizan forma parte de la información replicada en el centro de contingencia.