Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Contratación servicios de copia de seguridad para proyecto Batera

Especificaciones de compra / Pliego de condiciones técnicas

Enero de 2017

EJIE-076-2017

Mediterráneo, 14 · 01010 Vitoria-Gasteiz · Posta-kutxatila / Apartado: 809 · 01080 Vitoria-Gasteiz · Tel. 945 01 73 00* · Fax. 945 01 73 01 ·
www.ejie.net

Contenido

1 Definición de necesidad e idoneidad de la contratación 4
2 Objeto del contrato 5
3 Ámbito, descripción y alcance del contrato. 6
3.1 Ámbito y descripción del entorno 6
3.2 Descripción de infraestructuras 6
3.2.1 Arquitectura 7
3.2.2 Administración y consola de gestión 8
3.2.3 Seguridad 8
3.2.4 Soporte para Cloud 10
3.2.5 Gestión de media 10
3.2.6 Soporte de recuperación antes desastres 10
3.2.7 Copia y restauración 10
3.2.8 Políticas de protección de datos 14
3.2.9 Acuerdos de Nivel de servicio (ANS) 20
3.3 Descripción de Servicios. 23
3.3.1 Introducción 23
3.3.2 Fase de transición 23
3.3.3 Fase de transformación 24
3.3.4 Fase de servicio recurrente 25
3.3.5 Gestión del servicio 30
3.3.6 Fase de Devolución del servicio 30
3.3.7 Contingencia de los servicios que presta el proveedor 30
3.3.8 Perfiles profesionales 31
3.3.9 Modelo de relación y comunicación 31
4 Contenido de las ofertas 32
5 Presupuesto, plazo de ejecución y forma de pago 34
5.1 Presupuesto 34
5.2 Modificaciones previstas 34
5.3 Plazo de ejecución. 35
5.4 Forma de pago 35
6 Condiciones de seguridad generales 37
7 Criterios de adjudicación de las ofertas 38
7.1 Juicios de Valor: 35 puntos 38
7.2 Criterios de Fórmula: 65 puntos 40
8 Anexo I: Modelo de servicio actual EJIE 41
8.1 Tecnologías 41
8.2 Disponibilidad 41
8.3 Ámbito 41
8.4 Características del Servicio 41

8.5 Operación del servicio 42
8.6 Transición del servicio 47
8.7 Diseño del servicio 52
8.8 Mejora continua del servicio 56
8.9 Requisitos de servicio 58
8.10 Procedimiento y calidad 59
8.11 Plan de calidad 60
8.12 Seguimiento 62
8.13 Metodología aplicable y entorno tecnológico 62
8.14 Penalizaciones 63
8.15 Planificación y organización del servicio 64
8.16 Responsabilidades de dirección y gestión del servicio 64
8.17 Carga de trabajo 65
8.18 Prestación del servicio 66
8.19 Constitución inicial del equipo de trabajo 66
8.20 Modificaciones en la composición del equipo de trabajo 67
8.21 Interconexión con EJIE. 67
8.22 Dimensionamiento del equipo de trabajo 67
8.23 Actualización tecnológica 67
8.24 Garantía de la disponibilidad del servicio 68

1 Definición de necesidad e idoneidad de la contratación

Dentro del proyecto de convergencia de infraestructuras IT de gobierno, es necesario dotarse un servicio de copia y restauración de datos, capaz de abarcar las cargas de trabajo a converger de forma inmediata y las que vayan surgiendo a medida que avance el proyecto

La actividad objeto de contratación es necesaria para la prestación de un servicio que es competencia de EJIE. Dicha actividad está incluida entre los servicios que pueden ser contratados, conforme a la Instrucción sexta de las Instrucciones sobre las buenas prácticas en la contratación de servicios de Gobierno Vasco, y su objeto no contiene prestaciones que con arreglo a la Instrucción quinta deben ser satisfechas con medios propios.

Su prestación no puede ser asumida con los recursos humanos y técnicos de que dispone el EJIE siendo además inconveniente o imposible su reorganización.

Los documentos contractuales elaborados en la fase de preparación del contrato incorporan las debidas garantías para dar cumplimiento a la Instrucción octava, sobre las buenas prácticas en la celebración de contratos de servicios a fin de evitar que se incurra en los supuestos de cesión ilegal de trabajadores.

2 Objeto del contrato

El objeto del presente contrato son los servicios gestionados de implantación y operación de una solución de protección de datos empresarial que garantice el respaldo y la recuperación de datos, tanto de servicios de ficheros como de bases de datos y aplicaciones, en infraestructura tanto física como virtual en modalidad de pago por uso para EJIE

Este servicio se prestará a Osakidetza y el proyecto Batera.

El servicio que se solicita cubrirá las necesidades SW, HW y de gestión para las siguientes características obligatorias:

- Protección como servicio (BaaS)
- DR como servicio (DRaaS)
- Reportes avanzados
- Integración Cloud con portal de autoservicio
- Multitenancy por roles

Estos servicios deberán ser dimensionados para un volumen:

- 400 TB de frontal de copias
- 4000 VM
- 20.000 Jobs de copia diarios
- 70 Servidores BBDD Oracle RAC

Con una previsión de crecimiento de un 10% anual.

Además es requisito del contrato la gestión de la plataforma de copias de seguridad del entorno actual de EJIE hasta la finalización del contrato actual de hardware y software de copias de seguridad en el 2020. A su finalización, el servicio asumirá la migración de los procesos de copias y restauración mencionados.

3 Ámbito, descripción y alcance del contrato.

3.1 Ámbito y descripción del entorno

Se requiere un servicio de backup basado en SLAs que tenga en cuenta los siguientes parámetros:

- Debe disponer de un mecanismo de autoservicio controlado para que el consumo del BaaS sea fácil y accesible
- Se establecerán políticas de protección, con sus SLAs, según la importancia del dato.
- Se dispondrá de un repositorio de backup en disco en cada ubicación, que permita una rápida restauración de la información
- Se establecerá una réplica a otro centro para disponer de una externalización de los backups.
- El backup en disco se realizará deduplicado, con deduplicación global, de forma que permita disponer de un mayor ratio de reducción y por lo tanto una mayor retención del dato en el tiempo.

Toda la infraestructura del servicio de copias de seguridad se albergara en el CPD de EJIE, tomando como centro de respaldo el CPD de Interior.

3.2 Descripción de infraestructuras

En este aparto se describe el procedimiento de copias para el entorno físico y virtual de Osakidetza, repartido por la comunidad autónoma de la siguiente manera:

Datacenter	Osakloud.Servicio.Entorno	Cuenta de VM	Suma de Provisioned MB	Suma de In Use MB	Suma de Provisioned TB	Suma de In Use TB
H.U.B	PROD	1	65543	27154	0,06	0,03
	PRODEX	3	1746983	1326817	1,67	1,27
Total H.U.B		4	1812526	1353971	1,73	1,29
H.U.C		2	394654	148356	0,38	0,14
	NOPROD	33	5513314	3931819	5,26	3,75
	PROD	224	33162733	21212408	31,63	20,23
	PRODEX	24	7800529	5417540	7,44	5,17
	PRODSQL	6	873086	468083	0,83	0,45
Total H.U.C		289	47744316	31178206	45,53	29,73
H.U.D.	NOPROD	40	5790163	4337804	5,52	4,14
	PROD	108	18022980	11753548	17,19	11,21
	PRODEX	11	4872291	4305449	4,65	4,11
Total H.U.D.		159	28685434	20396801	27,36	19,45
H.U.G.	PRODEX	3	1746983	1347281	1,67	1,28
Total H.U.G.		3	1746983	1347281	1,67	1,28
H.U.T.		1	65622	23407	0,06	0,02
	NOPROD	12	1421020	932435	1,36	0,89
	PROD	86	15593196	10682195	14,87	10,19
	PRODEX	8	4272247	4255224	4,07	4,06
	PRODSQL	4	586918	493879	0,56	0,47

Total H.U.T.		111	21939003	16387140	20,92	15,63
H.U.U	NOPROD	3	233647	51833	0,22	0,05
Total H.U.U		3	233647	51833	0,22	0,05
Osakidetza		10	1325594	1063315	1,26	1,01
	CORE	182	18986811	18435537	18,11	17,58
	COREX	2	160066	160066	0,15	0,15
	NOPROD	434	59296258	34328396	56,55	32,74
	NOPRODEX	22	10158706	8350389	9,69	7,96
	PROD	983	204532424	182707845	195,06	174,24
	PRODEX	21	51277274	51233704	48,90	48,86
Total Osakidetza		1654	345737133	296279252	329,72	282,55
Total general		**2223**	**447899042**	**366994484**	**427,15**	**349,99**

3.2.1 Arquitectura

Se requiere una solución que cubra los siguientes requerimientos de gestión de datos en un entorno Enterprise:

La solución deberá ser capaz de gestionar una solución en una Arquitectura Actico/ Activo, creciendo en “Backup Building Blocks” según necesidades. Cada “Backup Building Blocks” será un conjunto homogéneo de equipos de gestión y repositorio de protección de datos (RPD).

La solución deberá poder mantener la arquitectura de catálogo único entre los varios CPDs del servicio de backup a fin de mantener una consistencia de todas las copias de seguridad y restauraciones de toda la infraestructura en cualquiera de los CPDs.

El servicio de protección de los datos de la central debe tener:

- Una copia principal, con las retenciones según la tipología e importancia del dato.
- Al menos otra copia en el segundo DataCenter
- Los centros dispondrán de una copia en local y una réplica a la central

Para los 3 hospitales territoriales, el repositorio de almacenamiento donde se repliquen las copias, estará en la central, pudiendo ser uno de los repositorios principales.

Cada nodo escribirá los datos de backup en su repositorio de discos.

En caso de fallo en alguno de los componentes de un CPD, o de desastre total en uno de los CPD, se podrá seguir haciendo backup/recuperaciones de los datos de todos los servidores de la plataforma desde el otro CPD.

La licencia debe consistir en la posibilidad de despliegue de un número ilimitado de todas las funcionalidades y módulos disponibles en cada momento dentro de la plataforma ofertada.

La solución debe incrementar la capacidad de ingesta de información a medida que aumente el volumen de Front End, de manera que en las 12 horas de ventana de copias sea posible copiar los TB de FE en su totalidad. Para la configuración inicial se requiere:

- **Rendimiento mínimo del repositorio 40TB/h**
- **Al menos 700 streams concurrentes en escritura**

3.2.2 Administración y consola de gestión

El software debe proveer una consola única y gráfica para la administración, configuración, monitorización y creación de informes de todas las tareas de gestión de datos.

El sistema debe permitir la definición de perfiles de acceso a la herramienta con diferentes privilegios, desde el administrador con control total del sistema hasta el operador con permisos exclusivos para la restauración de copias de seguridad.

El software debe ofrecer las siguientes interfaces de administración:

- GUI basada en acceso web
- Interfaz de Línea de Comandos
- API REST

Se valorará que el software permita hacer distribución electrónica de software para instalaciones y actualizaciones.

Se valorará que el software disponga de un sistema de alertas con las siguientes características

- Registrar entradas en el Visor de Eventos de Sistema del Servidor de consola
- Ejecutar scripts con comandos externos
- Personalizar las entradas y mensajes de alerta
- Escalar notificaciones si no se realizan medidas correctivas pasado un período de tiempo predefinido
- Integración SNMP con la solución de monitorización global del CPD (alertas gestión).

El sistema debe permitir la generación de, al menos, los informes necesarios para realizar el control de los niveles de servicio acordados:

3.2.3 Seguridad

La consola de administración debe estar protegida por usuario y contraseña, para prevenir accesos no autorizados al sistema. Esta medida se aplicará a todos los puestos de trabajo del proveedor que puedan intervenir en la provisión del servicio.

La consola de administración debe poder desconectar automáticamente sesiones cuando están inactivas durante un período de tiempo definible

El software debe permitir al administrador crear tanto usuarios adicionales con una cuenta de correo electrónico asociada para recibir informes, como grupos, para definir una seguridad granular conforme al siguiente esquema:

- Acceso a objetos de administración: Grupos de clientes, servidores, agentes, políticas, informes, contenido, recursos de almacenamiento, etc.
- Tipos de tarea permitida en el objeto accedido: búsqueda de objetos, operación, restauración al mismo/distinto destino, búsqueda de contenidos, programación, administración, gestión de trabajos, instalación de software, etc.

El software debe ofrecer la opción de integrarse con uno o más servidores de Directorio Activo para permitir single sign-on.

El software debe mantener un registro de auditoria para auditar las operaciones de usuarios y los cambios que hayan realizado.

Se utilizarán usuarios personales para todos los usuarios. El proveedor debe gestionar todos los usuarios de la plataforma y se compromete a mantener una lista permanentemente actualizada con todas las personas que tienen acceso a la plataforma, el código de usuario que utilizan y su rol. Se controlará también, si existen, los usuarios de proceso o producto que pudieran existir que deben estar inventariados, adecuadamente protegidos y utilizados sólo en las situaciones en las que se haya previsto su utilización, que deben estar documentadas.

También se utilizarán usuarios personales (e intransferibles) en la operación de las plataformas "Legacy".

EJIE se reserva el derecho de auditoría sobre el servicio y las infraestructuras que lo soporten, tal y como se establece en la política de seguridad para proveedores.

El software debe permitir realizar comunicaciones a través de cortafuegos.

El software debe proporcionar protección de la media por contraseña, para prevenir accesos no autorizados.

El software debe soportar encriptación de datos.

Se valorará que las claves de encriptación sean gestionadas de forma centralizada dentro de la infraestructura de copias para operaciones de Recuperación frente a Desastres.

En lo correspondiente a cifrado se deben utilizar algoritmos, tamaños de claves y protocolos adecuados. Se utilizará como referencia:

- GUÍA/NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-807) – "CRIPTOLOGÍA DE EMPLEO EN EL ESQUEMA NACIONAL DE SEGURIDAD"
- El sistema debe gestionar con nivel suficiente de seguridad datos catalogados como DE NIVEL ALTO en la dimensión de CONFIDENCIALIDAD.

3.2.3.1 Securización de plataforma tecnológica

El proveedor se compromete a mantener todos los sistemas actualizados con el objetivo de evitar, en la medida de lo posible, vulnerabilidades:

- Realizará un bastionado de los sistemas implicados en el servicio
- Actualizará hardware y software de todos los elementos implicados en base a las políticas de actualizaciones de los proveedores de las tecnologías utilizadas.
- Entregará un plan anual de actualizaciones previstas en los sistemas, y trimestralmente un informe de las actualizaciones realizadas.
- Informará a EJIE en caso de detectar cualquier vulnerabilidad, indicando su gravedad, explotabilidad y plan de mitigación previsto, con las fechas de aplicación.
- EJIE se reserva el derecho a realizar análisis de vulnerabilidades de la plataforma, con notificación previa al proveedor
- En el caso de que EJIE, directa (vía análisis de vulnerabilidades) o indirectamente (vía boletines de tecnologías, notificación de CERT, SOC u otro servicio) detecte una vulnerabilidad, el proveedor responderá con un informe que al menos contendrá la siguiente información:
  - Aplicabilidad de la vulnerabilidad (o no), razonada.
  - Alcance/gravedad/explotabilidad
  - Plan de mitigación

En lo correspondiente a protección de datos y a la fecha de publicación del presente expediente está en vigor RD1720/2007, que establece, en su artículo 94 "Copias de respaldo y recuperación", punto 3, que "El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación". El proveedor proporcionará a EJIE informes que permitan el cumplimiento de este requisito.

3.2.4 Soporte para Cloud

El software debe de trabajar en modo Cloud a la hora de presentar los recursos a usuarios y como gestor de almacenamiento temporal de proveedores cloud en este sentido, para asegurarnos la integración cloud para usuarios:

- La solución debe tener la capacidad de integrarse de forma nativa con vRealize Suite y con la API Rest, a fin de permitir el funcionamiento de características de dicho portal, para generar workflows avanzados de protección como proveedor de servicio hacia usuarios finales.
- Es requisito que soporte la creación de tenants, con administración independiente de cada tenant, aislamiento de los repositorios de backup de cada tenant, gestión y reporting independientes para cada tenant.

Para asegurarnos una integración correcta con proveedores de almacenamiento Cloud:

- Soporte para backup deduplicado y cifrado en repositorio cloud Amazon Web Services o soporte para proveedores que utilicen el estándar S3

3.2.5 Gestión de media

Debe tener integración con nubes Híbridas, Privadas o Públicas para realizar una externalización de datos hacia ella o desde ellas, mediante mecanismos basados en VM´s que incorporan la integración con los entornos de Cloud y siempre ese movimiento será cifrado y comprimido y de-duplicado

3.2.6 Soporte de recuperación antes desastres

Tanto para los clientes como para el propio sistema de copias de seguridad, el sistema de copias debe de tener un procedimiento claro de recuperación ante cualquier desastre lógico que pueda suceder.

La solución deberá incorporar mecanismos automáticos de backup del repositorio de metadatos que permitan realizar operaciones Disaster/Recovery del servicio de backup, así como recuperación de la base de datos en caso de desastre o pérdida del catálogo. La continuidad del servicio de backup debe ser válida en entornos de servidores físicos y/o virtuales.

El software de backup debe ser capaz de orquestar la replicación de los backups entre los equipo de backup ofertados, y tener catalogados tanto los backups de los dos CPD como sus distintas réplicas o clonados, de forma que en caso de desastre en un CPD o no accesibilidad al equipo de un CPD, el software de backup sea capaz de restaurar los backups del equipo situado en el centro de respaldo, sin necesidad de re catalogar los backups del centro de respaldo.

La solución debe proporcionar capacidad de replicación bidireccional sobre cualquier distancia:

- Los datos de backup se ingestarán de forma deduplicada en el sistema del site principal, replicándose sobre el site de contingencia.
- Las réplicas de los backups deben realizarse de forma deduplicada sobre redes IP y/o FC, y deben estar catalogadas en el software de backup de la solución

La información de backup debe tener la posibilidad de replicarse de manera automatizada y de-duplicada entre CPDs.

3.2.7 Copia y restauración

3.2.7.1 Versatilidad de políticas de backup y retención

El sistema debe permitir políticas de backup y retención lo suficientemente versátiles.

El sistema debe permitir la definición de SLAs tanto para el Backup como para la Retención

3.2.7.2 De-duplicación

El producto deberá contener, integrado con los clientes y servidores de backup, un elemento de preprocesado de deduplicación, a fin de trasmitir menos información y acelerar el rendimiento de la solución de backup a disco desplegada. Debe garantizar asimismo la réplica consistente entre los equipo de backup ofertados en este procedimiento, al objeto de posibilitar restauraciones de cualquier CPD sin intervención manual, todo ello gestionado desde la consola de gestión del software de backup ofertado.

Deberá tener mecanismos de deduplicación en origen a nivel de cliente y servidor de backup, no solamente para los datos de Sistema Operativo sino para los aplicativos en producción. El algoritmo de de-duplicación debe ser global para todo el entorno

3.2.7.3 Off-host backup

El sistema debe permitir realizar copias desde a otro servidor intermedio para realizar el backup liberando de este modo al servidor origen del procesamiento del backup.

3.2.7.4 Lan-free backup

El sistema debe permitir lanfree backup de servidores, entendiéndose como tal, la transferencia de los datos desde el servidor origen hasta el sistema de backup a través de red SAN.

3.2.7.5 Optimización de ancho de banda

El sistema debe permitir la definición de ventanas horarias para hacer backup y la limitación del ancho de banda consumido.

Se valorará que permita continuar con una tarea de backup interrumpida sin necesidad de recomenzar desde el principio.

El software debe ser capaz de definir ventanas de operación para diferentes tareas, a fin de controlar el impacto temporal en los servidores de producción.

La solución deberá poder realizar un full backup diario pero transmitiendo por la red únicamente los ficheros nuevos o que hayan sido modificados, reduciendo la ventana de backup pero al mismo tiempo permitiendo que la restauración se realice en un sólo paso.

3.2.7.6 Soporte multiplataforma

La solución debe disponer de agentes para los Sistemas Operativos de servidor Windows y Linux (incluidas configuraciones de Microsoft Cluster Server MSCS).

3.2.7.7 Integración con hipervisores de virtualización

El sistema debe integrarse con las plataformas de virtualización de VMWARE e HyperV de modo que no sea necesario instalar agentes en las máquinas virtuales para realizar backup de las mismas (salvo que se desee recuperación granular de aplicaciones contenidas en la máquina virtual como SQL, Exchange,…).

En concreto para VMWARE debe:

- Integrarse con las API´s de VMWARE para realizar backup en caliente a través de la SAN del fichero vmdk tanto completo como incremental.
- A partir de un único backup debe permitir tanto recuperación completa del servidor virtual como de ficheros individuales.
- Deduplicación a nivel de bloque utilizando los mismo hashes tanto para las máquinas virtuales como para las físicas.

- Incorporación automática al sistema de backup de las máquinas virtuales nuevas que se generen, o cuando menos, alertar al administrador del sistema.
- Debe permitir la realización de backup vía API VADP de los entornos virtuales VMware, permitiendo restauraciones completas de máquinas virtuales, así como recuperaciones granulares a nivel de fichero, tanto para máquinas virtuales Windows como Linux.
- Debe integrarse con la funcionalidad de CBT (Changed Block Tracking) de VMware tanto en backup como en restore.
- Para realizar el backup de entornos VMware debe utilizar proxies virtuales (no se aceptarán soluciones que requieran de un proxy físico) y el software deberá tener un sistema de balanceo de carga para repartir la carga de backups de las máquinas virtuales entre los diferentes proxies virtuales disponibles.
- Debe permitir la clonación de backups de máquinas virtuales VMware desde dispositivos de disco a dispositivos de cinta o cualquier otro medio que se requiera para larga retención
- Debe permitir la autoprotección de nuevas máquinas virtuales VMware que se creen, basado en políticas automáticas a nivel de folder/pool o servidor ESX, sin necesidad de intervención por parte del administrador.
- Debe estar integrado y hacer backup a nivel de imagen y de agente de entornos Microsoft Hyper-V, permitiendo la restauración granular a nivel de fichero.

Autodescubrimiento de máquinas virtuales VMware vSphere.

- La solución de backup deberá ser capaz de descubrir automáticamente las máquinas virtuales creadas, a través de interfaces desde VMware vCenter u otras herramientas de gestión vSphere.

Backup y recuperación granular en un solo paso.

- La solución deberá ser capaz de capturar una imagen completa de máquina virtual y realizar recuperaciones granulares de ficheros a partir de esta imagen, sin necesidad de tener que restaurar todo el contenido de la máquina virtual para poder recuperar ficheros individuales.

“Incremental Forever” VMware backup vía VADP/CBT.

- La solución deberá soportar la utilización de la tecnología CBT de VMware vía VADP (vStorage API for Data Protection).

Backups de imagen VMware a través de proxy.

- La solución deberá ser capaz de desplegar proxys de backup, de cara a descargar a las máquinas virtuales de consumo de CPU, memoria y recursos de I/O.

3.2.7.8 Copias de seguridad NDMP

Solución debe tener la capacidad para respaldar los sistemas de almacenamiento NAS (por protocolo NDMP), de forma deduplicada, permitiendo un movimiento a través de FC de los datos mantenidos en los sistemas NAS hacia los equipos orientados para Backup.

Integración de la solución con la herramienta de monitorización del Servicio gestionado de Protección de Datos.

Punto único de contacto para el soporte de toda la solución ofertada.

3.2.7.9 Copias de Exchange

El sistema debe disponer de agente específico para realizar copias de seguridad y restauraciones de Exchange 2007 y posteriores de forma directa y sin pasos intermedios (sin utilizar “Recovery storage groups/databases” de Exchange).

Debe ser compatible con instalaciones de Exchange en alta disponibilidad.

Las copias de seguridad se podrán realizar en caliente. Debe permitir la recuperación tanto total de una base de datos como granular de buzones y correos.

La gestión de las copias de seguridad de Exchange debe realizarse de forma centralizada desde la herramienta (instalación del agente, creación de las tareas y programación de las mismas).

Debe poder realizar backup en caliente consistente de Microsoft Exchange con la posibilidad de restaurar granular mente.

3.2.7.10 Copias de seguridad SQL Server

El sistema debe poder realizar copias de seguridad y restauraciones de SQL 2005 y posteriores de forma directa sin pasos, ni scripts intermedios.

Debe ser compatible con instalaciones de SQL en cluster.

Las copias de seguridad se podrán realizar en caliente. Debe permitir backup full, incremental y diferencial de las bases de datos.

La gestión de las copias de seguridad de SQL debe realizarse de forma centralizada desde la herramienta (instalación del agente, creación de las tareas y programación de las mismas).

Debe poder realizar backup en caliente consistente de Microsoft SQL Server con la posibilidad de restaurar granular mente. Así mismo, el administrador de SQL deberá poder realizar backups ad hoc desde la consola de gestión SQL Server Management Studio, sin necesidad de realizar la petición desde la consola de administración del software de backup.

Se valorará la integración con la herramienta de gestión de MS SQL Management Studio, permitiendo a los DBA´s de SQL la realización de sus propios Backups y restores.

3.2.7.11 Copias de seguridad Sharepoint

El sistema debe poder realizar copias de seguridad y restauraciones de SharePoint de forma directa sin pasos, ni scripts intermedios.

La solución de backup deberá soportar backups incrementales y completos, y recuperación granular a nivel de documento para la última mayor release y la versión N-1 de la solución Microsoft Sharepoint, tanto en entornos físicos como virtuales.

La restauración debe poderse hacer con la misma herramienta de backup desde una consola única, si herramientas de terceros.

3.2.7.12 Copias de seguridad Directorio Activo

El sistema debe poder realizar copias de seguridad y restauraciones del directorio Activo de Windows 2008 y posteriores de forma directa sin pasos, ni scripts intermedios.

Las copias de seguridad se podrán realizar en caliente. Debe permitir la recuperación tanto total del directorio activo como de elementos individuales.

3.2.7.13 Copias de seguridad de Oracle

El sistema debe poder realizar copias de seguridad y restauraciones de ORACLE de forma directa sin pasos, ni scripts intermedios.

Las copias de seguridad se podrán realizar en caliente, tanto de servidores físicos como virtuales. Debe permitir la recuperación tanto total como de elementos individuales.

La solución de backup deberá soportar la última mayor release y la versión N-1 de la base de datos Oracle, a través de integración con la herramienta RMAN

Debe poder realizar backup en caliente consistente de Oracle 11g y 12c con la posibilidad de restaurar granular mente. Así mismo, el administrador de Oracle podrá realizar backups ad hoc desde la utilidad de Oracle RMAN (sin necesidad de lanzarlo desde el software de backup), y el software de backup deberá catalogar los backups que se hayan lanzado desde RMAN, para que el administrador de backup tenga un control total sobre todos los respaldos realizados.

Se valorará la integración con la herramienta de gestión de Oracle Enterprise manager, permitiendo a los DBA´s de Oracle la realización de sus propios Backups y restores.

3.2.7.14 Copias de seguridad integradas con VSS

De cara a generar backups consistentes de aplicativos en entornos Microsoft Windows Server, el aplicativo de backup deberá disponer de soporte para “volumen shadow copy service” (VSS).

.

3.2.8 **Políticas de protección de datos**

Se han identificado en total los 5 niveles de protección de información dentro de EJIE que se detallan a continuación. El servicio deberá proveer de al menos estos niveles de protección.

Para el diseño de las políticas se ha tenido en cuenta:

- Los niveles de protección no se han asociado con ningún tipo de dato concreto, sino que podrá ser EJIE el que asocie cada conjunto de información en el nivel que aplique según los requisitos legales o funcionales de la organización.
- Las retenciones a aplicar se expresan en los márgenes de tiempo que se consideran recomendables para cada nivel de protección.
- Para el cálculo de los RPO de cada nivel de protección, se considera un tiempo de dos veces la frecuencia de la copia/snapshot/… respetando la recomendación de realizar políticas de protección con tolerancia al fallo individual de un trabajo de protección y/o posible duración total de la copia.
- Los RTO no se calculan para casos de duplicación/replicación ya que en caso de recurrir a estas copias, estamos en situaciones de recuperación “no óptimas”. Véase: largas retenciones o DR que generalmente no depender sólo de la infraestructura dedicada a la protección de los datos, y que deben ser estimadas periódicamente por los grupos involucrados en el mantenimiento y administración de dicha infraestructura.
- Los datos que se externalicen a terceros o que atraviesen redes no seguras, deberán ir encriptadas desde el origen.
- No se especifica en este documento los soportes físicos para estas copias, pero a día de hoy con las tecnologías de deduplicación a disco, se considera una buena práctica almacenar las copias que requieran mejores tiempos de recuperación en este formato. La cinta magnética sigue siendo la opción recomendada para almacenamiento fuera de los centros de datos o largas retenciones de datos “no deduplicables”.

3.2.8.1 Nivel 0

Se entiende por “Nivel 0” aquella información y/o servicio que por su criticidad deba disponer del tiempo mínimo de interrupción o indisponibilidad dentro de la organización.

Este nivel corresponde asimismo a información no histórica, y por tanto el tiempo de retención de la misma no es un valor añadido.

3.2.8.1.1 Tipo y frecuencia de copias

Snapshot

La segunda línea de protección tras la alta disponibilidad y/o replicación de volúmenes para este conjunto de datos/servicios será un snapshot.

Frecuencia máxima: 8 horas.

Primera copia

Siempre que el tipo de dato lo admita, se dotará a un subconjunto de los snapshots anteriores con una duplicación completa de los datos en disco que proteja ante la corrupción o pérdida de los volúmenes originales.

En caso de no ser posible la duplicación directamente del snapshot anterior, se deberá realizar de los datos originales.

Frecuencia máxima: 24 horas.

3.2.8.1.2 Duplicación y/o replicación

La primera copia deberá contar con replicación asíncrona o similar externalizada al centro de datos donde se encuentre dicha primera copia.

3.2.8.1.3 Retención y almacenamiento

Snapshot	> 72 horas
Primera copia	> 14 días < 3 meses
Segundas	> 14 días < 3 meses

3.2.8.1.4 RTO y RPO

RTO	Snapshot	< 1 hora
	Primera copia	< 8 horas
RPO	Snapshot (hasta 72 horas)	< 16 horas
	Primera copia (hasta 14 días)	< 48 horas
	Primera copia (a partir de 14 días)	< 21 días

3.2.8.2 Nivel 1

Se clasificará como “Nivel 1” aquella información que no estando regulada por unos requisitos de disponibilidad muy estrictos como el caso anterior, si lo está por motivos de nivel de protección de la información.

En este caso, se considera que esta información si contiene un valor en el tiempo, por lo que los tiempos de retención finales serán superiores al caso anterior.

Ejemplos de este tipo de datos podrían ser: informes médicos, servicios relacionados con registros de medicamentos, etc.

3.2.8.2.1 Tipo y frecuencia de copias

Snapshot

La segunda línea de protección tras la alta disponibilidad y/o replicación de volúmenes para este conjunto de datos/servicios será un snapshot.

Frecuencia máxima: 24 horas.

Primera copia

Siempre que el tipo de dato lo admita, se dotará al snapshot anterior con una duplicación completa de los datos en disco que proteja ante la corrupción o pérdida de los volúmenes originales.

En caso de no ser posible la duplicación directamente del snapshot anterior, se deberá realizar de los datos originales.

Frecuencia máxima: 24 horas.

3.2.8.2.2 Duplicación y/o replicación

La primera copia deberá contar con replicación asíncrona o similar externalizada al centro de datos donde se encuentre dicha primera copia.

Esta duplicación estará asociada a todas las primeras copias, y un subconjunto de las mismas estará regulado por una retención extendida...

3.2.8.2.3 Retención y almacenamiento

Snapshot	> 72 horas
Primera copia	> 28 días < 6 meses
Segundas copias en adelante	> 28 días < 1 año

3.2.8.2.4 RTO y RPO

RTO	Snapshot	< 1 hora

	Primera copia	< 8 horas
RPO	Snapshot (hasta 72 horas)	< 16 horas
	Primera copia (hasta 14 días)	< 48 horas
	Primera copia (a partir de 14 días)	< 21 días
	Primera copia (a partir de 28 días)	< 2 meses

3.2.8.3 Nivel 2

A este nivel de protección pertenecen los datos críticos por ser información histórica, por lo que la configuración de la misma se basa en múltiples copias y larga retención de la información.

Ejemplos de datos pertenecientes a este nivel: historiales de pacientes.

3.2.8.3.1 Tipo y frecuencia de copias

Primera copia

Se realizará una copia de los datos a un almacenamiento alternativo al original.

Frecuencia máxima: 24 horas.

Copia extendida

Para este nivel aparece el concepto de copia extendida, o copia de retención extendida. Esta no corresponderá con una copia adicional, sino que aprovechará las características de las herramientas de protección de datos del mercado para seleccionar entre las primeras copias un subconjunto que permanecerá accesible para su recuperación durante un tiempo prolongado.

Frecuencia máxima: 1 mes

3.2.8.3.2 Duplicación y/o replicación

La primera copia deberá contar con replicación asíncrona o similar externalizada al centro de datos donde se encuentre dicha primera copia.

Esta duplicación estará asociada a todas las primeras copias, y un subconjunto de las mismas estará regulado por una retención extendida. Las copias con retención extendida en origen mantendrán su retención original también en la duplicación.

3.2.8.3.3 Retención y almacenamiento

Primera copia	> 28 días < 3 meses
Copia extendida	> 3 meses < “sin expiración”
Segundas copias en adelante	> 28 días < “sin expiración”

3.2.8.3.4 RTO y RPO

RTO	Primera copia	< 24 horas

	Copia extendida	< 24 horas
RPO	Primera copia (hasta 14 días)	< 48 horas
	Primera copia (a partir de 14 días)	< 14dias
	Primera copia (a partir de 28 días)	< 2 meses
	Copia extendida (hasta 1 año)	< 2 meses
	Copia extendida (a partir de 1 año)	< 13 meses

3.2.8.4 Nivel 3

A este nivel de protección pertenecen los datos estándar sin necesidades sin valor histórico.

Ejemplos de datos: servicios IT de la organización (directorio activo, correo, etc.).

3.2.8.4.1 Tipo y frecuencia de copias

Primera copia

Se realizará una copia de los datos a un almacenamiento alternativo al original.

Frecuencia máxima: 24 horas.

Copia extendida

Al igual que en caso anterior, no corresponderá con una copia adicional, sino que aprovechará las características de las herramientas de protección de datos del mercado para seleccionar entre las primeras copias un subconjunto que permanecerá accesible para su recuperación durante un tiempo prolongado.

Frecuencia máxima: 1 mes

3.2.8.4.2 Duplicación y/o replicación

Tanto la primera copia, como la copia extendida deberán contar con replicación asíncrona o similar externalizada al centro de datos donde se encuentre dicha primera copia.

3.2.8.4.3 Retención y almacenamiento

Primera copia	> 7 días < 1 meses
Copia extendida	> 1 año
Segundas copias en adelante	> 7 días < 1 año

3.2.8.4.4 RTO y RPO

RTO	Primera copia	< 24 horas
	Copia extendida	< 24 horas
RPO	Primera copia (hasta 14 días)	< 48 horas
	Primera copia (a partir de 14 días)	< 14dias
	Copia extendida	< 2 meses

3.2.8.5 Nivel 4

Se trata de la protección de datos con menor restricción de protección. Se aplica a datos que no sufren cambios habituales o sin gran impacto en la organización. Estos datos en general son recuperables o reproducibles con otros métodos.

3.2.8.5.1 Tipo y frecuencia de copias

Primera copia

Se realizará una copia de los datos a un almacenamiento alternativo al original.

Frecuencia máxima: 7 días.

Copia extendida

Al igual que en caso anterior, no corresponderá con una copia adicional, sino que aprovechará las características de las herramientas de protección de datos del mercado para seleccionar entre las primeras copias un subconjunto que permanecerá accesible para su recuperación durante un tiempo prolongado.

Frecuencia máxima: 1 mes

3.2.8.5.2 Duplicación y/o replicación

Tan solo la copia extendida deberá contar con replicación asíncrona o similar externalizada al centro de datos donde se encuentre dicha primera copia.

3.2.8.5.3 Retención y almacenamiento

Primera copia	> 7 días < 1 meses
Copia extendida	3 meses
Segundas copias en adelante	3 meses

3.2.8.5.4 RTO y RPO

RTO	Primera copia	< 48 horas
	Copia extendida	< 48 horas
RPO	Primera copia (a partir de 14 días)	< 14dias
	Copia extendida	< 2 meses

3.2.9 Acuerdos de Nivel de servicio (ANS)

Se describen a continuación una serie de indicadores que constituyen la base para establecer los niveles de servicio según los que realizará la prestación.

El proveedor deberá incluir en su oferta una propuesta de acuerdos de nivel de servicio que se ajuste como mínimo a los SLA que se presentan en esta RFP para cada área de servicio.

El plan proveedor deberá incorporar los mecanismos necesarios para la revisión periódica tanto de los indicadores como de los objetivos, con el fin de ir adaptando los niveles de servicio a la evolución de los niveles de prestación del servicio.

Identificador	Indicador	Ventana	Objetivo	Penalización
SLA-BCK-01	Copias de seguridad correctas dentro de ventana y según planificación	24x7	>98%	
SLA-BCK-02	Recuperación de datos de negocio correctas	24x7	>98%	
SLA-BCK-03	Porcentaje de incidencias resueltas en plazo			
	Prioridad 1: resueltas en menos de 4h		95%	3%
	Prioridad 2: resueltas en menos de 6h		95%	2%
	Prioridad 3: resueltas en menos de 24h		92%	1%
	Prioridad 4: resueltas en menos de 48h		92%	0,5%
SLA-BCK-04	Tiempo medio de resolución de incidencias			
	Prioridad 1		3h	3%
	Prioridad 2		5h	2%

	Prioridad 3		12h	1%
	Prioridad 4		24h	0,5%
SLA-BCK-05	Cambios planificados realizados correctamente según planificación		97%	
SLA-BCK-06	Porcentaje de solicitudes de servicio realizadas en plazo		95%	1%

- Prioridad 1. Crítico. Sistema parado, gravemente afectado en la seguridad de los datos o con rendimientos tan malos que impiden en la practica el trabajo de la mayor parte de los usurarios sin posibilidad de uso de otra alternativa
- Prioridad 2. Urgente. El sistema no está totalmente parado, pero todos o un número relevante de usuarios están afectado por la incidencia.
- Prioridad 3. Normal. Incidencias que afectan significativamente al trabajo diario de uno o más usuarios.
- Prioridad 4. Poco urgente. Incidencias de menor importancia, mejoras, recomendaciones, sugerencias o consultas

Penalización: El cálculo se realizara de forma mensual y el porcentaje de aplicar se obtendrá una vez rebasados (superior y/o inferior) los objetivos indicados.

La máxima penalización a aplicar no podrá ser superior al 5% del importe mensual del contrato.

3.2.9.1 Medición de indicadores

3.2.9.1.1 SLA-BCK-01 Copias de seguridad correctas dentro de ventana y según planificación.

Definición:

Porcentaje de copias de seguridad (backups) de servidores y bases de datos completadas correctamente en un mes, dentro de las ventanas acordadas para ello, y según planificación, para cada copia de seguridad.

Método de Medida:

Se medirán a partir de la información extraída de las herramientas de backup y de la información sobre ventanas y planificaciones.

Se consideran todos los tipos de backup, tanto incrementales como totales.

Sólo se contabilizarán los backups ejecutados

3.2.9.1.2 SLA-BCK-02 Recuperación de datos de negocio correctas

Definición:

Porcentaje de recuperaciones de datos de Servidores de Negocio completadas correctamente en un mes.

Método de Medida:

Se medirán a partir de la información extraída de las herramientas de registro de peticiones.

La recuperación se considerará completada correctamente cuando se realice conforme a las políticas de backup/restore definidas y lo recuperado sea consistente con lo solicitado por el usuario.

3.2.9.1.3 SLA-BCK-03 Porcentaje de incidencias resueltas en plazo

Definición:

% de Incidencias asignadas a grupos de soporte del oferente de cada Prioridad resueltas en el objetivo de tiempo definido.

Método de Medida:

A partir de la información suministrada por la herramienta de gestión de incidencias.

3.2.9.1.4 SLA-BCK-04 Tiempo medio de resolución de incidencias

Definición:

Tiempo de resolución de Incidencias de categoría distinta de CAU de cada prioridad

Método de Medida:

Se extraerá de la herramienta de gestión de Incidencias. Será calculado como la suma del tiempo empleado en la resolución de los incidentes de una Prioridad dada, dividido por el número total de Incidencias.

3.2.9.1.5 SLA-BCK-05 Cambios planificados realizados correctamente según planificación

Definición:

Porcentaje de cambios planificados realizados correctamente dentro de la ventana planificada, frente al total de cambios planificados

Método de Medida:

Para que se pueda medir este indicador se registrara en la herramienta de cambios, service manager. El tiempo en función de la información de Inicio y Fin del cambio reflejada en la herramienta, existiendo Hora planificada y Hora Real

Las intervenciones que no cumplan este nivel de servicio por razones ajenas a los elementos de servicio gestionados por el oferente, no computarán en el cálculo de este indicador...

3.2.9.1.6 SLA-BCK-06 Porcentaje de solicitudes de servicio realizadas en plazo

Definición:

Porcentaje de Peticiones de servicio del catálogo solicitadas a través de service now por usuarios que se ejecutan en los plazos acordados

Método de Medida:

A través de la herramienta de gestión de peticiones, contabilizando el tiempo desde que se aprueba la petición, y es volcada en la herramienta de gestión de peticiones, y se dispone del material necesario, hasta su realización.

La tabla de tipo de Peticiones de Usuario se definirá en el catálogo (nuevas peticiones, ampliaciones, migraciones) y acordaran plazos con el oferente (aunque nunca operaran NBD). Sus plazos de ejecución se adecuan a cada petición y están definidos en este mismo catálogo

El horario de servicio para este indicador es el comprendido entre las 09:00 horas y las 19:00 horas salvo la excepción recogida arriba

3.3 Descripción de Servicios.

3.3.1 Introducción

Este pliego contempla tanto la gestión de la infraestructura de copias:

1. Servicios de copia y restauración de EJIE.
2. Servicio de copia y restauración para Batera y Osakidetza

Dentro del contrato se han de realizar las tareas necesarias que permitan la unificación tanto de infraestructuras como de modelo de servicio actual de EJIE con el nuevo entorno y modelo de gestión de Batera.

En el ANEXO A se detalla el modelo de servicio actual de EJIE, que habrá que mantener en tanto en cuanto no se unifiquen los dos modelos.

Se deberá presentar un Plan detallado que tenga en cuenta las características, fases y proyectos necesarios para garantizar una correcta transición y una correcta transformación de los servicios TIC. El servicio, tal como se concibe será abordado en cuatro fases diferenciadas:

- Fase de transición
- Fase de transformación
- Fase de servicio recurrente
- Fase de devolución del servicio

3.3.2 Fase de transición

La fase de transición tendrá una duración máxima de un mes, a partir de la fecha de entrada en vigor del contrato, valorándose su finalización en un plazo de tiempo inferior. Durante este período, el Adjudicatario, como proveedor entrante, implementará su solución para la prestación de los servicios (arquitecturas, herramientas, redes, comunicaciones, etc.), configurará sus equipos, adquirirá el conocimiento técnico y/o funcional en función de los servicios y, con carácter general, se preparará para la prestación de los mismos. Al finalizar este período de tiempo, el Adjudicatario se responsabilizará del servicio.

Principales actividades incluidas:

- Definición de la relación entre EJIE y el Adjudicatario, así como la que pudiera existir con otros actores involucrados en la prestación de los servicios.
- Creación de un Plan de Transferencia, que tenga en cuenta la criticidad de los servicios.
- Preparación de la infraestructura HW & SW necesaria para la prestación de los servicios.
- Implementación de arquitecturas, soluciones técnicas y medidas de seguridad para el despliegue, pruebas de configuración y compatibilidad.
- Configuración de las herramientas de soporte para la gestión de los servicios.
- Adquisición de conocimiento interno, en función del servicio adjudicado.
- Set-up general para la prestación de los servicios adjudicados.

3.3.3 Fase de transformación

La fase de transformación tendrá una duración máxima de 4 meses, a partir de la fecha de finalización de la fase anterior.

Durante este período, el Adjudicatario pondrá en marcha los servicios, definirá los procedimientos operativos, designará los comités para la implementación del Modelo de Relación y medirá y fijará los indicadores de ANS que pudiera aportar de forma adicional a los expuestos en este pliego, o que pudieran quedar pendientes de definir. Al finalizar este período, el Adjudicatario asumirá la responsabilidad completa sobre el cumplimiento de los Acuerdos de Nivel de Servicio y calidad percibida acordados.

Durante este periodo, el proveedor actual continúa realizando la prestación del y el Principales actividades incluidas:

Determinación del Manual de Procedimientos Operativos aplicables, así como del nuevo Manual de Procedimientos que va a regir la operación del contrato.

- Identificación y resolución de cualquier cuestión comercial y/o técnica, que pueda tener repercusiones sobre los servicios.
- Constitución de los comités acordados e implantar el Modelo de Relación.
- Realización del inventario de documentación existente relativa a los servicios bajo el alcance, identificando la información crítica para prestar el servicio, análisis e incorporación de mejoras de mutuo acuerdo, generación de documentación si ésta no existiera.
- Determinación de los ANS aún pendientes de definir.
- Establecimiento y aplicación de métodos, herramientas y procedimientos de medición, cálculo y reporting utilizados para medir el cumplimiento de los Acuerdos de Nivel de Servicio.
- Incorporación de recursos, organización de los equipos de trabajo, establecimiento y ejecución de planes de formación.
- Establecimiento y ejecución de los planes de seguridad, tratamiento de riesgos, continuidad de negocio y recuperación ante desastres, asociados para asegurar que se realiza en los plazos previstos y con los criterios de aceptación establecidos para cada hito, contemplando, de forma particular, todos los procedimientos e infraestructura de respaldo necesarios para asegurar la continuidad del servicio.
- Documentar las tareas ejecutadas durante la transferencia.

EJIE y el Adjudicatario deberán acordar la primera versión del Plan de transformación que entrará en vigor para llevarlo a la práctica. Posteriormente, y cuando proceda, podrán incluirse los cambios oportunos para adecuar el Plan a la situación de EJIE en cada instante.

EJIE y el Adjudicatario designarán cada uno a una persona responsable para el Establecimiento y Transición de los Servicios, los cuales se responsabilizarán de la supervisión del cumplimiento del Plan de Establecimiento y Transición previamente acordado y de la coordinación entre partes. Se reunirán regularmente, con calendario previamente consensuado, para revisar el estado del Plan y para resolver cualquier problema.

Se creará un equipo de establecimiento y transición, cuyos miembros tendrán asignadas tareas específicas que habrán de realizar dentro de los plazos establecidos en el Plan. La coordinación se realizará mediante reuniones planificadas que serán presididas por el responsable de EJIE nominado para tal fin. Como mínimo se celebrará una reunión quincenal con los responsables de gestión del servicio.

En estas reuniones, cada miembro del equipo presentará un informe de seguimiento a los responsables, incluyendo aquellos problemas y/o comentarios puestos de manifiesto. Las acciones derivadas del análisis de los problemas y/o comentarios que procedan, serán incluidas en planes específicos para su resolución, incluyendo la identificación de los miembros del equipo responsables y las fechas para su resolución.

El plan de transformación describirá:

- Objetivos generales y específicos de cada parte del Plan.
- Recursos que EJIE y del Adjudicatario necesitarán para llevar a cabo el establecimiento y la transición de los servicios durante sus períodos respectivos.
- Calendario del proceso: desglosado por Establecimiento y Transición.
- Fases, actividades detalladas, prioridades, dependencias, hitos, criterios de aceptación, supuestos técnicos y entregables aplicables.
- Plazos requeridos, fechas aplicables a las actividades y personas responsables de las tareas individuales.
- Detalle de las responsabilidades aplicables.
- Cualquier requisito específico para el Establecimiento y la Transición relativo adicional que se estime importante.
- Metodologías de seguimiento y control del Plan.
- Análisis de riesgos y controles para la mitigación de los mismos, asociados al Establecimiento y Transición.

Dentro del Plan se tratará, de forma específica, la transición de aquellas iniciativas que pudieran estar en curso.

El Plan de Establecimiento y Transición inicial, así como sus posibles modificaciones y actualizaciones, deben ser aprobados en todo caso por **EJIE** de forma previa a la implementación y ejecución de las actuaciones en él incluidas

3.3.4 Fase de servicio recurrente

El presente bloque describe el alcance y condiciones de los servicios de soporte. Esta fase incluye la gestión de las infraestructuras de copias de seguridad actuales de EJIE, durante dos años, hasta la finalización del contrato actual.

Esté servicio de copias de seguridad de EJIE, será absorbido en su totalidad a la finalización del contrato actual.

3.3.4.1 Descripción de tareas por parte del licitador

El alcance del servicio incluye las funciones de administración y soporte a componentes de la infraestructura de copias de seguridad.

Quedan incluidas en el alcance las ampliaciones o evoluciones dentro de esta tecnología, que pudieran surgir durante la duración del contrato.

El servicio contratado participara en los siguientes procesos:

Gestión del servicio

- Gestión del equipo y producción. Gestión del equipo técnico, distribución de tareas, planificación y seguimiento, gestión del conocimiento
- Gestión de los niveles de servicio. Cumplimiento, seguimiento y reporte de los niveles de servicio acordados, adecuación de los niveles a las variaciones de las necesidades
- Gestión de calidad del servicio. Informes, seguimiento, tendencias, recomendaciones, gestión de la satisfacción de las expectativas del cliente.
- Gestión de la documentación. Gestión de la documentación del servicio, generando y manteniendo la documentación de los nuevos procesos, procedimientos y proyectos que se definan durante el transcurso del servicio

- Gestión de eventos. Revisión de alertas de monitorización con el fin de prevenir el funcionamiento incorrecto de las diferentes aplicaciones. Documentación de las causas/soluciones del evento

Gestión de incidencias y problemas

El Objetivo del proceso de Gestión de incidencias y problemas es solventar las incidencias cuanto antes, afecten o no al servicio, y minimizar el impacto adverso sobre las operaciones de negocio ante cualquier problema que se produzca. Para evitar nuevas incidencias se deberán analizar las causas por las cuales se han producido y proponer las acciones correctivas necesarias para evitarlas.

Será responsabilidad del proveedor el identificar las posibles áreas donde puedan producirse problemas, proponer a EJIE las acciones preventivas, y en caso de ser aprobadas, aplicar las medidas acordadas.

La gestión de incidencias deberá cubrir los horarios de disponibilidad pactados para cada uno de los sistemas, información que le será entregada al Servicio, así como las sucesivas modificaciones, siendo en general de 24x7 para todos productivos y para el resto de los entornos cuando estén categorizadas como críticas. Se deberá dar soporte también a las paradas y arranques planificados de los servicios aunque no estén dentro de los de 24x7.

Gestión de cambios

El proveedor deberá planificar el cambio de manera que este se haga de forma segura e interfiriendo lo menos posible en los horarios de disponibilidad pactados para los sistemas o servicios afectados. Se deberá disponer, siempre, de un procedimiento de vuelta atrás, por si pudiera ser necesario.

Deberá planificar los cambios de aplicaciones, S.O., configuración, la aplicación de parches, notas y modificaciones en los sistemas de cada entorno tecnológico. La necesidad de los mismos deberá ser solicitada y en su caso validada por los grupos de personal interno de EJIE.

Gestion de disponibilidad y capacidad

El Servicio deberá realizar una serie de tareas proactivas con el objetivo de asegurar la disponibilidad y rendimiento de los sistemas. Deberá identificar los elementos a monitorizar, y obtener los datos de los sistemas que permitan realizar los Planes de Capacidad.

Se ha de establecer un calendario de auditorías periódicas en la que participen personal asignado por EJIE y personal por parte del licitador que no participe directamente en el servicio.

Gestión de peticiones

El propósito del proceso de Gestión de Peticiones es la realización de las solicitudes de necesidad o servicios bajo demanda consignadas en los catálogos de servicios publicados por EJIE para cada uno de los servicios.

El proveedor adjudicatario será responsable del mantenimiento de este catálogo, junto con el responsable del servicio afectado.

Para la gestión de estas solicitudes, se utilizara la herramienta escogida por EJIE, HP Service Manager, donde se proporciona una información permanente de la situación de cada solicitud a los implicados en ella.

Las solicitudes no incluidas en el Catálogo de Servicios deberán ser aprobadas por un responsable del servicio afectado.

Ejecución de proyectos

Las actividades de este proceso vienen motivadas por las demandas de peticiones de nuevos servicios o funcionalidades, o por las necesidades de evolución tecnológica propuestas por EJIE.

Los tipos de proyectos en los que podrán participar son Tres.

- Proyectos de Implantación de Nuevos Servicios o Tecnologías
- Proyectos de evolución tecnológica Incluida en el alcance

- Proyectos de valor añadido
- Tareas de evolución tecnológica

3.3.4.2 Descripción del servicio

Se plantea un servicio que contemple las siguientes disciplinas:

Disciplina	Procesos de gestión del servicio asociados
Helpdesk 24x7 y soporte telefónico de 1º nivel	Gestión de incidencias y problemas
Soporte Reactivo de 2º y 3º nivel 24x7	Gestión de Incidencias y problemas
Soporte Preventivo y Evolutivo 5x8	Gestión de Peticiones Gestión de la disponibilidad y capacidad Ejecución de Proyectos
Gestión del servicio	Gestión del servicio Gestión de calidad Gestión de cambios

A continuación se describe el alcance y los requerimientos mínimos del servicio dentro de cada uno de sus apartados.

3.3.4.3 Helpdesk y soporte telefónico de 1º nivel 24x7

3.3.4.3.1 Características del servicio

El suministrador pondrá a disposición de EJIE un servicio Helpdesk como vía de entrada al servicio de soporte. EJIE decidirá si los usuarios de este servicio serán los departamentos de informática de los Centros o el propio CAU de EJIE. En cualquier caso EJIE designará y comunicará al adjudicatario los interlocutores que tendrán acceso al servicio.

Los requerimientos mínimos que debe cumplir el servicio son:

- Canales de entrada: teléfono, correo electrónico y herramienta de gestión TI de EJIE. Los usuarios autorizados de EJIE deben tener acceso en tiempo real a la información de estado de las incidencias.
- El servicio deberá garantizar la respuesta en el 100% de los casos.
- Se pondrá en marcha al comienzo del contrato y de forma consensuada con EJIE un modelo de tipificaciones de incidencias desde el punto de vista técnico y de severidades y procedimiento de escalado de incidencias.
- El suministrador elaborará las guías de uso de los servicios de soporte para los usuarios finales del servicio.
- El servicio no solo estará destinado a la recepción y registro de incidencias sino que deberá incluir un servicio de soporte telefónico inmediato (máximo 1 hora de tiempo de respuesta) de primer nivel para resolución de incidencias o diagnóstico, discriminación y escalado de la misma al soporte especializados 24x7.

- Se realizará seguimiento y registro documental de la vida de cada incidencia a través de todos sus estados hasta su cierre y registro de la documentación técnica asociada. Esta documentación podrá ser solicitada por EJIE en cualquier momento durante la vida del contrato de soporte.

Las actividades que están dentro del alcance de este servicio son:

- Recepción de la incidencia
- Identificación de la incidencia, problema, avería o solicitud y asignación de prioridad
- Soporte telefónico de primer nivel. Se valorará un soporte telefónico de segundo nivel en el marco del servicio de Helpdesk.
- Gestión de escalado
- Control y cierre de incidencias y Registro de toda la documentación técnica asociada a la incidencia e información de seguimiento de todos los estados asociados a la vida de la misma para la obtención periódica de informes.

3.3.4.3.2 Compromiso de nivel de servicio particular

- Se requiere la prestación de este servicio en modalidad 24x7
- El tiempo de respuesta de la helpdesk debe ser inmediato, el tiempo de respuesta del soporte telefónico deberá ser inferior a 1 hora desde la recepción de la incidencia por parte del servicio de Helpdesk

3.3.4.4 Soporte reactivo de 2º y 3º nivel 24x7

3.3.4.4.1 Características del servicio

Mediante este servicio se prestará a los Departamentos de Informática de los Centros, soporte reactivo de 2º y 3º nivel ante cualquier incidencia relacionada con el entorno a soportar dentro del alcance. Este servicio deberá estar disponible en modalidad 24x7 y será prestado por un equipo multidisciplinar compuesto por perfiles especialistas en las tecnologías involucradas en el contrato de soporte, que deberán estar preparados para actuar en caso necesario, conforme a los tiempos de respuesta y resolución

Este equipo técnico deberá conocer en detalle la instalación particular, información relevante y peculiaridades de cada Centro a soportar. Los perfiles que conforman este equipo serán personal de sistemas, especialista en la implantación, administración y gestión de las infraestructuras desplegadas

El servicio de soporte reactivo 24x7 consistirá en la resolución de incidencias y problemas surgidos por cualquier motivo, en cualquiera de los componentes de la infraestructura objeto de soporte ya sean:

- Averías hardware e incidencias derivadas de ellas
- Incidencias motivadas por un problema software a nivel de plataforma, ya sea de versión, instalación incorrecta o configuración e incidencias derivadas del mismo
- Incidencias derivados de la configuración de los sistemas
- Degradación de los sistemas
- Incidencias motivadas por error en la operación
- Incidencias surgidas por desconocimiento de la arquitectura u operación de los sistemas
- Mal funcionamiento de los sistemas
- Otros……;

Las incidencias cubiertas por este servicio serán reportadas a la Helpdesk por parte de los Centros, desde donde el suministrador gestionará su escalado de acuerdo a los tiempos de los niveles de servicio especificados. Incluyendo, si fuera el caso de haberse incluido nuevas infraestructuras, el escalado al fabricante de las mismas a través de los contratos de mantenimiento que EJIE haya dispuesto con él.

El soporte puede ser prestado remotamente (por control remoto ej. vía Terminal Server y a través de un acceso VPN facilitado por EJIE) o insitu cuando el Centro o la naturaleza de la incidencia así lo requiera.

En el marco de los servicios reactivos, objeto del presente apartado, se debe contemplar la resolución de incidencias relacionadas con degradación o mal funcionamiento de los sistemas operativos de los servidores virtuales de los Centros que afecten al buen funcionamiento de los servicios en ellos contenidos. El servicio no incluye soporte a aplicaciones, únicamente a nivel de Sistema Operativo.

3.3.4.4.2 Compromiso de nivel de servicio particular

Este servicio se presta en modalidad 24x7.

La vía de acceso a este servicio será la Helpdesk y el tiempo de respuesta desde la recepción de la incidencia por parte de la helpdesk, será:

- Inferior a 2 horas si la atención es remota
- Inferior a 4 horas si la atención es insitu

Independientemente de los niveles de severidad que se establezcan para las incidencias al inicio del contrato, para aquellos incidentes que impliquen parada de servicios, el adjudicatario debe garantizar un tiempo de resolución de 8 horas (resolución en el día).

3.3.4.5 Soporte Preventivo y Evolutivo 5x8

3.3.4.5.1 Características del servicio

Este servicio, consiste en la prestación por parte del equipo de soporte especializado, de soporte orientado a la prevención de incidencias o problemas y a la evolución y explotación más eficiente de la plataforma. Se dimensionará una bolsa de horas de perfiles mixtos para cubrir los siguientes aspectos:

- Soporte a la implementación de nuevos servidores virtuales o ampliación de la infraestructura tanto hardware como software en el aspecto de virtualización, almacenamiento y backup
- Soporte a los procesos de virtualización de máquinas físicas existentes
- Necesidad de creación de nuevas plantillas de máquinas virtuales
- Mantenimiento de las plantillas de máquinas virtuales en los niveles de sistema operativo, software antivirus y fixes de seguridad que determine EJIE y mantenimiento de Service pack de agentes.
- Soporte a la infraestructura ante cambios del entorno
- Modificación de procedimientos de backup y soporte y asesoramiento en la creación de nuevos procedimientos
- Soporte a la Interlocución con proveedores (ej. Laboratorios) para asesoramiento o soporte a la instalación de nuevas aplicaciones y soporte durante la implantación.
- Aplicación de firmware preventivo.
- Recomendaciones de mejora para la ampliación, optimización, diseño y disponibilidad de infraestructuras y servicios
- Asesoramiento para la integración de nuevas funcionalidades o servicios
- Revisión y actualización la documentación de la instalación de cada centro para su puesta al día.

3.3.4.5.2 Compromiso de nivel de servicio particular

Este servicio se prestará en horario 5x8 de forma planificada.

3.3.4.5.3 Dimensionamiento del servicio

Este servicio se dimensionará en una bolsa de 200 horas de perfiles mixtos especialistas en las tecnologías involucradas.

3.3.5 Gestión del servicio

Además de los servicios especificados, helpdesk 24x7, servicios reactivos y preventivos, el adjudicatario gestionará las garantías y mejoras de garantías ofrecidas por los fabricantes.

La gestión del servicio en su totalidad debe ser cubierta por un perfil de Jefe de Proyecto que actué como Gestor especializado del servicio, que conocedor de las características y peculiaridades de los entornos de los Centros a soportar, se encargará de coordinar todos los aspectos del servicio, asegurar el cumplimiento de los compromisos de calidad y nivel de servicio. El Gestor del servicio, será el interlocutor final con los Centros para atender a todo el conjunto de demandas y necesidades, siendo el punto de entrada principal de todas las peticiones excepto las peticiones de servicio reactivo y algunas peticiones de carácter preventivo y evolutivo, que normalmente entrarán por la vía de la Helpdesk.

Se deberán especificar con detalle en la propuesta las tareas y actividades que realizarán en el ámbito de la gestión del servicio para garantizar la calidad del mismo y los niveles de servicio.

3.3.6 Fase de Devolución del servicio

La transferencia de los servicios entre proveedores será responsabilidad del proveedor entrante, aunque el proveedor saliente deberá colaborar para que en ningún caso esta transferencia afecte al funcionamiento del servicio. Con el fin de garantizar dicha colaboración, EJIE o quien éste designe supervisará los procesos de transferencia.

El licitador incluirá en su propuesta un Plan de Devolución que describa las obligaciones y tareas que tendrán que ser desarrolladas en relación con la devolución del servicio y que incluya los términos y condiciones en que se realizará esta reversión, que deberá cumplir con los siguientes principios y contenidos:

- El plazo de ejecución será de 3 meses desde la notificación oficial de expiración o cancelación total o parcial del servicio, tiempo tras el cual el adjudicatario tendrá que poner en marcha el Plan de Devolución ofertado.
- Incluirá la metodología de traspaso de conocimiento de los aspectos fundamentales de operaciones y proyectos en curso

Durante este período, el proveedor saliente no podrá incrementar las tarifas sobre los precios de servicio vigentes en el momento de la finalización formal de los contratos.

3.3.7 Contingencia de los servicios que presta el proveedor

El plan de contingencia busca asegurar la continuidad de todos los servicios que prestará el proveedor dentro del marco contractual que regulará el presente PBT, ante cualquier desastre que pudiera afectar de forma grave su operativa. Se entiende como contingencia una interrupción del servicio en las instalaciones desde donde se proveen los servicios por cualquier situación.

El proveedor deberá describir el plan de contingencia del que dispone, el cual deberá permitir continuar la ejecución del servicio en instalaciones alternativas a las habituales, así como los tiempos de recuperación que lo regulan.

Se realizarán simulacros periódicos, de los que se presentará informe y plan de acción sobre las deficiencias detectadas, en caso de existir alguna.

3.3.8 Perfiles profesionales

Para conformar el equipo de soporte, el suministrador debe ofrecer un equipo de trabajo dimensionado y con una serie de perfiles técnicos que garanticen el servicio y que deberán estar considerados entre los siguientes:

- Consultor especialista en sistemas de backup.
- Técnicos de sistemas en almacenamiento especialistas en la solución implantada.

Tanto la composición del equipo como la calidad del mismo serán evaluadas en la fase de valoración técnica de las ofertas, por lo que dichas características deberán detallarse en la oferta.

3.3.9 Modelo de relación y comunicación

Tal y como se ha mencionado en otros apartados, cada Centro dispone de su propio departamento de Informática desde el cual se administran y gestionan todas las infraestructuras de Sistemas de Información del Centro, por lo tanto los Centros serán usuarios directos del servicio de soporte.

A continuación se describen las pautas básicas en las que el suministrador se deberá basar a la hora de definir el modelo de relación a establecer:

- Los Departamentos de Informática de los Centros o bien el CAU de EJIE, si así se establece, accederán al servicio de soporte únicamente a través de la Helpdesk del adjudicatario o del Gestor especializado asignado por este para el servicio. En el caso del servicio de soporte reactivo, el punto de entrada y de cierre de incidencias será la Helpdesk del adjudicatario que a partir de aquí se encargará del escalado y seguimiento hasta el cierre total de la incidencia, incluyendo escalado al servicio de mantenimiento de los fabricantes.
- Servicios Centrales de EJIE tendrá acceso directo al Gestor de Servicio a efectos de consultas, reportes o peticiones y para consensuar acciones de mejora del servicio
- El gestor de servicio reporta a EJIE la información que se le solicite acerca del servicio prestado.
- Los grupos de soporte que se integran en el servicio del suministrador tienen línea directa con los Departamentos de Informática de los Centros en tiempo de resolución de una incidencia.
- En caso de requerir establecer contacto entre los grupos de soporte que integran el servicio del suministrador y los grupos de soporte de Servicios Centrales de EJIE, este contacto se canalizará a través del gestor del servicio de EJIE
- Las peticiones de servicio bajo demanda (servicios de sistemas, servicios de consultoría, ampliaciones, etc...;) serán canalizados a través del gestor de servicio del suministrador que reportará a Servicios Centrales.

4 Contenido de las ofertas

No se incluirá en la oferta técnica ningún precio, dato, etc…; susceptible de ser evaluado mediante fórmulas.

Así mismo se excluirán ofertas incompletas, o que no se ajusten a lo especificado en este PBT y Anexos.

Las empresas interesadas en la adjudicación presentarán en su propuesta al menos la siguiente información:

1. Identificación de la oferta
   - Visión general del servicio de cada uno de los bloques y resumen ejecutivo (12 páginas como máximo).
2. Descripción de la solución HW y SW

   Se ha de incluir una descripción detallada de la arquitectura ofertada para cumplir con los requisitos del presente pliego.
3. Contenidos y gestión del servicio

Por cada bloque de la oferta (soporte y evolución):

- Descripción de los contenidos de trabajo
- Descripción de los servicios ofertados, el plan, En el caso del bloque 2 se detallará el plan de contingencia del proceso de migración.
- Aspectos organizativos, entidades que intervienen directa o indirectamente, los grupos de trabajo a constituir, método de coordinación de los mismos, etc.
- Procedimiento de Control y Seguimiento del servicio a fin de detectar posibles desviaciones y tomar las acciones correctivas adecuadas.

4. Provisión del Servicio

Se especificarán la forma de proveer el servicio en las disciplinas que para cada bloque correspondan:

- Gestión de la Continuidad del servicio indicando los medios y mecanismos previstos para el desarrollo de esta actividad.
- Gestión del Nivel de Servicio indicando claramente el acuerdo de nivel de servicio propuesto para los diferentes aspectos del contrato y los mecanismos previstos para el control y gestión del proyecto.
- Gestión de la disponibilidad de servicio indicando los medios y mecanismos previstos para el desarrollo de esta actividad
- Gestión de la capacidad del servicio indicando los aspectos relevantes para llevar a cabo esta actividad.

5. Equipos de trabajo y perfiles técnicos
   - Detalle por cada área de servicio, del personal técnico certificado en cada una de las disciplinas y dedicado a ellas, los perfiles y recursos asociados, funciones y organización, así como los porcentajes de dedicación de cada una de los procesos del servicio.
   - Detalle de los Perfiles profesionales previstos
6. Garantías de Calidad

Los ofertantes deberán incluir para su valoración los certificados de garantía de calidad siguientes:

- Relativa a componentes y piezas de repuesto originales.
- Relativa al montaje de componentes-piezas.

- Relativa a los servicios de reparación...
- Relativa a la calidad de gestión de procesos
- Almacenamiento y Logística de Piezas
- Sistemas de stock de repuestos.

7. Identificación de los aspectos de mejora

   Se han de indicar por parte de las empresas licitadoras cualquier aspecto que consideren oportuno que suponga un impacto en la mejora de la calidad de la oferta describiendo los medios que justifiquen la viabilidad de la misma.

   - En cuanto al equipamiento Hw / Sw cedido para apoyo.
   - En cuanto a los servicios
   - En cuanto a las facilidades de gestión del contrato para EJIE

5 Presupuesto, plazo de ejecución y forma de pago

5.1 Presupuesto

El presupuesto máximo asignado para este expediente es de **4.120.000,00 € (sin IVA)** y de **4.985.200,00 € (con 21% de IVA)**.

Se prevé una posible ampliación de **500.000** € (sin IVA) y de **605.000** € (IVA 21% incl.) para atender un aumento del crecimiento imposible de estimar en el momento de adjudicación del contrato en el número de copias de seguridad a realizar. La incertidumbre del volumen final a contratar viene dado por la imposibilidad de concretar la velocidad de absorción de la nueva plataforma por el resto de entidades de gobierno, que no participan en esta primera fase de unificación.

El valor estimado del contrato es de **4.620.000 € (sin IVA)** y de **5.590.200,00 € (con 21% de IVA).**

Los importes reflejados son máximos, y en ellos estarán incluidos todos los costes de desplazamiento, mano de obra y kit de equipos y piezas necesarias, no siendo propiedad de EJIE, para mantener el correcto funcionamiento de los equipos relacionados.

5.2 Modificaciones previstas

Tal y como se ha indicado en el apartado anterior, se prevén las siguientes modificaciones:

1- Modificación por incremento de entidades a prestar servicios.
   a. Incremento del servicio por aumento del número de copias a realizar

La estimación de la capacidad necesaria para abordar este servicio se ha realizado en base a las cargas de trabajo de los proyectos que se transicionan a operación en la actualidad y previendo las futuras cargas de proyectos de convergencia en Batera.

La creación de nuevos servicios en Batera que impliquen la gestión y transición de nuevos proyectos, así como la demanda de proyectos de convergencia sobre los servicios ofrecidos desde Batera de entidades que a priori no es posible calcular, puede implicar que se realicen modificaciones sobre las necesidades estimadas en cuanto a la capacidad inicial.

Por lo tanto, el dimensionamiento actual previsto en el presupuesto de contratación se ha estimado con la siguiente base:

- Proyectos actuales de EJIE y Osakidetza. El cálculo se ha realizado en función de las cargas de proyectos de transición actuales en estas entidades.
- Dimensionamiento necesario para abordar proyectos de convergencia de entidades sobre los servicios actuales de Elkarlan (Correo, Colaboración y Lync)

La modificación prevista se realizará en función de los siguientes criterios:

Causa de modificación prevista	Modificación prevista	Indicadores
Creación de nuevos servicios en Batera que impliquen nuevos proyectos de construcción y de convergencia de Entidades sobre estos servicios.	Incremento de servicios prestados por coordinadores técnicos.	Métricas del servicio
Incremento del número de Entidades que se integren en Batera	Incremento de servicios prestados por gestores de proyectos. Incremento de servicios prestados por coordinadores técnicos	Métricas del servicio

5.3 Plazo de ejecución.

El contrato tendrá una duración de 4 años contado desde la fecha de formalización del mismo.

5.4 Forma de pago

La forma de pago se realizará en dos fases:

- Un pago inicial de **300.000** euros, que se abonara después de la aceptación del responsable asignado por EJIE de los siguientes puntos:
  - Instalación HW
  - Configuración SLA definidos
- La forma de pago mensual se realizara en función de la previsión de consumo anual, teniendo en cuenta los 400 TB de capacidad de inicio del proyecto, en base a la siguiente tabla:

HW y SW Fijo	CMIP
HW y SW Variable	CTFE
Servicios	CSRV

CTFE: Coste mensual por TB de “Front end” de copias

CSRV: Es el coste mensual de los servicios ofertados

CMIP: Coste mensual de la infraestructura de partida. Teniendo en cuenta que esta infraestructura debe soportar la carga de trabajo inicial descrita en este pliego para los 400 TB de Front End iniciales.

Facturación mensual = CMIP + CSRV + (CTFE x TB ampliados)

La infraestructura se estima que tendrá un incremento de capacidad de Front End:

Año 1 400 TB FE	Año 2 440 TB FE	Año 3 740 TB FE	Año 4 810 TB FE

Estas cifras son solo una estimación que ayude al dimensionamiento adecuado inicial del servicio**, NO obligan a EJIE a la contratación de esos TB de Front End de crecimiento.**

6 Condiciones de seguridad generales

EJIE S.A. proporcionará acceso a sus sistemas informáticos y entregará la información, software y documentación necesaria para poder llevar a cabo los Servicios especificados, debiendo la empresa adjudicataria comprometerse a no utilizar para otros fines que los recogidos en el presente Pliego de Condiciones Técnicas, así como a no extraerla, cederla, publicarla o venderla total o parcialmente, ni en soporte informático ni en papel, debiendo proceder a la devolución o destrucción de los soportes de la información facilitados por EJIE, S.A: , así como a la descarga de la misma de los equipos informáticos (si existieran), una vez se dé por concluido el trabajo. Queda terminantemente prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
- Los equipos y/o aplicaciones que no estén especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de EJIE o bajo supervisión de EJIE. Todos los ordenadores personales que se conecten a la red corporativa serán de las marcas y modelos homologados. El proveedor pondrá a disposición de EJIE dichos equipos para que se les instale el software necesario. Todos los ordenadores personales a los que EJIE les haya instalado software se llevarán a EJIE para que se formatee el disco duro a la finalización del servicio a EJIE.
- El proveedor se compromete a informar periódicamente a EJIE de los activos de información con los que proporciona el servicio.

Serán también de obligado cumplimiento las “Políticas de Seguridad para empresas proveedoras” (Anexo Seguridad del presente PCT, publicadas también en www.ejie.eus, apartado “Perfil de contratante”, “información”). El servicio objeto del presente pliego se proporcionará desde las oficinas del adjudicatario, de modo que:

- Según el apartado “Aplicabilidad de las Políticas Específicas de Seguridad para Proveedores” de dichas políticas:
  - El lugar de ejecución del servicio tendrá la consideración de “remoto”
  - La propiedad de las infraestructuras TIC utilizadas tendrá la consideración “del proveedor”
  - El “nivel de acceso” a los sistemas de EJIE tendrá la consideración de “con acceso privilegiado”
- EJIE se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

7 Criterios de adjudicación de las ofertas

Para la elección de los criterios de valoración y su ponderación se han tenido en consideración los aspectos más significativos recogidos en el Pliego de Bases Técnicas que se acompaña a este expediente, a fin de garantizar que las ofertas de los licitadores se ajusten a lo exigido para los servicios objeto de este expediente.

De acuerdo con lo antedicho, los criterios que servirán de base para la adjudicación del presente contrato serán los siguientes:

7.1 Juicios de Valor: 35 puntos

CRITERIOS DE JUICIO DE VALOR					35
A)	Calidad Técnica.			35	
	Descripción funcionalidades requeridas		15		
	Flexibilidad del servicio		5		
	Gestión del cambio/configuración		5		
	Asistencia técnica		5		
	Contact center		5		

- Descripción funcionalidades requeridas 15 puntos

Se evaluará el cumplimiento de las especificaciones técnicas detalladas en el PBT y el nivel de detalle y contenido de los trabajos a realizar herencia del modelo de colaboración desarrollado en la oferta

- Flexibilidad del servicio 5 puntos

Se valora la posibilidad de ajustar los recursos a lo largo del proyecto en base a las necesidades de EJIE

- Gestión del cambio/configuración 5 puntos

Se valorara la inclusión de acciones destinada a la gestión del cambio: Formación, difusión interna del proyecto, resistencia al cambio,..

- Asistencia técnica 5 puntos

Se valorará la disposición de recursos, humanos y materiales, así como la descripción de los procesos y niveles de servicio.

Se valorará el dimensionamiento del stock de repuestos y bases logísticas.

- Contact center 5 puntos

Se valorará la estrategia propuesta para dar servicio de soporte a usuarios, así como la disponibilidad de recursos humanos y materiales.

Por cada uno de estos apartados, la puntuación obtenida corresponderá a los siguientes criterios y rangos de porcentajes con respecto a los valores máximos indicados en cada apartado.

Calificación	***Puntuación obtenida***
Excelente	100%
Buena	66%
Regular	33%
Deficiente	0%

Excelente (100% de los puntos)

Cuando la propuesta realizada por el proveedor con respecto al criterio de valoración referido no solo cumpla con todas las especificaciones requeridas, sino que incorpore un alto nivel de desglose y detalle, y de este podamos deducir una alta calidad en la propuesta que vaya a redundar en una excelente calidad en el producto servicio.

Buena (66% de los puntos)

Cuando la propuesta realizada por el proveedor con respecto al criterio de valoración referido cumpla con todas las especificaciones requeridas.

Regular (33% de los puntos)

Cuando la propuesta realizada por el proveedor con respecto al criterio de valoración referido aun cumpliendo con todas las especificaciones requeridas, no incorpore un suficiente nivel de desglose y detalle, y de este no podamos deducir la calidad en la propuesta y no podamos deducir la calidad final del producto o servicio.

Deficiente (0% de los puntos)

Cuando la propuesta realizada por el proveedor con respecto al criterio de valoración referido, no cumpla con todas las especificaciones requeridas o no incorpore el mínimo nivel de desglose y detalle que nos permita deducir si el producto o servicio se va a realizar con la calidad mínima exigible.

Umbral mínimo puntuación que debe obtenerse en los criterios no evaluables mediante fórmulas:
Conforme al artículo 150.4 del TRLCSP, para ser admitidos a la valoración global, se exigirá que en los criterios no cuantificables por fórmulas los licitadores alcancen un umbral mínimo de puntuación, **de forma que no serán tenidas en cuenta las ofertas cuya puntuación no sea igual o superior a 20 puntos, y estas ofertas quedarán automáticamente excluidas del resto del proceso selectivo.**

7.2 Criterios de Fórmula: 65 puntos

- Precio : 65 puntos

Valoración coste mensual infraestructura inicial para el servicio

$$Puntuacion\ CMIP = 20 \times \frac{Precio\ tarifa\ mas\ ventajosa\ CMIP\ (la\ del\ precio\ mas\ bajo)}{Tarifa\ CMIP\ oferta\ evaluada}$$

Valoración precio coste mensual de “FrontEnd” de copias

$$Puntuacion\ CTFE = 20 \times \frac{Precio\ tarifa\ mas\ ventajosa\ CTFE\ (la\ del\ precio\ mas\ bajo)}{Tarifa\ CTFE\ oferta\ evaluada}$$

Donde CTFE = Coste por TB del Fronted de copias. (Hardware y Software)

Valoración precio coste mensual servicios de gestión

$$Puntuacion\ CSRV = 25 \times \frac{Precio\ tarifa\ CSRV\ mas\ ventajosa\ (la\ del\ precio\ mas\ bajo)}{Tarifa\ CSRV oferta\ evaluada}$$

Puntación final = Puntuación CTFE + Puntuación CSRV + Puntuación CMIP

8 Anexo I: Modelo de servicio actual EJIE

Se hace una descripción del servicio actual de copias de EJIE para que cada licitador pueda valorar el estado actual del servicio. Las condiciones en las que se habrá de dar el servicio se han detallado a lo largo del PCT.

8.1 Tecnologías

El alcance de los Servicios abarca la totalidad de las Tecnologías de Backup de las que EJIE es responsable, y que se encuentran especificados en el **punto 3.3 del presente PCT**

EJIE dispone de Soportes Avanzados, que denominaremos de Tercer Nivel, con sus principales proveedores tecnológicos. El servicio gestionará estos Soportes con los que EJIE cuenta, coordinando conjuntamente las acciones que garanticen el correcto funcionamiento de los Sistemas.

8.2 Disponibilidad

El servicio se ofrecerá en régimen de **24x7** (24 horas, 7 días a la semana) los 365 días del año, siendo los niveles de actuación los siguientes:

- **Horario Habitual**
  - Jornada partida: Lunes a jueves: 7.00h a 18.00h. Viernes: 7.00h a 16.00h.
  - Jornada continua: Lunes a Viernes: 7.00h a 16.00h.
- **Horario Extendido**
  - Horario no incluido en el horario habitual y mínimo los días laborables y las 24 horas de los fines de semana y festivos. 24x7x365.

En el horario Extendido el tipo de atención podrá ser:

- Soporte de atención telefónica.
- Acceso remoto vía RAS/VPN.
- Presencia in situ.

El tiempo de respuesta deberá ser como **máximo de 30 min desde que se solicita una actuación**, independientemente del método utilizado para la resolución de la incidencia. **El tiempo de Presencia in situ, si fuera necesario, deberá ser como máximo de 2 horas.**

Este servicio fuera de horas deberá ser atendido por los mismos técnicos que conforman el servicio en horario habitual.

8.3 Ámbito

Este servicio se suministrará para los CPDs que gestiona EJIE actualmente, ubicados en Vitoria-Gasteiz, uno en avenida del Mediterráneo 14, y otro en la calle Donostia -San Sebastián 1.

8.4 Características del Servicio

El Servicio se compone de **cuatro funciones principales,** basadas en el ciclo de vida de un servicio IT definido por ITIL v3:

- Operación del servicio
- Transición del servicio
- Diseño del servicio
- Mejora continua del servicio

Las tareas a realizar por el Servicio dentro de cada una de estas cuatro funciones se detallan en los siguientes apartados.

8.5 Operación del servicio

Los servicios principales para la Operación del servicio son los siguientes:

- Gestión de Incidencias
- Gestión de Problemas
- Operación y administración
- Mantenimiento
- Gestión de peticiones
- Gestión de eventos

8.5.1 Gestión de incidencias

El servicio de **Gestión de Incidencias** se encarga de las actividades asociadas con la restauración de la operación de servicio normal lo más rápido posible y minimizar el impacto adverso en las operaciones de negocio del Cliente, asegurando así que se mantienen los mejores niveles posibles de calidad y disponibilidad del servicio.

Las principales actividades del proceso de Gestión de Incidentes incluyen:

- Detección y grabación de incidentes
- Clasificación de incidentes y apoyo inicial
- Investigación y diagnóstico de incidentes
- Escalamiento de incidentes
- Resolución y recuperación de incidentes
- Cierre del incidente

Los siguientes puntos identifican las funciones y responsabilidades más relevantes de Gestión de Incidencias que el proveedor realizará:

- Mantener y desarrollar y procedimientos de Gestión de Incidentes que soporten los requisitos de soporte de la Gestión de Incidencias de EJIE.
- Resolver incidencias en el primer contacto de acuerdo con el Manual de Procedimientos, los documentos de base de datos de conocimiento y las bases de datos de configuración.
- Registrar todas las llamadas / consultas que lleguen
- Identificar, filtrar y clasificar eventos e incidencias a un nivel de prioridad y manejar de acuerdo con los procedimientos acordados de respuesta a incidencias
- Diagnosticar y resolver incidencias. Cuando sea posible, implementar acciones correctivas apropiadas para errores conocidos (por ejemplo, soluciones para problemas no resueltos conocidos)
- Escalar los incidentes al grupo de servicios de nivel siguiente apropiado dentro de los Fabricantes, EJIE o un Proveedor de Servicios de Terceros, tan pronto como esté claro que

la incidencia no puede ser resuelto sin ayuda adicional o como se requiera para cumplir con los requisitos de nivel de servicio tiempos de respuesta
- Monitorizar y rastrear el progreso de la resolución de incidencias hasta el cierre final y registrar / actualizar el estado del registro de las incidencias según corresponda
- Proporcionar asistencia técnica y de procesos de expertos para aplicaciones dentro del ámbito de aplicación en el Nivel 2 y escalar al recurso de Nivel 3 según sea necesario.
- Proveer asistencia de Nivel 2 a consultas sobre las características, funciones y uso de software para todo el hardware y software dentro del alcance.
- Proporcionar soporte de nivel 2 para aplicaciones de software en la lista de aplicaciones compatibles.
- Comprobar que todos los registros (por ejemplo, el inventario, el activo y los registros de Gestión de la configuración) se actualizan para reflejar la incidencia finalizada / resuelta
- Ayudar a los usuarios con preguntas relacionadas sobre funcionalidades del software dentro del alcance.
- Documentar soluciones para resolver incidencias en la base de conocimientos. Actualizar con precisión toda la información pertinente a los problemas.
- Notificar al personal designado de EJIE de todas las Incidencias de Prioridad 1 y Prioridad 2 dentro del plazo designado.
- Mantener registros actuales e históricos de todas las incidencias y la resolución de las mismas durante la vigencia del contrato y proporcionar capacidades de generación de informes y tendencias.
- Resolver problemas, diagnosticar y resolver incidencias para todo el software con garantía y sin garantía.
- Participar en la Identificación, Escalado y Resolución extremo a extremo de las incidencias, y en el proceso de cierre, incluyendo la gestión de tickets de escalado a terceros.
- Determinar si es posible si se debe abrir un problema para resolver una incidencia.
- Seguimiento del estado actual de cualquier incidencia y su registro de problemas correspondiente para asegurar que los problemas identificados sean registrados y resueltos
- Asegurar de que las actividades de resolución de incidencias se ajusten a los procedimientos definidos de Gestión del Cambio.
- Revisar periódicamente el estado de los incidentes abiertos y no resueltos y los problemas conexos, así como los progresos realizados en los problemas registrados.
- Participar en las sesiones de revisión de la gestión de problemas según corresponda.
- Llevar a cabo sesiones de revisión de incidencias y proporcionar listado y estado del mismo categorizado por impacto.
- Coordinar con otros grupos de soporte de nivel 2 de EJIE para adquirir y transferir conocimientos sobre resoluciones de incidencias y problemas y registrar este conocimiento adquirido en la base de conocimientos para facilitar una mayor capacidad para el servicio de nivel 1 de EJIE.
- Realizar un seguimiento con los Usuarios Finales que informaron del incidente para verificar que el incidente fue resuelto a satisfacción del Usuario Final
- Cerrar los incidentes que se resolvieron satisfactoriamente
- Proporcionar informes de la Gestión de Incidencias, según sea necesario

La clasificación de incidencias está tipificada actualmente en **Críticas, Altas, Medias y Bajas.**

8.5.2 Gestión de problemas

El servicio de Gestión de Problemas se encarga de minimizar el impacto adverso de incidencias y problemas en el negocio, causado por errores dentro de la Infraestructura de TI, y para prevenir la repetición de incidencias relacionadas con estos errores determinando la causa subyacente desconocida, asegurando que se inician acciones para mejorar o corregir la situación.

El Proveedor proporcionará servicios de gestión de problemas reactivos diagnosticando y resolviendo problemas en respuesta a uno o más incidentes que han sido reportados a través de la Gestión de Incidentes. Proporcionará un manejo proactivo de problemas para identificar y resolver problemas y errores conocidos antes de que ocurran las incidencias, incluyendo realizar actividades de análisis predictivo, donde sea práctico, identificar posibles problemas futuros, desarrollar planes de mitigación recomendados e implementar acciones y procesos correctivos de mitigación aprobados. El Proveedor también mantendrá, actualizará y difundirá información sobre problemas y las soluciones y resoluciones apropiadas, de manera que el número y el impacto de incidentes que ocurran dentro de la Infraestructura de TI del Cliente se reduzca con el tiempo.

Las principales actividades de la Gestión de Problemas son:

- Control de problemas
- Control de errores
- Prevención proactiva de problemas
- Realizar grandes revisiones de problemas
- Proporcionar informes de gestión de problemas

El Proveedor también es responsable de asegurar que las resoluciones a los problemas se implementan a través de los procedimientos de control apropiados, especialmente la Gestión del Cambio y la Gestión de Versiones. El Proveedor debe coordinar las actividades de Gestión de Problemas con los distintos equipos dentro del Proveedor, EJIE y los Proveedores de Terceros responsables de realizar las actividades de Gestión de Configuración, Gestión de Disponibilidad, Gestión de Capacidad, Gestión de Continuidad de Servicio de TI y Gestión de Nivel de Servicio.

Los siguientes puntos identifican las funciones y responsabilidades relevantes de la Gestión de problemas que el Proveedor deberá realizar:

- Mantener y documentar procedimientos apropiados y metodologías que apoyen los requisitos y políticas de la Gestión de Problemas aprobados y que cumplan con los requisitos de EJIE.
- Asegurar que las actividades de Gestión de Problemas se ajusten a los procedimientos definidos de Gestión del Cambio establecidos en el Manual de Procedimientos
- Coordinar con los equipos apropiados de Gestión de Incidentes y tomar posesión de las actividades de Gestión de Problemas de todos los problemas determinados para residir en el área de responsabilidad del Proveedor (por ejemplo, detección, registro, RCA, etc.)
- Coordinar, escalar y realizar un seguimiento de las actividades de Gestión de Problemas dentro de EJIE y Terceras Partes relacionadas con los problemas determinados para residir en todas las áreas responsabilidad del Proveedor.
- Señalar todos los incidentes que requieran que se realicen el estudio de causa raíz según procedimientos acordados.
- Asegurarse de que los problemas recurrentes que cumplan los criterios definidos relacionados con el área de responsabilidad en el servicio de TI del Proveedor se revisen mediante procedimientos RCA (Root Cause Analisys)
- Realizar análisis proactivos de tendencias de incidencias y problemas y otros elementos de datos para identificar situaciones recurrentes que son o pueden ser indicativas de problemas futuros y puntos de fallo.
- Seguir e informar sobre problemas y tendencias o fallos, e identificar las consecuencias asociadas de los problemas.
- Desarrollar y recomendar acciones correctivas o soluciones para abordar incidencias y problemas recurrentes, así como estrategias de mitigación y acciones a tomar para evitar posibles problemas identificados a través del análisis de tendencias.
- Identificar, desarrollar, documentar y recomendar soluciones adecuadas para detectar errores conocidos de problemas no resueltos, y notificar a Gestión de Incidencias y a todas las demás partes interesadas apropiadas de su disponibilidad si se aprueba. Documentar la solución en la base de conocimientos.

- Coordinar y monitorizar el estado de las actividades de RCA realizadas por EJIE y Proveedores de Terceros (es decir, de otras áreas de servicios de TI)
- Documentar y actualizar la base de conocimiento de Gestión de problemas con información sobre acciones, actividades y estado de resolución de problemas (por ejemplo, causa raíz, errores conocidos, soluciones alternativas, etc.) y notificar a todos los interesados apropiados sobre la disponibilidad de información
- Coordinar con EJIE y Proveedores de Servicios Terceros para asegurar que el conocimiento sobre problemas relacionados con otras áreas de servicios de TI sea capturado y entrado en una base de conocimiento centralizada de Gestión de Problemas
- Asegurar que las actividades de resolución de problemas se ajusten a los procedimientos definidos de Gestión del Cambio establecidos en el Manual de Procedimientos.
- Proporcionar informes de estado detallando la causa raíz y el procedimiento para corregir los problemas recurrentes, según lo determine EJIE
- Realizar reuniones de revisión de la Gestión de Problemas y proporcionar listado y estado de las mismas clasificadas por impacto de problemas
- Revisar periódicamente el estado de los incidentes abiertos y los problemas conexos, así como los progresos realizados en la solución de los problemas
- Crear la documentación de RFC con las acciones correctivas recomendadas que se deben tomar para resolver un problema y enviar a EJIE para su revisión y aprobación.
- Realizar sesiones periódicas de revisión proactiva de la Gestión de Problemas.
- Proporcionar informes de gestión de problemas según se requiera.

8.5.3 Operación y Administración

Operación y servicios de administración son las actividades asociadas con la provisión de una infraestructura de TI estable y con procedimientos efectivos y eficientes para asegurar que los servicios de TI cumplan con los objetivos y requerimientos de SLR (Service Level Requirement). Los siguientes puntos identifican las funciones y responsabilidades relevantes de Operaciones y Administración que el Proveedor debe realizar:

- Mantener y documentar procedimientos de Operaciones y Administración que cumplan con los requisitos y se adhieran a las políticas definidas.
- Desarrollar documentación operacional (es decir, libros de ejecución, listas de contactos, scripts de operaciones, etc.) que cumpla con los requisitos de EJIE.
- Coordinar con EJIE para implementar herramientas de administración para supervisar las aplicaciones de Infraestructura de TI y Cliente.
- Instalar y configurar o utilizar herramientas de administración de tal manera que las incidencias, problemas y eventos sean identificados, reportados y resueltos proactivamente de acuerdo con las SLRs prescritas.
- Realizar una monitorización de eventos de servicios de TI para detectar condiciones anormales o alarmas, registrar condiciones anormales, analizar la condición y tomar medidas correctivas
- Administrar software y para cumplir con las SLR, minimizar el tiempo de inactividad y minimizar los requerimientos de recursos de EJIE.
- Gestionar y coordinar a subcontratistas y Terceros para cumplir con SLRs.
- Desarrollar y proporcionar informes operacionales (diarios, semanales, mensuales) que proporcionen estado de las actividades operacionales, problemas de producción y métricas operativas clave.
- Proporcionar a EJIE o cualquier proveedor permitido una copia de documentación suministrada por terceros (incluyendo actualizaciones de los mismos)

8.5.4 Mantenimiento

Los servicios de mantenimiento son las actividades asociadas con el mantenimiento y la reparación de software incluyendo los servicios "parcheado". La plataforma instalada y los niveles de versión del producto no deben estar detrás del nivel de versionado especificado por EJIE. Los siguientes puntos identifican las funciones y responsabilidades relevantes de Mantenimiento que el Proveedor debe realizar:

- Mantener y documentar los Procedimientos de Mantenimiento que cumplan con los requisitos y se adhieran a las políticas definidas
- Desarrollar calendarios de mantenimiento.
- Asegurar una cobertura de mantenimiento apropiada para todos los componentes de la torre del servicio.
- Proporcione el mantenimiento y parcheado en las ubicaciones definidas por EJIE, incluyendo el envío de técnicos a la ubicación del servicio si es necesario.
- Realizar (y / o coordine con el proveedor de mantenimiento de terceros, si procede) diagnósticos y mantenimiento en los componentes de la torre de servicio.
- Realizar un análisis del impacto y / o aplicabilidad de los parches y / o service packs proporcionados por Fabricante, de acuerdo con las políticas y requisitos de EJIE.
- Revisar todos los parches relevantes para el entorno de TI y clasifique la necesidad y la velocidad a la que deben instalarse los parches de seguridad, según lo definido por las políticas y la Gestión del cambio.
- Instalar los parches por los procedimientos de la administración del cambio de EJIE incluyendo la adquisición de la aprobación requerida de EJIE.
- Instalar (y / o coordine con el Proveedor de Mantenimiento de Terceros, si procede) los Service Packs, las versiones de mantenimiento de software y firmware, etc.
- Realizar la distribución de software y el control de versiones relacionado con el mantenimiento, tanto electrónico como manual.
- Reemplazar (y / o coordine con el proveedor de mantenimiento de terceros, si procede) piezas defectuosas, incluido el mantenimiento preventivo, de acuerdo con las tasas de tiempo medio entre fallos publicadas por el fabricante.

8.5.5 Evolución Tecnológica

Los servicios de Evolución Tecnológica son las actividades asociadas con la modernización del entorno de TI de forma continua, para asegurar que los componentes del sistema permanezcan actualizados con las plataformas tecnológicas de la industria. Los siguientes puntos identifican las funciones y responsabilidades relevantes de Evolución Tecnológica que el Proveedor debe realizar:

- Recomendar procedimientos y planes de gestión del ciclo de vida de evolución tecnológica adecuados para respaldar los requisitos del negocio de EJIE
- Realizar las tareas necesarias para cumplir con los planes de evolución tecnológica.
- Proporcionar informes de gestión sobre el progreso de los planes de evolución tecnológica.

8.5.6 Gestión de Solicitudes

Los servicios de Gestión de solicitudes son actividades para cumplir las Solicitudes de Servicio por ejemplo, solicitudes de cambio de contraseña o información. Los siguientes puntos identifican las funciones y responsabilidades relevantes de Gestion de peticiones/solicitudes que el Proveedor debe realizar:

- Mantener y documentar los Procedimientos de Gestión de Peticiones que cumplan con los requisitos y se adhieran a las políticas definidas.
- Realizar las tareas necesarias para cumplir la solicitud.
- Proponer añadir nuevos servicios al catálogo en base a un análisis de todas las solicitudes recibidas.

- Proporcionar informes de gestión sobre el progreso y uso de los servicios.

8.5.7 Gestión Eventos

Los servicios de Gestión de eventos son actividades para asegurar que los elementos de Configuración (CI) y los servicios sean monitorizados constantemente, así como descartar y categorizar Eventos antes de decidir qué acciones son las adecuadas. Se considera un desencadenante muy importante de actividades en la Gestión de Incidentes y la Gestión de Problemas. Los siguientes puntos identifican las funciones y responsabilidades relevantes de Gestión de eventos que el Proveedor debe realizar:

- Mantener y documentar los Procedimientos de Gestión de Eventos que cumplan con los requisitos y se adhieran a las políticas definidas.
- Mantener de Mecanismos y Reglas de Monitorización de Eventos. Establecer y mantener los mecanismos para generar reglas efectivas para los procesos de descarte y correlación de Eventos.
- Clasificar y Categorizar de Eventos. Clasificar aquellos eventos que se pueden obviar, y asignar categorías a los que son significativos.
- Correlación de Eventos y Selección de Respuestas. Interpretar el significado de un Evento y elegir una respuesta adecuada.
- Revisar y Cerrar Eventos. Verificar que los Eventos hayan sido manejados adecuadamente y si se pueden cerrar. Este proceso también sirve para asegurar que los registros de eventos sean analizados de manera que se identifiquen tendencias y patrones que puedan sugerir medidas correctivas necesarias.

8.6 Transición del servicio

8.6.1 Gestión de cambio

Los Servicios de Gestión de Cambios son actividades para asegurar que se usan métodos y procedimientos estandarizados para el manejo eficiente y rápido de todos los cambios, para minimizar el impacto del cambio en la calidad del Servicio y, en consecuencia, mejorar las operaciones cotidianas de EJIE.

La Gestión del Cambio cubre todos los aspectos de la gestión de la introducción e implementación de todos los cambios que afectan a todas las pilas tecnológicas y en cualquiera de los procesos de gestión, herramientas y metodologías diseñados y utilizados para soportar los componentes de las Pilas.

Las actividades de Gestión del Cambio están interrelacionados y complementarios con la Gestión de la Versiones y la Gestión de la Configuración, así como con la Gestión de Incidencias y la Gestión de Problemas.

El proceso de Gestión de cambios incluye los siguientes pasos de proceso:

- Determinación de métricas para medir la efectividad de un cambio
- Proceso de solicitud de cambio (RFC)
- Proceso de seguimiento
- Proceso de priorización
- Proceso de asignación de responsabilidad
- Proceso de evaluación de impacto / riesgo
- Participación en la continuidad del servicio de TI y planificación de los “disaster recovery”
- Coordinación del Comité de gestión del Cambio (CAB)
- Proceso de revisión / aprobación
- Establecer y administrar el calendario de cambios aprobados
- Proceso de implementación
- Proceso de verificación (prueba)

- Proceso de cierre

Los siguientes puntos identifican las funciones y responsabilidades más relevantes dentro del servicio de gestión que el proveedor realizará:

- Mantener y documentar los procedimientos de Gestión de Cambios según los componentes del proceso de Gestión de Cambios descritos anteriormente
- Participar en la evaluación del riesgo para que el cambio sea introducido sin ser probado completamente.
- Ser consultado e informado de revisiones y auditorías de control de calidad de Gestión del Cambio de procesos y registros de Gestión de Cambios.

8.6.2 Gestión de la configuración

Los servicios relacionados con la Gestion de la Configuración son las actividades asociadas con la provisión de un modelo lógico de los activos de servicios (incluyendo licencias de software) y sus relaciones mediante la identificación, control, mantenimiento y verificación del hardware, software y documentación instalados (contratos de mantenimiento, documentos SLA, Etc.).

Los objetivos son dar cuenta de todos los activos y configuraciones de TI, proporcionar información precisa sobre las configuraciones, proporcionar una base sólida para la administración de incidencias, problemas, cambios y versiones, y verificar los registros de configuración en la infraestructura y corregir cualquier excepción. Los siguientes puntos identifican las funciones y responsabilidades más relevantes de Gestión de configuración que el proveedor realizará:

- Mantener y documentar el Procedimiento de Gestión de Configuración para que cumplan con los requisitos y se adhieran a las políticas definidas.
- Instalar y mantener herramientas de gestión de configuración asociadas a la pila tecnológica.
- Introducir / cargar datos de configuración en la base de datos de configuración asociadas a la pila tecnológica.
- Establecer interfaces de procesos para la Gestión de Incidencias y Problemas, Gestión de Cambios, Soporte Técnico, Mantenimiento y Gestión de Activos
- Establecer controles de autorización apropiados para modificar los elementos de configuración y verificar el cumplimiento de licencias de software.
- Mantener procedimientos para establecer líneas de base de configuración como puntos de referencia para reconstrucciones y proporcionar la capacidad de volver a estados de configuración estables.
- Proporcionar un informe de deficiencia y las medidas adoptadas para abordar los problemas identificados
- Ser informado de la auditoria de la gestión de la configuración y la precisión de los datos de configuración

8.6.3 Gestión de Activos

Los Servicios de Gestión de Activos son las actividades asociadas con el proceso de la gestión y seguimiento continuos del ciclo de vida de los componentes existentes de la Pila Tecnológica de Servicio (por ejemplo, hardware, software y licencias de software, mantenimiento, etc) y sus atributos (Contratos, proveedores, números de serie, etc.). Los siguientes puntos identifican las funciones y responsabilidades más relevantes de Asset Management que el Proveedor debe realizar:

- Mantener y gestionar un sistema de gestión de activos que cumpla los requisitos del cliente y se adhiera a las políticas definidas.
- Gestionar el ciclo de vida de todos los activos desde la identificación, ordenación de pedidos, inventario, instalación y mantenimiento hasta la eliminación.
- Actualizar registros de activos dentro del alcance relacionados con todas las actividades de cambio aprobadas.

- Ser consultado para proporcionar un plan de remediación de la Gestión de Activos para las deficiencias encontradas.
- Participar en los informes de auditoría y los planes de remediación de la información de la gestión de inventario de activos.
- Ser informado de la auditoría de calidad periódica del sistema de Gestión de Activos.

8.6.4 Gestión de licencias de software

Los servicios de gestión de licencias de software son las actividades asociadas con la identificación, adquisición y eliminación, así como la gestión y seguimiento continuos del software y sus licencias correspondientes. Los siguientes puntos identifican las funciones y responsabilidades más relevantes del servicio de licencias de software que el proveedor debe realizar:

- Recomendar mejoras a los requisitos y políticas de gestión de licencias de software.
- Mantener y documentar Procedimientos de Gestión de Licencias de Software que cumplan con los requisitos y se adhieran a políticas definidas como asignadas a la Gestión de Activos
- Administre y mantenga (p. Ej., Monitorice, rastree el estado, verifique, audite, realice el cumplimiento del contrato, reasigne) licencias de software y medios a través del ciclo de vida de la licencia de software
- Desarrollar y mantener el inventario de todas las licencias de software dentro del sistema de gestión de activos
- Informe al EJIE sobre cualquier excepción a los términos y condiciones del Vendedor, incluyendo incumplimiento de licencia
- Proporcionar a EJIE informes y recomendaciones para usar en la toma de decisiones de adquisición y descontinuación de software.
- Proporcionar recomendaciones para adquirir licencias adicionales, recomendar alternativas o restringir el uso cuando sea necesario y apropiado, para restaurar o continuar manteniendo el cumplimiento de las licencias
- Identificar y reportar problemas de cumplimiento de licencias a EJIE y proporcionar recomendaciones para resolver el problema de cumplimiento
- Gestionar y realizar auditorías y conciliar el número de licencias con el número de instalaciones, según lo solicitado por EJIE.
- Proporcionar recomendaciones a EJIE para resolver cualquier problema de conciliación de software.

8.6.5 Gestión de versiones/entregas

El servicio de Gestión de versiones/entregas se preocupa por implementar los cambios a los servicios de TI definidos y cubre tanto el software como el hardware. Los servicios de gestión de versiones son actividades que tienen una visión holística de un cambio en un servicio para garantizar que los aspectos técnicos y no técnicos de una versión relacionados con el software y el hardware cambian.

Estos cambios se pueden implementar desplegando una combinación de nuevas aplicaciones o software de infraestructura y / o hardware actualizado o nuevo, o simplemente haciendo cambios en la documentación, como horas de servicio o arreglos de soporte. Los procesos y actividades de gestión de la versión están relacionados entre sí y son complementarios con el proceso de Gestión del Cambio, así como la Gestión de la Configuración y la Gestión de Problemas.

La gestión de versiones incluye las siguientes actividades:

- Establecimiento de políticas y procedimientos estandarizados de Gestión de Versiones
- Gestionar la planificación y la programación global del calendario general de versiones, así como para las versiones individuales
- Establecer y administrar la documentación de versiones
- Gestión de los procesos de diseño, creación y configuración de la versión

- Liberación de pruebas y gestión de pruebas
- Planificación del despliegue incluyendo planes de calidad y planes de marcha atrás.
- Comunicación, preparación y formación de la versión
- Gestión del despliegue / distribución e instalación de todos los elementos de una versión
- Documentar cada versión y actualizar la base de datos de gestión de configuración (CMDB).

Las versiones también pueden consistir en una serie de correcciones de problemas y mejoras a los servicios de TI existentes. También pueden ser servicios de migración como actividades asociadas con la instalación de componentes de TI nuevos o mejorados (por ejemplo, hardware, software [sistema operativo] y componentes de red).

Una versión consiste en el software nuevo requerido y cualquier hardware nuevo o modificado necesario para implementar los cambios aprobados. Las versiones se dividen generalmente en:

- **Versiones mayores de software y actualizaciones de hardware** o reemplazos, que normalmente contiene grandes áreas de nueva funcionalidad. Normalmente, actualización principal reemplaza todas las actualizaciones menores anteriores, las revisiones y las correcciones de emergencia.
- **Versiones menores de software y actualizaciones de hardware**, que contiene normalmente pequeñas mejoras y correcciones, algunos de los cuales ya han sido emitidos como correcciones de emergencia. Normalmente, una actualización o actualización secundaria reemplaza todas las correcciones de emergencia anteriores.
- **Software y correcciones de hardware de emergencia**, normalmente contiene las correcciones a un pequeño número de problemas conocidos.

Los siguientes puntos identifican las funciones y responsabilidades más relevantes de gestión de versiones/entregas que el proveedor realizará:

- Establecer y mantener un entorno o entornos seguros apropiados en los que todas las versiones autorizadas de todos los programas informáticos, y donde todos los repuestos de hardware estén almacenados y contabilizado
- Mantener copias maestras de todas las versiones nuevas del software y del elemento de configuración de actualización.
- Asegúrese de que todos los repuestos de hardware están protegidos reflejados en la (s) base (s) de administración de configuración (s).
- Desarrollar planes de calidad y planes de marcha atrás según sea apropiado para cada versión.
- Asegurar de que todos los entornos de prueba necesarios estén disponibles y configurados adecuadamente para admitir pruebas de la versión.
- Revisar los planes de prueba de aceptación de la versión.
- Instalar mejoras en la arquitectura técnica o Servicios proporcionados
- Instalar componentes de la pila de servicio nuevos o mejorados (por ejemplo, hardware, software, middleware, utilidades, redes, periféricos, configuraciones) de acuerdo con los procedimientos de gestión de cambios de EJIE.
- Realizar actualizaciones de componentes de la pila de Servicio como resultado de nuevas y mejoradas aplicaciones y arquitecturas, y planes y requisitos de actualización de EJIE (por ejemplo, hardware, software, middleware, utilidades, redes, periféricos, configuraciones).
- Instalar la infraestructura física según sea necesario de acuerdo con los procedimientos de Gestión del Cambio de EJIE.
- Realizar la migración y conversión de datos mediante métodos electrónicos o manuales como resultado de la implementación o migración (por ejemplo, bases de datos, repositorios de administración de sistemas de red, tablas de direcciones, Bases de Información de Gestión [MIB]).
- Realizar pruebas apropiadas en todas las instalaciones, movimientos, agregados y cambios por requerimientos, de acuerdo con los procedimientos de la Gestión del Cambio de EJIE.
- Administrar y programar el entorno de prueba de integración.
- Instalar equipos, software o servicios nuevos y mejorados para transitar sin problemas al entorno existente, basándose en los requisitos definidos en los requisitos y en los documentos de diseño.

- Realizar modificaciones y ajustes de rendimiento - Mejoras en el software del sistema y utilidades como resultado de cambios en las normas de arquitectura o adiciones y mejoras del entorno.
- Probar las nuevas versiones de hardware y software soportados para garantizar que el rendimiento y la funcionalidad requeridos se mantengan en conformidad con requerimientos de servicio de EJIE.
- Documentar las verificaciones post-despliegue, planes de marcha atrás y resultados.
- Proporcionar al personal técnico de TI de EJIE y los usuarios finales formación relacionada con la implementación de nuevos productos y servicios por requerimientos.

8.6.6 Formación y transferencia de conocimiento

Los Servicios de Formación y Transferencia de Conocimiento consisten en los siguientes 2 tipos de formaciones que el Proveedor proporcionará:

- Transferencia de conocimientos para la mejora de habilidades a través de la instrucción al personal del Proveedor. El Proveedor participará en cualquier transferencia de conocimientos inicial y continua impartida por EJIE, según sea necesario, que proporcionaría una oportunidad de aprendizaje sobre el entorno de negocio y técnico de EJIE.
- Formación para personal técnico de EJIE o terceros con el propósito expreso de explotar las funciones y características del entorno informático de EJIE. Los métodos de entrega pueden incluir métodos de instrucción en clases individuales u otros medios apropiados.

Los siguientes puntos identifican las funciones y responsabilidades más relevantes de formación y Transferencia de Conocimiento que el Proveedor debe realizar:

- Mantener y documentar procedimientos de Transferencia de Conocimiento para asegurar que más de un individuo entienda los componentes claves técnicos
- Participar en la formación impartida por EJIE en el entorno técnico y de negocio.
- Desarrollar, documentar y entregar los requisitos de formación que apoyen la provisión continua de Servicios a EJIE, incluyendo cursos de actualización según sea necesario e instrucción sobre nuevas funcionalidades.
- Realizar formaciones según sea necesario para mantenerse al día con los sistemas, software, características y funciones para las que se presta asistencia técnica, con el fin de mejorar el rendimiento del Servicio.
- Proporcionar materiales de formación de operación nivel 1 para el personal técnico de EJIE.
- Proporcionar materiales de formación continua para el personal del cau en los entornos empresariales y técnicos, según lo definido por el EJIE.
- Proporcionar una formación en el aula y en el equipo (caso por caso) seleccionada por el cliente para las aplicaciones COTS estándar, según lo solicitado por el Cliente.

Adicionalmente Ejie podrá exigir a la empresa adjudicataria un mínimo de 2 certificados oficiales de las nuevas tecnologías recepcionadas. El no cumplimiento de este requisito en un tiempo de 6 meses desde el momento que se oficializa la petición será penalizado.

8.6.7 Documentación

Servicios de Documentación son las actividades asociadas con el desarrollo, revisión, mantenimiento, reproducción y distribución de información de la pila del servicio en forma impresa y electrónica. Los siguientes puntos identifican las funciones y responsabilidades relevantes de la Documentación que el Proveedor debe realizar:

- Proporcionar resultados en formato acordado para apoyar las actividades a lo largo del ciclo de vida de los Servicios, tal como se especifica en la pila del servicio.
- Documentar especificaciones y configuraciones del sistema (p. Ej., Topología de interconexión, configuraciones, diagramas de red, diagrama de flujo de datos, mapas del sistema)

- Mantener y Documentar los procedimientos operativos estándar (por ejemplo, arranque, conmutación por error / recuperación de desastres, gestión del pool, procesamiento por lotes, copia de seguridad)
- Mantener y Documentar la producción de trabajos y los horarios de mantenimiento

8.7 Diseño del servicio

8.7.1 Monitorización y reporte del Nivel de servicio.

El servicio para la monitorización y reporte corresponde a las actividades asociadas con la monitorización y los servicios de reporte relacionados con los requerimientos de los niveles de servicio (SLRs). Adicionalmente, el proveedor podría facilitar información sobre la administración del sistema (p. ej: métricas de rendimiento, estadísticas, etc.) en un formato que sea acordado con EJIE, que resulte representativo y diseñado para el mismo. Los siguientes puntos identifican los roles y responsabilidades relevantes que el proveedor debe realizar para desarrollar los niveles de servicio y monitorización:

- Mantener y documentar el manual de procedimientos del servicio de monitorización y reporte siguiendo los requerimientos y las políticas definidas.
- Reportar un SLR de rendimiento y mejora de resultados.
- Medir, analizar y proporcionar informes de gestión sobre el rendimiento en relación con las SLR.
- Realizar reuniones de mejora de SLR para revisar SLRs y recomendaciones de mejoras.
- Implementar mejoras para los planes SLR.
- Otorgar acceso a EJIE para visualizar el rendimiento del sistema, informes de monitorización de SLR así como el acceso a datos relevantes.

8.7.2 Gestión del rendimiento.

Los servicios de gestión de rendimiento son las actividades asociadas con la gestión y el ajuste de los componentes de la pila de servicio para un rendimiento óptimo. El proceso abarca los siguientes:

- Monitorización del rendimiento de los servicios de TI y de los componentes de TI de apoyo
- Evaluación de los resultados de los informes
- Realización de análisis de tendencias
- Proporcionar recomendaciones para tunear el rendimiento.
- Realización de actividades de ajuste.
- Actualización periódica (al menos anualmente)

Los siguientes puntos identifican los roles de gestión del rendimiento y las responsabilidades que proveedor debe realizar:

- Mantener y documentar los procedimientos de gestión del rendimiento siguiendo los requisitos y políticas previamente definidos.
- Realizar la optimización de los componentes de la pila de servicio para mantener un rendimiento óptimo de acuerdo con los procedimientos de la gestión del cambio.
- Administrar los recursos de componentes de la pila de servicio (por ejemplo, dispositivos y tráfico) para cumplir con las especificaciones del SLR en términos de disponibilidad y rendimiento.
- Proporcionar monitorización y reportes de rendimiento, la utilización y la eficiencia de los componentes de la pila de servicio basados en un marco de tiempo y secuencia definidos (por ejemplo, mensualmente).
- Evaluar, identificar y recomendar de forma proactiva configuraciones o cambios en configuraciones que mejoren el rendimiento.
- Llevar a cabo un análisis de tendencias para recomendar cambios para mejorar el rendimiento basado en el marco de tiempo especificado (por ejemplo, mensualmente).
- Desarrollar y proporcionar planes de mejora según sea necesario para satisfacer las SLR basado en el marco de tiempo definido (por ejemplo, mensualmente).
- Implementar planes de mejora para coordinar con terceros, según sea necesario.
- Proporcionar asesoramiento y apoyo técnico al personal de soporte y desarrollo de aplicaciónes según sea necesario.

Algunas de estas responsabilidades están incluidas dentro del Catálogo de servicios de referencia “Anexo II en los apartados de mantenimiento y evolución.

8.7.3 Gestión de la disponibilidad

El objetivo de la Gestión de Disponibilidad es comprender los requisitos generales de disponibilidad de las necesidades de negocio de EJIE y planificar, medir, supervisar y esforzarse continuamente por mejorar la disponibilidad de la Infraestructura de TI, los servicios y la organización de TI de soporte para garantizar que estos requisitos se cumplan de forma coherente. Se centran en ofrecer mejoras de disponibilidad que ofrecen beneficios de negocio medibles. La Gestión de Disponibilidad abarca la evaluación, diseño, implementación, medición y gestión de la Disponibilidad de Infraestructura de TI desde un componente y una perspectiva de extremo a extremo (es decir, Servicios), incluyendo metodologías y herramientas nuevas o modificadas de Gestión de Servicios de TI, modificaciones o actualizaciones de los sistemas y componentes de infraestructura de TI. El objetivo del proceso de gestión de disponibilidad es optimizar la capacidad de la infraestructura de TI, los servicios y la organización de apoyo para ofrecer un nivel de disponibilidad sostenido que permita a EJIE satisfacer sus objetivos de negocio.

Las actividades clave del proceso de gestión de disponibilidad son las siguientes:

- Determinar los requisitos de disponibilidad de unidades de negocio (generalmente como parte del desarrollo del SLA) para un servicio de TI nuevo o mejorado y formular los criterios de diseño de disponibilidad y recuperación para la infraestructura de TI para garantizar que los servicios de TI estén diseñados para proporcionar los niveles apropiados.
- Determinar las funciones críticas del negocio, así como el impacto derivado del fallo del componente de TI. Cuando sea apropiado, revisar los criterios de diseño de disponibilidad para proporcionar información adicional para prevenir o minimizar el impacto de al negocio.
- Identificar oportunidades para optimizar la disponibilidad de la Infraestructura de TI para ofrecer mejoras costo-efectivas que proporcionen beneficios empresariales tangibles.
- Establecer medidas y reportes de disponibilidad, confiabilidad y mantenibilidad que reflejen las perspectivas de la empresa, del usuario final y de la organización de soporte de TI.
- Monitorizar y análisis de tendencias de la disponibilidad, confiabilidad y mantenibilidad de sistemas y componentes de TI.
- Revisar el servicio de TI, la disponibilidad de sistemas y componentes, identificando de niveles inaceptables y adoptando medidas correctivas apropiadas para abordar los déficits de disponibilidad.
- Investigar las razones subyacentes de la disponibilidad inaceptable y proporcionar recomendaciones para la resolución.
- Producir y mantener un Plan de Disponibilidad orientado hacia el futuro que priorice y planifique mejoras generales de la disponibilidad de TI para mejorar la disponibilidad general de componentes de Servicios de TI e Infraestructura para asegurar que los requerimientos de disponibilidad del negocio existente y futuro sean los acordados
- Proporcionar información de disponibilidad de TI: informes para asegurar que los niveles acordados de disponibilidad, confiabilidad y mantenibilidad se midan y monitoricen continuamente

Los siguientes puntos identifican los roles y responsabilidades de la gestión de la disponibilidad que deben ser adquiridas por el cliente y por el proveedor.

- Implementar procedimientos de gestión de disponibilidad acordados.
- Proporcionar acceso de lectura sin restricciones a EJIE y el personal designado a todos los datos y registros de disponibilidad actuales e históricos de la base de conocimiento.
- Participar con EJIE en la definición de las medidas de disponibilidad y los requisitos de presentación de informes
- Asegurarse de que se implementan herramientas y prácticas de medición de disponibilidad.
- Participar en las sesiones de revisión de la Gestión de Problemas según corresponda, específicamente aquellos problemas relacionados con cortes de sistemas críticos.

- Monitorizar la disponibilidad real de TI lograda frente a los objetivos y asegurar que los déficits se aborden con prontitud y efectividad.
- Lleve a cabo sesiones de revisión de la evaluación de la disponibilidad y proporcione recomendaciones de mejora justificadas por costes.
- Producir y mantener un Plan de Disponibilidad que priorice y planifique mejoras de disponibilidad de TI aprobadas.
- Proporcionar informes de disponibilidad de TI para asegurar que los niveles acordados de disponibilidad, confiabilidad y mantenibilidad se miden, reporten y monitoricen de manera continua.

8.7.4 Gestión Capacidad

Los Servicios de Gestión de Capacidades son las actividades asociadas a asegurar que la capacidad de las pilas de Servicio coincida con la evolución de las demandas del negocio del EJIE de la manera más rentable y oportuna. El servicio abarca lo siguiente:

- Supervisión del rendimiento de los servicios de TI y de los componentes de TI de apoyo
- Comprender las demandas actuales y pronosticar las necesidades futuras
- Desarrollar planes de capacidad que satisfagan la demanda y las SLR
- Desarrollar modelos y realizar simulaciones para gestionar la capacidad
- Realizar evaluaciones de riesgo de las recomendaciones de capacidad
- Desarrollar e implementar un plan de capacidad que incluya el impacto financiero de las pilas de Servicio
- Realización de actividades de ajuste

Los siguientes puntos identifican las funciones y responsabilidades relevantes de Gestión de Capacidad que el Proveedor debe realizar:

- Mantener y documentar los procedimientos de Gestión de Capacidad que cumplan los requisitos y se adhieran a las políticas definidas.
- Desarrollar un plan de capacidad periódico (usualmente anual), incluyendo actualizaciones trimestrales.
- Desarrollar e implementar modelos de capacidad y ejecutar simulaciones para validar el plan de capacidad
- Evaluar los impactos de la capacidad al agregar, eliminar o modificar aplicaciones y componentes de infraestructura.
- Supervisar continuamente el uso de los recursos de TI para permitir la identificación proactiva de los problemas de capacidad y rendimiento.
- Captura de información de tendencias y pronóstico de futuros requisitos de capacidad de clientes basados en umbrales definidos por el cliente.
- Evaluar los incidentes / problemas relacionados con la capacidad y formular recomendaciones para su resolución.
- Recomendar cambios a la capacidad para mejorar el rendimiento del servicio.
- Evaluar el impacto / riesgo y el coste de los cambios de capacidad.
- Mantener los niveles de capacidad para optimizar el uso de los recursos de TI existentes y minimizar los costes de EJIE para ofrecer servicios en las SLR acordadas.
- Asegurar que exista una capacidad adecuada dentro del entorno de TI para satisfacer las SLR y requisitos, teniendo en cuenta las variaciones diarias, semanales y estacionales en las demandas de capacidad.

8.7.5 Backup y recuperación de aplicaciones específicas

Los servicios de copia de seguridad y recuperación son las actividades asociadas con la provisión de capacidades de copia de seguridad y recuperación de acuerdo con los programas y requisitos de EJIE. El

Proveedor debe demostrar que cumplirá o excederá los requisitos de Backup and Recovery de EJIE. Los siguientes puntos identifican las funciones y responsabilidades relevantes de Copia de seguridad y Recuperación que el Proveedor debe realizar:

- Recomendar las mejores prácticas para las estrategias, políticas y procesos y procedimientos del Backup y Recuperación.
- Mantener y documentar los Procedimientos de Backup y Recuperación que se adhieren a los requisitos y políticas de EJIE.
- Definir requisitos y políticas de supervisión y generación de informes de copia de seguridad y recuperación.
- Administrar el inventario de medios de copia de seguridad (cinta, disco, óptico y otro tipo de medios), incluyendo el orden y la distribución de los medios
- Realizar copias de seguridad del componente de la pila del servicio y la rotación asociada de los medios según sea necesario.
- Archivar medios de datos en una ubicación segura fuera de sitio.
- Asegurar la capacidad continua para recuperar los datos archivados de los medios como se especifica (compatibilidad hacia atrás del equipo de respaldo más reciente).
- Pruebe los medios de copia de seguridad para garantizar la recuperación incremental y completa de los datos y asegúrese de que la integridad del componente de la pila de servicio, según lo requiera o solicite EJIE.
- Recuperar archivos, sistema de archivos u otros datos requeridos de los medios de copia de seguridad, según sea requerido o solicitado por EJIE.

8.7.6 Continuidad del servicio de TI y recuperación de desastres

Servicios de Continuidad de Servicios de TI y Recuperación de Desastres (DR) son las actividades asociadas con el suministro de dichos Servicios para proporcionar aplicaciones cliente y su infraestructura asociada (por ejemplo, CPU, servidores, red, dispositivos de datos y salida, dispositivos de usuario final…). Las aplicaciones cliente y la infraestructura asociada recibirán servicios de DR de acuerdo con el plan de continuidad de negocio de EJIE. El Proveedor debe demostrar que cumplirá o excederá los requisitos de Continuidad de Servicio de TI y Servicios de DR del Cliente. Los siguientes puntos identifican las funciones y responsabilidades de Servicio de Continuidad y Servicios de DR que el Proveedor debe realizar:

- Cuando sea necesario, ayudar al EJIE en otras actividades de continuidad de TI y gestión de emergencias
- Mantener y documentar un plan de DR detallado para cumplir con los requisitos de Continuidad de Servicio de TI y DR. Incluir planes de datos, replicación, copias de seguridad, administración de almacenamiento y operaciones de contingencia que proporcionen la recuperación de los sistemas de EJIE dentro de los marcos de tiempo de requisito de recuperación establecidos después de que un desastre afecte al uso de los Servicios por parte de EJIE.
- Realizar pruebas de DR programadas por políticas de EJIE
- Revisar e informar los resultados de la prueba de DR a EJIE
- Desarrollar un plan de acción para abordar los resultados de las pruebas DR
- Implementar el plan de acción y proporcionar un estado continuo hasta la terminación
- Coordinar con EJIE durante una situación de DR de Proveedor según las políticas y procedimientos de DR
- Proporcionar acceso a EJIE a la continuidad de los servicios de TI ya los sistemas y datos de notificación y monitorización de DR

8.7.7 Seguridad

Servicios de seguridad son las actividades asociadas con el mantenimiento de la seguridad física y lógica

de todos los componentes de la pila de servicio (hardware y software) y protección de datos, virus, protección de acceso y otros servicios de seguridad en cumplimiento con los requisitos de seguridad de EJIE. Los siguientes puntos identifican las funciones y responsabilidades relevantes de seguridad que el proveedor debe realizar:

- Generales:
  - Mantenerse al día con las actuales tendencias de seguridad, amenazas y vulnerabilidades comunes, así como políticas de seguridad, procedimientos y mejores prácticas.
  - Llevar a cabo autoevaluaciones para identificar los agujeros de control o seguridad.
  - Implementar planes de seguridad física y lógica coherentes con las políticas de Seguridad de usuario y los estándares de la industria
  - Denunciar infracciones de seguridad a directivas cliente por EJIE.
  - Resolver violaciones de seguridad por políticas de cliente.
  - Revisar todos los parches de seguridad relevantes para el entorno de TI y clasifique la necesidad y la velocidad con la que deben instalarse los parches de seguridad según lo definido por las políticas de seguridad y la administración del cambio
  - Instalar los parches de seguridad por proceso y procedimientos de Gestión del Cambio del Cliente, incluyendo la adquisición de la aprobación del Cliente requerida
  - Mantener toda la documentación requerida para las evaluaciones de Seguridad, auditorías y pruebas de control y control interno.
  - Permitir auditorías de seguridad de terceros.
  - Implementar en el servicio un programa de concienciación sobre seguridad.
  - Asegúrese de que todo el personal del proveedor complete el entrenamiento de seguridad requerido por EJIE, basado en roles de seguridad de información definidos por EJIE
- Seguridad física. Se centra en los controles de acceso físicos implementados para garantizar la seguridad de los datos de EJIE y el Proveedor, instalaciones y sus sistemas de gestión asociados.
- La seguridad de los datos consiste en las actividades asociadas con la clasificación, gestión, seguridad y encriptación de los datos confidenciales y el almacenamiento de los medios que contienen esos datos.
- El Proveedor proporcionará Servicios de Detección / Prevención de Intrusión basados en la red y Servicios de Detección / Prevención de Intrusión basados en Host utilizando hardware y software propiedad de EJIE. El proveedor también realizará un monitorización interno de amenazas para actividades maliciosas y / o sospechosas.
- Los Servicios de Gestión de Incidentes de Seguridad son las actividades asociadas con la identificación, clasificación, gestión y notificación de un evento de seguridad.
- Los Servicios de Cumplimiento y Auditoría de Seguridad son las actividades para identificar los estándares que EJIE debe cumplir y modificar prácticas, políticas y procedimientos para permitir el cumplimiento.

8.8 Mejora continua del servicio

8.8.1 Definición del servicio

Es la fase que engloba el conjunto de todas y el significado de “ciclo” con el resto de actividades, poniendo foco en la mejora de los servicios para mantener la idea principal de alinear la tecnología con el negocio.

Para lograrlo es necesario identificar oportunidades de mejora y realizar las tareas necesarias para conseguir dichas mejoras. Por lo que se adoptarán y adaptarán los procesos de Negocio para alinear los servicios y proveer beneficios justificados. Referente a los beneficios, aparecen dos términos en esta fase a tener Evaluación y mejora de un servicio TI mediante ITIL en cuenta, por un lado el Retorno de Inversión (ROI – Return On Inversion) que refleja la diferencia entre los beneficios y la cantidad invertida; y por otro, Valor de la Inversión (VOI – Value Of Inversion) es la cuantía adicional a partir de los resultados del servicio que no constituyen un beneficio económico, y que se obtiene a largo plazo.

Los objetivos a alcanzar en esta fase aún se pueden concretar más en:

- Revisar, analizar y hacer las recomendaciones de mejora para cada una de las etapas.
- Revisar y analizar los resultados de los Niveles de Servicio y compararlos con los SLAs establecidos.
- Identificar e implementar mejoras que aumenten el ROI y VOI de los servicios TI, sin sacrificar la satisfacción del cliente.
- Mejorar la calidad de los servicios, incorporando nuevos procesos adaptados a los requisitos del cliente, aumentando la eficiencia y efectividad.

El objetivo a conseguir es el de vigilancia y optimización de las configuraciones de las tecnologías de su competencia para que el rendimiento de los Sistemas de Información que las utilicen sea el adecuado.

Este servicio deberá formalizar, llevar a cabo y automatizar aquellas tareas de mantenimiento, tunning y optimización que le sean encomendadas asegurando el correcto rendimiento de los productos estratégicos y estándares que se detallan en el Anexo I.

Así mismo, como parte de sus labores, se identificarán acciones proactivas de mejora en los sistemas administrados que den lugar a un incremento en la calidad del servicio suministrado por EJIE a sus clientes y usuarios. Estas acciones serán estructuradas en planes de mejora cuando así lo requiera y podrán contar con la colaboración de otros grupos de EJIE siempre y cuando los beneficios para EJIE lo justifiquen.

8.8.2 Metodología

El trabajo que realice se organizará como proyectos de desarrollo de software que seguirá metodología ágil SCRUM.

En la oferta se deberá presentar una propuesta al respecto identificando claramente cómo se organizarán los eventos de:

- Planificación del Sprint.
- Seguimiento diario del sprint (Scrum diario)
- El propio sprint
- Revisión del sprint
- Retrospectiva

Los roles de:

- Los diferentes propietarios del producto
- Equipo de desarrollo
- Scrum Master

Y los artefactos:

- Pila de Producto
- Pila del Sprint
- Incremento
- Documentación del trabajo realizado

Se deberá además utilizar como herramienta de apoyo SCRUM/Agile JIRA Agile para organizar y gestionar el proyecto siendo ésta de uso obligatorio. El coste que de las licencias o cuotas lo asumirá el prestatario del servicio. La modalidad de entrega de dicha herramienta deberá ser SaaS, y además EJIE

debe poder tener acceso a dicha herramienta por lo que se le suministrarán credenciales de acceso sin coste para EJIE.

8.9 Requisitos de servicio

8.9.1 Niveles de servicio ante incidencias

A continuación se definen los conceptos a tener en cuenta para los ANS ante incidencias:

- Se entiende por **tiempo de respuesta** del servicio, el tiempo transcurrido desde la notificación de la avería al adjudicatario, dentro del horario de cobertura, hasta el momento en el que el personal técnico del adjudicatario comienza a proceder con el diagnóstico de la misma.
- Se entiende por **tiempo de resolución** del servicio, el tiempo que va desde la notificación de la avería al adjudicatario, dentro del horario de cobertura, hasta el momento en que la avería está reparada o el servicio en funcionamiento.
- Dada la siguiente clasificación de incidencias:
  - **Critica**
  - **Alta**
  - **Media**
  - **Baja**

La siguiente tabla muestra los tiempos máximos, a cumplir por el adjudicatario en las resoluciones, según la severidad de las incidencias:

Tiempos máximos	**Críticas**	**Alto**	**Medio**	**Bajo**
Respuesta	Media hora en horario extendido y 5 minutos en horario habitual			
Resolución	4 horas	4 horas	12 horas	24 horas

En caso de necesidad o a solicitud de Ejie, un técnico de soporte del presente expediente tendrá que desplazarse a cualquier ubicación donde haya o vaya a haber infraestructura administrada por el servicio.

8.9.2 Monitorización

Será responsabilidad del adjudicatario la:

- Monitorización continua del estado de los servicios
- Monitorización continua de los recursos de sistemas implicados en cada servicio
- Ingeniería asociada a la correlación de eventos de seguridad y generación de alarmas.
- Seguimiento mensual de indicadores
- Planteamiento de actividad anual

El adjudicatario deberá integrar los sistemas objetos de este contrato con las diferentes plataformas de monitorización en diferentes entornos para la gestión de las alertas 24x7.Por lo tanto deberá identificar que se necesita monitorizar para su configuración en la plataforma corporativa. Las plataformas con las que se deben integrar se detallan en el punto 5.9.

8.9.3 Automatización

En el entorno objeto de este contrato se está trabajando en la automatización de las configuraciones para el despliegue de nuevas aplicaciones, entornos, etc.

Será responsabilidad del adjudicatario colaborar de forma activa con el grupo de automatización para la integración de las plataformas objeto del presente expediente.

8.9.4 Perito acreditado

Bajo demanda y ante un incidente de relevancia, EJIE podrá solicitar servicios de un perito acreditado para la realización de un informe pericial que pueda ser necesario en la gestión de algún incidente.

Adicionalmente a los informes periciales de las incidencias en la oferta se deberán incluir los servicios necesarios para la realización de **UN INFORME DETALLADO AL AÑO** por parte de un perito acreditado donde ofrezca una visión independiente, según tendencias de mercado, de la forma de dar servicio, del diseño optimo recomendado para el entorno y de la operación de toda la infraestructura de backup que posee y/o necesite `EJIE.

Se desea que los informes obtenidos cumplan con la normativa UNE 197001:2011 (“UNE 197001:2011. Criterios generales para la elaboración de informes y dictámenes periciales”).

En la oferta deberá estar específicamente indicado el perfil del perito o de la empresa (el perito nunca será parte del servicio) y experiencia en labores similares ya que se valorara expresamente.

8.9.5 Tareas específicas

A continuación se detallan otras tareas específicas objeto de este expediente además de todas las expuestas anteriormente:

- Optimización de la infraestructura
- Análisis de los informes de vulnerabilidades y performance. De dicho análisis deberán obtenerse recomendaciones en función de la criticidad de los datos obtenidos, viabilidad e impacto.
- Colaboración en el desarrollo de pilotos y en la implantación de nuevos productos e infraestructuras.
- Participación en la definición y ejecución de la estrategia que las diferentes infraestructuras requieran para un funcionamiento óptimo.
- Elaboración de los planes de Obsolescencia Tecnológica

8.10 Procedimiento y calidad

Los niveles de Servicio ofertados deberán cumplir como mínimo los indicados en este pliego. Adicionalmente el adjudicatario podrá ofrecer otros ANS que complementen a los anteriores. Estos ANS, junto con sus penalizaciones asociadas, serán revisados trimestralmente entre el adjudicatario y EJIE. El incumplimiento de dichos niveles será penalizado según se acuerde con la empresa adjudicataria.

También serán revisados trimestralmente estos ANS y podrán ser actualizados o añadidos nuevos si fuera necesario para mejorar la calidad del servicio que EJIE presta a sus clientes.

El licitador deberá proponer un Plan de Calidad que garantice la correcta ejecución del servicio prestado y seguimiento del mismo.

Este plan deberá contemplar al menos:

- Medidas de calidad a implementar en el servicio y sistemas de información para garantizar la calidad del servicio.
- Control de los Niveles de Servicio.
- Plan de formación detallado.
- Planteamiento de actividades de mejora continua del servicio debidamente formalizado en los informes mensuales y trimestrales.
- Cuadro de Mando de Evolución del Servicio

8.11 Plan de calidad

Proceso	Descripción	Objetivo	Periodo de Cómputo	Tipo de penalización
Gestión de Incidencias	Nº de Incidencias Reabiertas	< 3%	Mensual	3
Gestión de Cambios	Nº de Intervenciones sobre los sistemas realizadas sin registrar un cambio	0	Mensual	3
Mejora continua	Nº de Peticiones genéricas promovidas a paquetizadas	>=1	Mensual	3
Mejora continua	Nº de altas nuevas en la BBDD de conocimiento para operadores/clientes/técnicos en relación a incidencias frecuentes	>=2	Mensual	3
Mejora continua	Nº de altas nuevas en la BBDD de conocimiento para operadores/clientes/técnicos en relación a tareas paquetizadas	>=1	Mensual	3
	Nº de nuevos paneles (o modificaciones sobre los existentes) propuestos	>=1	Trimestral	3
Gestión de Cambios	% cumplimiento SLA/OLA servicios	>= 90%	Mensual	3
Gestión de Cambios	% cambios que generan incidencias	<= 1%	Mensual	3
Gestión de Incidencias	% de incidencias con prioridad Crítica y Alta asignadas antes de 5 minutos.	>= 90%	Mensual	1
Gestión de Incidencias	% de incidencias críticas resueltas antes de 4 horas.	>= 95%	Mensual	1
Gestión de Incidencias	% de incidencias altas resueltas antes de 4 horas.	>= 95%	Mensual	2
Gestión de incidencias	% de incidencias medias resueltas antes de 12 horas.	>= 95%	Mensual	2
Gestión de Incidencias	% de incidencias bajas resueltas antes de 24 horas.	>= 95%	Mensual	2

Gestión de incidencias	Llamadas al 24x7 no atendidas o no contestadas en plazo (30 minutos).	<1	Mensual	1
Gestión de incidencias	No presencia en EJIE del 24x7 si fuera necesario en plazo (2 horas).	<1	Mensual	1
Gestión de incidencias	Incidencias con más de 5 días	< 4	Mensual	3
Gestión de Incidencias	Cumplimiento plan entregables	100%		3
Gestión de Problemas	Tiempo medio para terminar un problema crítico	<=15 días	Mensual	3
Gestión de Problemas	Porcentaje de Problemas que se han detectado de forma proactiva con respecto al total de Problemas	>25%	Mensual	3
Gestión de Problemas	Cumplimiento plan entregables	100%		3
Gestión de solicitudes	Cumplimiento plan entregables	100%		3
Gestión de Versiones y Parches	Entrega Informes Trimestrales de Riesgos	≥4		3
Gestión de Versiones y Parches	Cumplimiento Política de Parches	95%		3
Gestión de la Seguridad	Entrega Informes Trimestrales de Riesgos	≥4		3
Gestión de Capacidad	Entrega Informes trimestral de estado	≥4		3
Gestión de Capacidad	Nº de incidencias críticas debidas a carga en los sistemas no detectadas con antelación	<2		1
Gestión de Peticiones	% Peticiones que finalizan en plazo	>= 90%		3
Gestión de Peticiones	% Peticiones que generan incidencias	<= 1 %		3
Gestión de activos	Actualización de activos en menos de 1 día	>=95%		3

Habrá indicadores de incidencias y problemas con variables de tiempo que se medirán desde que la incidencia/problema son abiertas en el proceso y sobre los incidencias/problemas asignados al servicio, es decir, sobre el total del proceso buscando que el servicio se involucre en la mejora del proceso y de mejorar las relaciones con otros servicios que participen en dicho proceso.

Estos indicadores tendrán una revisión mensual, y Ejie podrá pedir indicadores para diferentes entornos de gobierno si los necesitase.

8.12 Seguimiento

	Objetivo	Participantes EJIE	Entregables
Seguimiento interno (semanal)	Revisión del estado de tareas diarias y tareas activas	Responsable tecnológico Responsable transición	Información relevante Acta
Comité de seguimiento técnico (mensual)	Seguimiento de la consecución de los objetivos del servicio	Responsable tecnológico Responsables de procesos Responsable de explotación Directora técnica de Operaciones	Informe mensual del servicio Acta
Comité de gestión (trimestral)	Revisión ejecutiva del servicio	Dirección I&O Osakidetza y proyectos Batera Dirección de Producción Directora técnica de Operaciones Responsable tecnológico	Informe trimestral del servicio Acta

Si lo considera necesario cada coordinador podrá requerir reuniones de seguimiento específicas.

El licitante deberá presentar un modelo tipo de cada uno de los entregables identificados. Se valorará el formato y contenido propuesto de dichos informes.

8.13 Metodología aplicable y entorno tecnológico

EJIE dispone de procedimientos y normativas propios para la gestión de los procesos que deberán cumplirse. La empresa adjudicataria deberá asumir y adecuarse a los procesos de trabajo definidos (gestión de incidencias, gestión de peticiones de servicio, gestión del cambio, etc) en la organización de EJIE para poder desarrollar su trabajo. Se valorará positivamente toda mejora aportada a dichas normativas

Dentro del sentido del proyecto BATERA dichas plataformas irán convergiendo durante el contrato. Las herramientas a utilizar en cada uno de los entornos a día de hoy se detallan en la siguiente tabla.

	EJIE	Batera
Gestión IT	BMC ITSM 8.1 Atrium CMDB	ServiceNow
Operación	BMC Patrol BMC Event Manager Lighthouse BMC Control-M	vRealize Operations Manager vRealize Automation
Seguridad	Bitacora	N/A

Gestión de configuración	Puppet Microsoft SCCM Oracle EM	N/A
Automatización	vRealize Automation Puppet Oracle EM Microsoft SCCM/SCOM	vRealize Automation/ vRealize orchestrator
Automatización de despliegue de aplicaciones	AntHillpro	N/A
Monitorización	Aplicaciones/productos:: • Patrol • Nagios Comunicaciones: • BMC Event and impact management (BEM)	Realize Operations Manager y otras herramientas administrativas específicas por tecnología
Gestión y análisis de logs	Bitácora Elasticsearch	vRealize Log Insight

Las herramientas de gestión son los estándares de los productos

El servicio dispondrá de un portal de consumo propio sobre Microsoft SharePoint, que se pretende como herramienta central de gestión y colaboración.

8.14 Penalizaciones

EJIE controlará periódicamente el cumplimiento de los niveles de servicio exigidos. Con carácter mensual se comprobará los posibles incumplimientos de dichos niveles. En caso de encontrarse incumplimientos, se penalizará a la empresa adjudicataria según la siguiente tabla:

Código	Tipo de Nivel de Servicio	Penalización
1	Incumplimiento de alguno de los objetivos de los ANS comprometidos por el proveedor en la oferta realizada en relación a incidencias críticas.	4% de la factura del servicio recurrente por cada incumplimiento.
2	Incumplimiento de alguno de los objetivos de los ANS comprometidos por el proveedor en la oferta realizada en relación a resto de incidencias	3% de la factura del servicio recurrente por cada incumplimiento.
3	Incumplimiento de alguno de los objetivos de los ANS descritos en el punto 5.7 del presente pliego (resto).	2% de la factura del servicio recurrente por cada incumplimiento.

4	Incumplimiento del dimensionamiento mínimo de recursos (en cuanto al número, funciones o tareas de los perfiles) asignados en la oferta adjudicataria, ó incumplimiento de sustitución de recursos según la oferta	5% de la factura del servicio recurrente por cada mes de incumplimiento redondeando hacia arriba.
5	Incumplimiento del tiempo mínimo de solape entre un recurso entrante y uno saliente (15 días)	5% de la factura del servicio redondeando hacia arriba.
6	Incumplimientos en actualización tecnológica del equipo descritos en el punto 5.2.6. del presente pliego (resto).	3% de la factura del servicio recurrente por cada mes de incumplimiento redondeando hacia arriba.

Las penalizaciones se calcularán sobre el importe a pagar al adjudicatario mensualmente (sobre la factura mensual siguiente al establecimiento de la penalización) descontándose de dicha facturación el importe de penalización resultante de los incumplimientos.

8.15 Planificación y organización del servicio

8.16 Responsabilidades de dirección y gestión del servicio

Los roles del Servicio de Técnica de Infraestructuras de Backup y su relación a nivel funcional:

- Responsable de servicio
  - Interlocución para procesos IT
  - Gestión global del servicio.
- Referente Ejie
  - Interlocutores con los coordinadores tecnológicos de Osakidetza\EJIE
  - Coordinar los equipos de soporte
  - Líder tecnologico
- Soporte Técnico básico
  - Colaboración procesos de gestión IT
  - Colaboración CAU
  - Colaboración PCN
- Soporte Técnico avanzado
  - Colaboración procesos de gestión IT en segundo nivel
  - Tareas proactivas
  - Participación en proyectos
  - Propuestas de mejora continua e implantación.

De los distintos roles del servicio y su relación a nivel orgánico:

- Operación básica y avanzada
  - Colaboración de los técnicos de sistemas agrupados en Operación básica y avanzada con la Operación de EJIE, otras operaciones de otras pilas tecnológicas y soporte fabricantes
- Procesos transición
  - Colaboración de los técnicos de sistemas agrupados en Operación básica con los coordinadores de transición

- Proyectos
  - Colaboración de los técnicos de sistemas agrupados en Operación avanzada con los gestores de proyectos y coordinadores de transición
- Resto Procesos IT
  - Colaboración de los técnicos de sistemas agrupados en Operación básica y avanzada con los gestores del resto de procesos IT.
- Mejora continua,
  - Colaboración de los coordinadores tecnológicos de EJIE con los responsables tecnológicos del servicio y Operación avanzada

La empresa adjudicataria deberá comunicar por escrito la designación de una persona de su organización, encargada de ejercer las facultades de Dirección en lo referente al servicio contratado, responsabilizándose frente a EJIE de las personas que prestan el servicio.

8.16.1.1 Roles en el equipo de trabajo

El equipo de trabajo encargado de construir el entorno objeto de este contrato deberá tener los siguientes roles:

- Responsable de Servicio.
- Técnicos Backup.

El rol de “Responsable de Servicio” debe cubrir un mínimo de 1.700 horas anuales. Además, deberá acreditar una experiencia en los últimos 5 años (2012/2016) en entornos de backup, y en los tres últimos ejercicios (2014/2016) al menos un proyecto o participación en proyectos que sumados sean al menos de un importe de 150.000 €, con participación de perfil de Responsable, desde el inicio a fin, en entornos de backup tipo al objeto de contratación, indicando objeto, fechas inicio y fin, cliente e importe.

8.17 Carga de trabajo

A continuación se indica, a modo de referencia y sin implicaciones contractuales de ningún tipo, el número de peticiones registradas que atendieron los grupos de soporte existentes en finales de 2016, inicios de 2017. Tener en cuenta que sólo se registran las peticiones de usuarios, no están registradas todas las tareas de coordinación, mantenimiento preventivo, evolución de entornos, migraciones, proyectos, etc. que pueden suponer una parte muy importante del trabajo total.

	Año 2016
Incidencias	900
Peticiones (Tareas + Cambios)	250

8.18 Prestación del servicio

El servicio deberá prestarse en oficinas propias del adjudicatario. Las ubicaciones que pueda plantear el adjudicatario no serán más de 2. Debido a la criticidad de la infraestructura gestionada por el grupo de soporte se tendrá en cuenta lo siguiente:

- **Una única ubicación**.
  - En el caso de que se plantee el servicio con una única ubicación, ésta deberá estar situada de forma que se garantice la actuación en los CPDs principales de EJIE ubicados en Vitoria, en un tiempo inferior a 30 minutos. Un mínimo del 80% de los recursos empleados para el servicio deberá llevar a cabo sus trabajos desde dicha ubicación.

- **Ubicación principal más adicionales**.
  - Una ubicación respetará lo establecido en el punto anterior y además las otras adicionales deberán permitir al adjudicatario llegar a los CPDs principales de EJIE ubicados en Vitoria en un tiempo inferior a 60 minutos. Un mínimo del 80% de los recursos empleados para el servicio deberá llevar a cabo sus trabajos desde la ubicación principal y las adicionales.

En algún caso justificado por su necesidad, se podrá realizar en las instalaciones de EJIE, cumpliendo las medidas de seguridad de EJIE descritas en el **apartado de "condiciones de seguridad/generales"** y en los Anexos de Seguridad. Entre otras medidas es imprescindible que cuando el servicio se proporcione desde las instalaciones del adjudicatario se cumplan las **medidas especificadas sobre seguridad física**, entre las que están el que el servicio se proporcione desde una zona con control de acceso específico en el que la única red disponible sea la Red Corporativa.

Los casos que podrán realizarse en las instalaciones de EJIE serán de los siguientes tipos:

- Incidencias importantes definidas por EJIE
- Necesidad de inmediatez en la prestación del servicio, como puede ser la función de proyectos priorizados.

La localización será separada de la plantilla de EJIE.

Además, EJIE podrá solicitar la presencia física de uno o varios integrantes del grupo en sus oficinas: reuniones de seguimiento, nuevos proyectos, evolución de plataforma, reuniones multidisciplinares, etc. Todas estas solicitudes en ningún caso podrán suponer un sobrecoste para EJIE.

8.19 Constitución inicial del equipo de trabajo

El equipo técnico a incorporar tras la formalización del contrato para la ejecución de los trabajos deberá estar formado por componentes y perfiles relacionados en la oferta adjudicataria y consecuentemente valorados.

Si tras la adjudicación se observara que el equipo de proyecto no se corresponde con el establecido en la oferta técnica y:

- Caso que el adjudicatario presente justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio, se procederá a:
  - La presentación por el adjudicatario de sustituto/s con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.
  - Aceptación del sustituto/s por parte del Responsable del servicio de EJIE.
- Caso de que se demostrase que el cambio no se corresponde con causa justificada, EJIE se reserva el derecho no solo a la aprobación del sustituto/s sino incluso a la revisión de la adjudicación y en su caso la rescisión del pedido/contrato, si este hecho fuera elemento determinante en la mencionada adjudicación.
  - Las empresas licitadores deberán rellenar el Anexo III relacionado con el equipo de trabajo y sus certificaciones y experiencia.

8.20 Modificaciones en la composición del equipo de trabajo

La valoración de la calidad de los trabajos objeto del presente pliego corresponde al Responsable de EJIE, siendo potestad suya solicitar el cambio de cualquiera de los componentes del equipo de trabajo, con un preaviso de quince días, por otro de igual categoría o superior, si existen razones justificadas que lo aconsejen.

Si el adjudicatario propusiera el cambio de alguna de las personas del equipo de trabajo, se deberá solicitar por escrito con quince días naturales de antelación, y requerirá de las siguientes condiciones:

- Justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio.
- Presentación de sustituto/s con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.
- Aceptación del sustituto/s por parte del Responsable del servicio de EJIE

Los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto debidos a las sustituciones de personal, deberán subsanarse mediante periodos de solapamiento sin coste adicional, durante un mínimo de 15 días. Por lo tanto, si a criterio del Responsable de EJIE, esto no fuera posible, las dos primeras semanas de trabajo del sustituto/s no serán facturables corriendo a cargo del adjudicatario.

8.21 Interconexión con EJIE.

El adjudicatario deberá disponer de infraestructura de comunicaciones que le permita establecer VPNs contra los entornos objeto del expediente: EJIE tradicional:

- Línea a internet:
  - El caudal lo determinará la empresa adjudicataria
- Terminador de túneles VPN

8.22 Dimensionamiento del equipo de trabajo

Los recursos con los que se dimensione el servicio dependerán de las ofertas presentadas, pero se considera, y por tanto es un requisito mínimo, que para cubrir los roles planteados al menos es necesario que el equipo tenga la capacidad equivalente a 5.100 horas de dedicación en un periodo de un año, más la disponibilidad 24x7 en las tareas que por su naturaleza se tengan que realizar fuera del horario normal.

Las empresas candidatas deberán presentar una metodología detallada de forma de trabajo (planning respecto a las nuevas incorporaciones, planing de formación, forma detallada de cubrir las horas, forma de cubrir vacaciones, bajas médicas…etc), cumpliendo los diferentes requisitos que se explican en diferentes puntos (gestión de tareas proactivas , tareas de proyectos, tareas de mejora continua…), y el incumplimiento de dicho planing incurrirá en penalización.

8.23 Actualización tecnológica

En el transcurso de la ejecución del contrato podrán surgir nuevas tecnologías, de necesaria adaptación por parte de los recursos asignados a los servicios. La transición de éstas se llevará a cabo con la coordinación del Responsable o Responsables de EJIE.

Se deberá garantizar la actualización de los conocimientos en los componentes de los servicios. Esta actualización de conocimientos deberá ser evaluable por EJIE, semestralmente, siendo responsabilidad del adjudicatario la adaptación de los recursos. .

Para poder cubrir los roles planteados de forma efectiva se establecen los siguientes **requisitos de solvencia** que deberán cumplir los recursos presentados:

(*):Se considera este requisito como cumplido si aunque no disponga de la certificación sí que acredite al menos 10 años de experiencia laboral en esa tecnología en el ámbito de la Informática

8.24 Garantía de la disponibilidad del servicio

En la oferta se deberá presentar un plan de contingencias del servicio. El contenido que debe transmitir este plan es definir las políticas o mecanismos de contingencias habilitados para el caso de indisponibilidad ante desastre, emergencia o ante falta de respuesta en el plazo necesario de los recursos habitualmente utilizados en la entrega del servicio. El fin último es garantizar la prestación del servicio en cualquier circunstancia.