



5746 - PLIEGO DE PRESCRIPCIONES TÉCNICAS

Área de Atención y Digitalización del Negocio

Área de Arquitectura Tecnológica



ÍNDICE

1 ANTECEDENTES.....	6
2 OBJETO.....	6
3 PRECIO POR UNIDADES.....	6
4 ESPECIFICACIONES TÉCNICAS.....	7
4.1 Suscripciones ERP y CRM.....	7
4.1.1 Suscripciones mínimas requeridas para el primer año	7
4.1.2 Suscripciones mínimas requeridas para el segundo año.....	7
4.1.3 Suscripciones mínimas requeridas para el tercer año	8
4.1.4 Soporte a las suscripciones de las soluciones ERP Y CRM	8
4.2 Servicio gestionado de administración	8
4.2.1 Características del servicio gestionado de administración.....	9
4.3 Implantación de soluciones de negocio.....	10
4.3.1 Alcance específico	10
4.3.2 Alcance bajo demanda.....	25
4.3.3 Horario del servicio	25
4.3.4 Modalidad de trabajo.....	26
4.3.5 Fases de ejecución - Documentación.....	26
4.4 Equipo técnico	27
5 CONDICIONES PARTICULARES.....	35
5.1 Responsabilidades de la empresa adjudicataria.....	35
5.2 Control y seguimiento.....	35



5.3	Modelo de gestión	36
5.4	Propuesta técnica (estructura)	36
5.5	Equipo de trabajo	37
5.6	Finalización del contrato	37
5.7	Perspectiva de género	38
5.8	Seguridad de la información	38
5.8.1	Deber de confidencialidad	38
5.8.2	Medidas de seguridad	40
5.8.3	Gestión interna de Lantik S.A. M.P. (medidas de securización interna) previas a la prestación	42
5.8.4	Documentación	42
5.8.5	Auditoría, monitorización y reporte periódico del rendimiento de los controles de seguridad y notificación de evolución en la resolución de incidentes de seguridad a Lantik	42
5.8.6	Informe periódico del cumplimiento de la “Normativa de Seguridad para Proveedores”	43
5.8.7	Evidencia de buenas prácticas de seguridad acreditada en una norma de referencia para la gestión de la seguridad de la información, en el entorno de prestación. ...	43
5.8.8	Medidas de seguridad y compromisos de la empresa adjudicataria en materia de seguridad de la información de los servicios de administración electrónica	44
5.8.9	Subcontratación	44
5.8.10	Coordinación en caso de incidentes y desastres	45
5.8.11	Regulación de la finalización del contrato: transferencia de tecnología	46
5.8.12	Normativa	47
5.8.13	Objeto del encargo del tratamiento	47
5.8.14	Identificación de la información afectada	48



5.8.15 Duración	49
5.8.16 Obligaciones de la entidad encargada de tratamiento.....	49
5.8.17 Obligaciones de la entidad responsable del tratamiento.....	53
5.8.18 Evidencia de cumplimiento de la normativa de Protección de Datos.....	53
5.8.19 Responsabilidad y causas de resolución del contrato	54
5.8.20 Normativa de securización de entornos para prestación de servicio remoto	54
5.8.21 Informe periódico del cumplimiento de la “Normativa de securización de entornos para prestación de servicio remoto”	54
5.8.22 Monitorización de las conexiones remotas	54
5.8.23 Evidencias de las buenas prácticas relativas al objetivo de control 11 “Seguridad Física y del entorno” de la norma de referencia ISO/IEC 27002 en el entorno de prestación	54
5.8.24 Teletrabajo	55
5.8.25 Certificación de inexistencia de vulnerabilidades de seguridad.....	56
5.8.26 Conformidad con el Esquema Nacional de Seguridad (ENS).....	56
5.8.27 Declaración de ubicación.....	56
5.8.28 Transferencia Internacional de Datos Personales.....	57
5.8.29 Servicio asociado a la verificación electrónica de la identidad y tratamiento de datos de los tipos descritos en el artículo 46bis de la Ley 40/2015	57
5.8.30 Gestión de copias de seguridad y restauración de datos	58
5.8.31 Medidas de continuidad del servicio o proyecto	58
5.8.32 Registros de actividad.....	59
5.8.33 Claves criptográficas	59
5.8.34 Transparencia e información	59
5.8.35 Resolución del Contrato.....	60
5.8.36 Fuero	60



6	ANEXO A	62
7	ANEXO B	65



1 ANTECEDENTES

En el ámbito de la Diputación Foral de Bizkaia se dispone de las plataformas ERP y CRM basadas en las soluciones Business Central de Microsoft y Customer 360 de Salesforce. Y recientemente ha surgido un proyecto en una de sus entidades públicas cuyo enfoque funcional se resuelve con el uso de estas plataformas.

2 OBJETO

Provisión de suscripciones ERP y CRM e implantación de soluciones de negocio sobre ellas.

El objeto del contrato incluirá:

- La adquisición de las suscripciones de las soluciones de ERP de Microsoft y CRM de Salesforce.
- Servicios gestionados de administración de las plataformas ERP Y CRM.
- Implantaciones de soluciones de negocio, bien las definidas con alcance concreto bien las que puedan solicitarse bajo demanda por necesidades que puedan surgir a lo largo del contrato.

3 PRECIO POR UNIDADES

La empresa licitadora deberá indicar precios (sin IVA) separados para los siguientes conceptos, teniendo en cuenta el precio unitario máximo establecido para cada uno de ellos:

SUSCRIPCIONES ERP y CRM

- La empresa adjudicataria deberá indicar el importe por cada una de las suscripciones definidas en el ANEXO A (Tablas 1 y 2).

SERVICIOS

- Importe máximo para los servicios "Implantación de soluciones de negocio - Alcance específico", establecido en un máximo de 480.000,00 euros.
- Precio/hora para el "Servicio gestionado de administración", establecido en un máximo de:
 - Perfil persona técnica de la empresa licitadora: 70,00 euros/hora (sin IVA).
- Precio/hora para el servicio "Implantación de soluciones de negocio - Alcance bajo demanda", establecidos en un máximo de:
 - Perfil persona técnica de la empresa licitadora: 65,00 euros/hora (sin IVA).



4 ESPECIFICACIONES TÉCNICAS

4.1 Suscripciones ERP y CRM

Las suscripciones que las empresas licitadoras deberán incluir en la oferta son las detalladas en el **ANEXO A**.

Durante la vigencia del contrato, se podrá solicitar la activación de cualquier suscripción especificada en el ANEXO A. La fecha de inicio corresponderá al mes de adquisición y finalizará en la fecha de terminación del contrato, prorrateándose su importe en función de la fecha de alta del producto.

Se deberá indicar el plazo de entrega desde la recepción de la solicitud.

Todas las suscripciones conllevan los derechos de actualización de los productos, aunque estos cambien de denominación siempre que su funcionalidad sea la misma o mejorada sobre las actuales.

A continuación, se especifican las suscripciones mínimas a adquirir con el fin de cubrir el “Alcance específico” del apartado 4.3.1.

4.1.1 Suscripciones mínimas requeridas para el primer año

El primer año de contrato se adquirirán las siguientes suscripciones base del ERP por un periodo de tres años:

Fabricante	Suscripción	Cantidad
MICROSOFT	CFQ7TTC0LH34-0001 BUSINESS CENTRAL ESSENTIAL	20
MICROSOFT	CFQ7TTC0HD7P-0001 INSTANCIA BUSINESS CENTRAL (ENVIRONMENT)	3

4.1.2 Suscripciones mínimas requeridas para el segundo año

El segundo año de contrato se adquirirán las siguientes suscripciones base del CRM por un periodo de dos años.

Fabricante	Suscripción	Cantidad
SALESFORCE	MARKETING CLOUD ENGAGEMENT CORPORATE	1
SALESFORCE	SALES CLOUD ENTERPRISE	47



4.1.3 Suscripciones mínimas requeridas para el tercer año

El tercer año de contrato se adquirirán las siguientes suscripciones base del CRM/ERP por un periodo de un año.

Fabricante	Suscripción	Cantidad
SALESFORCE	SERVICE CLOUD ENTERPRISE EDITION	1
MICROSOFT	CFQ7TTC0LH34-0001 BUSINESS CENTRAL ESSENTIAL	40

4.1.4 Soporte a las suscripciones de las soluciones ERP Y CRM

Se incluirá el soporte y mantenimiento oficial para la plataforma CRM acreditado por el fabricante Salesforce. Los Servicios de Soporte serán realizados por el fabricante, siendo la empresa adjudicataria responsable del seguimiento de los casos, pero no de su resolución.

En el caso de la plataforma ERP, los Servicios de Soporte de primer nivel para la asistencia y resolución de casos serán realizados por la empresa adjudicataria. Deberán contar con el respaldo del servicio de soporte del fabricante para el escalado de incidencias en caso necesario

En general las suscripciones de la plataforma CRM y ERP deberán incluir, como mínimo, sin coste adicional alguno:

- Acceso a la última versión del producto.
- Deberá especificar el mecanismo de apertura de casos de soporte y los niveles de criticidad y los tiempos de respuesta, siendo un servicio 24X7 de fabricante.
- Con acceso a consultas y apertura de casos de soporte ilimitados durante la vigencia del contrato.
- Acceso al portal de fabricante para la gestión de las suscripciones activadas.

Se deberán detallar las condiciones del servicio ante posibles incidencias, incluyendo método de apertura de caso, niveles de criticidad y tiempos de respuesta.

4.2 Servicio gestionado de administración

En este apartado se describen los trabajos que la empresa adjudicataria, como mínimo, debe ser capaz de realizar para administrar las plataformas ERP Y CRM. No pretende ser un listado con una relación exhaustiva de tareas, ni de obligatoria realización, ya que se deberán acometer los trabajos necesarios para lograr los objetivos marcados en función de las necesidades.

- Instalación, configuración, parametrización, mantenimiento y tuning de las plataformas ERP y CRM.

- Aplicación de hot fixes o parches.
- Revisión de logs y errores.
- Análisis de incidencias y asistencia técnica en la resolución de estas.
- Recomendaciones de arquitectura.
- Automatización de tareas.
- Documentación.
- Interlocución con el soporte de fabricante.
- Testing de la plataforma.

Estos servicios se consumirán bajo demanda sin compromiso de consumo por parte de Lantik S.A.M.P. (en adelante Lantik).

4.2.1 Características del servicio gestionado de administración

- La empresa contratada deberá nombrar una persona coordinadora para que actúe de interlocutora con las personas responsables del servicio en Lantik. Así mismo, será suya la responsabilidad de dirigir los trabajos realizados por el personal de su empresa y verificar su nivel de calidad.
- Lantik nombrará una o varias personas responsables para los aspectos organizativos, funcionales y técnicos. Estas personas actuarán como interlocutoras con la empresa adjudicataria, y acudirán a cuantas reuniones de seguimiento se propongan. Asimismo, se encargarán de realizar cuantos controles consideren oportunos para garantizar la calidad del producto entregado y dar el Vº Bº a los trabajos.
- El modelo de contacto y notificación para la solicitud de trabajos se realizará por e-mail: (se utilizará siempre el e-mail que indique la empresa adjudicataria para notificar cualquier acción y tener constancia de esta). Adicionalmente y siempre tras usar la vía anterior, se deberá tener acceso a un número de teléfono y personas referentes (al menos dos). Durante la vigencia del contrato, se podrán incorporar nuevas vías de contacto y comunicación, como, por ejemplo, la herramienta de ticketing que se encuentre vigente en Lantik.
- El "Horario del servicio" mínimo requerido será: todas las semanas del año de lunes a viernes de 8:00 a 18:00, excluidos festivos en Bilbao.
- Se determinará un Tiempo de respuesta (Tr) máximo en 4 horas, definido como:
 - Tr: tiempo desde que se comunica la petición de servicio hasta que una persona del equipo de trabajo adscrito al contrato se ponga en contacto con Lantik. Este tiempo de respuesta contará dentro del "Horario del servicio".
- La cancelación de un servicio solicitado no conllevará ningún cargo asociado a Lantik siempre que se comunique con una antelación mínima de 3 días naturales a la fecha requerida.
- Se requiere una ventana de atención 24x7 basada en poder disponer de algún teléfono móvil de alguna persona responsable del servicio, para poder comunicar situaciones de emergencia o situaciones de contingencia excepcionales y realizar el seguimiento.
- Para los casos en que Lantik necesite que el servicio se dé fuera del "Horario del servicio", el precio de la hora será el de la hora estipulada con un coeficiente de 1,5.
- Lantik podrá solicitar que el servicio se dé "In situ" o "En remoto", y el precio de la hora no variará.



- Para el seguimiento de los trabajos se debe presentar un informe mensual de consumo de horas debidamente desglosadas, indicando las actuaciones realizadas, describiendo para cada una la fecha, una pequeña descripción y el tiempo dedicado. Incluirá el volumen de horas total consumidas a lo largo del mes y un acumulado. Este informe deberá enviarse a Lantik el último día hábil de cada mes.

4.3 Implantación de soluciones de negocio

El alcance de los servicios de implantación se ha dividido en dos apartados diferenciados: “Alcance específico” y “Alcance bajo demanda”. A continuación, se describen las tareas que en cada apartado se llevarán a cabo.

4.3.1 Alcance específico

Implementar una Plataforma Informacional corporativa que permita a BEAZ, sociedad pública perteneciente a la Diputación Foral de Bizkaia, cuyo objetivo es apoyar a personas y empresas en su esfuerzo por crear nuevos proyectos, innovar e internacionalizarse, recopilar, almacenar, procesar y analizar los datos disponibles de manera centralizada y eficiente, para poder disponer de una visión 360º de toda su actividad, poniendo especial foco en su clientela y poder así orientar su oferta de manera proactiva a las necesidades de cada momento.

En este sentido, internamente el objetivo es modernizarse digitalmente no sólo para mejorar el trabajo que se realiza, sino para servir de referente a su clientela; para ello la plataforma debe garantizar:

- Colaboración eficiente con la clientela
- Integridad e integración de los datos
- Visión 360º de clientes
- Simplicidad
- Seguridad
- Escalabilidad

Para ello, el concepto de solución definido implica la implantación de los productos Dynamics 365 Business Central de Microsoft, Power APPs de Microsoft y Customer 360 de Salesforce.

Además, será necesario realizar integraciones tanto con componentes/soluciones desarrolladas a medida por Lantik S.A.M.P (en adelante Lantik), como con soluciones de mercado que puedan estar implantadas o que decidan implantarse en Lantik.

Bajo el “Alcance específico” la solución deberá integrarse con:

- Microsoft Power BI
- Microsoft Sharepoint + Onedrive
- Microsoft Outlook, Teams
- Microsoft Power Automate

Cualquier otra integración que surja durante la implantación de la solución se trasladará al “Alcance bajo demanda” realizándose una valoración previa y su aprobación, si procede. Entre otras, podrán ser:

- Smart Mobile LMS: plataforma de formación e-learning



- SAGE: sistema de gestión empresarial
- Ekunet (propia de Lantik): sistema de gestión de expedientes
- Dorlet: sistema de control y gestión de accesos. (mediante fichero)
- TicketBAI/Batuz: Declaración de operaciones de facturación de clientes emitida
- Pixelware: plataforma de licitación electrónica
- Lotus Notes (mediante fichero)
- Smartsheet: software de gestión de proyectos
- MideNet: software de gestión estratégica

Para garantizar el éxito de implantación, se deberá realizar un plan de implantación que incluya sesiones de formación a los diferentes perfiles de personas usuarias de ambas soluciones (ERP y CRM), gestión del cambio, asistencia en el uso de la nueva herramienta ...

4.3.1.1 Ámbitos funcionales y sus procesos:

CRM

- Clientes
 - a. PN-001: Captación
 - b. PN-002: Gestión Clientes
 - c. PN-003: Valoración y Dinamización
 - d. PN-004: Auditorías de calidad de Clientes
- Negocio
 - a. PN-006: Gestión del Catálogo de Servicios genéricos
 - b. PN-007: Calificación Fiscal
 - c. PN-008: Ayudas
 - d. PN-009: Gestión de espacios
 - e. PN-010: Incubación
- De apoyo al Negocio
 - a. PS-001: Vigilancia y Estrategia
 - b. PS-002: Comunicación
 - c. PS-028: Gestión de incidencias, mejoras y sugerencias (externas)
- Gestión de Empresas Proveedoras
 - a. PS-005: Homologación de empresas proveedoras (formulario solicitud)
 - b. PS-006: Auditorías de Calidad de las empresas proveedoras
- Administrativos
 - a. PS-028- Gestión de incidencias y sugerencias de mejora (internas)

ERP

- Administrativos/as
 - a. PS-028: Gestión de incidencias y sugerencias de mejora (internas)
 - b. PS-029: Gestión de Activos TIC
 - c. PS-030: Registro de entradas y salidas
- Económico Financiero
 - a. PS-020: Deudores/ acreedores
 - b. PS-021: Tesorería
 - c. PS-022: Viajes (solicitud)
 - d. PS-023: Contabilidad general
 - e. PS-025: Gestión de Activos
 - f. PS-026: Gestión de Anticipos



- Estrategia y Planificación
 - a. PE-003: Gestión Presupuestaria
 - b. PE-004: Reporting económico-financiero, compras y RRHH
- Gestión de Empresas Proveedoras
 - a. PS-004: Gestión de Compras
 - b. PS-005: Homologación de empresas proveedoras
- Negocio
 - a. PN-011: Gestión de proyectos
- Recursos Humanos
 - a. PS-011: Gestión de Altas/Bajas
 - b. PS-013: Gestión de Formación
 - c. PS-014: Gestión de beneficios Sociales

Los procesos “PS-028 - Gestión de incidencias y sugerencias de mejora (internas)”, “PS-030 - Registro de entradas y salidas”, “PS-011 - Gestión de Altas/Bajas (ficha persona empleada)”, “PS-014 - Gestión de Beneficios Sociales”, “PS-013 - Gestión de la Formación (Plan de formación. Gestión solicitudes)”, “PS-022 - Viajes (solicitud)” y “PS-029 - Gestión de Activos TIC” serán implantados con MS Power App.

4.3.1.2 Mapas de situación actual

A continuación, se detallan el mapa actual de procesos y el mapa de sistemas.

- **Mapa actual de procesos:**

Se representa a continuación el mapa actual de sistemas identificados con los que interactúa el personal de BEAZ para la realización de los trabajos. Para cada herramienta se han identificado los procesos principales a los que da respuesta. Además, también se distinguen entre los que pertenecen a BEAZ, y por lo tanto se puede influir en su desarrollo y evolución, como los que quedan bajo la gestión de DFB.

Existe un tercer grupo que son los sistemas de terceros que pueden ser herramientas de carácter autonómico o estatal.



Estratégicos

Estrategia y Planificación

PE-001- Plan Estratégico

PE-002- Plan de Gestión Anual

PE-003- Gestión Presupuestaria

PE-004- Reporting, económico, financiero, compras y RRHH

Negocio

Clientes

PN-001- Captación

PN-002- Gestión de Clientes

PN-003- Valoración y Dinamización

PN-004- Auditoría de calidad de clientes

Negocio

PN-005- Gestión de oportunidades de negocio

PN-006- Gestión del catálogo de servicios genérico

PN-007- Gestión de servicios de informes de calificación fiscal

PN-008- Ayudas

PN-009 Gestión de espacios

PN-010- Incubación

PN-011- Gestión de proyectos

Soporte

Apoyo a Negocio

PS-001- Vigilancia y Estrategia

PS-002- Comunicación

PS-003- Gestión del conocimiento

Gestión de Proveedores

PS-004- Gestión de compras

PS-005- Homologación de proveedores

PS-006- Auditoría de calidad de proveedores

Gestión de calidad/medioambiente/I+D+i/Accesibilidad

PS-007- Auditoría

Legal

PS-008- Cumplimiento Normativo

Recursos Humanos

PS-010- Procesos de Selección

PS-011- Gestión de altas/bajas

PS-012- Prevención de riesgos laborales

PS-013- Gestión de la formación

PS-014- Gestión de beneficios sociales

PS-015- Gestión de calendario laboral

PS-016- Gestión de vacaciones

PS-017- Gestión de licencias y permisos

PS-018- Seguimiento plan de igualdad y registro retributivo

PS-019- Plan de carrera

PS-024- Gestión de nóminas



Soporte

Económico financiero

PS-020-
Deudores/Acreedores

PS-021- Tesorería

PS-022- Liquidación de
gastos de viaje

PS-023- Contabilidad
general

PS-025- Gestión de
activos

PS-026- Gestión de
anticipos

Administrativos

PS-027- Gestión de
accesos y seguridad
física

PS-028- Gestión de
incidencias y
sugerencias de mejora

PS-029- Gestión de
activos TIC

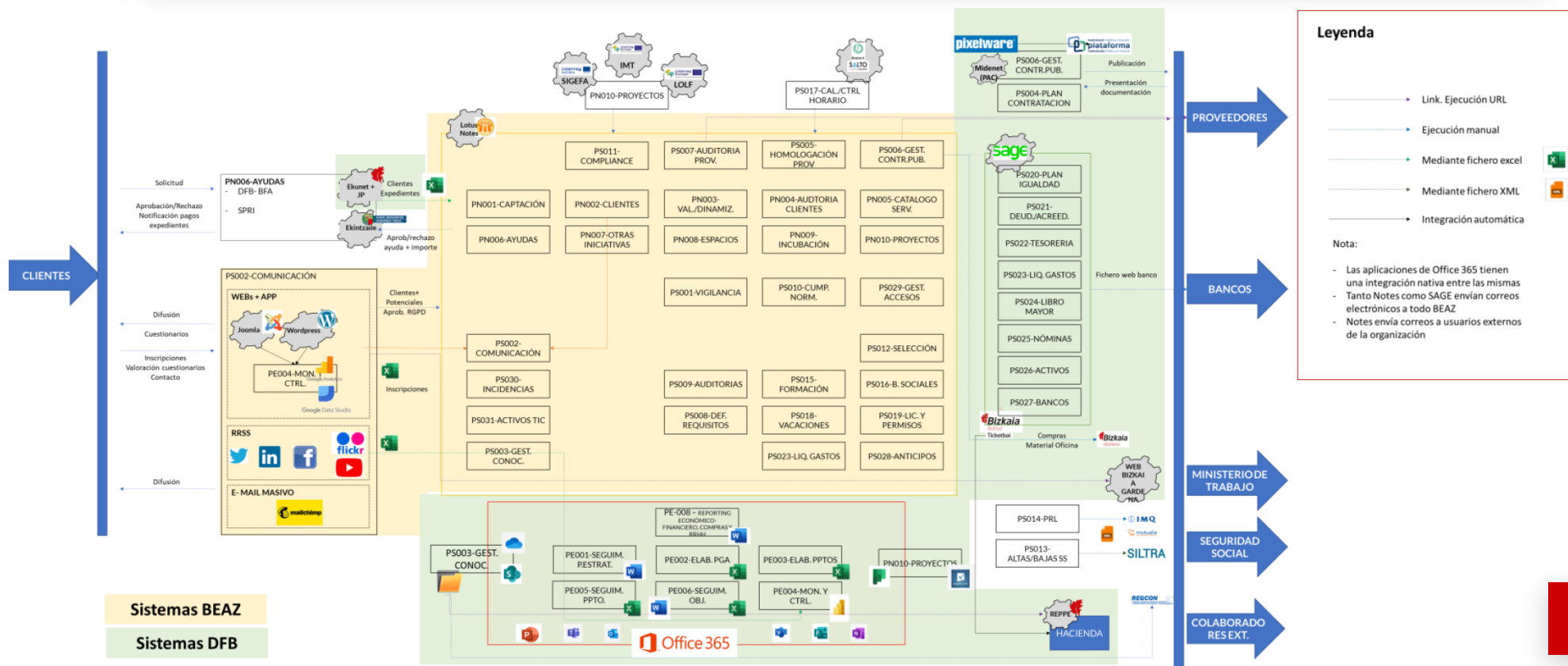
PS-030- Registro de
entradas y salidas

Nota: En estos momentos se están realizando una implantación de Dorlet, incluyendo los procesos “PS-027 - Gestión de Accesos y Seguridad Física”, “PS-016 - Gestión de Vacaciones”, “PS-015 - Gestión Calendario Laboral” y “PS-017 - Gestión de Licencias y Permisos”.



• Mapa actual de sistemas:

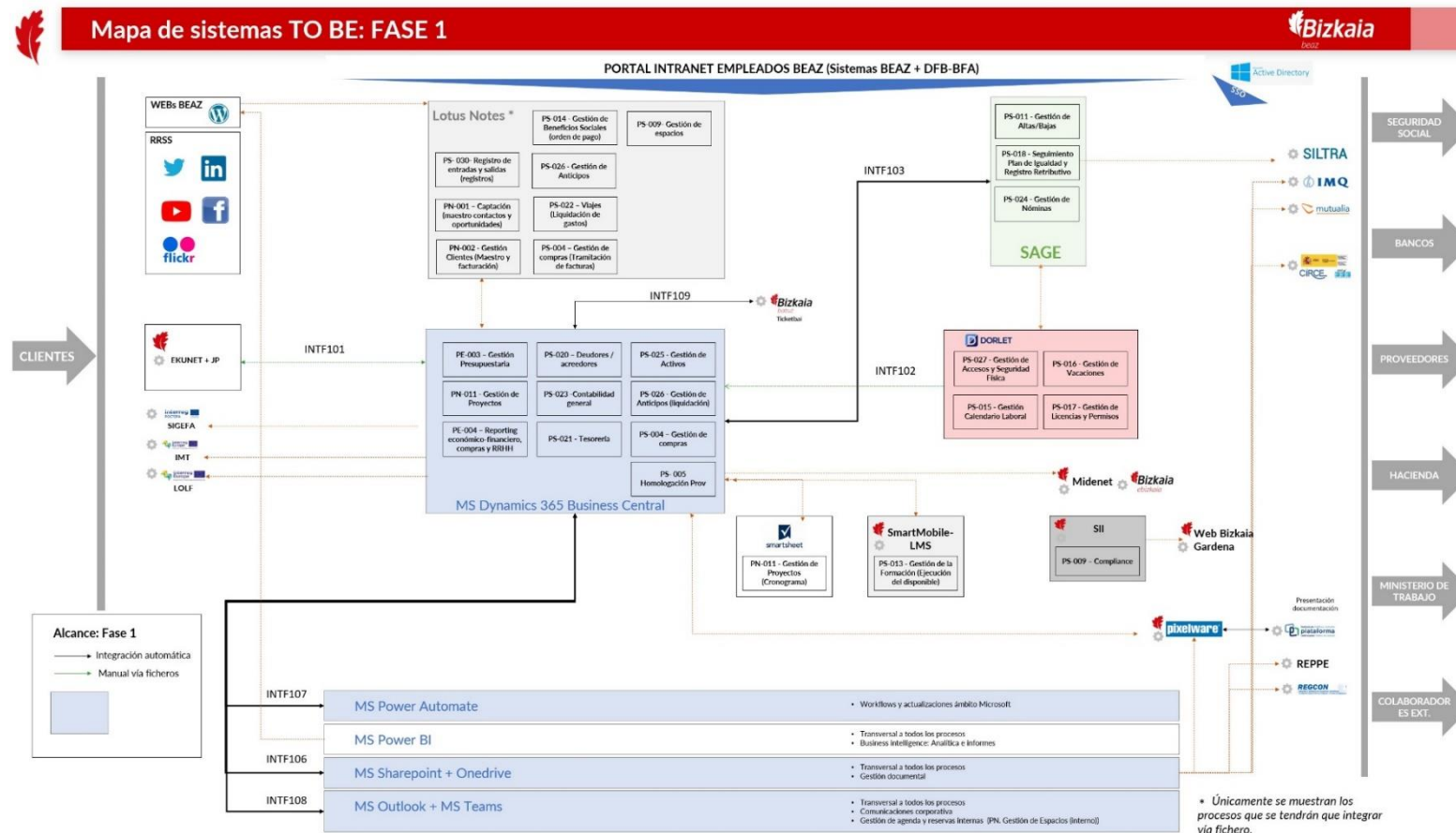
A continuación, se muestra el mapa de sistemas que se ha obtenido del análisis de los procesos y sistemas identificados y la interacción existente entre los sistemas, ya sea automática, manual, a través de fichero Excel, de fichero XML o acceso directo con un link (como se muestra en la leyenda):



4.3.1.3 Mapas de situación TO BE

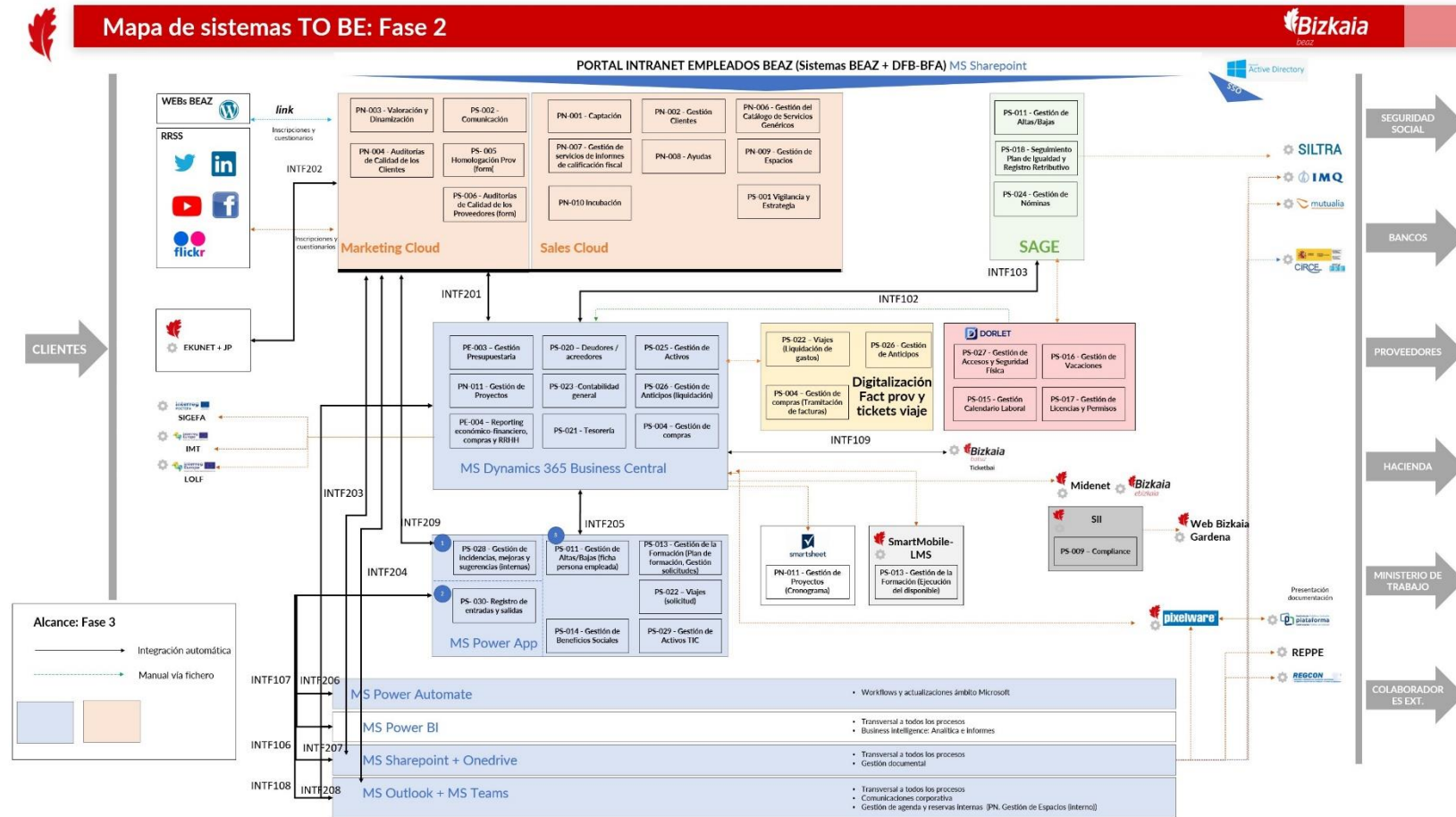
El proyecto se llevará a cabo durante los tres años que abarca el contrato y se ha estimado su ejecución en tres fases donde cada fase podría ser anual. Se muestran los mapas de cada fase y una evolución orientativa de los módulos a desarrollar en cada una de las fases:

FASE 1:



FASE 2

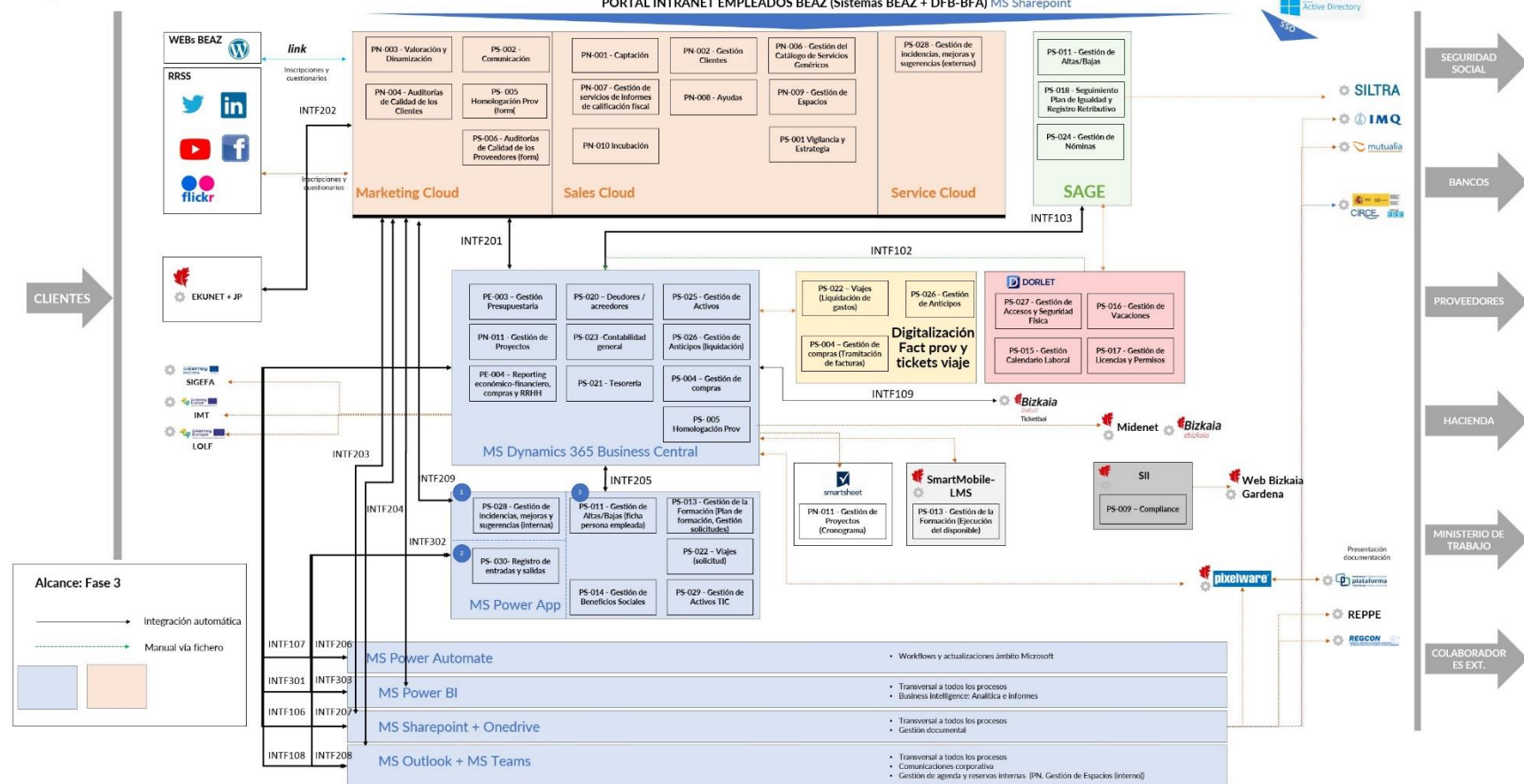
Mapa de sistemas TO BE: Fase 2



FASE 3



Mapa de sistemas TO BE: Fase 3



4.3.1.4 Requisitos funcionales generales

La solución, en su conjunto, deberá cumplir con los siguientes requisitos funcionales.

Funcionalidad	Detalle
Gestión de multi-sociedades	El ERP y CRM deberán permitir la administración centralizada de múltiples sociedades, asegurando la segregación adecuada de datos, el cumplimiento normativo específico de cada entidad y la consolidación eficiente de información financiera y operativa. En este proyecto se va a implantar 1 sociedad, BEAZ, pero es un requerimiento para posibilitar que otras sociedades de la DFB puedan también implantar la solución.
Movilidad	El sistema debe facilitar el trabajo en entornos colaborativos y móviles, permitiendo el acceso desde dispositivos como smartphones y tablets. Esto incluye tanto la visualización de información adaptada a la resolución específica del dispositivo como la ejecución de acciones, incluyendo la aprobación o el rechazo de solicitudes. Tanto Microsoft como Salesforce ofrecen aplicaciones estándar que las personas usuarias pueden descargar directamente en sus dispositivos móviles. No será necesario realizar desarrollos adicionales, ya que estas aplicaciones estándar cumplen con los requisitos necesarios para estos dispositivos.
Analítica de información	El sistema debe facilitar el análisis y la explotación de toda la información de la empresa de forma ágil y visual. Los sistemas contarán con informes de análisis estándar que las personas usuarias finales podrán personalizar fácilmente, permitiendo agregar o eliminar campos de visualización, aplicar filtros predefinidos y establecer criterios de ordenación, todo ello sin necesidad de conocimientos de programación. Adicionalmente, en la fase 3 se integrarán los sistemas implementados con PowerBI, lo que permitirá una visualización consolidada y avanzada de la información.
Gestión documental	Es necesaria la integración con SharePoint para optimizar la gestión documental de toda la actividad de BEAZ. Esta integración permitirá un almacenamiento centralizado, facilitando el acceso y la colaboración en los documentos, así como una mejor organización y control de la información relacionada con las operaciones de BEAZ. Los sistemas implementados se integrarán en las diferentes fases a sharepoint para la gestión documental con metadatos. Además, se desarrollará la migración total de los archivos de red de BEAZ a sharepoint.
Carga de Datos	El sistema deberá incluir mecanismos que faciliten tanto la carga de datos masiva desde aplicaciones existentes como la extracción de datos del propio sistema. Se valorarán los siguientes formatos: XLSX, CSV, CSV, XML, ODBC (open data connectivity), API (REST/JSON), OData Además, el sistema debe garantizar la calidad de los datos, validando la información en el momento de la carga.



Perfiles y roles de persona usuaria	El sistema debe optimizar la gestión de autorizaciones de acceso a la información, permitiendo la visualización, modificación y actualización de datos según el rol asignado a cada persona usuaria. Esta gestión deberá ser específica para cada área y proceso, garantizando que las personas usuarias accedan únicamente a la información relevante para sus funciones. Aspectos clave a considerar: • Roles definidos: Establecer roles claros que determinen los niveles de acceso. • Autorizaciones personalizadas: Permitir configuraciones específicas de autorización adaptadas a las necesidades de cada área y proceso. • Registro de cambios: Implementar un sistema de seguimiento de modificaciones realizadas, asegurando mayor transparencia y control.
Idiomas	El sistema debe ser multi- idioma (castellano, inglés y euskera) aunque la configuración estará realizada en castellano sin embargo todos los informes/formularios que se vayan a compartir con otras administraciones públicas deberán estar en euskera y castellano. La configuración de toda la comunicación con terceros deberá estar en euskera, castellano e inglés. Los casos concretos están detallados en las páginas de detalle de las fichas de los procesos concretos.
Formularios de Impresión con formatos estándar	El sistema debe incluir la funcionalidad de impresión de formularios estándar y otros que requerirán una personalización como, por ejemplo, pedidos y facturas, y otros detallados las páginas de detalle de las fichas de los procesos concretos. Formato de Impresión: Asegurar que los formularios se puedan imprimir en formatos comunes, como Word, Excel y PDF
Acceso seguro	La gestión de accesos se realizará a través de Microsoft Active Directory, permitiendo el alta de usuarios en todos los sistemas nuevos mediante Single Sign-On (SSO). El sistema deberá registrar los accesos con autenticación basada en usuario y contraseña dentro del dominio corporativo de Bizkaia, que será único para todos los sistemas implementados. Además, cumplirá con los requerimientos previamente definidos en cuanto a perfiles y roles. Características clave: • Auditoría: El sistema deberá incluir herramientas de auditoría para registrar todas las operaciones realizadas, identificando al usuario responsable de cada acción, garantizando trazabilidad y control. • Cumplimiento Normativo: El sistema se ajustará a las disposiciones del Reglamento General de Protección de Datos (RGPD), asegurando el cumplimiento legal en la gestión de datos. • Seguridad Corporativa: El acceso estará basado en el producto de seguridad corporativa de la DFB (definido por Lantik), utilizando LDAP (Directorio Activo) para la validación de usuarios en cada conexión. • Acceso Externo: Para conexiones desde fuera de la red corporativa de BEAZ- DFB, se permitirá el acceso sin necesidad de VPN, a través de un nuevo portal seguro que autentique mediante usuario y contraseña.



Pantallas personalizables	El sistema debe permitir la configuración de las pantallas de trabajo, ofreciendo a las personas usuarias la capacidad de personalizar su experiencia mediante las siguientes funcionalidades: • Personalización de Opciones: Permitir a las personas usuarias añadir o eliminar opciones y elementos en las pantallas según sus necesidades específicas. • Interfaz Intuitiva: Proporcionar una interfaz fácil de usar que permita realizar estas configuraciones sin necesidad de conocimientos técnicos avanzados. • Guardado de Preferencias: Ofrecer la opción de guardar configuraciones personalizadas para su uso en futuras sesiones. • Visualización Dinámica: Asegurar que los cambios en las pantallas se reflejen de manera inmediata, permitiendo una experiencia de persona usuaria fluida.
Desarrollo a medida	Aunque el espíritu del proyecto es ir al estándar, en los casos excepcionales que fuera necesario, el sistema debe contar con la capacidad de adaptación mediante programación para implementar cambios específicos.
Configuración y administración de las estadísticas	El sistema debe proporcionar visibilidad de las estadísticas relevantes del software, incluyendo: • Acceso: Información sobre la frecuencia y la duración de las sesiones de los usuarios. • Utilización de Aplicaciones: Análisis del uso de las diferentes aplicaciones dentro del sistema, identificando las más y menos utilizadas. • Rendimiento: Métricas sobre la velocidad de respuesta del sistema, tiempos de carga y disponibilidad. • Dashboard Interactivo: Panel de control que permita a las personas usuarias visualizar estas estadísticas de manera clara y en tiempo real. • Exportación de datos: Ofrecer la opción exportar los datos de actividad en Excel, Word o pdf. • Alertas y Notificaciones: Establecer alertas automáticas para identificar anomalías en el rendimiento o en el uso del software. • Análisis Histórico: Proporcionar acceso a datos históricos para permitir comparaciones y análisis de tendencias a lo largo del tiempo.
Configuración y administración de logs	El sistema debe permitir la visualización de logs para el seguimiento de procesos específicos, así como del rendimiento general del sistema y la identificación de posibles errores. • Registro Detallado: Proporcionar logs que incluyan información detallada sobre la ejecución de procesos, tiempos de respuesta y eventos del sistema. • Interfaz de Visualización: Proporcionar una interfaz intuitiva que permita filtrar y buscar información en los logs de manera eficiente. • Exportación de Logs: Permitir la exportación de registros en formatos comunes (CSV, PDF) para análisis posteriores. • Historial de Logs: Mantener un historial de logs accesible, permitiendo a las personas usuarias revisar eventos pasados y tendencias en el rendimiento.



Jobs y Notificaciones	El sistema debe permitir la gestión de Jobs (tareas automáticas en fondo) para la automatización de ejecuciones en segundo plano: • Creación y Programación: Facilitar la creación y programación de jobs para que se ejecuten automáticamente en horarios específicos o en respuesta a eventos determinados. • Monitoreo de Ejecuciones: Proporcionar herramientas para monitorear el estado de los jobs, mostrando si están en ejecución, completados o si han fallado. • Notificaciones y Alertas: Implementar un sistema de notificaciones que informe a las personas usuarias sobre el estado de los jobs, especialmente en caso de errores o fallos durante la ejecución. • Configuración Personalizada: Permitir la configuración personalizada de los jobs, incluyendo parámetros de ejecución, frecuencia y condiciones bajo las cuales deben ejecutarse. • Registro de Actividades: Mantener un registro detallado de todas las ejecuciones de jobs, con información sobre resultados, tiempos de ejecución y cualquier error encontrado. • Interfaz Intuitiva: Proporcionar una interfaz fácil de usar que permita a los administradores gestionar y configurar los jobs sin complicaciones.
Integración y conectividad con herramientas corporativas	Los sistemas para implantar se podrán integrar con el resto de los sistemas corporativos que se requiera. Los sistemas deberán disponer de diferentes herramientas para ello como, por ejemplo: API REST/JSON, Web services SOAP/SML, PowerAutomate.
Entornos	El sistema debe disponer de 3 entornos: • Desarrollo: Entorno para realizar la construcción, modificaciones y pruebas/correcciones de las funcionalidades. • Pruebas: Tendrá condiciones similares al de producción y se utilizará para la formación de personas usuarias, pruebas estructuradas y garantizar que el sistema funcione correctamente antes de enviarlo a producción. • Producción: Entorno donde el sistema está disponible para las personas usuarias finales y funciona de operativa. En este entorno se podrán llevar a cabo todas las funcionalidades requeridas por las personas usuarias.
Gestión de diferentes ubicaciones	Los sistemas deben permitir visualizar toda la actividad ofrecida, así como la gestión económica y financiera para cada centro de trabajo.



Motor de búsqueda	Los sistemas deben incluir un motor de búsqueda robusto que permita realizar búsquedas completas y complejas entre los datos registrados. Los sistemas cubrirán los siguientes requisitos: • Búsquedas Avanzadas: Facilitar búsquedas detalladas utilizando múltiples criterios y operadores lógicos, como por ejemplo AND, OR y NOT. • Filtrado Personalizado: Permitir a las personas usuarias aplicar diferentes lógicas de filtrado basadas en campos de uso habitual, como fechas, categorías, estados y otros atributos relevantes. • Sugerencias de Búsqueda: Ofrecer sugerencias automáticas a medida que la persona usuaria escribe, mejorando la experiencia de búsqueda y ayudando a encontrar resultados relevantes rápidamente. • Resultados Relevantes: Presentar los resultados de búsqueda de manera clara y ordenada, con la opción de clasificarlos según diferentes criterios (por ejemplo, relevancia, fecha, etc.). • Exportación de Resultados: Ofrecer la opción de exportar los resultados de búsqueda en Excel para su análisis o uso posterior.
Flexibilidad	El sistema debe ser lo suficientemente flexible para abarcar la complejidad y diversidad de los procesos de BEAZ, además de permitir la rápida implementación de nuevos requerimientos que surjan de las necesidades futuras: • Adaptabilidad a Procesos: Permitir ajustes en los flujos de trabajo y procesos existentes para acomodar cambios en las operaciones de BEAZ sin complicaciones. • Interfaz Configurable: Proporcionar herramientas intuitivas para que los administradores puedan personalizar el sistema sin depender de recursos técnicos externos. • Escalabilidad: Facilitar la adición de nuevas funcionalidades y módulos a medida que evolucionen las necesidades del negocio, asegurando un crecimiento sostenible (nuevos servicios, normativas ISO, cambios de legalidad, etc.).
Gobernanza del dato	El sistema implementará una serie de características diseñadas para optimizar la gobernanza de datos, asegurando así: • Estandarización de Procesos: Establecimiento de protocolos claros para la gestión de datos, garantizando que todas las personas usuarias sigan las mismas pautas. • Transparencia y Trazabilidad: Registro detallado de todas las acciones realizadas sobre los datos, lo que permitirá una fácil auditoría y seguimiento de cambios. • Seguridad y Cumplimiento: Implementación de medidas de seguridad robustas para proteger la integridad y confidencialidad de los datos, asegurando el cumplimiento con normativas vigentes.
Accesibilidad	El sistema debe acceder a través de la web, garantizando compatibilidad con los navegadores actuales y dispositivos, incluidos ordenadores personales y móviles. • Compatibilidad Multiplataforma: El sistema debe funcionar en todos los sistemas operativos, incluyendo Windows, macOS, iOS y Android. • Diseño Responsivo: La interfaz debe adaptarse automáticamente a diferentes tamaños de pantalla, asegurando una experiencia de la persona usuaria óptima en dispositivos móviles y tablets. • Interfaz Intuitiva: Garantizar que la interfaz sea fácil de navegar y usar en todos los dispositivos, facilitando la accesibilidad para todas las personas usuarias.



Conectividad	Es esencial que el sistema permita la integración fluida con una variedad de plataformas y aplicaciones, tales como: • Agenda: Sincronización con calendarios para gestionar citas y recordatorios. • Correo electrónico: Integración con servicios de correo para facilitar la comunicación y el intercambio de información. • Teléfonos/Teams: Capacidad para realizar y recibir llamadas temas directamente desde la aplicación, así como la gestión de contactos. (Exclusivo Salesforce)
Disponibilidad	El sistema debe garantizar una disponibilidad ininterrumpida de 24 horas al día, 7 días a la semana, durante todo el año (24x7x365). Para facilitarlo el sistema dispondrá de: • Monitoreo Proactivo: Establecer un monitoreo constante del sistema para detectar y resolver problemas antes de que afecten la disponibilidad. • Plan de Recuperación ante Desastres: Desarrollar un plan de contingencia que permita la rápida recuperación del sistema en caso de fallos o incidentes críticos. • Mantenimiento Programado: Realizar mantenimientos de sistema de forma planificada y comunicada con antelación, minimizando su impacto en la disponibilidad. • Escalabilidad: Asegurar que la infraestructura soporte un aumento en la carga de trabajo sin comprometer la disponibilidad del servicio. • En caso de ser necesarias paradas para la realización de mantenimientos programados, estas deben ser planificadas y acordadas previamente entre Lantik y BEAZ. • Planificación Anticipada: Las paradas deben ser programadas con suficiente antelación para minimizar el impacto en las operaciones diarias. • Comunicación Clara: Informar a todas las personas usuarias afectados sobre las fechas y horarios de las paradas, así como los motivos y la duración estimada. • Aprobación Conjunta: Asegurar que tanto Lantik como BEAZ lleguen a un acuerdo sobre el calendario y los procedimientos de mantenimiento. • Documentación: Mantener un registro de todas las paradas programadas, incluyendo detalles sobre las actividades realizadas y los resultados obtenidos.
Soporte	• El soporte del sistema proporcionado por la empresa adjudicataria debe estar disponible en castellano. • Asistencia Continua: Garantizar que el soporte esté disponible en el horario del apartado 4.3.3. • Atención en Castellano: Asegurar que todo el soporte técnico se brinde en castellano, facilitando la comunicación efectiva con las personas usuarias. • Canales de Contacto: Ofrecer múltiples canales de contacto, como teléfono, correo electrónico y teams, para que las personas usuarias puedan acceder al soporte de la manera que les resulte más conveniente. • Registro de Incidencias: Mantener un sistema de registro para todas las incidencias reportadas, permitiendo un seguimiento adecuado y la resolución de problemas de manera eficiente.



4.3.1.5 Requisitos funcionales específicos

Durante los tres años que abarca el contrato, el proyecto deberá completarse y todas las funcionalidades deberán desarrollarse en su totalidad. Es importante señalar que las funcionalidades originalmente planificadas para cada fase del desarrollo pueden ser reprogramadas a diferentes etapas debido a consideraciones presupuestarias.

Para mayor definición de las funcionalidades se ha trabajado en un documento detallado que por su contenido no se considera conveniente adjuntarlo al expediente. La empresa que considere presentarse a la licitación podrá disponer de dicho documento detallado para poder evaluar con mayor profundidad las especificaciones técnicas.

Para solicitar el documento detallado, la empresa interesada deberá enviar un correo electrónico al buzón "eskaintzak.lantik@bizkaia.eus" con asunto "Expediente XXXX - Solicitud de información técnica adicional" y se deberá adjuntar obligatoriamente el ANEXO B firmado y en formato PDF.

La fecha límite para solicitar el documento detallado será al menos 12 días antes de la finalización del plazo de presentación de ofertas.

4.3.2 Alcance bajo demanda

Es alcance de este contrato cualquier nueva necesidad que pueda surgir en el ámbito de soluciones de negocio sobre los productos Dynamics 365 Business Central de Microsoft, Power APPs de Microsoft y Customer 360 de Salesforce.

Estos servicios y sus requisitos se irán trasladando a lo largo de la vigencia del contrato y tras una previa valoración se determinará su posible ejecución.

Valoraciones y aprobaciones

La empresa adjudicataria deberá realizar un cuadro de valoración detallado, en horas y plazos, y los trabajos se iniciarán tras la aceptación por parte de Lantik de esta valoración.

A su finalización, la empresa adjudicataria facturará los trabajos en base a la valoración aceptada.

Lantik revisará los trabajos efectivamente entregados, comprobando que se corresponden con lo aceptado anteriormente y dará su aprobación en cada caso.

Se podrán también, establecer trabajos en formato "llave en mano" para los que la valoración en horas, funcionalidades y plazos será fija, procediéndose al pago en base a la propuesta de entregas funcionales acordadas entre las partes.

4.3.3 Horario del servicio

El horario mínimo requerido, aplicable a todas las semanas del año con excepción de los días festivos en Bilbao y el 24 y 31 de diciembre, será:

INVIERNO (de lunes a jueves)

Periodos: del 1 de enero al 30 de junio y del 1 de septiembre al 31 de diciembre.

Horario: de 8:00 a 18:00.



INVIERNO (viernes) y VERANO

Periodo: del 1 de julio al 31 de agosto y todos los viernes del año.

Horario: de lunes a viernes de 8:00 a 15:00.

El tiempo de respuesta dentro del horario de servicio deberá ser inmediato. (Definido como el tiempo que pasa desde que se envía una comunicación y se recibe una respuesta.)

Es requisito contar con una disponibilidad de atención 24/7 basada en tener acceso al teléfono móvil de una persona responsable, para poder informar sobre emergencias o situaciones imprevistas y que así pueda organizar el equipo necesario para manejar la situación. Este contacto deberá estar disponible durante toda la vigencia de contrato independientemente de periodos vacacionales.

Lantik podrá solicitar intervenciones planificadas fuera del horario de servicio, principalmente pases a producción, facturándose estos con un coeficiente de 1,5 sobre los precios unitarios establecidos.

4.3.4 Modalidad de trabajo

Si bien el trabajo se desempeñará con carácter ordinario en remoto, Lantik puede requerir que el trabajo se realice presencialmente en sus instalaciones, o en cualquiera de las dependencias de la DFB y de sus empresas u organismos forales, cuando sea necesario por necesidades del servicio sin coste adicional.

4.3.5 Fases de ejecución - Documentación

Durante la implantación de las soluciones de negocio se deberán llevar a cabo todas las fases definidas en la metodología propuesta, así como garantizar la puesta en marcha de los sistemas:

- Despliegue de la solución en entorno de Producción de Lantik en modalidad nube.
- Despliegue de la solución en entorno de No Producción de Lantik (desarrollo) en modalidad nube.
- Despliegue de la solución en entorno de No Producción de Lantik (pruebas) en modalidad nube.
- Puesta en marcha de la solución.

Se deberá realizar como mínimo la siguiente documentación:

- Plan de Gestión del Proyecto (PGP) incluyendo: Alcance, objetivos, estructura, organización y responsabilidades del equipo (de la empresa adjudicataria, Lantik y sus clientes), metodología, cronograma de detalle (actividades, hitos, dependencias y responsables), estrategia de gestión del cambio y gestión de la calidad.
- Visión y Alcance (VyA): Detalle de cómo los nuevos sistemas cubrirán los requisitos funcionales requeridos
- GAP análisis (GAP): Comparativa entre los procesos optimizados con los nuevos sistemas respecto a cómo se trabaja actualmente.



- Documento de Requisitos de Desarrollo (DRD): detalle de las personalizaciones, integraciones y configuraciones técnicas.
- Documento de Pruebas (DPR): plan de pruebas y resultado de las pruebas
- Manual de Usuario/a (MDU)
- Documento relativo a la instalación y configuración de la solución, incluirá esquema de arquitectura.
- Plan de formación

4.4 Equipo técnico

El equipo técnico corresponde a las personas, adscritas al contrato, que deben acreditar unos conocimientos y/o experiencia mínimos para garantizar una correcta ejecución del servicio. Si estas se identificasen mediante identificativos no personales en las tablas solicitadas para la verificación de los requisitos, deberán ser detalladas con nombre y apellidos una vez se firme el contrato.

Para la correcta ejecución del objeto de contrato será necesario contar con un equipo técnico estable compuesto por al menos la siguiente relación de personas que cubran la siguiente experiencia y/o conocimiento:

- 1 persona responsable del servicio:
 - Haber gestionado la implantación de al menos dos proyectos ERP Dynamics 365 Business Central y al menos un proyecto CRM Customer 360 de Salesforce.
 - Experiencia mínima de 5 años gestionando proyectos y equipos.
- 5 personas ERP consultoras funcionales y técnicas
 - Las 5 personas deberán haber participado en la implantación de al menos tres proyectos de soluciones en Dynamics 365 Business Central.
 - Tres de ellas deberán acreditar al menos una de las siguientes certificaciones:
 - "Dynamics 365 Business Central Functional Consultant Associate - MB-800 certification"
 - "Dynamics 365 Business Central Developer Associate - MB-820 Certification".
- 3 personas CRM consultoras funcionales y técnicas
 - Las 3 personas deberán haber participado en la implantación de al menos tres proyectos de soluciones en Customer 360 Salesforce.
 - Entre las 3 personas deberán acreditar al menos las siguientes certificaciones de Salesforce:
 - "Sales Cloud Consultant"
 - "Platform Developer I" o "Platform Developer II"



- 1 persona Administradora de la plataforma ERP:
 - Experiencia mínima de tres años realizando tareas de instalación, configuración, parametrización y mantenimiento de ERP Dynamics 365 Business Central.
 - Acreditar la certificación “Dynamics 365 Business Central Functional Consultant Associate – MB-800 certification” o la “Dynamics 365 Business Central Developer Associate – MB-820 Certification”.
- 1 persona Administradora de la plataforma CRM:
 - Experiencia mínima de tres años realizando tareas de instalación, configuración, parametrización y mantenimiento de CRM en Customer 360 Salesforce.
 - Acreditar la certificación “Administrator” o la “Advanced Administrator” de Salesforce.

Es requisito que todas las empresas licitadoras presenten debidamente cumplimentadas las tablas RESUMEN y DETALLE. Las ofertas que no incluyan las tablas serán excluidas de la licitación.



TABLAS Responsable servicio

TABLA 1: ERP

Id. (1)	Descripción del proyecto	Cliente (Entidad)	Periodo			Al menos dos proyectos ERP Dynamics 365 Business Central
			Fecha inicio (2)	Fecha fin (2)	Suma	Descripción de tareas realizadas
1			mm/aaaa	mm/aaaa	Σ meses	
1			mm/aaaa	mm/aaaa	Σ meses	

- (1) Identificador: nº correlativo que identifica a cada persona del equipo.
(2) El formato de fechas deberá ser de mes y año, no se admitirá solo el año. Se analizará el solape de fechas.

TABLA 2: CRM

Id. (1)	Descripción del proyecto	Cliente (Entidad)	Periodo			Al menos un proyecto CRM Customer 360 de Salesforce
			Fecha inicio (2)	Fecha fin (2)	Suma	Descripción de tareas realizadas
1			mm/aaaa	mm/aaaa	Σ meses	
1			mm/aaaa	mm/aaaa	Σ meses	

- (1) Identificador: nº correlativo que identifica a cada persona del equipo.
(2) El formato de fechas deberá ser de mes y año, no se admitirá solo el año. Se analizará el solape de fechas.



TABLA 3: Gestión proyectos y equipos

Id. (1)	Descripción del proyecto	Cliente (Entidad)	Periodo			Gestión de proyectos y equipos
			Fecha inicio (2)	Fecha fin (2)	Suma	Descripción de tareas realizadas
1			mm/aaaa	mm/aaaa	Σ meses	
1			mm/aaaa	mm/aaaa	Σ meses	
TOTAL					Σ meses (3)	

- (1) Identificador: nº correlativo que identifica a cada persona del equipo.
- (2) El formato de fechas deberá ser de mes y año, no se admitirá solo el año. Se analizará el solape de fechas.
- (3) El total de meses.



TABLA RESUMEN Equipo ERP

Id.(1)	Implantación de proyectos de soluciones en Dynamics 365 Business Central	Instalación, configuración, parametrización y mantenimiento de ERP Dynamics 365 Business Central	Dynamics 365 Business Central Functional Consultant Associate – MB-800 certification (2)	Dynamics 365 Business Central Developer Associate – MB-820 Certification (2)
2	(nº proyectos)	-	(si/no)	(si/no)
3	(nº proyectos)	-	(si/no)	(si/no)
4	(nº proyectos)	-	(si/no)	(si/no)
5	(nº proyectos)	-	(si/no)	(si/no)
6	(nº proyectos)	-	(si/no)	(si/no)
7	-	(meses)	(si/no)	(si/no)

(1) Identificador: nº correlativo que identifica a cada persona del equipo.

(2) Presentar certificados de las personas.



TABLA DETALLE ERP 1: una tabla para cada persona identificada desde id2 hasta id6.

Id. (1)	Descripción del proyecto	Cliente (Entidad)	Periodo			Implantación de al menos 3 proyectos de soluciones en Dynamics 365 Business Central
			Fecha inicio (2)	Fecha fin (2)	Suma	Descripción de tareas realizadas
x			mm/aaaa	mm/aaaa	Σ meses	
x			mm/aaaa	mm/aaaa	Σ meses	

(1) Identificador: n° correlativo que identifica a cada persona del equipo.

(2) El formato de fechas deberá ser de mes y año, no se admitirá solo el año. Se analizará el solape de fechas.

TABLA DETALLE ERP 2: una tabla para id7.

Id. (1)	Descripción del proyecto	Cliente (Entidad)	Periodo			Instalación, configuración, parametrización y mantenimiento de ERP Dynamics 365 Business Central
			Fecha inicio (2)	Fecha fin (2)	Suma	Descripción de tareas realizadas
7			mm/aaaa	mm/aaaa	Σ meses	
7			mm/aaaa	mm/aaaa	Σ meses	
TOTAL					Σ meses (3)	

(1) Identificador: n° correlativo que identifica a cada persona del equipo.

(2) El formato de fechas deberá ser de mes y año, no se admitirá solo el año. Se analizará el solape de fechas.

(3) El total de meses.



TABLA RESUMEN: Equipo CRM

Id.(1)	Implantación de proyectos de soluciones en Customer 360 Salesforce	Instalación, configuración, parametrización y mantenimiento de CRM en Customer 360 Salesforce	Sales Cloud Consultant	"Platform Developer I" o "Platform Developer II"	"Administrator" o la "Advanced Administrator"
8	(nº proyectos)		(si/no)	(si/no)	-
9	(nº proyectos)		(si/no)	(si/no)	-
10	(nº proyectos)	-	(si/no)	(si/no)	-
11	-	(meses)			(si/no)

- (1) Identificador: nº correlativo que identifica a cada persona del equipo.
(2) Presentar certificados de las personas.

TABLA DETALLE CRM 1: una tabla para cada persona identificada desde id8 hasta id10.

Id. (1)	Descripción del proyecto	Cliente (Entidad)	Periodo			Implantación de al menos 3 proyectos de soluciones en Customer 360 Salesforce
			Fecha inicio (2)	Fecha fin (2)	Suma	Descripción de tareas realizadas
x			mm/aaaa	mm/aaaa	Σ meses	
x			mm/aaaa	mm/aaaa	Σ meses	

- (1) Identificador: nº correlativo que identifica a cada persona del equipo.
(2) El formato de fechas deberá ser de mes y año, no se admitirá solo el año. Se analizará el solape de fechas.



TABLA DETALLE CRM 2: una tabla para id11.

Id. (1)	Descripción del proyecto	Cliente (Entidad)	Periodo			Instalación, configuración, parametrización y mantenimiento de CRM en Customer 360 Salesforce
			Fecha inicio (2)	Fecha fin (2)	Suma	Descripción de tareas realizadas
11			mm/aaaa	mm/aaaa	Σ meses	
11			mm/aaaa	mm/aaaa	Σ meses	
TOTAL					Σ meses (3)	

- (1) Identificador: nº correlativo que identifica a cada persona del equipo.
- (2) El formato de fechas deberá ser de mes y año, no se admitirá solo el año. Se analizará el solape de fechas.
- (3) El total de meses.



5 CONDICIONES PARTICULARES

5.1 Responsabilidades de la empresa adjudicataria

Las responsabilidades de la empresa adjudicataria serán, entre otras:

- Cumplir los procedimientos, normas y estándares establecidos por Lantik relativos al servicio demandado.
- Los trabajos se desarrollarán mayormente en los locales y equipos de la empresa adjudicataria, quien dispondrá y gestionará los entornos necesarios para la prestación del servicio, y solo en caso de que sea necesario, mediante conexión con la infraestructura de Lantik.
- Llevar a cabo todas las fases definidas, ejecutando las acciones necesarias para garantizar la puesta en marcha completa de los sistemas en los tres entornos establecidos: desarrollo, pruebas y producción
- Analizar cada demanda de trabajo y estimar el esfuerzo necesario para su ejecución incluyendo y detallando cada actividad; utilizando procedimientos de valoración.
- Facilitar a Lantik el detalle de esfuerzo dedicado a la implementación de cada demanda, comparado con la estimación prevista.
- Entregar a Lantik los informes de situación definidos que permitan el control continuo del servicio.
- En todos los casos, a no ser que se autorice expresamente y para un tema puntual, será obligatorio acudir con personal de Lantik a cualquiera de las dependencias de la DFB, de sus empresas u organismos forales.
- Asignar al servicio las personas técnicas que cumplan con el perfil profesional requerido.
- Alimentar los sistemas de información acordados para asegurar la calidad del servicio.

5.2 Control y seguimiento

La empresa licitadora deberá presentar una propuesta detallada de seguimiento del servicio, incluyendo los informes correspondientes que considere pertinentes.

Durante la ejecución del contrato, se podrá solicitar la realización de cuantos informes sean necesarios, para un mejor análisis del servicio.

La empresa adjudicataria utilizará los sistemas de Lantik para el registro de incidencias, consultas y problemas, así como para la gestión de las peticiones asignadas. Podrá complementar la información de dichos sistemas con sus propias herramientas si así lo considerase oportuno.

Sistemas actuales de Lantik:

Gestión de incidencias, consultas y problemas: BMC Remedy dispone de ajustes para ajustarse al modelo de seguimiento establecido en las normativas de Lantik).

Plataforma Zeregin: conjunto de aplicaciones de desarrollo interno para la gestión del ciclo de vida de las peticiones o proyectos.



5.3 Modelo de gestión

El modelo de gestión, cuya propuesta inicial deberá ser planteada por la empresa licitadora, deberá incluir los siguientes elementos:

Modelo Organizativo

La empresa licitadora deberá detallar la organización del equipo de trabajo y sus funciones en relación con los servicios a prestar.

Modelo Operativo

La empresa licitadora presentará una propuesta de funcionamiento para cubrir las actividades del servicio.

5.4 Propuesta técnica (estructura)

De cara a la correcta valoración de los criterios no cuantificables automáticamente (sobre C), la propuesta técnica presentada por la empresa licitadora en el **sobre C deberá ajustarse como máximo a 75 páginas** a una sola cara, tamaño de letra mínimo equivalente al tipo "Arial" de 10 pt y con márgenes de al menos 2,5 cm, y deberá contener como mínimo los siguientes apartados:

- Introducción
- Descripción servicio
 - Suscripciones ERP y CRM (no especificar ningún precio)
 - Servicio gestionado de administración
 - Modelo organizativo
 - Modelo operativo
 - Implantación de soluciones de negocio
 - "Alcance específico": entendimiento global, plan de proyecto, plan de implantación, modelo organizativo, modelo operativo, seguimiento, plan de formación ...
 - "Alcance bajo demanda": modelo organizativo, modelo operativo, seguimiento general, formación ...
 - Equipo técnico (las tablas solicitadas en el apartado 4.4)

No contabilizará en las 75 páginas las tablas que se deben incluir para acreditar el apartado "Equipo técnico", ni los informes de seguimiento en caso de presentar ejemplos. Esta información se podrá presentar en anexos.

Se podrán añadir otro tipo de anexos a modo informativo, pero en ningún caso la información contenida en ellos será considerada para la valoración de los criterios no cuantificables automáticamente.



5.5 Equipo de trabajo

El equipo de trabajo estará integrado, como mínimo, por las personas especificadas en el apartado “Equipo técnico”. Durante la ejecución del contrato, la empresa adjudicataria podrá incorporar los perfiles que juzgue necesarios para garantizar la adecuada prestación del servicio, considerando posibles variaciones en la carga de trabajo.

Se deberá garantizar la gestión de un equipo variable que se adecue a la demanda del servicio en función de las necesidades de cada momento.

Cualquier cambio en el “Equipo técnico” deberá justificarse (con la presentación de la información solicitada en las tablas del “Equipo técnico”) y las sustituciones deberán realizarse con un perfil de cualificación técnica igual o superior a la solicitada. La empresa adjudicataria tendrá obligación de formar a la persona cuya incorporación haya sido aprobada por Lantik, entre otros, con los conocimientos generales y específicos de las labores a realizar, la situación actual de las mismas, los procedimientos de trabajo a seguir, los roles y responsabilidades del equipo, etc. La empresa adjudicataria lo hará por sus propios medios, sin coste adicional para Lantik.

Del mismo modo, cualquier modificación en la composición del “Equipo de trabajo” a lo largo de la duración del contrato, especialmente cuando se trate de personas que dejan el equipo y tienen acceso a los sistemas de Lantik, debe ser comunicada con la mayor brevedad posible.

Todos los miembros del “Equipo de trabajo” deberán hablar castellano y/o euskera como lengua nativa o ser capaces de comunicarse en castellano y/o euskera de forma fluida. En caso de incluir recursos que no cumplan este perfil, la empresa adjudicataria deberá proporcionar, a petición de Lantik, intérpretes que faciliten la comunicación sin cargo adicional para Lantik.

Lantik podrá solicitar la sustitución de cualquier persona del equipo de trabajo, aunque cumpla con el conocimiento técnico requerido, si no tuviese las aptitudes necesarias para la realización de los trabajos en equipo y/o un mínimo de calidad en los trabajos realizados. Si se llegase a esta situación, se informará a la persona responsable de la empresa adjudicataria con las evidencias oportunas.

Debido a la evolución tecnológica es responsabilidad de la empresa adjudicataria la formación continua del personal adscrito al contrato.

5.6 Finalización del contrato

Se habrán cumplido con las obligaciones contractuales, cuando alguna de las siguientes circunstancias se dé primero:

- Se alcance la fecha de terminación del contrato o se alcancen las horas totales establecidas.
- Lantik decida dar por terminado el servicio.



5.7 Perspectiva de género

Las empresas licitadoras, en la elaboración y presentación de sus respectivas propuestas deberán hacer un uso no sexista del lenguaje. Asimismo, la empresa adjudicataria, a lo largo de la vigencia del contrato, deberá hacer un uso no sexista del lenguaje en cualquier documento definitivo escrito o digital, así como, deberá desagregar los datos por sexo en cualquier estadística referida a personas que se genere, todo ello al amparo del artículo 2.3 de la Ley 4/2005, de 18 de febrero, para la Igualdad de Mujeres y Hombres en el que se señalan los principios generales que deberán respetarse.

La empresa adjudicataria presentará en la justificación final de la realización de la prestación objeto del contrato, en su caso, una memoria sobre el impacto de género de la contratación, con los indicadores y datos desagregados por sexo de las personas usuarias o beneficiarias, o del personal prestador del servicio, que posibiliten evaluar la eficacia de las medidas de igualdad aplicadas.

5.8 Seguridad de la información

Contrato, acuerdo de confidencialidad, Normativa de seguridad para empresas proveedoras, y protección de datos de carácter personal

En el contrato a firmar se incluirá:

- Acuerdo de confidencialidad.
- Conocimiento y compromiso de cumplimiento por parte de la empresa adjudicataria de:
 - Política de seguridad de la información de Bizkaiko Foru Aldundia / Diputación Foral de Bizkaia.
 - [Norma NCS-1/1 "Norma de Política de Seguridad: Código de Conducta Informático para Proveedores"](#).
 - [Norma NCS-1/2 "Normativa de Seguridad de la Información para Proveedores"](#).

El acuse de recibo y compromiso de cumplimiento de las normativas internas existentes en Lantik S.A. M.P., previa a la prestación del servicio, deberá realizarse por todo el personal interviniente en el mismo (tanto el de la empresa proveedora y como el de posibles subcontrataciones que haga esta), de lo cual se encargará de recoger y custodiar la empresa proveedora que responderá en su nombre.

5.8.1 Deber de confidencialidad

I. Prohibición expresa de acceso a datos privados o confidenciales

Para la realización de los trabajos objeto del presente contrato es posible que el personal de la empresa adjudicataria tenga acceso a locales donde se realizan tratamientos de datos de carácter personal, a soportes o recursos que los contengan o a otro tipo de documentación de carácter privado o confidencial, para la realización de trabajos que no impliquen directamente un



tratamiento de este tipo de datos. En particular, será considerado como Información Confidencial todo el know how o saber hacer resultante de la ejecución de los servicios contratados, debiendo el adjudicatario mantener dicha información en reserva y secreto y no revelarla de ninguna forma, en todo o en parte, a ninguna persona física o jurídica que no sea parte del contrato. De este modo, se considerará confidencial, a todos los efectos, toda la información y documentación relativa a Lantik S.A. M.P. y/o que esta trate a cuenta de terceros, así como los buenos usos, prácticas y procedimientos internos, que pudiera conocer la empresa adjudicataria con motivo de la ejecución del contrato. En la misma línea, se confiere el carácter confidencial a aquella información a la que tenga acceso con ocasión de la ejecución del contrato, que se le hubiese dado el referido carácter en los pliegos o en el contrato, o que por su propia naturaleza deba ser tratada como tal, incluyendo, expresamente, toda la información asociada a medidas de seguridad y de protección, configuraciones desarrolladas, protecciones del servicio y aplicaciones, elementos y descripciones de infraestructura y arquitectura, procesos de autenticación y protocolos de seguridad, comunicaciones, incidencias, informes de terceros, controles de capacidad y evaluaciones de las disponibilidades implicadas, análisis automáticos, redes y protecciones del perímetro, elementos adscritos a la continuidad, registros de actividad y protecciones asociadas, protocolos de copias y restauraciones, elementos de mantenimiento y garantías implicadas, y cuantos otros elementos puedan considerarse un riesgo a los efectos del servicio contratado o la información vinculada al mismo. En cualquier caso, se prohíbe expresamente el acceso a este tipo de datos, ni a ningún dato que no sea objeto de tratamiento del presente. Con ello, la empresa adjudicataria se compromete a no divulgar, no ceder o exponer la información titularidad de Lantik S.A. M.P. y /o que esta trate a cuenta de terceros, sin su previo consentimiento expreso y por escrito. Asimismo, la empresa adjudicataria deberá abstenerse de emplear la documentación y/o información conocida o facilitada durante la ejecución del contrato para fines ajenos a los propios de la ejecución del contrato.

Cuando el contrato no requiera el acceso al sistema de información de Lantik S.A. M.P. pero suponga el acceso a sus instalaciones, la empresa adjudicataria se compromete a mantener plena confidencialidad de la información que pudiera conocer de manera accidental por los accesos a las instalaciones, y especialmente, aquella que pueda suponer un riesgo para Lantik S.A. M.P. y/o para terceros en caso de ser conocida y/o pueda suponer una brecha de seguridad.

II. Deber de secreto

El personal de la empresa adjudicataria deberá observar en todo momento el secreto profesional y deber de confidencialidad sobre todos los datos de carácter privado o confidencial, a los que pudiera tener acceso incidentalmente en el cumplimiento de las tareas encomendadas.

El personal de la empresa adjudicataria queda obligado a no revelar, transferir, ceder o comunicar de cualquier forma este tipo de datos a terceras personas, obligación que se mantendrá aún finalizada su relación con esta.

La empresa adjudicataria se compromete a comunicar y hacer cumplir a su personal las obligaciones establecidas en el presente pliego y, en concreto, las relativas al deber de secreto.

Si se produjera una incidencia durante la ejecución del contrato que conllevará un acceso accidental o incidental a Datos Personales no contemplados en el presente pliego, la empresa



adjudicataria deberá ponerlo en conocimiento de Lantik S.A. M.P., en concreto, a la persona interlocutora del contrato, con la mayor diligencia y a más tardar en el plazo de 72 horas.

Serán motivos de resolución del contrato la vulneración del deber de secreto por la empresa adjudicataria o su personal.

III. Garantía de confidencialidad

La empresa adjudicataria certifica que el personal a su cargo ha firmado una cláusula de confidencialidad por la cual se compromete a no revelar la información que conozca en función de su cargo o cometido durante la prestación del contrato y posteriormente al mismo. Así como que conoce las medidas de seguridad tendentes a garantizar el cumplimiento de la normativa relativa a protección de los datos de carácter personal.

IV. Tratamiento de datos para la gestión de los servicios de contratación de Lantik

En cumplimiento de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, LANTIK S.A. M.P. como responsable del tratamiento, informa al personal de la empresa adjudicataria que sus datos de carácter personal serán tratados e incorporados a su actividad de tratamiento que tiene como finalidad la gestión de los servicios de contratación de Lantik. El tratamiento de dichos datos es necesario para el cumplimiento de una obligación legal y no se comunicarán los datos a terceros salvo obligación legal. Las personas interesadas podrán ejercer sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad, en la medida que sean aplicables, ante el responsable del tratamiento (<https://lantik.bizkaia.eus/es/aviso-legal>) y podrán consultar información adicional y detallada sobre protección de datos en <https://lantik.bizkaia.eus/es/-/gestion-de-los-servicios-de-contratacion-de-lantik>.

En caso de que la empresa adjudicataria facilitara datos personales de terceros, incluidos los relativos al personal a su servicio, previamente a su inclusión deberá informar a las personas interesadas de los extremos establecidos en el párrafo anterior.

5.8.2 Medidas de seguridad

La empresa adjudicataria garantizará que la información de la que disponga por razón de la prestación del servicio no pueda ser visible por personas no autorizadas. Así, los lugares donde almacene, guarde o conserve la información deberán ser aptos para garantizar el deber de confidencialidad.

Asimismo, la empresa adjudicataria se compromete a no revelar, transferir, ceder o de otra forma comunicar información confidencial o datos personales, ya sea verbalmente o por escrito, por medios electrónicos, papel o mediante acceso informático, ni siquiera para su conservación a ningún tercero (exceptuándose las cesiones autorizadas por ley).

La empresa adjudicataria comunicará a Lantik S.A. M.P. toda filtración de información de la que tenga o llegue a tener conocimiento, producida por la vulneración del presente acuerdo de



confidencialidad de las personas que hayan accedido a la información. Tal comunicación no exime a la empresa adjudicataria de su responsabilidad, pero si la incumple dará lugar a cuantas responsabilidades se deriven de dicha omisión en particular.

El presente acuerdo no supondrá, en ningún caso, la concesión de permiso o derecho expreso o implícito para el uso de licencias o derechos de autor, propiedad de la parte que revele la información. El receptor de la información se compromete a no copiar, reproducir, ni por cualquier otro procedimiento, ceder información o material facilitado por Lantik S.A. M.P. o al que hubiere tenido acceso, así como a no permitir a ninguna otra persona, empresa o institución la copia, reproducción o divulgación, sea total, parcial o de cualquier forma, de información o materiales facilitados por Lantik S.A. M.P. o a los que se hubieren tenido acceso en cualquier momento y que obren en poder de la empresa adjudicataria, sin la autorización previa de Lantik S.A. M.P., manifestada expresamente y por escrito.

Con el fin de coordinar y ser eficientes ante cualquier ciberincidente o ajuste de seguridad que se requiera, una vez haya sido firmado el contrato, la empresa adjudicataria debe indicar quién ocupa el rol de responsable de seguridad en su organización. Para ello, notificará por escrito a la persona responsable del contrato de Lantik S.A. M.P. el nombre, apellidos, correo electrónico y teléfono de la persona o servicio que desempeñe este rol.

Por parte de Lantik S.A. M.P, el contacto en relación a la gestión de cualquier ciberincidente o ajuste de seguridad en el ámbito o servicio objeto del pliego será:

Contacto: Área de plataforma tecnológica (Operación)

Teléfono: 944 068 989

Correo electrónico: alertas.operacion@bizkaia.eus

Dirección: Avenida Sabino Arana, 44 48013 Bilbao (Bizkaia)

Las partes acuerdan que en el caso de que sea necesario contactar a la otra parte para aclarar cualquier aspecto relacionado con la seguridad incluyendo cualquier duda, aspecto técnico o cualquier incidencia durante la prestación del servicio, se deberá realizar a las personas de contacto referidas anteriormente.

El personal de Lantik S.A. M.P, tendrá los siguientes roles y funciones en el ámbito de la seguridad:

- Transmitir a la empresa adjudicataria los requisitos y medidas de seguridad.
- En su caso, dar instrucciones y coordinar las actuaciones de mantenimiento.
- Dar instrucciones y coordinar las actuaciones en caso de que se produzca un incidente de seguridad de la información o desastre.
- En su caso, comprobar el cumplimiento del presente contrato, pudiendo requerir para ello la documentación que sea necesaria para acreditarlo.



El personal de la empresa adjudicataria tendrá los siguientes roles y funciones en el ámbito de la seguridad:

- Atender y asegurarse del cumplimiento de las medidas de seguridad que Lantik S.A. M.P. pudiera establecer.
- Transmitir a Lantik S.A. M.P., el cumplimiento de los requisitos y medidas de seguridad requeridos, realizando en caso necesario, las salvedades u observaciones que pudieran ser oportunas.
- En su caso, atender a las peticiones realizadas por el personal responsable de Lantik S.A. M.P., en materia de mantenimiento.
- Comunicar con antelación a la persona responsable de Lantik S.A. M.P., de cualquier actuación planificada que pudiera afectar a la disponibilidad, confidencialidad, integridad, autenticidad o trazabilidad de la información o servicios de la entidad.
- Comunicar a la persona responsable de Lantik S.A. M.P., cualquier incidente de seguridad de la información que se produzca a la mayor brevedad.
- Atender a las instrucciones dadas por Lantik S.A. M.P., en caso de que se produzca un incidente de seguridad de la información o desastre.
- Proporcionar la documentación o evidencias que sean necesarias para acreditar el cumplimiento del presente contrato.

5.8.3 Gestión interna de Lantik S.A. M.P. (medidas de securización interna) previas a la prestación

Lantik S.A. M.P. establecerá los mecanismos de control y securización interna que considere en su propia infraestructura, por ejemplo, asignación de usuarios temporales, rutado específico, perímetros de seguridad, etc.

5.8.4 Documentación

En caso de que la empresa adjudicataria preste en el ámbito del contrato un producto o servicio soportado por sistemas de información propios, deberá proporcionar a requerimiento de Lantik S.A. M.P. la información necesaria sobre la arquitectura de seguridad de dicho sistema de información, con el objeto de facilitar a esta el cumplimiento de sus obligaciones.

5.8.5 Auditoría, monitorización y reporte periódico del rendimiento de los controles de seguridad y notificación de evolución en la resolución de incidentes de seguridad a Lantik

Lantik S.A. M.P. se reserva el derecho de auditar y monitorizar las actividades realizadas por la empresa adjudicataria durante el servicio con el objetivo de prevenir y detectar incidentes de seguridad.



La empresa adjudicataria del servicio deberá remitir a requerimiento de Lantik S.A. M.P., sin perjuicio de otros plazos establecidos en el pliego, información sobre el nivel de rendimiento de los controles de seguridad establecidos, así como información de los incidentes no graves ocurridos en el periodo.

5.8.6 Informe periódico del cumplimiento de la “Normativa de Seguridad para Proveedores”

La empresa adjudicataria del servicio deberá remitir, a requerimiento de Lantik S.A. M.P., información sobre el nivel de cumplimiento de lo establecido en la Normativa de Seguridad para Proveedores.

5.8.7 Evidencia de buenas prácticas de seguridad acreditada en una norma de referencia para la gestión de la seguridad de la información, en el entorno de prestación.

A requerimiento de Lantik S.A. M.P., la empresa adjudicataria del servicio deberá aportar evidencias de buenas prácticas de seguridad en el servicio, preferiblemente mediante certificado de la implantación y uso de un modelo de gestión de la seguridad de la información en base las normas de referencia existentes para la gestión de la seguridad de la información, como por ejemplo la ISO/IEC 27001.

En el caso de que el alcance del contrato esté relacionado con la prestación de un producto o servicio correspondiente al diseño, instalación, configuración, puesta en marcha o mantenimiento de un sistema de información sobre el que se soporten servicios relacionados con la gestión de las competencias de Lantik S.A. M.P. (o de cualquier otra entidad del Sector Público a la que Lantik S.A. M.P. preste servicio) o desarrollen o ayuden a desarrollar el Procedimiento Administrativo regulado por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la empresa adjudicataria deberá cumplir la normativa legal aplicable en materia de seguridad en el marco de los servicios prestados.

Con carácter general deberá prestarse especial atención a la observancia de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. En este caso, la empresa adjudicataria asumirá el cumplimiento de lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, “Esquema Nacional de Seguridad”), en particular las medidas de seguridad establecidas en su Anexo II, en las dimensiones de seguridad que le apliquen y según el nivel de clasificación determinado en cada caso. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos en el Esquema Nacional de Seguridad, se aplicarán las medidas de seguridad indicadas en su Anexo II, ya sean pertenecientes al marco organizativo, operacional o de protección.

De este modo, con el fin de facilitar la realización de los controles periódicos exigidos para el cumplimiento de la citada legislación, la empresa adjudicataria deberá proporcionar a Lantik S.A. M.P. tras la firma del contrato:

- Bajo petición de Lantik S.A. M.P., la empresa adjudicataria proporcionará el detalle de la Declaración de Aplicabilidad y, en su caso, de las medidas compensatorias y complementarias de vigilancia utilizadas.



- Bajo petición de Lantik S.A. M.P. mecanismos y funcionalidades que permitan a Lantik S.A. M.P. conocer y analizar los controles llevados a cabo por parte de la empresa adjudicataria (auditorías de seguridad, informes de hacking ético, renovación de certificaciones de seguridad, utilización de componentes cualificados o certificados, etc.).

5.8.8 Medidas de seguridad y compromisos de la empresa adjudicataria en materia de seguridad de la información de los servicios de administración electrónica

[Las empresas adjudicatarias deben garantizar la seguridad de los productos o servicios que suministren. Para ello, los productos o servicios deben superar un proceso de cualificación y estar incluidos en el Catálogo de Productos y Servicios TIC del Centro Criptológico Nacional \(CPSTIC\), o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento establecidos en el artículo 19 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.](#)

La empresa adjudicataria del servicio deberá realizar las acciones necesarias para concienciar regularmente al personal interviniente en la prestación del servicio acerca de su papel y responsabilidad para que la seguridad del sistema y de los servicios prestados alcance los niveles exigidos.

Se formará regularmente al personal interviniente en la prestación del servicio en aquellas materias que requieran para el desempeño de sus funciones, en cuanto al servicio prestado.

Con carácter general, la empresa adjudicataria aplicará las medidas de seguridad correspondientes a un sistema de información de categoría MEDIA, según lo establecido en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Asimismo, deberá cumplir con las obligaciones exigidas para los prestadores de servicios por las entidades públicas.

Con carácter general, el intercambio de información confidencial se realizará de acuerdo a lo establecido en la normativa de clasificación de la información de Lantik S.A. M.P. La empresa adjudicataria deberá atender las peticiones y requisitos que pudiera realizar el personal de Lantik S.A. M.P. para dicho intercambio.

5.8.9 Subcontratación

En caso de exista una cadena de subcontratación para la prestación del producto o servicio, la empresa adjudicataria deberá disponer de una documentación que detalle claramente los elementos que forman parte de la cadena de subcontratación, así como las implicaciones derivadas de cualquier cambio o modificación que pueda sufrir algún eslabón de dicha cadena, todo ello previo conocimiento y aceptación por Lantik S.A. M.P. Si el producto o servicio objeto de contrato está sujeto al cumplimiento del Esquema Nacional de Seguridad según lo estipulado en el punto “Evidencia de buenas prácticas de seguridad acreditada en una norma de referencia para la gestión de la seguridad de la información en el entorno de prestación”, la empresa adjudicataria deberá asegurar que los sistemas de información de las empresas subcontratadas son conformes con el Esquema Nacional de Seguridad en lo que respecta a los servicios que



afecten a Lantik S.A. M.P., por lo que el contenido del presente documento resultará asimismo de aplicación a la cadena de suministro de la empresa adjudicataria.

5.8.10 Coordinación en caso de incidentes y desastres

En caso de que la empresa adjudicataria tenga acceso a la información de Lantik S.A. M.P. o información que trate Lantik, S.A. M.P. o su actuación pueda afectar a los servicios de la entidad, debe atenerse a lo indicado en la presente cláusula en caso de que se produzca una incidencia de seguridad, entendiendo como tal, cualquier acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traduzca en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta.

La empresa adjudicataria deberá, a través de su Persona de Contacto, notificar al interlocutor de Lantik identificado en el pliego, tan pronto como sea consciente, de cualquier incidente de seguridad que pueda afectar a los activos de información y servicios y en general sistemas de información y comunicaciones de Lantik S.A. M.P.

La coordinación de las labores de resolución del incidente tendrá en cuenta los siguientes requerimientos:

- La coordinación la realizarán las personas responsables de Lantik S.A. M.P. y la Persona de Contacto designada en la empresa adjudicataria.
- La empresa adjudicataria estará obligada a seguir las indicaciones de la persona responsable de Lantik S.A. M.P. para la resolución de la incidencia.
- La persona responsable de Lantik S.A. M.P. podrá requerir la realización de determinadas acciones en un periodo concreto o el envío por parte de la empresa adjudicataria de una previsión de actuaciones a realizar, fecha y hora, riesgos asociados y, en su caso, medidas de seguridad.

Será obligatorio que la empresa adjudicataria disponga de un registro operativo de las incidencias de seguridad ocurridas en el marco del presente contrato, empleando, en su caso, la herramienta señalada por Lantik S.A. M.P. Las incidencias mantendrán un flujo con el comunicante, debiendo proceder a su cierre cuando se hubiera comunicado al mismo y no se considere ninguna acción adicional. Se incluirá necesariamente en el registro:

- Hora de inicio de incidencia y hora de finalización (incluyendo la hora en la que se produce la incidencia, la hora en la que se notifica y la hora de finalización de la resolución).
- Hora de comunicación de inicio y hora de comunicación de finalización.
- Tiempos de resolución.
- Conclusiones y mejora.

En este sentido se tendrán en cuenta los puntos requeridos por la normativa aplicable, para la identificación, gestión y registro de incidencias, que puedan afectar al servicio, incluyendo:



- Reglamento general de protección de datos.
- Guía CCN-STIC-817 Gestión de ciberincidentes.
- Guía nacional de notificación y gestión de ciberincidentes.

En caso de que la incidencia afecte a datos de carácter personal, será de aplicación lo establecido en el capítulo referente a protección de datos personales.

En cualquier caso, la resolución de un incidente de seguridad, especialmente cuando sea de peligrosidad alta o superior, requerirá la participación de la empresa adjudicataria de los servicios afectados para evaluar el impacto de la incidencia y adoptar las medidas necesarias de contención, mitigación, respuesta y recuperación.

Estas actividades, por su especialización, podrán requerir el concurso de su CSIRT de referencia, en este caso el CCN-CERT del Centro Criptológico Nacional especialmente cuando el incidente hubiere afectado a sistemas que traten información de naturaleza administrativa o datos de los ciudadanos administrados. Dicha respuesta deberá gozar por tanto de las preceptivas medidas de seguridad y confidencialidad de la actuación administrativa que exige el art. 3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y que obliga a que tal conocimiento solo pueda extenderse a un organismo de las administraciones públicas, como el Centro Criptológico Nacional.

5.8.11 Regulación de la finalización del contrato: transferencia de tecnología

Durante la ejecución del contrato, la empresa adjudicataria se compromete a facilitar a las personas designadas por Lantik S.A. M.P. toda la información y documentación que estas soliciten para disponer de un total conocimiento técnico de las circunstancias en las que se desarrollan los servicios, sus actividades y, en general, de todas las operaciones técnicas, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizadas para resolverlos.

Una vez finalizado el contrato, la empresa adjudicataria deberá desarrollar las acciones precisas para la transferencia del conocimiento y de la información, implicados en el servicio. Asimismo, la empresa adjudicataria debe realizar, en el plazo máximo de un (1) mes:

- a. Devolver a Lantik S.A. M.P. la información confidencial y, si procede, los soportes donde conste, una vez cumplida la prestación. La devolución debe comportar el borrado total y seguro de la información confidencial existente en los equipos informáticos utilizados por la empresa adjudicataria.

No obstante, Lantik S.A. M.P. podrá requerir a la empresa adjudicataria para que en vez de la opción a), cumpla con la b) o con la c) siguientes:

- b. Devolver a la empresa que designe por escrito Lantik S.A. M.P., la información confidencial y, si procede, los soportes donde conste, una vez cumplida prestación. La devolución debe comportar el borrado total y seguro de la información confidencial existente en los equipos informáticos utilizados por la empresa adjudicataria.



- c. Destruir de manera segura los datos, una vez cumplida la prestación.

La empresa adjudicataria deberá certificar la destrucción final de los datos de manera segura por escrito, entregando el certificado correspondiente a Lantik S.A. M.P.

En caso de imposibilidad de cumplimiento del plazo establecido, la empresa adjudicataria realizará un requerimiento de prórroga debidamente justificado a Lantik S.A. M.P. quien, en su caso, podrá conceder o rechazarlo.

Cuando sea necesario, para el proceso de restitución y transferencia tecnológica la empresa adjudicataria presentará una planificación detallada, contemplando los medios que serán empleados, las acciones de contingencia diseñadas y los riesgos que pudieran presentarse en el proceso. Cuando sea necesario, y especialmente cuando existiera una nueva entidad adjudicataria, se incluirá el periodo de transición destinado a la gestión organizada del proceso de transferencia y restitución.

Esta cláusula será obligatoria cuando la finalización del servicio fuera anticipada, siendo responsabilidad de la entidad adjudicataria saliente, una transferencia y restitución ordenada.

5.8.12 Normativa

De conformidad con la Disposición adicional 25ª de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, los contratos que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD), y la normativa complementaria. Para el caso de que la contratación implique el acceso de la empresa adjudicataria a datos de carácter personal de cuyo tratamiento sea responsable Lantik S.A. M.P., aquella tendrá la consideración de encargada del tratamiento. En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 28 del RGPD. En todo caso, las previsiones de este deberán de constar por escrito.

5.8.13 Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a la empresa adjudicataria que resulte encargada del tratamiento, de ahora en adelante entidad encargada de tratamiento, para tratar por cuenta de Lantik S.A. M.P., como entidad encargada de tratamiento de los datos cuyo responsable de tratamiento es la Diputación Foral de Bizkaia los datos de carácter personal necesarios para prestar el servicio detallado en el apartado "Objeto".

El tratamiento consistirá en: durante la vigencia de contrato pudiera ser necesario el tratamiento de datos de carácter personal para prestar el servicio detallado en el apartado "Objeto". En este caso, la empresa licitadora deberá notificar a Lantik S.A. M.P. el tipo de tratamiento a realizar y deberá contar con su aprobación.



La entidad encargada de tratamiento tratará los datos personales únicamente siguiendo instrucciones documentadas de la entidad responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique a la encargada. En tal caso, la entidad encargada informará a la responsable de tratamiento de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público. La entidad responsable también podrá dar instrucciones ulteriores en cualquier momento del período de tratamiento de los datos personales. Dichas instrucciones deberán estar siempre documentadas.

La entidad encargada de tratamiento informará inmediatamente a la responsable si las instrucciones dadas por esta infringen, a juicio de la encargada, el Reglamento (UE) 2016/679, el Reglamento (UE) 2018/1725 o las disposiciones aplicables del Derecho de la Unión o de los Estados miembros en materia de protección de datos.

5.8.14 Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este contrato, Lantik S.A., M.P. como entidad encargada de tratamiento de los datos cuya responsable de tratamiento es la Diputación Foral de Bizkaia o sus empresas forales pone a disposición de la entidad encargada de tratamiento, la información que se describe a continuación (detallando categoría de personas interesadas y datos personales del tratamiento a los que se puede acceder):

- Categoría de personas interesadas: Empresas, personas emprendedoras, personal trabajador del sector público Foral.
- Categoría de datos personales:
 - Identificativos y de contacto
 - Circunstancias sociales y personales
 - Bancarios y económico patrimoniales
 - Académicos y profesionales
 - Detalles del empleo
 - Contactos institucionales
 - Datos comerciales
 - Datos de transacciones de bienes y servicios
 - Categorías especiales de datos
 - Datos de violencia de género
 - Relativos a condenas e infracciones penales
 - Relativos a infracciones administrativas
 - Otros datos personales: potencialmente cualquier tipología que pudiera ser tratada por motivo del servicio de manera excepcional.

Si el tratamiento afecta a datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales («datos sensibles»), la entidad encargada de tratamiento aplicará restricciones específicas y/o garantías adicionales.



En caso de que como consecuencia de la ejecución del contrato resultara necesario en algún momento la modificación de lo aquí estipulado, la empresa adjudicataria lo requerirá razonadamente y señalará los cambios que solicita. En caso de que Lantik S.A. M.P. estuviese de acuerdo con lo solicitado, Lantik S.A. M.P. emitiría un Anexo, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

5.8.15 Duración

Tendrá la duración indicada en el apartado "Plazo de entrega" y "Prórroga", si procede, del Pliego de Prescripciones Técnicas.

Una vez finalice el contrato, la empresa adjudicataria deberá realizar la devolución o destrucción de los datos personales según lo estipulado en la cláusula "Regulación de la finalización del contrato: transferencia de tecnología", considerando que la referencia a información confidencial incluye en este caso los datos de carácter personal.

En su caso, la entidad encargada de tratamiento podrá conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación. Para ello, deberá notificar con antelación a Lantik S.A. M.P. las causas que justifican esta actuación.

5.8.16 Obligaciones de la entidad encargada de tratamiento

La entidad encargada de tratamiento y el personal de su organización se obliga a:

- a) La empresa adjudicataria se obliga a respetar todas las obligaciones que pudieran corresponderle como encargada del tratamiento con arreglo a las disposiciones de la normativa actual nacional y de la Unión Europea de protección de datos y, concretamente a lo dispuesto en:
 - o Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD).
 - o Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD).
- b) Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este contrato. En ningún caso podrá utilizar los datos para fines propios.
- c) Tratar los datos de acuerdo con las instrucciones de Lantik S.A. M.P.
- d) Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de la empresa responsable, que contenga:
 - o Nombre y los datos de contacto de la entidad encargada de tratamiento y de cada empresa responsable por cuenta de la cual actúe la entidad encargada de tratamiento y, en su caso, de la persona delegada de protección de datos.
 - o Categorías de tratamientos efectuados por cuenta de la empresa responsable.
 - o Una descripción de las medidas técnicas y organizativas de seguridad, en caso de que proceda su aplicación, relativas a:
 - Seudonimización y el cifrado de datos personales.
 - La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.



- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
 - El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
- e) No comunicar los datos a terceras personas u organizaciones, salvo que cuente con la autorización expresa de la empresa responsable del tratamiento. La autorización requiere identificar de forma previa y por escrito, la entidad a la que se pueden o deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación. En el caso de transferencias de datos a un tercer país o a una organización internacional por requerimientos jurídicos inequívocos y fundamentados, se informará a la empresa responsable de la exigencia de manera previa y específica.
- f) Presentar, antes de la formalización del contrato, una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos, así como comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en dicha declaración.
- g) Entidades subencargadas

Se prohíbe subcontratar las prestaciones que formen parte del objeto del contrato.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito a Lantik S.A. M.P., con una antelación de 15 días, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la entidad subcontratista y sus datos de contacto. En caso de que sea intención de la entidad encargada de tratamiento subcontratar los servidores o los servicios asociados a los mismos, deberá indicar expresamente este hecho, así como el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de las empresas subcontratistas a las que se vaya a encomendar su realización. La subcontratación podrá llevarse a cabo si Lantik S.A. M.P. no manifiesta su oposición en el plazo establecido.

La empresa subcontratista, que también tendrá la condición de entidad encargada de tratamiento, está obligada igualmente a cumplir las obligaciones establecidas en el contrato y las instrucciones que dicte Lantik S.A. M.P. Corresponde a la entidad encargada de tratamiento regular la relación jurídica con la empresa subencargada mediante un instrumento jurídico que refleje las mismas condiciones, medidas de seguridad aplicables e instrucciones del contrato.

De acuerdo con el art. 28.4 del RGPD:

“Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo



plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.”

- h) Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente contrato, incluso después de que finalice su objeto.
- i) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes. Manteniendo a disposición de Lantik S.A. M.P. la documentación acreditativa del cumplimiento de dicha obligación.
- j) Garantizar la formación necesaria en materia de protección de datos personales del personal de la entidad encargada de tratamiento autorizada a tratar datos personales.
- k) Asistir a Lantik S.A. M.P. en la respuesta al ejercicio de los derechos de acceso, rectificación, supresión y oposición; limitación del tratamiento; a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles). En caso de que la entidad encargada de tratamiento reciba alguna petición de ejercicio de derechos correspondiente a tratamientos de datos de Lantik S.A. M.P., deberá comunicarla en un plazo máximo de 48 horas a Lantik S.A. M.P.
- l) Corresponde a Lantik S.A. M.P. facilitar el derecho de información a las personas interesadas, de tal modo que la entidad encargada de tratamiento se abstendrá de aportar sus propios modelos de información, recurriendo en todo caso a aquellos aportados por Lantik S.A. M.P. o solicitándolos en caso de que se precisen incluir en cualquier medio o canal de recogida de datos.
- m) Notificación de violaciones de la seguridad de los datos personales tratados por la entidad encargada de tratamiento:

En caso de violación de seguridad de los datos personales tratados por la entidad encargada de tratamiento, esta lo notificará a Lantik S.A. M.P., sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, a través de correo electrónico a la persona responsable de ejecución y/o supervisión del objeto del contrato. Informará de las violaciones de la seguridad de los datos personales de las que tenga conocimiento, así como toda la información relevante para la documentación y comunicación de la incidencia. Dicha información contendrá al menos:

- o Una descripción de la naturaleza de la violación de la seguridad (inclusive, cuando sea posible, las categorías y el número aproximado de personas interesadas y de registros de datos afectados);
- o Los datos de un punto de contacto en el que pueda obtenerse más información sobre la violación de la seguridad de los datos personales;
- o Sus consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, incluyendo las medidas adoptadas para mitigar los posibles efectos negativos.

En la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

- n) Notificación de violaciones de la seguridad de los datos personales en relación con los datos tratados por Lantik S.A. M.P.

En caso de violación de seguridad de los datos personales en relación con los datos tratados por Lantik S.A. M.P., la entidad encargada de tratamiento ayudará a la responsable en lo siguiente:

- o Notificar la violación de la seguridad de los datos personales a las autoridades de control competentes sin dilación indebida una vez tenga constancia de ella, si procede (a menos



que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas).

- Recabar la información siguiente, que, de conformidad con el artículo 33, apartado 3, del Reglamento (UE) 2016/679 deberá figurar en la notificación de la entidad responsable, que debe incluir como mínimo:
 1. La naturaleza de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de personas interesadas afectadas, y las categorías y el número aproximado de registros de datos personales afectados;
 2. Las consecuencias probables de la violación de la seguridad de los datos personales;
 3. Las medidas adoptadas o propuestas por la entidad responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

- Cumplir, con arreglo al artículo 34 del Reglamento (UE) 2016/679, la obligación de comunicar sin dilación indebida a las personas interesadas la violación de la seguridad de los datos personales cuando sea probable que la violación de la seguridad entrañe un alto riesgo para los derechos y libertades de las personas físicas.
- o) Dar apoyo a Lantik S.A. M.P. en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
- p) Dar apoyo a Lantik S.A. M.P. en la realización de las consultas previas a la autoridad de control, cuando proceda.
- q) Dar apoyo a Lantik S.A. M.P. en el cumplimiento de las obligaciones de esta última.
- r) Poner a disposición de Lantik S.A. M.P. toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen Lantik S.A. M.P. u otra empresa auditora autorizada por ella.
- s) Adoptar todas las medidas de índole técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo tal y como dispone el artículo 32 del RGPD. De esta forma, la empresa adjudicataria aplica todas y cada una de las medidas de seguridad que resultan de aplicación a los tratamientos de datos personales, tras un análisis de los riesgos que conlleva el tratamiento de los datos personales, implantando las medidas de dispuestas en el catálogo de medidas de seguridad aplicables del Esquema Nacional de Seguridad.
- t) Si una entidad encargada de tratamiento infringe lo establecido al determinar los fines y medios del tratamiento, adquiere la condición de responsable del tratamiento con respecto a dicho tratamiento (Art. 28.10 del RGPD).
- u) La entidad encargada de tratamiento estará obligada a someterse en todo caso a la normativa nacional y de la Unión Europea en materia de protección de datos (incluyendo, sin limitación, el RGPD y la LOPDGD).
- v) Transferencias internacionales:
 - Las transferencias de datos a un tercer país o a una organización internacional por parte de la entidad encargada solo podrán realizarse siguiendo instrucciones documentadas de la entidad responsable o en virtud de una exigencia expresa del Derecho de la Unión o



del Estado miembro al que esté sujeto la encargada; se llevarán a cabo de conformidad con el capítulo V del Reglamento (UE) 2016/679 o del Reglamento (UE) 2018/1725.

- La entidad responsable se aviene a que, cuando la encargada recurra a una subencargada de conformidad con lo establecido en el presente para llevar a cabo actividades de tratamiento específicas (por cuenta de la responsable) y dichas actividades conlleven una transferencia de datos personales en el sentido del capítulo V del Reglamento (UE) 2016/679, la entidad encargada y la subencargada puedan garantizar el cumplimiento del capítulo V del Reglamento (UE) 2016/679 utilizando cláusulas contractuales tipo adoptadas por la Comisión, con arreglo al artículo 46, apartado 2, del Reglamento (UE) 2016/679, siempre que se cumplan las condiciones para la utilización de dichas cláusulas contractuales tipo.

5.8.17 Obligaciones de la entidad responsable del tratamiento

Corresponde a Lantik S.A. M.P.:

- a) Entregar a la entidad encargada de tratamiento los datos a los que se refiere la cláusula "Identificación de la información afectada" de este documento.
- b) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte de la entidad encargada de tratamiento.
- c) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.
- d) Realizar, en su caso, una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por la entidad encargada de tratamiento.
- e) Realizar las consultas previas que corresponda.

5.8.18 Evidencia de cumplimiento de la normativa de Protección de Datos

La empresa adjudicataria deberá disponer de evidencias que demuestren su cumplimiento de la normativa de protección de Datos Personales y del deber de responsabilidad activa, como, a título de ejemplo, certificados previos sobre el grado de cumplimiento o resultados de auditorías, que habrá de poner a disposición de Lantik S.A. M.P. a requerimiento de ésta.

Asimismo, a instancia de Lantik S.A. M.P., la entidad encargada de tratamiento permitirá y contribuirá a la realización de auditorías de las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Al decidir si se realiza un examen o una auditoría, Lantik S.A. M.P. podrá tener en cuenta las certificaciones pertinentes que obren en poder de la entidad encargada de tratamiento.

Lantik S.A. M.P. podrá optar por realizar la auditoría por sí misma o autorizar a un auditor independiente. Las auditorías también podrán consistir en inspecciones de los locales o instalaciones físicas de la entidad encargada de tratamiento y, cuando proceda, realizarse con un preaviso razonable.

Las partes pondrán a disposición de las autoridades de control competentes, a instancia de estas, la información a que se refiere la presente cláusula y, en particular, los resultados de las auditorías.



5.8.19 Responsabilidad y causas de resolución del contrato

La empresa adjudicataria que incumpla lo establecido en los apartados anteriores será considerada responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido, así como de cualquier reclamación que por las personas interesadas se interponga ante la Agencia de Protección de Datos competente y de la indemnización que, en su caso, se reconozca a la persona afectada que ejercite la acción de responsabilidad por el daño o lesión que sufra en sus bienes o derechos.

El incumplimiento de la normativa sobre protección de datos de carácter personal será motivo de resolución del contrato.

5.8.20 Normativa de securización de entornos para prestación de servicio remoto

Se deberá conocer y dar compromiso de cumplimiento por parte de la empresa adjudicataria del servicio la norma NCS-1/3 relativa a la “Normativa de securización de entornos para prestación de servicio remoto”.

5.8.21 Informe periódico del cumplimiento de la “Normativa de securización de entornos para prestación de servicio remoto”

La empresa adjudicataria del servicio deberá remitir a requerimiento de Lantik S.A. M.P., información sobre el nivel de cumplimiento de lo establecido en la Normativa de securización de entornos para prestación de servicio remoto; para ello deberá cumplimentar el Formato cuestionario normativa securización de entornos que le será entregado, por la persona responsable del servicio o proyecto por parte de Lantik S.A. M.P. y que está disponible en el Plan de Calidad.

5.8.22 Monitorización de las conexiones remotas

Lantik S.A. M.P. monitorizará las conexiones remotas a sus sistemas de información. La empresa adjudicataria notificará este hecho a su personal, de modo que sean informados de que sus actuaciones pueden ser auditadas en caso necesario por Lantik S.A. M.P. para la comprobación del cumplimiento del conjunto de medidas de seguridad especificados en el presente documento y demás normativa referenciada.

5.8.23 Instalación de herramientas de seguridad

Lantik se reserva el derecho a la instalación de herramientas de seguridad y monitorización, en los equipos propiedad de la entidad adjudicataria que vayan a conectarse al dominio Bizkaia.

5.8.24 Evidencias de las buenas prácticas relativas al objetivo de control 11 “Seguridad Física y del entorno” de la norma de referencia ISO/IEC 27002 en el entorno de prestación

La empresa adjudicataria del servicio deberá evidenciar a requerimiento del Dpto. de Seguridad de Lantik S.A. M.P., el grado de cumplimiento de las buenas prácticas de seguridad física establecidas en el dominio 11 “Seguridad Física y del entorno” de la norma de referencia ISO27002; así como informar de los incidentes no graves ocurridos en el periodo. Los incidentes graves deberán ser notificados al Dpto. de Seguridad de Lantik S.A. M.P. a la mayor brevedad.



5.8.25 Teletrabajo

En aquellos supuestos en los que el servicio se preste en modalidad de teletrabajo o remota en un entorno no corporativo, la empresa adjudicataria del servicio objeto del presente pliego deberá garantizar el mismo nivel de seguridad, garantizando el uso de medidas de seguridad. Para tal fin, deberá observar las recomendaciones establecidas en “Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo” de la Agencia Española de Protección de Datos y el informe “CCN-CERT BP/18 Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia” del Centro Criptológico Nacional.

En este sentido, la empresa adjudicataria deberá como mínimo utilizar las siguientes medidas de seguridad y/o medidas análogas, tales como:

- El personal de la empresa adjudicataria no podrá descargar a sus equipos en conexión remota información confidencial ni datos de carácter personal de los que Lantik S.A. M.P. sea responsable ni imprimir dicha información, salvo que tenga autorización expresa por parte de Lantik S.A. M.P. Tomará todas las precauciones necesarias para evitar acceso por personal no autorizado (familiares, compañeras/os, etc.) a su dispositivo y, por tanto, a la información almacenada.
- La empresa adjudicataria deberá disponer de una política o normativa de seguridad que incluya consejos y recomendaciones a su personal relativos a situaciones de teletrabajo o acceso remoto para mantener la seguridad de la información. Esta documentación deberá ser conocida por todas las personas que participen como resultado de la adjudicación.
- Si el equipamiento (portátil, móvil, tablet) empleado para la conexión remota a los sistemas de información de Lantik S.A. M.P. no es proporcionado por esta, la empresa adjudicataria se asegurará de que dicho equipamiento cumple los requerimientos de seguridad generales especificados en el presente documento y en la normativa referenciada. En particular, el equipamiento deberá incluir como mínimo las siguientes medidas de seguridad:
 - Software antimalware y protección mediante firewall activados y actualizados.
 - Tendrá instaladas exclusivamente las aplicaciones software que sean necesarias para que el personal desarrolle sus funciones. Estas aplicaciones deberán ser aprobadas por la propia entidad y descargadas de repositorios fiables.
 - El sistema operativo y las aplicaciones software deberán estar actualizados.
 - Cifrado de disco duro (algoritmo AES, con longitud de clave mínima de 128 bits) en caso de que Lantik S.A. M.P. hubiera autorizado al personal de la empresa adjudicataria a descargarse a su dispositivo información sensible o datos personales.
 - Conexión remota a los sistemas de información de Lantik S.A. M.P. exclusivamente a través de las herramientas autorizadas por Lantik S.A. M.P. referenciadas con anterioridad.
 - No tendrá elementos externos conectados, como memorias USB, lectores CD/DVD, etc.

El personal no podrá almacenar credenciales de acceso en claro en los dispositivos que emplee para el acceso remoto a los sistemas de información de Lantik S.A. M.P. En caso de que el almacenamiento de credenciales sea necesario, empleará un contenedor cifrado o herramienta de gestión de contraseñas que soporte algoritmo de encriptación simétrica AES con una longitud de clave mínima de 128 bits.



5.8.26 Certificación de inexistencia de vulnerabilidades de seguridad

La empresa adjudicataria se comprometerá en la firma del contrato a mantener actualizada y libre de vulnerabilidades de seguridad la infraestructura TI de su propiedad empleada durante la prestación del servicio.

5.8.27 Conformidad con el Esquema Nacional de Seguridad (ENS)

De conformidad con el ENS, todo sistema que suministre un servicio en la nube a organismos del sector público deberá cumplir las medidas de seguridad definidas en las guías CCN-STIC que le sean de aplicación.

Cuando el contrato contemple, total o parcialmente, el uso de sistemas cloud on-premise, la empresa adjudicataria deberá cumplir lo establecido en la Guía CCN-STIC-858 Implantación de sistemas SaaS en modo local (on-premise). De este modo, deberá aportar los siguientes documentos:

- Guía de instalación (dirigida a administradores).
- Guía de uso seguro (dirigida a usuarios).
- Guía de relación entre empresa proveedora y Lantik S.A M.P.

El servicio en la nube debe contar con una certificación de seguridad reconocida por el ENECSTI.

En caso de que exista un Perfil de Cumplimiento Específico aprobado por el CCN para el servicio proporcionado, Lantik S.A. M.P. podrá acogerse a este, siendo entonces de aplicación la declaración de aplicabilidad asociada a este perfil en concreto.

5.8.28 Declaración de ubicación

Tal y como se establece en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, considerando la naturaleza del servicio, la empresa adjudicataria deberá facilitar la identificación de la ubicación de los sistemas de información vinculados con los servicios objeto del contrato, incluyendo todas las ubicaciones asociadas al almacenamiento y prestación del servicio, contemplando todas las actividades implicadas, tales como recogida, almacenamiento, procesamiento y gestión.

Es necesario que la empresa adjudicataria identifique a todas las entidades subcontratadas que participarán en la ejecución de los servicios objeto del contrato, durante la vigencia del mismo, debiendo identificar la ubicación y los servicios concretos prestados por cada una de ellas. La subcontratación quedará en todo caso sometida a las disposiciones contenidas en la normativa de protección de datos, sin excepción.

Se considerarán, a todos los efectos, las limitaciones establecidas en la normativa de protección de datos relativas a transferencias internacionales de datos, siendo condición esencial el cumplimiento de tales previsiones, que se extenderán a las entidades subcontratadas. Esta obligación se considera esencial al contrato y se mantendrá durante toda la vigencia del mismo.



Cualquier modificación a lo largo del contrato relativa a las exigencias establecidas en el presente apartado, deberá ser comunicada sin dilación, a Lantik S.A. M.P.

5.8.29 Transferencia Internacional de Datos Personales

No podrán realizarse transferencias a un tercer país u organización internacional fuera de la Unión Europea, salvo en los supuestos específicamente autorizados por el Reglamento (UE) 2016/679 General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), siendo la única excepción contemplada, la transferencia a países, organizaciones o territorios que hayan sido declarados con un nivel adecuado de protección por parte de las autoridades de control en materia de protección de datos, o cuando sea precisa la transferencia en cumplimiento de una obligación legal, convenio internacional o requerimiento judicial.

La entidad adjudicataria deberá comunicar sin dilación indebida, cualquier cambio en relación a las condiciones para la transferencia de datos personales, especialmente la pérdida de la condición de “nivel adecuado de protección” para transferencia internacional, conforme al RGPD. Se considera expresamente incluidos los supuestos en los que la Comisión determine la pérdida de adecuación de un país, organización, entidad o empresa, incluidas aquellas que dejen de estar adheridas a eventuales acuerdos internacionales que permitan transferencias internacionales de datos.

5.8.30 Servicio asociado a la verificación electrónica de la identidad y tratamiento de datos de los tipos descritos en el artículo 46bis de la Ley 40/2015

Considerando lo dispuesto en la Ley 39/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y en el caso de que el servicio licitado por Lantik S.A. M.P. incluya un sistema de identificación mediante clave concertada a los efectos de lo descrito el artículo 9.2c) de la precitada ley, será necesario que la empresa adjudicataria incluya o facilite la identificación de la ubicación y prestación del servicio, así como los recursos técnicos que vayan a ser asignados para la recogida, almacenamiento, tratamiento y gestión, los cuales solo podrán estar ubicados en el territorio de la Unión Europea, según lo dispuesto en el artículo 122.2c) de la ley 9/2017, de 8 de noviembre de Contratos del Sector Público. Cuando estuvieran implicadas categorías especiales de datos, según lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), la ubicación se circunscribirá al territorio nacional.

Asimismo, considerando lo dispuesto en el artículo 46 bis de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y en los casos en que el servicio licitado por Lantik S.A. M.P. afectara a datos relativos al censo electoral, padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de las persona usuarias del Sistema Nacional de Salud, será necesario que la entidad adjudicataria comunique a Lantik S.A. M.P. la ubicación y prestación del servicio, que solo podrá prestarse dentro del territorio de la Unión Europea.

A todos los efectos, cuando el servicio licitado permitiera la subcontratación, esta quedará sometida en idénticos términos a lo descrito. Por ello, será necesario declarar expresamente la localización de los servicios o recursos concernientes a los procesos subcontratados. Cuando



existieran varios subcontratados, será necesario declararlo de cada uno de ellos, de manera individualizada.

Cuando el contrato ya hubiera sido adjudicado, y existiera una modificación que afectara a la ubicación o prestación del servicio, incluyendo cambios en la subcontratación, deberán ser comunicados sin demora, a Lantik S.A. M.P. identificando claramente los cambios producidos, quedando esta facultada para resolver el contrato.

La empresa adjudicataria será a todos los efectos responsable directo de los incumplimientos derivados de tal subcontratación y de las obligaciones declaradas.

5.8.31 Gestión de copias de seguridad y restauración de datos

La empresa adjudicataria deberá disponer de los mecanismos necesarios para implementar una política de respaldo y de pruebas de recuperación que contemplen como mínimo los siguientes requisitos:

- Identificación del alcance de los respaldos.
- Política de copias de seguridad.
- Medidas de cifrado de información en respaldo.
- Procedimiento de solicitud de restauraciones de respaldo.
- Realización de pruebas de restauración.
- Traslado de copias de seguridad (si aplica).

5.8.32 Medidas de continuidad del servicio o proyecto

La empresa licitadora deberá disponer de un Plan de Continuidad para el servicio que garantice que se cumplan los Acuerdos de Nivel de Servicio especificados en el pliego técnico. Este plan se activará ante la indisponibilidad total o parcial de los recursos principales, que por cualquier motivo provoque la indisponibilidad de los servicios objeto del contrato e incluirá:

- La identificación y descripción de los medios alternativos planificados para la provisión de los servicios, personal alternativo, existencia o planificación de instalaciones y medios de comunicación alternativos, etc.
- Realización de, al menos, una prueba de recuperación anual.
- Actualización de la documentación del plan de recuperación ante desastres tanto como sea necesario.

Bajo requerimiento de Lantik S.A. M.P. la empresa licitadora deberá presentar:

- Evidencias de disponer de un Plan de Continuidad para el servicio (p.ej. Certificaciones, compromiso de la empresa proveedora...).
- Informe final de pruebas anuales del Plan de Continuidad, así como un plan de trabajo con acciones correctivas si se detectaran eventos o acciones a corregir.



5.8.33 Registros de actividad

La empresa adjudicataria dispondrá de los registros de actividad de las personas usuarias que permiten monitorizar, analizar, investigar y documentar acciones indebidas o no autorizadas, tanto a nivel operativo como de administración.

La empresa adjudicataria será responsable de:

- Realizar la configuración necesaria para llevar a cabo el registro de las actividades de las personas usuarias.
- Definir y establecer las medidas de seguridad necesarias para la protección de los registros.
- Mantener los registros durante un periodo no inferior a dos (2) años.

En caso de que así lo requiera Lantik S.A. M.P., la empresa adjudicataria pondrá a disposición de esta los registros de actividad correspondientes a las personas usuarias cuyo acceso al sistema cloud esté incluido en el ámbito del contrato.

5.8.34 Claves criptográficas

En caso de conservar claves criptográficas en su infraestructura, la empresa adjudicataria pondrá en conocimiento de Lantik S.A. M.P. las medidas implementadas para proteger las claves criptográficas durante todo su ciclo de vida.

El servicio deberá disponer de mecanismos de cifra que permitan que la información del usuario esté protegida, en tránsito y en reposo, para que no pueda ser leída o modificada en caso de acceso ilegítimo. Los mecanismos criptográficos deberán cumplir con lo especificado en la guía CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad.

El proveedor deberá cumplir uno de los siguientes casos:

- Ser capaz de garantizar el funcionamiento de los mecanismos de cifra sin que las claves sean almacenadas en la nube. Estas estarán en disposición de Lantik S.A. M.P. quien es la persona encargada de su gestión y almacenamiento.
- Almacenar las claves del cifrado en módulos de seguridad de hardware denominados dispositivos HSM (Hardware Security Modules), no accesibles por terceros. Dichos dispositivos deberán estar cualificados por el Centro Criptológico Nacional (CCN) e incluidos en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, o en su defecto, dispongan de una declaración de seguridad que cumpla los requisitos definidos en la Guía de Seguridad CCN-STIC 140.

5.8.35 Transparencia e información

La empresa adjudicataria proporcionará a Lantik S.A. M.P. información relativa a:

- Herramientas de seguridad de que dispone, incluyendo aquellas destinadas a la monitorización, análisis, recuperación y notificación de incidentes de seguridad.



- Tipo de virtualización utilizada y nivel y mecanismos de segregación de los datos o aplicaciones de Lantik S.A. M.P. alojadas en la nube.
- Mecanismos y procedimientos de borrado seguro de la información almacenada por la empresa adjudicataria, que serán utilizados en el momento de terminación del vínculo contractual.
- Bajo petición de Lantik S.A. M.P., características del hardware contratado: tamaño de disco, memoria RAM, tipo de procesador, CPU o transferencia de datos. La empresa adjudicataria asegurará la existencia de servicios que permitan monitorizar el uso de estas capacidades por parte de Lantik S.A. M.P.
- Ubicación geográfica de sus datos (incluidos backups y almacenamiento de logs), antes y durante el suministro del servicio.
- El acceso y análisis de logs, registros de acceso y cualquier otra información que pudiera ser solicitada por parte de Lantik S.A. M.P. para garantizar el cumplimiento de sus obligaciones legales. En caso de incidente de seguridad, toda la información requerida (configuración, logs, etc...) de los equipos físicos, dispositivos de red, servicios compartidos y dispositivos de seguridad debe ser entregada a Lantik S.A. M.P.

5.8.36 Resolución del Contrato

El incumplimiento por parte de la empresa adjudicataria de cualesquiera de las presentes disposiciones podrá ser motivo de resolución del contrato de manera unilateral.

5.8.37 Fuero

Ambas partes se someten, con renuncia a su fuero propio si lo tuvieran, a los Juzgados y Tribunales de Bilbao para la interpretación de cualquier cuestión litigiosa que se derive de este contrato.



Para cualquier aclaración o ampliación de información se deben dirigir a:

Lantik S.A. M.P.

Sabino Arana, 44 – 48013 Bilbao

Teléfono: 944068900

ppt.sc.lantik@bizkaia.eus

Sin./Fdo.: JOSE JAVIER GARCIA MARIN - 2025-01-24
KONPONBIDEAK/BEZEROA 150 TALDEA - HAINBAT SAIL
EQUIPO DE SOLUCIONES/CLIENTE 150-VARIOS DPTOS.

Sin./Fdo.: JOSE IGNACIO HERNANDEZ GARCIA - 2025-01-24
IKUSPEGI TEKNOLOGIKOKO ARLOA
VISIÓN TECNOLÓGICA

Sin./Fdo.: IBAI CONDE GURREA - 2025-01-24
ARRETAKO ETA NEGOZIOAREN DIGITALIZAZIOKO ARLOA
ÁREA DE ATENCIÓN Y DIGITALIZACIÓN DEL NEGOCIO

Sin./Fdo.: MARTIN BERASATEGUI MEJIAS - 2025-01-24
ARKITEKTURA TEKNOLOGIKOKO ARLOA
ÁREA DE ARQUITECTURA TECNOLÓGICA

Sin./Fdo.: IRATXE GUILLERNA CAMPO - 2025-01-24
DIGITALIZAZIO-UNITATEKO ETA DATA ZUZENDARITZA
DIRECCIÓN UNIDAD DE DIGITALIZACIÓN Y DATA

Sin./Fdo.: IMANOL SAUTO AVELLANAL - 2025-01-24
SEGURTASUN ETA TEKNOLOGIA UNITATEKO ZUZENDARITZA
DIRECCIÓN DE UNIDAD DE SEGURIDAD Y TECNOLOGÍA



6 ANEXO A

TABLA 1: Importes mensuales

Item	Fabricante	Suscripción	Importe máximo unitario mensual (sin IVA)
1	MICROSOFT	CFQ7TTC0LH34-0001 BUSINESS CENTRAL ESSENTIAL	66,00 €
2	MICROSOFT	CFQ7TTC0HD3R-0001 DATABASE CAPACITY 1 GB	10,00 €
3	MICROSOFT	CFQ7TTC0HD3R-0002 DATABASE CAPACITY 100 GB	468,00 €
4	MICROSOFT	CFQ7TTC0HD3R-0003 DATABASE CAPACITY OVERAGE 1 GB	5,00 €
5	MICROSOFT	CFQ7TTC0J4GS-0002 Power Apps per app plan (1 app or website)	5,00 €
6	MICROSOFT	CFQ7TTC0LH2H-0002 POWER APPS PREMIUM	19,00 €
7	MICROSOFT	CFQ7TTC0LH15-0001 Power Platform Requests add-on	47,00 €
8	MICROSOFT	CFQ7TTC0LSGZ-0001 Power Automate Premium	14,00 €
9	MICROSOFT	CFQ7TTC0MFT9-0001 Power Automate Process	141,00 €
10	MICROSOFT	CFQ7TTC0HD7P-0001 INSTANCIA BUSINESS CENTRAL (ENVIRONMENT)	281,00 €
11	MICROSOFT	CFQ7TTC0LHRL-0002 Dataverse Database Capacity add-on	38,00 €
12	MICROSOFT	CFQ7TTC0LHQ3-0001 Dataverse File Capacity add-on	1,90 €
13	MICROSOFT	CFQ7TTC0HBSL-0001 Dataverse Log Capacity add-on	9,50 €
14	MICROSOFT [1]	Nivel Premium, EP1: Núcleos: 1, 3.5 GB de RAM, 250 GB de almacenamiento, 1 instancias activadas previamente, 1 unidades más de escalado horizontal	290,00 €
15	MICROSOFT [1]	Nivel Premium, Pago por uso, EP2: Núcleos: 2, 7 GB de RAM, 250 GB de almacenamiento, 1 instancias activadas previamente, 1 unidades más de escalado horizontal	575,00 €



16	MICROSOFT [1]	Nivel Premium, Pago por uso, EP3 : Núcleos: 4, 14 GB de RAM, 250 GB de almacenamiento, 1 instancias activadas previamente, 1 unidades más de escalado horizontal	1.145,00 €
17	SALESFORCE	SALES CLOUD ENTERPRISE EDITION	165,00 €
18	SALESFORCE	SERVICE CLOUD ENTERPRISE EDITION	165,00 €
19	SALESFORCE	MARKETING CLOUD ENGAGEMENT CORPORATE MARKETING CLOUD ENGAGEMENT - SUPER MESSAGES-Excluding SMS/MMS (1000) MARKETING CLOUD ENGAGEMENT - Additional contacts Corporate Edition (1000)	4.700,00 €
20	SALESFORCE	COMMUNITY CLOUD(ANTES EXPERIENCE CLOUD)	10,00 € Login (24 horas) 25,00 € MEMBER
Importe TOTAL (suma de todas las licencias mensuales)			Σ = 8.180,40€

[1] Las suscripciones de Azure Functions deberán desplegarse en la región de Europa con menos latencia a la región donde se despliegue Business Central.

TABLA 2: Importes anuales

Item	Fabricante	Suscripción	Importe máximo unitario anual (sin IVA)
21	SALESFORCE	MARKETING CLOUD ENGAGEMENT - SUPER MESSAGES (1000)	12,00 €
22	SALESFORCE	MARKETING CLOUD ENGAGEMENT - Additional contacts Corporate Edition	225,00 €
23	SALESFORCE	ALMACENAMIENTO DATA STORAGE 10 GB	12.690,00 €
24	SALESFORCE	ALMACENAMIENTO DATA STORAGE 500 MB	1.620,00 €
25	SALESFORCE	ALMACENAMIENTO DATA STORAGE 50 MB	324,00 €
26	SALESFORCE	ALMACENAMIENTO FILE STORAGE 10 GB	384,00 €
27	SALESFORCE	ALMACENAMIENTO FILE STORAGE 1 TB	3.780,00 €



28	SALESFORCE	Sandbox (Full Copy)	30% del coste del neto de suscripciones
29	SALESFORCE	SandBox Developer Pro	5% del coste del neto de suscripciones
Importe TOTAL (suma de todas las licencias anuales, sin filas 28 y 29)			$\Sigma = 19.035,00\text{€}$



7 ANEXO B

Don / Doña:

Con nº de D.N.I.:

En representación de la empresa:

Con el N.I.F.:

Solicita la entrega del documento detallado.

Y se compromete a:

Guardar secreto sobre la información contenida en el documento detallado, no ser compartida con terceros y ser utilizada únicamente para el desarrollo de la oferta.

Una vez cumplido este propósito, la información deberá ser destruida de manera inmediata.

La contravención de esta cláusula será motivo suficiente para tomar las acciones que legalmente correspondan.

Lugar, fecha y firma.

En, a de de

FIRMADO,

Firma





Sabino Arana, 44
48013 BILBAO (Bizkaia)

Tel: (+34) 944 068 900
Fax: (+34) 944 068 800

e-mail: lantik@bizkaia.eus
<http://lantik.bizkaia.eus>



ER-2023/2005
El Diseño, el Desarrollo y el Mantenimiento de Aplicaciones Informáticas.

ER-0739/2006
La Compra de Bienes y Servicios y el Suministro e Instalación de Equipamiento Informático para la Diputación Foral de Bizkaia.

ER-0811/2008
La Atención al Cliente.