PLIEGO DE PRESCRIPCIONES TÉCNICAS (PPT) QUE HAN DE REGIR EN LA CONTRATACIÓN DEL SERVICIO DE IMPLANTACIÓN Y MANTENIMIENTO DE UN SOFTWARE PARA LA GESTIÓN DE LOS ÓRGANOS DE GOBIERNO Y PARTICIPACIÓN DE MUTUA MONTAÑESA

INDICE

1. OBJETO DEL CONTRATO

El objeto del contrato lo constituye la prestación a MUTUA MONTAÑESA del servicio de implantación y mantenimiento de un software para la gestión de los órganos de gobierno y participación de Mutua Montañesa, de la forma más eficiente posible.

2. ALCANCE

2.1. ESPECIFICACIONES TÉCNICAS

Multiplataforma: La solución debe ser multiplataforma, pudiendo ser utilizada por cualquier dispositivo con conexión a internet, con independencia del sistema operativo del terminal. Debe ser accesible desde cualquier navegador con acceso a internet independientemente del dispositivo utilizado (ordenador, smartphone, tableta..). Igualmente deberá de disponer de una app para dispositivos móviles tipo tableta con sistema operativo IOS, Windows 10 y Android, facilitando la utilización del servicio y que permite consultar la información más relevante incluso en ausencia de conexión a internet.

Desacoplamiento entre capas: Debe presentar una clara separación entre las diferentes capas en que se estructura, facilitando de este modo la evolución del sistema, así como la reutilización de componentes.

Modularización: La solución debe estar construida siguiendo criterios de modularidad, favoreciendo su mantenimiento y evolución.

Rendimiento: la solución debe ofrecer un elevado rendimiento. Para ello se utilizarán por ejemplo sistemas de indexación de información, motores de búsqueda, etc.

Cloud y escalabilidad del sistema: La solución incorporará los elementos software y la infraestructura (servidores y comunicaciones) necesarios para su funcionamiento. Debe ser una solución escalable y flexible, cuyo diseño podrá dar cobertura a las necesidades futuras de Mutua Montañesa, tanto respecto a la incorporación de nuevos usuarios como a su evolución conforme a los cambios que se produzcan en las áreas de negocio a las que la nueva aplicación dará soporte.

Auditabilidad y trazabilidad lóqica: El sistema debe ser auditable, pudiendo revisar el histórico de los accesos de usuarios, seguimiento de las convocatorias y accesos a documentos.
Se valorará que la traza auditable pueda ser directamente explotada a través del propio interfaz de la aplicación (por ejemplo, mediante generadores de informes), ofreciendo de este modo una fuente de información de gran interés para los responsables de la gestión de los órganos de gobierno.

Complemento Móvil: No sólo debe permitir su utilización desde cualquier dispositivo con conexión a internet mediante un navegador web, sino que debe permitir además la utilización de un complemento aplicativo móvil disponible en las plataformas Android (google Play) e iOS (app Store).

Mantenimiento: En el caso de que por cualquier otro motivo fuera necesario llevar a cabo actuaciones de contingencia o mantenimiento por parte de la empresa adjudicataria, éstas se llevarán a cabo con autorización expresa de Mutua Montañesa y dentro del horario laboral de la empresa, salvo que bajo un acuerdo específico para la ocasión se decida actuar de modo diferente.

2.2. ESPECIFICACIONES FUNCIONALES

Gestión de Usuarios con mantenimiento de perfiles. Sistema de creación/gestión de usuarios incluyendo la capacidad de asignar permisos de acceso a la información y a la funcionalidad de la herramienta basado en el perfil del usuario y su pertenencia a cada uno de los órganos de gobierno/equipos de trabajo. Mantenimiento de estos perfiles y permisos que se puedan realizar de forma autónoma por parte de los administradores del sistema desde el propio interface software, es decir, sin necesidad de conocimientos técnicos particulares.

Creación de un repositorio unificado de documentación para los miembros de los órganos de Gobierno y participación de MM. La herramienta permitirá la Gestión de la Documentación: Publicar documento, Borrar documento, Crear versiones, Realizar consultas, Modificar ubicación y/o visibilidad, añadir comentarios, Crear secuencias de aprobación previas a la publicación, Generar marcas de agua.

Herramientas de Coordinación y Seguimiento de cada órgano, incluso con **integración en las agendas electrónicas** personales de sus miembros más estandarizadas del mercado, y **accesos desde distintos dispositivos móviles** (móvil y Tabletas con Android, IOS y Windows 10), así como Gestión de flujos de aprobación, comentarios y votación de documentos y/o puntos del orden del día: Organización de Reuniones y Tareas: Convocatorias, Recordatorios, Orden del día,
Comentarios sobre reuniones, Contenido de reuniones en Tareas, Asistencias, Votaciones, Documentación asociada, Mantenimiento de Tareas sus Estados.

Guardar registro de toda la actividad realizada en la plataforma por usuarios, administradores o técnicos. Independientemente del perfil del usuario, conservar registro histórico y auditable de toda la actividad realizada, permitiendo así en todo momento trazabilidad de cualquier acción realizada o documento gestionado desde la plataforma.

Planificación y gestión de reuniones, envío automático de convocatorias a los miembros de cada órgano, capacidad de registro de la respuestas a la convocatoria; disponibilidad de recordatorios automáticos para confirmaciones y seguimiento de las convocatorias. Integración de avisos vía correo electrónico que incorporen eventos compatibles con las agendas electrónicas habituales (Outlook, Google Calendar, etc). Capacidad de registro de asistencia a la reunión. Confección de Actas Proforma y soporte de la delegación de la representación incorporada en la herramienta.

La herramienta se instalará sobre la infraestructura Cloud y se hospedará en la plataforma cloud o servidores de la empresa adjudicataria sin coste adicional para Mutua Montañesa, permitiendo su acceso en modo offline. Se incluirá la opción de instalación en los servidores de Mutua Montañesa.

2.3. ESPECIFICACIONES DE SEGURIDAD

La herramienta debe permitir mantener **trazabilidad** de la acciones realizadas por cada usuario. Entre otras, mantener registro en formato log de acciones como el acceso a la información de la aplicación, donde se recoge la identificación del usuario, el tipo de acceso, la fecha y hora de acceso, si el acceso ha sido autorizado o denegado y la información accedida.

Ofrecerá opciones de **personalización de la política de contraseñas** tales como longitud, combinación de caracteres, caducidad o histórico de claves

Deberá contar con **mecanismos para limitar o impedir la descarga de la información** consultada a través de la misma, de cara a evitar salidas de datos no autorizadas, mediante una opción seleccionable de forma individual para cada documento, aportando de este modo gran flexibilidad en la gestión de permisos de acceso y uso de la documentación.

Las comunicaciones para el acceso a la información se deben realizar a través de conexiones seguras https, con **protocolo seguro TLS** v1.2 (HTTPS) o posterior. El proveedor deberá incluir en el coste del proyecto la obtención, gestión y mantenimiento del certificado de seguridad que sea necesario para la protección del servicio.

Deberá permitir trabajar con los **formatos de archivos electrónicos** más habituales, incluidos multimedia (pdf, csv, xlsx, doc, docx, html, bmp, tiff, jpeg, etc.) y con archivos de gran tamaño (hasta 300 MB).

Gestión de Usarios. Se podrá determinar los **permisos de acceso en base a perfiles de usuario** que accederán a las funcionalidades (consulta, gestión) y a las entidades y órganos en función de su perfil, permitiendo a MM a definir el perfil de cada usuario con acceso a los espacios de trabajo determinados.

El proveedor dispondrá de certificaciones que acrediten la solvencia de los procedimientos y procesos internos en la gestión de la información, se precisará la certificación en la norma **ISO 27001** y el **Esquema Nacional de Seguridad** de grado Medio.

2.4. SERVICIO DE USO DEL PRODUCTO

El adjudicatario garantizará los derechos de uso de la licencia correspondiente durante el periodo contratado, garantizando su uso por un total de 10 órganos de gobierno o comités y 50 usuarios; y que el servicio cumple las especificaciones funcionales detalladas en el punto anterior y a tal efecto, la instalación dispondrá del Manual funcional para el usuario, subido en la aplicación y disponible en todo momento a los usuarios.

2.5. SERVICIO DE SOPORTE TÉCNICO

Al arranque del servicio, se realizarán las tareas de parametrización y personalización de los órganos de gobierno y participación incluidos, así como del resto del sistema si fuese necesario, y este plan de **implantación** será acordado con los responsables funcionales y técnicos de Mutua Montañesa.

Incluirá la **infraestructura técnica** de servidores y comunicaciones necesaria para la prestación del servicio en toda la funcionalidad indicada en la especificaciones del PTT. Asímismo el servicio contará con la monitorización activa de disponibilidad y las copias de seguridad necesarias para su operativa.

Incluirá el **mantenimiento** correctivo de la aplicación, en particular la instalación del software de la Aplicación para la corrección de errores y mal funcionamiento. Las

actualizaciones de la herramienta o mantenimientos se llevarán a cabo durante periodos acordados con Mutua Montañesa que minimicen el impacto a los usuarios finales. Igualmente durante toda la vigencia del contrato Mutua Montañesa podrá disfrutar, sin coste, de todas las funcionalidades que aporten las nuevas versiones del producto.

Incluirá la **migración** de datos existentes para la gestión de los órganos en la herramienta disponible actualmente, de esta forma se garantiza el acceso de los usuarios al histórico y contexto de las iniciativas previas que puedan ser necesarias para el seguimiento actual.

2.6. SERVICIO DE ATENCIÓN A USUARIOS

Se ofrecerá un **servicio Atención a Usuarios** que permitirá que cualquier usuario tenga acceso a un equipo de expertos en la utilización de la aplicación que responderá a cualquier duda o incidencia que pueda encontrarse. Este servicio de soporte especializado del servicio deberá:

- Estar disponible tanto a través de correo electrónico como de línea telefónica. Los números de teléfono deberán ser números de tarificación local o nacional. No se aceptarán números de teléfono de soporte internacionales y/o de tarificación especial.

- Atender en español.

- Estar disponible durante el horario laboral: lunes a viernes de 9:00 a 19:00.

Igualmente, se designará a un interlocutor único, que realizará las siguientes tareas:

- Organizar, dirigir, representar y coordinar el equipo de trabajo que preste los servicios de configuración, parametrización, puesta en marcha y formación, asi como asegurar el nivel de calidad de dichos servicios

- Proporcionar a Mutua Montañesa la información periódica necesaria para el seguimiento de la implantación de la solución.

- Participará en todas las reuniones a las que sea convocado por Mutua Montañesa, con una antelación mínima de 72 horas naturales.

2.7. ACUERDOS DE NIVEL DE SERVICIO

Las incidencias correctivas o de soporte se clasificarán en función de la gravedad, y se exigirá un nivel de servicio mínimo en cuanto a tiempo de respuesta y tiempo de resolución tal y como se muestra en la siguiente tabla, en base a las siguientes consideraciones:

- **Tiempo de respuesta**: Tiempo transcurrido desde que se comunica la avería al Servicio de Mantenimiento, hasta que dicho servicio se pone en contacto con el/la usuario/a o cliente.

- **Tiempo de resolución**: Tiempo transcurrido desde el instante en el que se ha notificado por el/la cliente un aviso de avería, hasta el momento en que el elemento del servicio, o servicios, se ha restablecido a su normal funcionamiento

Asimismo, esta tabla de acuerdos de nivel de servicio se ajusta teniendo en cuenta la importancia de una incidencia, valorando si el fallo o incidencia impide la utilización de una funcionalidad, si esta puede ser suplida por otra vía o si el fallo se produce en una funcionalidad no crítica. A continuación se detalle el nivel de la incidencia y como se define.

- **Tipo de incidencia 1 (Crítica)**: Fallo en el sistema impidiendo la ejecución de funcionalidad clave sin que el sistema permita un camino alternativo para el desarrollo de la misma funcionalidad.

- **Tipo de incidencia 2 (Alta)**: Fallo en el sistema impidiendo la ejecución de funcionalidad clave aunque el sistema permite un camino alternativo para el desarrollo de la misma funcionalidad o fallo en el sistema impidiendo la ejecución de funcionalidad no clave pero que afecta a un elevado número de usuarios/as.

- **Tipo de incidencia 3 (Media)**: Fallo en el sistema impidiendo la ejecución de funcionalidad no clave y que no afecta a un elevado número de usuarios/as.

- **Tipo de incidencia 4 (Baja)**: Solicitud de información sobre el uso y la configuración del sistema, asociada al soporte.

A continuación se detallan los tiempos de respuesta y resolución, para garantizar el servicio (horas laborables).

INCIDENCIA	TIEMPO DE RESPUESTA	TIEMPO DE RESOLUCIÓN
Tipo 1	2 horas	8 horas
Tipo 2	6 horas	48 horas
Tipo 3	8 horas	Compromiso de involucrarse para resolver la incidencia en el menor tiempo posible
Tipo 4	8 horas	Compromiso de involucrarse para resolver la incidencia en el menor tiempo posible

2.8. DEVOLUCIÓN DEL SERVICIO

La empresa adjudicataria estará obligada a devolver el servicio tanto por la finalización del mismo como ante una eventual cancelación del mismo. El objeto de este proyecto sería recuperar la información propiedad de Mutua Montañesa contenida en la base de datos de la aplicación, así como en el repositorio documental, quedando sin acceso tras la finalización de la implantación, salvo por autorización expresa de Mutua Montañesa. Igualmente, la Empresa adjudicataria deberá facilitar la migración de información para que pueda ser explotada sin utilizar su producto.

2.9. APLICABILIDAD ENS

La aplicación solicitada esta identificada dentro del sistema de categorización de Mutua Montañesa como nivel Medio dentro del ENS

ID	Servicio / Información	Disponibilidad	Autenticidad	Integridad	Confidencialidad	Trazabilidad	Responsable
IN_01_02	Información coordinación de órganos de gobierno y Comunicación institucional	BAJO	MEDIO	MEDIO	MEDIO	BAJO	Director Gerente

Por lo tanto y dada la naturaliza del sistema que se requiere, el proveedor deberá garantizar de manera fehaciente y objetiva el cumplimiento de, al menos, las siguientes medidas de seguridad. Mutua Montañesa se reserva el derecho de poder llevar a cabo en cualquier momento verificaciones respecto del cumplimiento de las mismas **(ver cuadro a continuación)**

Codigo ENS	Título	Baja	Media
[op.acc.1]	Identificación	1. Se podrán utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación. 2. Cuando el usuario tenga diferentes roles frente al sistema (por ejemplo, como ciudadano, como trabajador interno del organismo y como administrador de los sistemas) recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad. 3. Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular de tal forma que: a. Se puede saber quién recibe y qué derechos de acceso recibe. b. Se puede saber quién ha hecho algo y qué ha hecho. 4. Las cuentas de usuario se gestionarán de la siguiente forma: a. Cada cuenta estará asociada a un identificador único. b. Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario. c. Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará periodo de retención.	
[op.acc.2]	Requisitos de acceso	Los requisitos de acceso se atenderán a lo que a continuación se indica: a) Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. b) Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema. c) Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.	
[op.acc.3]	Segregación de funciones y tareas		El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita. En concreto, se separarán al menos las siguientes funciones: a) Desarrollo de operación. b) Configuración y mantenimiento del sistema de operación. c) Auditoría o supervisión de cualquier otra función
[op.acc.4]	Proceso de gestión de derechos de acceso	Los derechos de acceso de cada usuario, se limitarán atendiendo a los siguientes principios: a) Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar una entidad, de forma accidental o intencionada. b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones. c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.	
[op.acc.5]	Mecanismo de autenticación	Antes de proporcionar las credenciales de autenticación a los usuarios, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se contemplan varias posibilidades de registro de los usuarios: – Mediante la presentación física del usuario y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello. – De forma telemática, mediante DNI electrónico o un certificado electrónico cualificado. – De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los contemplados en la normativa de aplicación. a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor. b) En el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma. c) Se atenderá a la seguridad de las credenciales de forma que: 1. Las credenciales se activarán una vez estén bajo el control efectivo del usuario. 2. Las credenciales estarán bajo el control exclusivo del usuario. 3. El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida. 4. Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede. 5. Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.	a) Se exigirá el uso de al menos dos factores de autenticación. b) En el caso de utilización de "algo que se sabe" como factor de autenticación, se establecerán exigencias rigurosas de calidad y renovación. c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo: 1. Presencial. 2. Telemático usando certificado electrónico cualificado. 3. Telemático mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

[op.acc.7]	Acceso remoto (remote login)	Se garantizará la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implicará proteger tanto el acceso en sí mismo (como [op.acc.6]) como el canal de acceso remoto (como en [mp.com.2] y [mp.com.3]).	
[op.exp.2]	Configuración de seguridad	Se configurarán los equipos previamente a su entrada en operación, de forma que: a) Se retiren cuentas y contraseñas estándar. b) Se aplicará la regla de "mínima funcionalidad": 1. El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad, 2. No proporcionará funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible. 3. Se eliminará o desactivará mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue. c) Se aplicará la regla de "seguridad por defecto": 1. Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo. 2. Para reducir la seguridad, el usuario tiene que realizar acciones conscientes. 3. El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.	
[op.exp.3]	Gestión de la configuración		Se gestionará de forma continua la configuración de los componentes del sistema de forma que: a) Se mantenga en todo momento la regla de "funcionalidad mínima? ([op.exp.2]). b) Se mantenga en todo momento la regla de "seguridad por defecto? ([op.exp.2]). c) El sistema se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]). d) El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]). e) El sistema reaccione a incidentes (ver [op.exp.7]).
[op.exp.5]	Gestión de cambios		Se mantendrá un control continuo de cambios realizados en el sistema, de forma que: a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no. b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban. c) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. d) Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación.
[op.exp.7]	Gestión de incidentes		Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo: a) Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación. b) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso. c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente. d) Procedimientos para informar a las partes interesadas, internas y externas. e) Procedimientos para: 1. Prevenir que se repita el incidente. 2. Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente. 3. Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes. La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto.
[op.exp.8]	Registro de la actividad de los usuarios	Se registrarán las actividades de los usuarios en el sistema, de forma que: a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información. b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema. c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados. d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema	

[op.exp.9]	Registro de la gestión de incidentes		Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que: a) Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente. b) Se registrará aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado. c) Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.
[op.exp.11]	Protección de claves criptográficas	Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final. a) Los medios de generación estarán aislados de los medios de explotación. b) Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.	a) Se usarán programas evaluados o dispositivos criptográficos certificados conforme a lo establecido en [op.pl.5]. b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
[op.mon.1]	Detección de intrusión		Se dispondrán de herramientas de detección o de prevención de intrusión.
[op.mon.2]	Sistema de métricas	Se recopilarán los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35.	Además, se recopilarán datos para valorar el sistema de gestión de incidentes, permitiendo conocer – Número de incidentes de seguridad tratados. – Tiempo empleado para cerrar el 50% de los incidentes. – Tiempo empleado para cerrar el 90% de los incidentes.
[mp.com.2]	Protección de la confidencialidad	a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad. b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.	a) Se emplearán, preferentemente, dispositivos hardware en el establecimiento y utilización de la red privada virtual. b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5].
[mp.com.3]	Protección de la autenticidad y de la integridad	a) Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna (ver [op.acc.5]). b) Se prevendrán ataques activos, garantizando que al menos serán detectados. y se activarán los procedimientos previstos de tratamiento del incidente Se considerarán ataques activos: 1. La alteración de la información en transito 2. La inyección de información espuria 3. El secuestro de la sesión por una tercera parte c) Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación.	a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad. b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional. c) Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación. En caso de uso de claves concertadas se aplicarán exigencias medias en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.
[mp.si.5]	Borrado y destrucción	La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos. a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su contenido.	b) Se destruirán de forma segura los soportes, en los siguientes casos: 1. Cuando la naturaleza del soporte no permita un borrado seguro. 2. Cuando así lo requiera el procedimiento asociado al tipo de la información contenida,. c) Se emplearán productos certificados conforme a lo establecido en [op.pl.5].
[mp.sw.1]	Desarrollo		a) El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción. b) Se aplicará una metodología de desarrollo reconocida que: 1. Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida. 2. Trate específicamente los datos usados en pruebas. 3. Permita la inspección del código fuente. 4. Incluya normas de programación segura. c) Los siguientes elementos serán parte integral del diseño del sistema: 1. Los mecanismos de identificación y autenticación. 2. Los mecanismos de protección de la información tratada. 3. La generación y tratamiento de pistas de auditoría. d) Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.
[mp.s.8]	Protección frente a la denegación de servicio		Se establecerán medidas preventivas y reactivas frente a ataques de denegación de servicio (DOS Denial of Service). Para ello: a) Se planificará y dotará al sistema de capacidad suficiente para atender a la carga prevista con holgura. b) Se desplegarán tecnologías para prevenir los ataques conocidos.

3. DOCUMENTACION DE LOS TRABAJOS

El adjudicatario deberá presentar una programa de trabajo donde se especifiquen las tareas a realizar desde el inicio del proyecto hasta su puesta en marcha (incluyendo las tareas de formación), adjuntando un cronograma.

Las tareas de configuración, parametrización, puesta en marcha, migración y formación no deberán demorarse más de 6 semanas desde la fecha de inicio del contrato.

4. PRESUPUESTO BASE Y FACTURACION

- Licencia anual ..... 8.600,00 €

Para hasta 10 órganos de gobierno o comités internos y 45 usuarios. Incluye la gestión de la infraestructura y mantenimiento del software y soporte de usuarios.

- Puesta en marcha: Implementación, parametrización y formación. .. 1.950,00 €

- Migración..... 1.950,00 €

Los pagos se realizarán siempre mediante transferencia bancaria, siendo obligatoria la factura electrónica registradas a través del portal FACE (Registro de entrada de Facturas) de la Seguridad Social.

La facturación será anual, dentro de los 30 días siguientes a la firma del contrato o renovación anual de la licencia cuando corresponda.