



**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE REGIRÁ LA ADJUDICACIÓN
MEDIANTE PROCEDIMIENTO ABIERTO SUJETO A REGULACION ARMONIZADA PARA
LA CONTRATACIÓN DEL SERVICIO DE AUTOMATIZACIÓN DE PROCESOS MEDIANTE
EL USO DE TECNOLOGÍA DE ROBOTIZACIÓN EN MUTUA MONTAÑESA**

Indice

1. Introducción	4
1.1. Antecedentes	4
1.2. Objeto del contrato	4
2. Alcance.....	5
2.1. Servicio de infraestructura	5
2.2. Software de robotización	6
2.3. Servicios desarrollo.....	6
2.4. Mantenimiento procesos.....	6
2.5. Incorporación nuevos procesos robotizables	7
2.6. Seguimiento procesos	7
2.7. Integración piloto a la nueva plataforma	7
3. Requerimientos técnicos.....	8
4. Especificaciones de Seguridad de la información	9
4.1. Especificaciones de Seguridad de la información	9
4.2. Incidentes de seguridad	30
4.3. Seguridad y confidencialidad	31
4.4. Auditoria de calidad y seguridad.....	31
5. Condiciones ejecución del contrato	33
5.1. Duración y plan del contrato.....	33
5.2. Estimación económica	33
5.3. Volumetrias y estimación prevista.....	34
5.4. Condiciones de ejecución del servicio	35
5.5. Planning y fases servicio.....	35
5.5.1. Identificación de procesos y análisis de viabilidad	36
5.5.2. Desarrollo del proceso robotizable	37
5.6. Equipo de trabajo.....	38
6. Seguimiento ejecución servicio.....	41
6.1. Seguimiento Proyecto	41
6.2. Seguimiento servicio mantenimiento	42
6.2.1. Asistencia Técnica	42
6.2.2. Disponibilidad.....	42
6.2.3. Gestión de incidencias.....	42
6.2.4. Acuerdos nivel de servicio.....	43
6.2.5. Informes de control y seguimiento.....	45
6.2.6. Penalizaciones.....	46
6.2.7. Cese del Servicio.....	47



**Mutua
Montañesa**
Muy fácil

7. Anexo I – Listado Procesos Robotizables.....	48
8. Anexo II – Matriz Priorización.....	49

1. INTRODUCCIÓN

1.1. ANTECEDENTES

Mutua Montañesa se encuentra en un proceso de Transformación de su modelo de servicio hacia un modelo más digital y centralizado en nuestros mutualistas y trabajadores protegidos, buscando ofrecer nuestros servicios de una forma fácil e inteligente (Smart). Hemos confeccionado una hoja de ruta de proyectos, focalizados en la aplicación de nuevas tecnologías que nos permitan estar más cerca de las personas, mejorando su bienestar y salud laboral, y todo ello de una forma sencilla y fácil. Dentro de esta hoja de ruta, se identificaron como palancas de transformación la utilización de tecnologías de robotización de procesos, en adelante RPA, como una pieza clave en la mejora de la eficiencia de nuestros procesos y en la gestión de los recursos personales en Mutua Montañesa, así mismo como un proceso de mejora continua y aseguramiento de la calidad de nuestros procesos.

Después de un proceso de análisis de los diferentes fabricantes de este tipo de software, concluimos que UiPath era el software elegido por los siguientes motivos:

- Compatibilidad con procesos en entornos en la nube
- Solución escalable y flexible que nos permitirá ir creciendo a medida que vamos implantando esta nueva tecnología.
- Seguridad y auditoria de grado empresarial, que incluye control de acceso y fiabilidad en la confidencialidad de la información.
- Agilidad en la gestión de excepciones

Esto nos llevó a contratar en 2019 un, Proyecto Piloto o Prueba de Concepto, que nos permitiese evaluar con mayor detalle y seguridad, la eficiencia de este tipo de procesos. Para este piloto se decidió automatizar la validación de los bloqueos en el pago directo a trabajadores. El resultado ha sido positivo en cuanto a su resultado, con un 85-90% de ejecución finalizada con éxito. También nos ha permitido reafirmarnos en la tecnología seleccionada y las capacidades de este producto para el mantenimiento y seguimiento de los procesos robotizados.

1.2. OBJETO DEL CONTRATO

El objeto del presente pliego es la contratación de los servicios profesionales necesarios para llevar a cabo la implementación y mantenimiento de un servicio o solución RPA bajo un modelo SaaS, desarrollado sobre tecnología UiPath. Por tanto, el servicio debe incluir:

- Infraestructura alojada en la empresa adjudicataria.
- Infraestructura de comunicaciones y seguridad entre Mutua Montañesa y la empresa adjudicataria
- Software requerido para la implantación de los procesos identificados dentro del Plan de robotización de Mutua Montañesa
- Servicios de desarrollo para implantar los procesos identificados
- Mantenimiento y revisión de los procesos
- Soporte evolutivo de los procesos
- Cualquier otro elemento necesario para la implantación de los procesos identificados dentro del Plan de robotización de Mutua Montañesa

2. ALCANCE

Como punto de partida, y con las enseñanzas aprendidas con el desarrollo de la prueba de concepto, se ha trabajado internamente en un listado de procesos robotizables, definido dentro del Anexo I – Listado procesos robotizables.

El alcance de este proyecto se centra en la robotización de este listado de procesos ya evaluados (5), y otros todavía no identificados que se incorporarán a medida que se finalice la Fase I de Identificación y análisis de viabilidad, llegando hasta un máximo de 10 procesos robotizables durante la ejecución del contrato.

Dentro de la prueba de concepto se realizó una pequeña consultoría para valorar la viabilidad de robotizar ciertos procesos, clasificándolos como procesos sencillos, medios y complejos, teniendo en cuenta las aplicaciones impactadas, las reglas de negocio, la estabilidad de los sistemas y el formato de los datos. Esta clasificación se reevaluará al inicio del proyecto entre la empresa adjudicataria y Mutua Montañesa, ajustando y acordando conjuntamente su valoración.

Adicionalmente, al inicio del proyecto se evaluará el índice de robotización de cada proceso atendiendo a una matriz de priorización definida en el Anexo II.

A continuación, definiremos más detalladamente los servicios que formarán parte del alcance del proyecto.

2.1. SERVICIO DE INFRAESTRUCTURA

La plataforma o solución deberá estar alojada en una nube privada y segura y será operada por el adjudicatario del servicio. El proveedor garantizará en su extremo la “estanchidad” de la solución de robotización dedicada a Mutua Montañesa de las soluciones que pueda dar a otros clientes en la misma nube privada, en lo que a comunicaciones y acceso a sistemas respecta. La plataforma RPA propuesta por el adjudicatario deberá ser compatible con los requerimientos técnicos de la plataforma de trabajo de Mutua Montañesa, basada en una infraestructura de Citrix XenApp para la ejecución de todas las aplicaciones core de negocio de la organización. En la medida de lo posible, el proveedor, para facilitar el proceso de identificación de pantallas y procesos instalará en su nube privada los clientes de software y configuraciones necesarias para el acceso a los sistemas corporativos de Mutua Montañesa, siendo el acceso a través de cliente Citrix el último recurso a emplear, aunque deberá estar contemplado e incluido en el alcance del proyecto.

En cuanto a las comunicaciones, el acceso del software RPA a las aplicaciones de Mutua Montañesa se realizará a través de una VPN Ipsec punto a punto entre los sistemas de seguridad del cloud privado de la empresa adjudicataria y la intranet de Mutua Montañesa donde se alojen las aplicaciones.

El adjudicatario asumirá los costes implicados en la configuración, adecuación, o cualquier otra necesidad técnica que el propio adjudicatario requiera, para la correcta instalación y/o comunicación con los sistemas de Mutua Montañesa.

La arquitectura a implantar para este servicio será responsabilidad de la empresa adjudicataria, y por tanto se incluye la completa administración y gestión de la infraestructura implicada en el servicio: seguridad, monitorización, parametrización, optimización y evolución de la infraestructura.

2.2. SOFTWARE DE ROBOTIZACIÓN

La empresa adjudicataria debe suministrar todas las licencias necesarias para el desarrollo de los procesos definidos en el Anexo I – Listado procesos robotizables, así como los procesos potenciales que serán implementados a lo largo de la ejecución del contrato, en una modalidad pago por uso.

Asimismo, la empresa adjudicataria deberá incorporar las nuevas versiones del producto UiPath que permitan una evolución del producto standard con el fin de garantizar una correcta evolución del producto. Todos estos trabajos correrán por cuenta del licitador.

Como punto de partida, y para la evaluación de tiempos y costes, vamos a definir como “robot” la capacidad máxima de ejecución en 24 horas, de uno o más procesos automatizados en modo secuencial, pudiendo ser atendidos o desatendidos. La tecnología UiPath permite la gestión de estos procesos desatendidos mediante colas de trabajos gestionados por un orquestador, capaz de ejecutar “n” procesos diferentes de modo secuencial hasta utilizar la capacidad máxima del robot.

Dentro del plan de implantación que debe presentar la empresa adjudicataria, se valorará la estrategia de implantación del orquestador para maximizar el tiempo de un robot, priorizando las colas de trabajo y utilizando los tiempos “disponibles” por el robot. Teniendo en cuenta esta estrategia será requerido el suministro de la licencia de orquestador, herramienta clave para la optimización del tiempo.

Se prevee que para la ejecución el servicio, se requiere un máximo de 2 hilos de ejecución dependiendo de la demanda de los procesos que se vayan robotizando. Para el cálculo del presupuesto base de licitación, se estima que en el segundo año de servicio se empleen 2 hilos de ejecución. La facturación de este servicio se realizará según el uso del hilo de ejecución, y se activará su pago en el mes que se ponga en marcha.

2.3. SERVICIOS DESARROLLO

Los servicios profesionales requeridos para implantar en la tecnología UiPath las reglas de negocio y programación necesaria para implantar los procesos robotizables, desde el análisis, diseño e implementación de los servicios, hasta su puesta en producción. Se entenderá que el desarrollo del proceso robotizable ha terminado cuando el proceso además de haberse puesto en producción se haya realizado un par de análisis de resultados o ejecuciones, con un éxito en la ejecución mayor del %75.

La entrega de los procesos conllevará obligatoriamente un año de garantía por parte del adjudicatario, el cual deberá solucionar, sin coste adicional para Mutua Montañesa todas las incidencias que aparezcan, siempre y cuando sean imputables al desarrollo realizado por el adjudicatario.

2.4. MANTENIMIENTO PROCESOS

Entendemos la necesidad de un servicio de mantenimiento de los procesos robotizables en relación al seguimiento de la actividad, posibles incidencias correctivas o errores, los cuales no quedaron cubiertos por la garantía de la solución. Este servicio de mantenimiento debe cubrir los ajustes, pequeñas modificaciones o cambios solicitados por Mutua Montañesa, como consecuencia de la evolución de los procesos internos o por ajuste del propio proceso

robotizable, una vez que se va obteniendo resultados de las ejecuciones del proceso robotizable.

Este mantenimiento se activará a partir de la validación del proceso robotizable, tal y como se establece en el punto 2.3 Servicios de Desarrollo. Una vez validado por Mutua Montañesa, se pasará a la fase de mantenimiento evolutivo y garantía. Es a partir de ese momento cuando se incorporará el coste de mantenimiento de cada proceso, al coste de mantenimiento global.

2.5. INCORPORACIÓN NUEVOS PROCESOS ROBOTIZABLES

Dentro del Plan de Robotización se requiere un proceso de análisis y continua revisión de nuevos procesos susceptibles de ser robotizados, como mínimo se realizará una revisión anual. Para ello anualmente, se realizará un análisis por parte de la empresa adjudicataria junto a los responsables de procesos de Mutua Montañesa para analizar y priorizar nuevas funcionalidades a robotizar. Como resultado de esto, se validará internamente y se incorporará al alcance d, o al Anexo I – Listado de procesos robotizables.

Se valorará la metodología de revisión de procesos de forma que sea ágil y nos permita incorporar, priorizar y anteponer ciertas necesidades que pueden surgir por parte de negocio.

Adicionalmente se valorará la posibilidad de incorporar al proceso de desarrollo de procesos robotizables algún cambio en la planificación anual realizada, por necesidades urgentes de Mutua Montañesa, derivadas por cambios normativos o por necesidades críticas de gestión de Mutua Montañesa. Se valorará la presentación de un plan de contingencia por parte de la empresa adjudicataria para cubrir estos imprevistos.

2.6. SEGUIMIENTO PROCESOS

Se requiere que con carácter trimestral se facilite un informe con el análisis de actividad de los procesos robotizados con los ratio de acierto y fallo, así como el análisis de los puntos de control a analizar y ajustar.

Se valorará la utilización de procesos de extracción masiva y automáticos que nos permita ser autónomos, ya que deberán validarlos o revisarlos personas de los diferentes equipos de Mutua Montañesa, no teniendo perfiles técnicos.

2.7. INTEGRACIÓN PILOTO A LA NUEVA PLATAFORMA

Dentro del alcance de este servicio, se requiere la migración de nuestro actual proceso robotizable en la validación de pago directo con el GISS realizado en tecnología UiPath, para que pueda seguir ejecutándose en la nueva plataforma.

Para ello la empresa proveedora de este servicio, trasladará la configuración y parametrizaciones realizadas en su plataforma para que de una forma sencilla pueda ser migrado a la nueva plataforma.

Todos los trabajos para poner en funcionamiento este proceso robotizable correrán a cuenta de la empresa adjudicataria de este servicio. A partir de la instalación del proceso, las cuotas de mantenimiento se pagarán asimilado a un proceso sencillo.

3. REQUERIMIENTOS TÉCNICOS

La plataforma RPA que se solicita deberá cumplir con los siguientes requisitos mínimos:

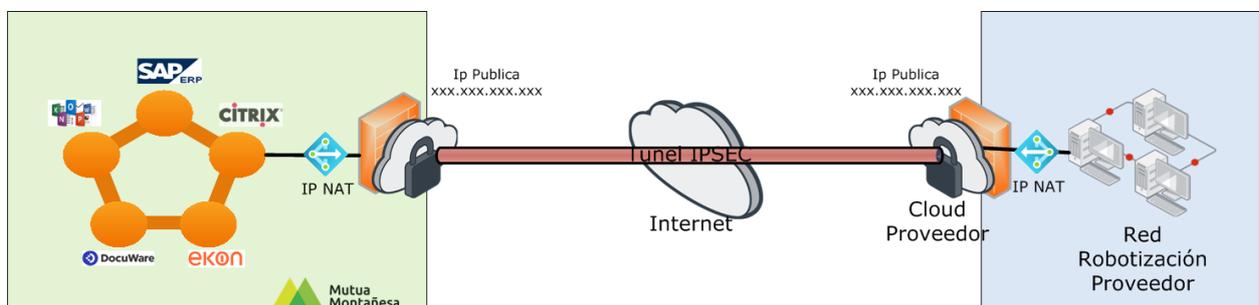
- Ser escalable a nuevos procesos y no verse afectados sus tiempos de respuesta y rendimiento.
- Tener capacidad de recuperación antes fallos o defectos (servicio de mantenimiento y soporte) que se puedan dar, manteniendo el grado de eficiencia y operatividad, confirmando la utilización de servidores de backup (sistema espejo)
- Garantizar la confidencialidad y seguridad de los datos almacenados.
- Incluir la infraestructura, la operación de ésta y las licencias que se necesiten para cubrir el alcance del proyecto a lo largo de toda la vigencia del contrato sin coste adicional para MUTUA MONTAÑESA.
- Deberá ser posible (sobre la misma tecnología RPA desplegada en el contrato) una futura migración a un modelo on-premise o hacia otro entorno cloud (fase de reversión) de forma no disruptiva para el servicio y con una mínima intervención potencial.

Los procesos desarrollados en la plataforma RPA deberán ser capaces de interactuar con las aplicaciones y sistemas de Mutua Montañesa.

Como ya se ha comentado en el apartado anterior, la plataforma de automatización de procesos se deberá proponer mediante una nube privada. Las empresas licitadoras podrán optar por generar esta nube privada mediante infraestructura en operadores de Hosting (manteniendo los requisitos de seguridad establecidos en la licitación), y para ello, se permitirá la subcontratación de esta parte del contrato, sin que repercuta en gastos extras para Mutua Montañesa.

El adjudicatario asumirá los costes implicados en la configuración, adecuación o cualquier otra necesidad técnica que el propio adjudicatario requiera, para la correcta instalación y/o comunicación con los sistemas/redes de Mutua Montañesa.

A continuación se muestra esquemáticamente, a modo de ejemplo, el modelo de explotación de la plataforma RPA para Mutua Montañesa propuesto en esta licitación:



El adjudicatario deberá configurar 2 entornos, para mantener la alineación con el sistema productivo y con el sistema de integración de Mutua Montañesa.

- El entorno productivo, se conectará al entorno productivo de Mutua Montañesa, y es donde se ejecutarán las tareas y procesos.
- El entorno de desarrollo, se conectará al entorno de calidad (TEST) de Mutua Montañesa, tal y como hacemos con aplicaciones no core de negocio. En este entorno se realizará el desarrollo y pruebas.

4. ESPECIFICACIONES DE SEGURIDAD DE LA INFORMACIÓN

El adjudicatario deberá cumplir la normativa legal aplicable en materia de seguridad de la información en el marco de los servicios prestados, específicamente, con el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y las guías de apoyo elaboradas por el CCN en este sentido.

La conformidad con lo dispuesto en el ENS se alcanza satisfaciendo los mandatos contenidos en su texto articulado y mediante la adecuada implantación de las medidas de seguridad contempladas en el Anexo II del citado Real Decreto 3/2010, para la siguiente categorización del sistema objeto del contrato:

- Nivel de Disponibilidad: Bajo
- Nivel de Integridad: Medio
- Nivel de Confidencialidad: Bajo
- Nivel de Autenticidad: Medio
- Nivel de Trazabilidad: Bajo

El adjudicatario del servicio se obliga a facilitar a Mutua Montañesa la correspondiente Declaración de Conformidad para el tratamiento de sistemas de información de categoría BÁSICA, y la correspondiente Certificación de Conformidad para el caso de sistemas de categoría MEDIA o ALTA, exigidas en la Guía de Seguridad CCN-STIC-809, con el objetivo de garantizar el compromiso de la entidad en cuestión con la seguridad de los sistemas, respecto de la información que trata o los servicios que presta. No obstante, el adjudicatario del servicio deberá permitir de forma adicional el acceso por parte de Mutua Montañesa el informe de auditoría emitido, con el objetivo de verificar las posibles deficiencias del sistema.

En caso de sistemas de categoría MEDIA o ALTA, el adjudicatario del servicio deberá contar con una Certificación de Conformidad expedida por una Entidad Acreditada por la ENAC.

El adjudicatario del servicio notificará a Mutua Montañesa, con carácter urgente, la existencia de cualquier incidente que conociera en el desarrollo de las tareas y que pudieran afectar a la seguridad de los Sistemas de Información de Mutua Montañesa.

Mutua Montañesa podrá exigir las responsabilidades oportunas al adjudicatario del servicio en caso de que surjan o se verifiquen deficiencias relativas a las obligaciones contenidas en esta cláusula. Para valorar el impacto de las deficiencias verificadas, se tendrán en cuenta conceptos como la gravedad de la deficiencia detectada, el carácter negligente o doloso de la misma o las consecuencias y perjuicios que se pudieran ocasionar en el desarrollo de la actividad de Mutua Montañesa, y de su relación con terceros.

4.1. ESPECIFICACIONES DE SEGURIDAD DE LA INFORMACIÓN

El adjudicatario deberá desarrollar en materia de seguridad todas las modificaciones requeridas que cumplan con la normativa en RGPD y 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
----	------------------------	----------------	--------------	------------	------------------	--------------

IN_02_30	Análisis de la información (Business Intelligence)	BAJO	MEDIO	BAJO	MEDIO	BAJO
----------	--	------	-------	------	-------	------

Por lo tanto y dada la naturaleza del sistema que se requiere, el adjudicatario 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 estas.

La siguiente tabla recoge las medidas que el proveedor deberá tener en cuenta durante el desarrollo del proyecto.

Código ENS	Título	BAJA	MEDIA
[op.acc]	Control de acceso		
[op.acc.1]	Identificación	<p>1. Se podrán utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación.</p> <p>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.</p> <p>3. Cada entidad (usuario o proceso) que accede al sistema, contará con un identificador singular de tal forma que:</p> <p>a) Se puede saber quién recibe y qué derechos de acceso recibe.</p> <p>b) Se puede saber quién ha hecho algo y qué ha hecho.</p> <p>4. Las cuentas de usuario se gestionarán de la siguiente forma:</p> <p>a) Cada cuenta estará asociada a un identificador único.</p> <p>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.</p> <p>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.</p>	

Codigo ENS	Título	BAJA	MEDIA
[op.acc.2]	Requisitos de acceso	<p>Los requisitos de acceso se atenderán a lo que a continuación se indica:</p> <p>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.</p> <p>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.</p> <p>c) Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.</p>	
[op.acc.3]	Segregación de funciones y tareas		<p>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.</p> <p>En concreto, se separarán al menos las siguientes funciones:</p> <p>a) Desarrollo de operación.</p> <p>b) Configuración y mantenimiento del sistema de operación.</p> <p>c) Auditoría o supervisión de cualquier otra función</p>

Codigo ENS	Título	BAJA	MEDIA
[op.acc.4]	Proceso de gestión de derechos de acceso	<p>Los derechos de acceso de cada usuario, se limitarán atendiendo a los siguientes principios:</p> <p>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.</p> <p>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.</p> <p>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.</p>	
[op.acc.5]	Mecanismo de autenticación	<p>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:</p> <ul style="list-style-type: none"> - 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. <p>a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.</p>	<p>a) Se exigirá el uso de al menos dos factores de autenticación.</p> <p>b) En el caso de utilización de "algo que se sabe" como factor de autenticación, se establecerán exigencias rigurosas de calidad y renovación.</p> <p>c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo:</p> <ol style="list-style-type: none"> 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

Codigo ENS	Título	BAJA	MEDIA
		<p>b) En el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma.</p> <p>c) Se atenderá a la seguridad de las credenciales de forma que:</p> <ol style="list-style-type: none"> 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. 	<p>cualificado en dispositivo cualificado de creación de firma.</p>
[op.acc.6]	Acceso local (local logon)	<ol style="list-style-type: none"> a) Se prevendrán ataques que puedan revelar información del sistema sin llegar a acceder al mismo. La información revelada a quien intenta acceder, debe ser la mínima imprescindible (los diálogos de acceso proporcionarán solamente la información indispensable). b) El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos. c) Se registrarán los accesos con éxito, y los fallidos. d) El sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso. 	<p>Se informará al usuario del último acceso efectuado con su identidad.</p>

Código ENS	Título	BAJA	MEDIA
[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]).	Se establecerá una política específica de lo que puede hacerse remotamente, requiriéndose autorización positiva.
[op.exp]	Explotación		
[op.exp.1]	Inventario de activos	Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo.	

Codigo ENS	Título	BAJA	MEDIA
[op.exp.2]	Configuración de seguridad	<p>Se configurarán los equipos previamente a su entrada en operación, de forma que:</p> <ul style="list-style-type: none"> a) Se retiren cuentas y contraseñas estándar. b) Se aplicará la regla de "mínima funcionalidad": <ul style="list-style-type: none"> 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": <ul style="list-style-type: none"> 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. 	



Codigo ENS	Título	BAJA	MEDIA
[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.4]	Mantenimiento	Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente: a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas. b) Se efectuará un seguimiento continuo de los anuncios de defectos. c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.	

Código ENS	Título	BAJA	MEDIA
[op.exp.5]	Gestión de cambios		<p>Se mantendrá un control continuo de cambios realizados en el sistema, de forma que:</p> <p>a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no.</p> <p>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.</p> <p>c) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.</p> <p>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.</p>
[op.exp.6]	Protección frente a código dañino	<p>Se considera código dañino: los virus, los gusanos, los troyanos, los programas espías, conocidos en terminología inglesa como "spyware?", y en general, todo lo conocido como "malware?".</p> <p>Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante.</p>	



**Mutua
Montañesa**

Muy fácil

Codigo ENS	Título	BAJA	MEDIA
[op.exp.7]	Gestión de incidentes		<p>Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo:</p> <ul style="list-style-type: none">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:<ul style="list-style-type: none">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. <p>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.</p>



Codigo ENS	Título	BAJA	MEDIA
[op.exp.8]	Registro de la actividad de los usuarios	<p>Se registrarán las actividades de los usuarios en el sistema, de forma que:</p> <ul style="list-style-type: none">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		<p>Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:</p> <ul style="list-style-type: none">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.

Código ENS	Título	BAJA	MEDIA
[op.exp.11]	Protección de claves criptográficas	<p>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.</p> <p>a) Los medios de generación estarán aislados de los medios de explotación.</p> <p>b) Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.</p>	<p>a) Se usarán programas evaluados o dispositivos criptográficos certificados conforme a lo establecido en [op.pl.5].</p> <p>b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.</p>
[op.ext]	Servicios externos		
[op.ext.2]	Gestión diaria		<p>Para la gestión diaria del sistema, se establecerán los siguientes puntos:</p> <p>a) Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).</p> <p>b) El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo.</p> <p>c) El mecanismo y los procedimientos de coordinación en caso de incidentes y desastres (ver [op.exp.7]).</p>
[op.mon]	Monitorización del sistema		
[op.mon.1]	Detección de intrusión		Se dispondrán de herramientas de detección o de prevención de intrusión.



**Mutua
Montañesa**
Muy fácil

Codigo ENS	Título	BAJA	MEDIA
[mp.per.1]	Caracterización del puesto de trabajo		<p>Cada puesto de trabajo se caracterizará de la siguiente forma:</p> <ul style="list-style-type: none">a) Se definirán las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad. La definición se basará en el análisis de riesgos.b) Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad.c) Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias.
[mp.eq]	Protección de los equipos		
[mp.eq.2]	Bloqueo de puesto de trabajo		<p>El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.</p>

Codigo ENS	Título	BAJA	MEDIA
[mp.eq.3]	Protección de equipos portátiles	<p>Los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.</p> <p>Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:</p> <p>a) Se llevará un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.</p> <p>b) Se establecerá un canal de comunicación para informar, al servicio de gestión de incidentes, de pérdidas o sustracciones.</p> <p>c) Cuando un equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de Internet y otras redes que no sean de confianza.</p> <p>d) Se evitará, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.</p>	

Código ENS	Título	BAJA	MEDIA
[mp.com]	Protección de las comunicaciones		
[mp.com.1]	Perímetro seguro	Se dispondrá un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos que sólo dejara transitar los flujos previamente autorizados	
[mp.com.2]	Protección de la confidencialidad		<p>a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.</p> <p>b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.</p>
[mp.com.3]	Protección de la autenticidad y de la integridad	<p>a) Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna (ver [op.acc.5]).</p> <p>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:</p> <ol style="list-style-type: none"> 1. La alteración de la información en tránsito 2. La inyección de información espuria 3. El secuestro de la sesión por una tercera parte <p>c) Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación.</p>	<p>a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.</p> <p>b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.</p> <p>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.</p>

Código ENS	Título	BAJA	MEDIA
[mp.si.5]	Borrado y destrucción	<p>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.</p> <p>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.</p>	<p>b) Se destruirán de forma segura los soportes, en los siguientes casos:</p> <ol style="list-style-type: none"> 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]	Protección de las aplicaciones informáticas		
[mp.sw.1]	Desarrollo		<p>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.</p> <p>b) Se aplicará una metodología de desarrollo reconocida que:</p> <ol style="list-style-type: none"> 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. <p>c) Los siguientes elementos serán parte integral del diseño del sistema:</p> <ol style="list-style-type: none"> 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. <p>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.</p>



**Mutua
Montañesa**

Muy fácil

Codigo ENS	Título	BAJA	MEDIA
[mp.sw.2]	Aceptación y puesta en servicio	Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación. a) Se comprobará que: 1. Se cumplen los criterios de aceptación en materia de seguridad. 2. No se deteriora la seguridad de otros componentes del servicio. b) Las pruebas se realizarán en un entorno aislado (pre-producción). c) Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.	Se realizarán las siguientes inspecciones previas a la entrada en servicio: a) Análisis de vulnerabilidades. b) Pruebas de penetración.
[mp.info]	Protección de la información		
[mp.info.1]	Datos de carácter personal	Cuando el sistema trate datos de carácter personal, se estará a 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.	

Codigo ENS	Título	BAJA	MEDIA
[mp.info.4]	Firma electrónica	Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.	<p>a) Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.</p> <p>b) Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional.</p> <p>c) Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin:</p> <p>d) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:</p> <ol style="list-style-type: none"> 1. Certificados. 2. Datos de verificación y validación. <p>e) El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes 1 y 2 del apartado d).</p> <p>f) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes 1 y 2.</p>



**Mutua
Montañesa**

Muy fácil

Codigo ENS	Título	BAJA	MEDIA
[mp.info.9]	Copias de seguridad (<i>backup</i>)	<p>Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada. Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad.</p> <p>Las copias de seguridad deberán abarcar:</p> <ul style="list-style-type: none">a) Información de trabajo de la organización.b) Aplicaciones en explotación, incluyendo los sistemas operativos.c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.d) Claves utilizadas para preservar la confidencialidad de la información.	

Codigo ENS	Título	BAJA	MEDIA
[mp.s]	Protección de los servicios		
[mp.s.2]	Protección de servicios y aplicaciones web	<p>Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias.</p> <p>a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:</p> <ol style="list-style-type: none"> 1. Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado. 2. Se prevendrán ataques de manipulación de URL. 3. Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como "cookies". 4. Se prevendrán ataques de inyección de código. <p>b) Se prevendrán intentos de escalado de privilegios.</p> <p>c) Se prevendrán ataques de "cross site scripting".</p> <p>d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "proxies" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "cachés".</p> <p>Se emplearán "certificados de autenticación de sitio web" acordes a la normativa europea en la materia.</p>	

En el caso de que el proveedor sea el titular de un CPD (aunque sea remoto) en el que se soporte la infraestructura SaaS de robotización, esta infraestructura deberá cumplir, adicionalmente las siguientes medidas:

Código ENS	Título	Medida
[mp.if]	Protección de las instalaciones e infraestructuras	
[mp.if.1]	◆ Áreas separadas y con control de acceso	El equipamiento se instalará en áreas separadas específicas para su función. Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas
[mp.if.2]	Identificación de las personas	El mecanismo de control de acceso se atenderá a lo que se dispone a continuación: a) Se identificará a todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información. b) Se registrarán las entradas y salidas de personas.
[mp.if.3]	Acondicionamiento de los locales	Los locales donde se ubiquen los sistemas de información y sus componentes, dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado. Y, en especial: a) Condiciones de temperatura y humedad. b) Protección frente a las amenazas identificadas en el análisis de riesgos. c) Protección del cableado frente a incidentes fortuitos o deliberados.
[mp.if.4]	Energía eléctrica	Los locales donde se ubiquen los sistemas de información y sus componentes dispondrán de la energía eléctrica, y sus tomas correspondientes, necesaria para su funcionamiento, de forma que en los mismos: a) Se garantizará el suministro de potencia eléctrica. b) Se garantizará el correcto funcionamiento de las luces de emergencia.
[mp.if.5]	Protección frente a incendios	Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incendios fortuitos o deliberados, aplicando al menos la normativa industrial pertinente.
[mp.if.7]	Registro de entrada y salida de equipamiento	Se llevará un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza el movimiento.

4.2. INCIDENTES DE SEGURIDAD

En el caso de que el adjudicatario detecte un incidente de seguridad en la implantación o durante la prestación del servicio, deberá notificarlo de inmediato al personal responsable del proyecto designado por Mutua Montañesa, perteneciente al Comité de Seguridad.

Por otro lado, deberá habilitar un canal de comunicación de potenciales incidentes de seguridad detectados por Mutua Montañesa. Para este tipo de notificación de incidentes también se deberá presentar, en el plazo que se establezca, un informe de situación y un plan de remediación si procede.

Adicionalmente, cualquier notificación de incidente que tenga una potencial trascendencia pública irá acompañada de una propuesta de plan de comunicación a seguir por parte de Mutua Montañesa.

4.3. SEGURIDAD Y CONFIDENCIALIDAD

El sistema de identificación de usuarios, asignación de roles y control de los usuarios administradores, deberá garantizar la seguridad lógica de la información, eliminando cualquier posibilidad de accesos incontrolados y no autorizados por personal no autorizado por Mutua Montañesa, así como el cumplimiento a la normativa vigente en materia de protección de datos.

Para la identificación de usuarios robot en el acceso a web externas, la acreditación podrá ser mediante usuario y contraseña o certificado persona física. Para ello se deberá garantizar la conexión segura entre robot y orchestrator con el acceso externo, garantizando en todo momento, la custodia de la acreditación de forma encriptada.

El servicio dispondrá de un módulo de auditoría que permita la trazabilidad de las acciones del usuario, en especial aquellas que implique un mayor riesgo para la integridad de la base de datos. En cualquier caso, los usuarios que operen el servicio dispondrán de usuarios nominales.

Durante el proyecto de personalización del servicio, el equipo de implantación e integración de la empresa adjudicataria, deberá tomar todas las precauciones y medidas necesarias para que el servicio resultante sea robusto, minimizando el riesgo de pérdida de integridad.

Todos los miembros de los equipos de implantación, integración y soporte de la empresa adjudicataria están obligados a guardar el secreto profesional y estricta confidencialidad sobre toda la información a la que tengan acceso durante el desarrollo del contrato, y por tiempo indefinido a partir de la finalización de éste.

Todo el desarrollo realizado, código fuente del desarrollo así como la documentación generada para cada uno de los procesos robotizados, será propiedad de Mutua Montañesa. Se incluyen pruebas, borradores, estudios previos o cualquier otro documento que tenga relación con el objeto de la licitación. El adjudicatario no podrá utilizar dicha documentación, arquitectura o diseño (entre otros) para proyectos que no sean el incluido en esta licitación. En caso de incumplimiento de este apartado por parte del adjudicatario, Mutua Montañesa se reserva el derecho de aplicar las acciones legales que considere. A finalización del contrato, el adjudicatario entregará copia de toda esta información a Mutua Montañesa.

El licitador deberá disponer de una política o metodología formal y documentada en materia de desarrollo seguro de software que describirá, como mínimo, qué controles o criterios se contemplan en los siguientes ámbitos: validación de entrada/salida, formato de datos, asignación de memoria, gestión de errores y excepciones, mecanismos de trazabilidad y documentación del código. La descripción de esta metodología deberá plasmarse en la oferta que da respuesta al presente pliego.

4.4. AUDITORIA DE CALIDAD Y SEGURIDAD

Asimismo, Mutua Montañesa se reserva el derecho a llevar a cabo auditorías sobre la plataforma desplegada, con frecuencia máxima semestral. Cualquier vulnerabilidad



encontrada en estas potenciales auditorías deberá ser subsanada por parte de la empresa adjudicataria en un plazo máximo de dos semanas. Si Mutua Montañesa considera que una vulnerabilidad encontrada pone gravemente en peligro el servicio o su información, podrá requerir la desconexión de la plataforma por motivos de seguridad, debiendo la empresa adjudicataria dejar de facturar los conceptos facturables afectados por esta desconexión.

5. CONDICIONES EJECUCIÓN DEL CONTRATO

5.1. DURACIÓN Y PLAN DEL CONTRATO

La duración del contrato será de 36 meses a contar desde la fecha de inicio del servicio con posibilidad de prorrogarlo adicionalmente por un máximo de un periodo de 12 meses. En esta prórroga, el alcance del servicio anual será el asociado al punto 5.3 de Volumetría y estimación prevista.

5.2. ESTIMACIÓN ECONÓMICA

En este punto se presenta la estimación de los costes por proceso que se ha tenido en cuenta para la estimación del presupuesto base de licitación del cuadro económico del pliego de cláusulas particulares.

Esta estimación se ha realizado teniendo en cuenta los diferentes servicios requeridos en el en el alcance, donde fundamentalmente debe valorarse económicamente:

- La infraestructura tanto plataforma como servicio SaaS de las licencias requeridas de UiPath.
- La implantación de los procesos robotizables
- El soporte y mantenimiento evolutivo de los procesos robotizables.

Por ello, hemos establecido un cuadro económico para cada una de estos servicios requeridos, teniendo en cuenta un primer análisis realizado sobre los procesos susceptibles de robotizar que ya identificamos en el Anexo I, de acuerdo a la complejidad (sencillo, medio y complejo) y a la volumetría estimada de los procesos.

Infraestructura o "hilo de ejecución":

Nº hilos ejecución o "robots"	Importe máximo hilo ejecución/año
1	11.250 €
2	22.500 €

Implantación y mantenimiento Procesos robotizables:

Tipo de Proceso	Importe máximo implantación proceso	Importe máximo mto. año proceso	Importe máximo mto. Mes
Sencillo	14.110 €	2.000€	166,67 €/mes
Medio	21.340 €	3.000€	250,00 €/mes
Complejo	38.475€	5.400€	450,00 €/mes

5.3. VOLUMETRIAS Y ESTIMACIÓN PREVISTA

Dado el tipo de procesos identificados en el Anexo I, y teniendo en cuenta nuestro plan de robotización anual, estimamos el desarrollo de 3/4 procesos anuales, teniendo en cuenta el siguiente Planning, el cual será revisado anualmente:

Nº procesos a robotizar:

Implantación procesos robotizables/Año	2022	2023	2024
Proceso sencillo	2	2	2
Proceso medio	1	2	1
Proceso complejo		0	0
TOTAL Procesos	3	4	3

A continuación se estima una volumetría del número de cuotas mantenimiento teniendo en cuenta los procesos a implantar cada año y su activación del mantenimiento.

Nº cuotas mantenimiento mensual:

A continuación las cuotas por mensualidades de los procesos robotizables en ese año.

Cuota mantenimiento mensual	2022	2023	2024
Mantenimiento proceso sencillo	12	9	12
Mantenimiento proceso medio	6	9	6
Mantenimiento proceso complejo	0	0	0

A continuación las cuotas de mantenimiento anual de los años anteriores:

Cuota mantenimiento anual	2022	2023	2024	2025
Mantenimiento proceso sencillo	1 (*)	3	5	7
Mantenimiento proceso medio	0	1	3	4
Mantenimiento proceso complejo	0	0	0	0

(*) En este primer año, se tendrá en cuenta la cuota de mantenimiento anual del proceso que Mutua Montañesa ya tiene en ejecución, y que en primer término deberá ser migrado a la nueva plataforma del adjudicatario.

Nº hilos ejecución:

	2022	2023	2024	2025
Nº hilo ejecución	1	2	2	2

Dentro del total de los procesos a mantener, se deberá tener en cuenta el proceso robotizable que actualmente Mutua Montañesa tiene ejecutándose en modalidad Saas y que el actual proveedor deberá hacer una transferencia de conocimiento y dar traslado de todas las configuraciones y parametrizaciones para que pueda mantenerse y soportarse con la misma plataforma que la que es objeto del presente contrato por el nuevo prestador del servicio.

5.4. CONDICIONES DE EJECUCION DEL SERVICIO

Como modelo global de servicio, la modalidad predominante será trabajo en remoto por parte de la empresa adjudicataria, para la mayor parte de las fases del proyecto.

Se requiere la presencia del equipo de la empresa adjudicataria en las diferentes fases o hitos del proyecto:

- Revisión y priorización de los procesos robotizables definidos en el Anexo I.
- Análisis de requerimientos de los procesos robotizables

En cualquier caso, durante la ejecución del proyecto, puede requerirse presencia puntual en los centros de Mutua Montañesa ubicados en la provincia de Cantabria, para llevar a cabo reuniones funcionales con las áreas implicadas en los procesos a robotizar.

Los costes de desplazamiento, comidas, así como cualquier otro coste relacionado con la relación laboral de las personas de la empresa adjudicataria y Mutua Montañesa, correrá por parte de la empresa adjudicataria, sin que puedan repercutirse a Mutua Montañesa.

5.5. PLANNING Y FASES SERVICIO

Las empresas licitadoras deberán presentar un plan anual, especificando las fases y la duración de cada una de ellas, los hitos destacables y los entregables en cada una de las fases. Se valorará que dentro del planning se detalle las jornadas de cada uno de los perfiles asignados a la ejecución del proyecto.

La empresa adjudicataria deberá aportar un plan de proyecto, indicando las fases, con el detalle de sus actividades, hitos y entregables que se valorará.

El adjudicatario efectuará un detalle del modelo de servicio global del proyecto, ya que la implantación de cada uno de los procesos robotizables será gradual, y por lo tanto convivirá el desarrollo o implementación de la automatización de procesos con la ejecución y mantenimiento de los ya puestos en producción. Por tanto, debemos trabajar con un modelo PDCA de mejora continua, que nos permitirá ir incorporando conocimientos del proyecto a los siguientes procesos robotizables.

El proyecto se iniciará con el Kick-off del proyecto, en el cual se acordará el calendario definitivo del proyecto para el primer año el cual deberá ser acordado entre la empresa adjudicataria y Mutua Montañesa.

No obstante todo lo expuesto en este apartado, Mutua Montañesa se reserva el derecho de incluir en la planificación del proyecto una serie de hitos intermedios o puntos de control con el fin de minimizar los riesgos que puedan detectarse.

Dentro de la ejecución del proyecto, la empresa adjudicataria por lo menos deberá desarrollar en su propuesta y plan de trabajo, las siguientes fases:

- Identificación de procesos y análisis de viabilidad
- Desarrollo del proceso a automatizar
- Mantenimiento y seguimiento procesos robotizados

5.5.1. IDENTIFICACIÓN DE PROCESOS Y ANÁLISIS DE VIABILIDAD

En esta primera fase del proyecto se deberá acordar y ajustar el trabajo ya realizado por Mutua Montañesa en relación al listado de procesos robotizables y su priorización. La empresa adjudicataria deberá validar y con ese punto de partida realizar un Plan Director de Robotización para la ejecución del contrato, así como para sus fases posteriores de evolución.

Este anexo I debe considerarse como prioritario, pero al ser un proceso dinámico debido a los cambios de requerimientos del negocio, puede ser susceptible de modificarse por considerarse otros procesos más prioritarios o con un índice de robotización mayor.

En esta primera fase se deberá realizar el levantamiento de procesos desde una doble perspectiva:

- Procesos potenciales, donde se valorará el potencial de automatización de procesos dentro de las siguientes áreas de negocio: Prestaciones Sanitarias y Económicas, Operaciones y Desarrollo de Negocio. Para ello se realizará el estudio económico, análisis de viabilidad y costes de oportunidad de robotizar el proceso.
- Procesos ya identificados en Anexo I.

Para esto se deberá:

1. Proponer la metodología de levantamiento, diseño y priorización de procesos creando las mejores prácticas para el programa de automatización
2. Análisis junto a la unidad de negocio la necesidad de automatización y digitalización del proceso. Buscar la mejor manera de automatizar y proponiendo su división en subprocesos más sencillos y automatizables por las diferentes soluciones técnicas
3. Llevar a cabo el diseño del nuevo proceso TO BE y documentación asociada
4. Elaboración el caso de negocio asociado a cada proceso identificando los ahorros realizables que tendrán que ser confirmados por Mutua Montañesa
5. Dar formación a las áreas de negocio usuarias del proceso automatizado y soporte post-implementación de los diferentes procesos a desarrollar
6. Análisis de los procesos del área de negocio e identificación de nuevas oportunidades para la automatización

Los principales entregables de esta fase son:

- Documento de Cualificación del proceso
- Revisión y adecuación de los criterios de valoración tanto de potencial de proceso como de complejidad para la validación bondad de la matriz de priorización a partir del análisis de los parámetros y ponderaciones utilizadas para su elaboración. Modelo de priorización con la matriz de priorización validada
- Acompañamiento y definición de metodología propia para el levantamiento de procesos a robotizar. Enfoque metodológico con el detalle de actividades necesarias para el levantamiento de procesos. Metodología de levantamiento de procesos a robotizar
- Hoja de ruta de procesos a robotizar y procesos priorizados para las diferentes colas de automatización sprints (planificación y recursos necesarios). Plan director.
- Elaborar el caso de negocio asociado a cada proceso identificando los ahorros realizables que tendrán que ser confirmados por Mutua Montañesa.
- Levantamiento de procesos:
 - Identificación de los requerimientos y el diseño del proceso seleccionado
 - Viabilidad de la automatización: análisis de viabilidad, análisis FTE y análisis económico. Coste automatización según la complejidad de desarrollo: alta, media, baja
 - Alcance: selección excepciones a gestionar por el robot

El tiempo estimado para esta primera fase no debe ser superior a 1 mes. Como se solicita en el presente pliego esta fase del proyecto, será recurrente año a año, ya que se valorará de nuevo los procesos a robotizar.

5.5.2. DESARROLLO DEL PROCESO ROBOTIZABLE

Se entiende por desarrollo de procesos automatizados, el análisis, diseño, programación y puesta en producción de los procesos de negocio seleccionados.

Incluye las siguientes fases:

1. **Levantamiento funcional de procesos priorizados:** En esta fase se realiza un análisis detallado del proceso a robotizar, para ello se deberá incluir toda la información relevante como excepciones de negocio, variables a parametrizar, datos para reporting,... El adjudicatario deberá elaborar los documentos de requisitos necesarios para la validación del equipo de desarrollo de Mutua Montañesa y entrega al terminar la implementación. Las principales tareas por proceso priorizado de esta fase son:
 - a. Detallar el proceso AS-IS
 - b. Detallar el proceso TO BE
 - c. Diseño de pruebas
 - d. Aprobar diseño

El principal entregable de esta fase es el documento de levantamiento funcional para cada proceso.

2. **Diseño técnico de la solución y desarrollo:** En esta fase se detalla el desarrollo del proceso con los diagramas de flujos, lógicas del proceso, módulos y variables que intervienen
 - a. Estimación de esfuerzos
 - b. Diseño de la solución
 - c. Organización del trabajo
 - d. Desarrollo de las automatizaciones seleccionadas
 - e. Desarrollo de los scripts

El principal entregable de esta fase es el Diseño técnico

3. **Pruebas e integración:** En esta fase se define el plan de pruebas e integración (integradas, UAT y recurrentes), el objetivo es guardar evidencia de las pruebas ejecutadas, de los datos utilizados, de los resultados obtenidos, etc. El adjudicatario deberá realizar la propuesta del documento de pruebas que se validará con el equipo de Mutua Montañesa y ejecución conjunta detallando las mejoras, fallos o cambios necesarios. Estas pruebas incluirán además del funcionamiento en general, pruebas específicas de carga y rendimiento, y solución de recovery en caso de fallo parcial o total. Cada uno de los procesos deberá superar un ciclo de pruebas determinados y previos a la puesta en producción:
 - a. Plan de pruebas
 - b. Definir plan de integración
 - c. Formación

Los principales entregables de esta fase son: Plan de pruebas y manual técnico de proceso.

4. **Producción o Paso a producción: En esta fase se define**
 - a. Plan de mantenimiento
 - b. Manual del proceso. Se entregará un manual específico por proceso que deberá contener toda la información necesaria para su mantenimiento (variables parametrizadas, tipo de variable, etc).

Los principales entregables de esta fase son: o Cuadro de mando por robot o Plan de transferencia de conocimiento. Documentación de traspaso para el mantenimiento del proceso automatizado. Manual del proceso o Bitácora de versiones

La duración de esta fase se definirá en el Plan Director, teniendo en cuenta la complejidad de los procesos, y que anualmente se prevee una implantación de 3/4 procesos por año.

5.6. EQUIPO DE TRABAJO

A continuación se establece el perfil de las personas que Mutua Montañesa considera necesario para un correcto desarrollo del proyecto, estableciéndose los requisitos mínimos en cuanto a funciones para cada uno de ellos.

PERFIL	CONOCIMIENTOS Y FUNCIONES
Jefe Proyecto	Perfil de gestión o líder de proyecto de la empresa adjudicataria, realizando tareas organizativas de control y seguimiento de la ejecución del servicio. Para ello debe tener expertise y formación en metodologías de gestión de proyecto tipo PMI, Scrum, etc..
Consultor Negocio y/o RPA	Perfil funcional, es el enlace entre negocio y equipo análisis de Mutua Montañesa, encargado de evaluar, levantar y probar los procesos a desarrollar. Como mínimo un perfil consultor senior deberá tener conocimientos en la herramienta UiPath y todo el equipo deberá estar certificados como mínimo en la modalidad de Advance Developer.
Ingeniero Infraestructura	Perfil técnico encargado de definir la infraestructura de la solución RPA en tecnología UiPath (comunicaciones, seguridad, y los componentes de robotización necesarios, así como su alojamiento en la nube privada que proponga el adjudicatario). Además velará por el buen funcionamiento y rendimiento de la aplicación RPA, y conectividad con la intranet de Mutua Montañesa.
Desarrollador o Técnico	Perfil técnico encargado del desarrollo de los procesos y con capacidad de análisis de los procesos y datos derivados de la propia operativa del robot. Debe conocer profundamente la tecnología UiPath, así como todos los productos para su manejo y gestión. Deberá estar certificado en la modalidad de Advance Developer.

Para cada uno de los perfiles presentados en la oferta que como mínimo tienen que cubrir los descritos en este punto, las empresas licitadoras deberán presentar:

- Años de experiencia
- Detalle de los proyectos que acrediten su conocimiento
- Desglose de las horas que cada perfil deberá dedicar.

Dentro de las capacidades generales o conocimientos necesarios para que la empresa licitadora pueda desarrollar este servicio, se incluye:

- Profundo conocimiento de los requisitos de diseño y automatización de procesos utilizando la herramienta UiPath de RPA.
- Tener conocimientos y experiencia previa en el diseño e reingeniería de procesos de negocio, o mejora y automatización de los mismos.
- Conocimiento en el sector de las mutuas colaboradoras con la seguridad social.

6. SEGUIMIENTO EJECUCIÓN SERVICIO

Las empresas licitadoras deberán presentar en su oferta el plan de servicio global, especificando la metodología del servicio SaaS, la atención técnica, la gestión de incidencias, los acuerdos de nivel de servicio, así como la monitorización del servicio.

6.1. SEGUIMIENTO PROYECTO

Las empresas licitadoras deberán presentar un modelo de gestión o metodología de proyecto, así como el modelo de relación entre adjudicatario y Mutua Montañesa.

Las propuestas deberán indicar la estructura y funcionamiento de los comités específicos para la gestión y desarrollo del proyecto, con el fin de mantener un modelo de relación que avale el buen desarrollo del proyecto, la interlocución entre ambas partes, así como una gestión estratégica y operativa exitosa. En la oferta como mínimo se deberá presentar:

Comité Estratégico/Dirección Proyecto. Este comité tendrá las siguientes funciones:

- Toma de decisiones estratégicas a medio-largo plazo. Actualización criterios calificación procesos a robotizar
- Valoración y conformación de nuevos procesos de desarrollo. Actualización hoja de ruta de procesos a robotizar
- Seguimiento económico global del contrato, evolución de la facturación y del consumo realizado
- Seguimiento global de expectativas y feedback de Mutua Montañesa al adjudicatario con el servicio prestado
- Decisión respecto riesgos escalados desde el comité operativo

Comité Operativo. Este comité tendrá las siguientes funciones:

- Supervisión desarrollo nuevos procesos y las pruebas de aceptación
- Elaboración del documento de evaluación de nuevos procesos a robotizar, dirigido al comité estratégico. En dicho documento se especificará: el nivel de complejidad, así como las características del proceso a robotizar y el ROI obtenido con la robotización
- Seguimiento del proceso a robotizar y los informes de ejecución de los procesos robotizados.
- Gestión de incidencias y riesgos
- Traslado de propuestas de mejoras hacia el comité estratégico.

Como mínimo las siguientes tareas deberán ser realizadas por el adjudicatario:

1. Redactar las actas de cada reunión
2. Actualizar la documentación del repositorio facilitado por Mutua Montañesa. En dicho repositorio estarán todos los documentos relacionados con el contrato adjudicado
3. Agendar – según periodicidad definida donde al menos, el Comité estratégico deberá ser trimestral y el operativo mensual - y definir los integrantes mínimos que deberán tener cada comité. Existe la posibilidad que puedan convocarse a demanda por parte de Mutua Montañesa o del adjudicatario reuniones extraordinarias fuera de los plazos establecidos
4. Preparar agenda del día y documentación necesaria para cada comité

6.2. SEGUIMIENTO SERVICIO MANTENIMIENTO

Las empresas licitadoras deberán presentar un modelo de soporte para la fase de mantenimiento de los procesos robotizables, que debe tener una gestión paralela con el proyecto de desarrollo e implantación. Para ello tiene que ponerse a disposición de Mutua Montañesa, una persona responsable del servicio que pueda dar respuesta a todos los servicios incluidos dentro del alcance de este contrato.

6.2.1. ASISTENCIA TÉCNICA

Se incluirá en la oferta el modelo de servicio o atención técnica al usuario. La asistencia técnica al usuario se podrá rerealizar vía telefónica o vía email para la resolución de dudas o problemas en relación al funcionamiento del servicio.

Esta asistencia técnica dará soporte al equipo técnico de Mutua Montañesa y a las personas clave o key users de los procesos robotizados.

6.2.2. DISPONIBILIDAD

A fin de garantizar la alta disponibilidad con operación continua, el servicio debe ofrecer una disponibilidad 24x7. El servicio deberá estar disponible como mínimo un 99,5% al mes.

Se entenderá que el servicio no está disponible, cuando por motivos directamente imputables al adjudicatario, el servicio no permite llevar a cabo alguno de los procesos configurados, ya sea de forma continuada o de forma interrumpida durante un mismo mes.

Las intervenciones de mantenimiento deberán planificarse con antelación y Mutua Montañesa elegirá la franja horaria mas adecuada en función de las necesidades del servicio. El adjudicatario nunca actuará sobre la instalación en producción de forma directa. Además, la puesta en producción de cualquier actualización o modificación de la herramienta, no deberá afectar al funcionamiento diario del software así como a su disponibilidad.

6.2.3. GESTIÓN DE INDICENCIAS

El adjudicatario deberá presentar modelo de gestión de incidencias sobre los procesos robotizados, así como los niveles de servicio propuestos para éstas según los criterios de clasificación en función de la prioridad (crítica, alta, media y baja). En esta propuesta el adjudicatario debe poner a disposición de Mutua Montañesa una herramienta de ticketing para la gestión de incidencias del servicio de mantenimiento, y garantizar los niveles de servicio presentados por la empresa adjudicataria.

A cada petición de soporte o incidencia, se le asignará una de las prioridades abajo descritas. El Adjudicatario utilizará la prioridad especificada por Mutua Montañesa, a menos que esté en clara discordancia con la naturaleza del problema, en cuyo caso la prioridad revisada se acordará entre las partes. El procedimiento de escalado se aplicará si las partes no son capaces de acordar la prioridad adecuada.

Prioridad crítica: Esta prioridad debe asignarse a una petición de soporte por una parada de la plataforma de robotización o alguno de los hilos de ejecución, que impida el

funcionamiento de los procesos robotizados, sin que haya una alternativa a esta parada de funcionamiento, y como resultado no puede continuar con el curso ordinario del mismo.

Prioridad alta: Esta prioridad debe asignarse a una petición de soporte por una parada de uno de los procesos de robotizados, impidiendo la ejecución total de alguno de ellos.

Prioridad media: Esta prioridad debe asignarse a una petición de soporte por una parada de uno de los procesos de robotizados, pero con la posibilidad de ejecutar parcialmente la funcionalidad de alguno de ellos.

Prioridad baja: Esta prioridad debe asignarse a una petición de soporte sobre el uso y la configuración de cualquiera de los procesos robotizables, así como de su definición, que en ningún caso impide la ejecución de los procesos robotizados.

Las incidencias se clasificarán según el nivel de prioridad/criticidad antes indicando, y se exigirá un servicio mínimo en cuanto a la resolución de incidencias y tiempo de respuesta, en base a la siguiente definición:

Tiempo de respuesta: Tiempo transcurrido desde que se comunica la incidencia al servicio de mantenimiento propuesto, hasta que dicho servicio se pone en contacto con el usuario o cliente

Tiempo de resolución: Tiempo transcurrido desde el instante que se comunica la incidencia al servicio de mantenimiento propuesto, hasta el momento en que la incidencia o el servicio se ha restablecido o solucionado.

Teniendo en cuenta esta definición, estos son los tiempos mínimos exigidos para la respuesta o resolución de incidencias, teniendo en cuenta la prioridad definida:

Prioridad	Tiempo de respuesta	Tiempo de resolución
Crítica	0,5 horas	4 horas
Alta	1 hora	8 horas
Media	2 horas	24 horas
Baja	5 horas	48 horas

El horario laborable se establece de lunes a viernes, de 08:00h a 20:00h. excepto festivos de ámbito nacional y las tardes del 24 y 31 de diciembre. Las incidencias de prioridad crítica se solventarán en horario 24x7, al ser situaciones críticas y que afectan a la disponibilidad del servicio.

6.2.4. ACUERDOS NIVEL DE SERVICIO

La empresa adjudicataria deberá cumplir con los acuerdos de nivel de servicio para la disponibilidad del sistema, los tiempos de respuesta y los tiempos de resolución de incidencias que puedan surgir durante la fase de mantenimiento y soporte de los procesos robotizados. Dado que existirá un registro en el momento del alta de la incidencia, así como

de la respuesta y resolución, se establecerán unos indicadores objetivos (resolución en plazo) para el cumplimiento de los tiempos de respuesta y resolución mínimos por cada prioridad.

A continuación definimos el indicador Nivel de cumplimiento:

$$\text{Nivel de cumplimiento (\%)} = \text{Nº incidencias que cumplen en plazo} * 100 / \text{Nº Total incidencias}$$

Se entiende que una incidencia cumple en plazo cuando el tiempo de respuesta y tiempo de resolución es igual o está por debajo del tiempo máximo establecido, en el cuadro anterior.

La empresa adjudicataria se responsabilizará de alcanzar estos niveles de cumplimiento establecido en el pliego de prescripciones técnicas, con independencia de los recursos técnicos y/o personales que tenga que incorporar en el servicio.

Disponibilidad:

El adjudicatario debe ofrecer un nivel de continuidad en el servicio, dentro de un alcance determinado, y acorde con la naturaleza del mismo. Se determina que el servicio debe tener una disponibilidad mínima del 99,5%. El cálculo de la disponibilidad se realizará en base a la siguiente fórmula:

$$\text{Disponibilidad} = 100 \times (T - T_c) / T$$

Siendo T, el tiempo total mensual y T_c, el tiempo de pérdida de disponibilidad, entendido como tiempo transcurrido desde la apertura de la incidencia por parte del cliente hasta la restitución de la conectividad del servicio afectado.

Tiempo de respuesta:

En base a la definición de "Tiempo de respuesta" facilitado en el apartado anterior, cabe indicar que se diferenciará para su cálculo por la prioridad de la incidencia. El nivel de cumplimiento mínimo admitido según la prioridad será el siguiente

Prioridad	Nivel de Cumplimiento
Crítica	95%
Alta	95%
Media	85%
Baja	80%

Tiempo de resolución:

En base a la definición de "Tiempo de resolución" facilitado en el apartado anterior, cabe indicar que se diferenciará para su cálculo por la prioridad de la incidencia. El nivel de cumplimiento mínimo admitido según la prioridad será el siguiente

Prioridad	Nivel de Cumplimiento
Crítica	90%
Alta	90%
Media	85%

Baja	80%
------	-----

Con la finalidad de garantizar los acuerdos de servicio detallados por parte del adjudicatario, y según se define y establece en el presente pliego de prescripciones técnicas, Mutua Montañesa se reserva el derecho de aplicar unas penalizaciones por el incumplimiento de estos ANS. En la cláusula de penalizaciones del pliego de condiciones particulares se establecen las deducciones por incidencias o faltas cometidas que sean imputables al adjudicatario, y que se clasificarán como faltas leves y faltas graves.

6.2.5. INFORMES DE CONTROL Y SEGUIMIENTO

La empresa adjudicataria deberá presentar y facilitar durante la ejecución del contrato los siguientes informes de control del proyecto y de seguimiento de servicio:

- Situación global proyecto
- Análisis de desviaciones del proyecto (tiempo y coste).
- Informe de gestión de incidencias e informe de cumplimiento de los ANS.

En relación al informe de gestión de incidencias y seguimiento de los ANS, se deberá como mínimo presentar trimestralmente con la siguiente información:

- Incidentes de Seguridad: ante un incidente de seguridad en la implantación o durante la prestación del servicio, el adjudicatario deberá notificarlo de inmediato al personal responsable del proyecto designado por Mutua Montañesa, y hacer un registro del mismo.
- Disponibilidad: deberá incluir una relación de las indisponibilidades acontecidas durante el mes anterior, incluyendo:
 - Fecha y hora de inicio de indisponibilidad de la infraestructura
 - Fecha y hora de finalización de indisponibilidad de la infraestructura
 - Motivo detallado de la indisponibilidad
 - Solución adoptada
 - Indisponibilidad SI/NO
 - Adicionalmente, el informe deberá también relacionar las paradas planificadas, incluyendo:
 - Fecha y hora de notificación de la parada
 - Previsión de fecha y hora de inicio de la parada
 - Previsión de fecha y hora de finalización de la parada
 - Fecha y hora de inicio reales de la parada
 - Fecha y hora de finalización reales de la parada
 - Motivo detallado de la parada
- Incidencias: informe que refleje el % de resolución de incidencias dentro de los plazos de tiempo establecidos correspondiente al mes anterior. Dicho informe deberá incluir una relación de las incidencias acontecidas el mes anterior, incluyendo:
 - Fecha y hora de comunicación de la incidencia
 - Aceptación de la incidencia por tener que ver con los servicios ofertados
 - Explicación detallada de la incidencia
 - Prioridad aplicada
 - Fecha y hora estimada de resolución de la incidencia
 - Fecha y hora real de resolución de la incidencia
 - Solución adoptada

6.2.6. PENALIZACIONES

Para el caso de que el licitador incumpla la ejecución parcial de los servicios que constituyen el objeto de este contrato, se determinan específicamente las penalizaciones siguientes, en función de las circunstancias que asimismo se definen:

- **Incumplimientos en la resolución de incidencias**

Se define incidencia como el mal funcionamiento de los procesos robotizados y se determinará su prioridad teniendo en cuenta el punto 6.2.4 Acuerdos de nivel de servicio del presente documento. La prioridad establecerá el plazo de resolución máximo por cada una de las incidencias, y el tipo de incumplimiento de incidencias se segmentará en:

- Incumplimiento muy grave: $\% \text{resolución en plazo} < 75\%$, para incidencias de prioridad crítica y alta. Se aplicará una penalización correspondiente al 10% del importe mensual del contrato correspondiente al coste de mantenimiento -IMPORTE sin I.V.A-, que consta en el apartado 3 del Anexo I del Pliego de Cláusulas Particulares.
- Incumplimiento grave: $75\% \leq \% \text{resolución en plazo} < 85\%$ para incidencias de prioridad crítica y alta, y $\% \text{resolución en plazo} < 75\%$, para las incidencias de prioridad alta y media. Se aplicará una penalización correspondiente al 5% del importe mensual del contrato correspondiente al coste de mantenimiento, -IMPORTE sin I.V.A-, que consta en el apartado 3 del Anexo I del Pliego de Cláusulas Particulares.
- Incumplimiento leve: $75\% \leq \% \text{resolución en plazo} < 85\%$ para incidencias de prioridad alta y media. Se aplicará una penalización correspondiente al 3% del importe mensual del contrato correspondiente al coste de mantenimiento -IMPORTE sin I.V.A-, que consta en el apartado 3 del Anexo 1 del Pliego de Cláusulas Particulares.

- **Incumplimientos en la disponibilidad de la infraestructura**

Se define disponibilidad de la infraestructura como la capacidad que tiene la misma para permitir a un proceso robotizable ejecutarse según la planificación y definición del proceso, cuando éste lo requiere y con el rendimiento y funcionalidad de la plataforma esperado. No se considerarán indisponibilidades de la infraestructura todas aquellas paradas planificadas y previamente notificadas y acordadas por el Órgano de Contratación.

Se cifra como % de disponibilidad objetivo mensual de la infraestructura el 99,5% de disponibilidad, en horario 24x7 o en caso de mejora de dicha cifra, la que el proveedor haya expresado en su oferta. Por debajo de este porcentaje se establecen los siguientes incumplimientos:

- Incumplimiento leve: $99\% \leq \text{Disponibilidad} < \% \text{Disponibilidad Objetivo}$
- Incumplimiento medio: $98\% \leq \text{Disponibilidad} < 99\%$
- Incumplimiento grave: $97\% \leq \text{Disponibilidad} < 98\%$
- Incumplimiento muy grave: $\text{Disponibilidad} < 97\%$

El importe máximo anual de las sanciones no podrá exceder del 10% del Importe Total Anual del Coste de Mantenimiento e hilo de ejecución que consta en el Anexo I del Pliego de

Cláusulas Particulares de la oferta, valor a partir del cual se iniciará el correspondiente expediente de resolución de contrato.

El incumplimiento durante 3 periodos de facturación consecutivos, o durante 3 periodos de facturación en un periodo de 12 meses, legitimará a la Entidad contratante a proceder a la resolución del contrato sin indemnización alguna para el adjudicatario, debiendo proceder a la ejecución de las tareas especificadas en el apartado Finalización del Servicio.

6.2.7. CESE DEL SERVICIO

El Responsable del servicio de la empresa adjudicataria tres meses antes del cese del servicio comenzará a preparar y consensuar la transición del servicio, así como a planificar junto el equipo técnico de Mutua Montañesa las actividades a realizar para asegurar la transición del servicio.

En este caso, la empresa adjudicataria deberá preparar todos los entregables, es decir, configuraciones, parametrizaciones del producto y desarrollos de los servicios implantados en el software UiPath para que puedan ser migrados a otra plataforma de las mismas características, sin pérdidas en la migración.

Tanto los desarrollos de los procesos robotizados, así como las configuraciones del orquestador para la ejecución de los procesos robotizados, deberán poder ser portados a otra infraestructura, sin coste adicional para el siguiente proveedor ni para Mutua Montañesa.

7. ANEXO I – LISTADO PROCESOS ROBOTIZABLES

Después de un trabajo de análisis realizado en 2020, estos son los procesos ya identificados y valorados por su complejidad que deberán realizarse dentro del alcance de este proyecto.

ÁREA NEGOCIO	PROCESO ROBOTIZABLE
S03 - Operaciones	Grabación de Facturas Digitales
S03 - Operaciones	Grabación de Facturas Contabilidad FACE + Generación fichero FACE
N03 – Prestaciones (Absentismo)	Validación Pago Directo (Grupos II)
N03 - Prestaciones (Absentismo)	Descarga y Carga protocolo ATRIUM + Carga y Descarga Suspjal
N03 - Prestaciones (Absentismo)	Descarga de Sentencias, Demandas, etc. + Notificaciones Electrónicas para Capital Coste

Código	Nombre del proceso:	Complejidad	% Ocupación
RPAS03-02	Grabación de Facturas Digitales	1 Sencillo	10%
RPAS03-01	Grabación de Facturas Contabilidad FACE + Generación fichero FACE	1 Sencillo	15%
RPAN01-02	Validación Pago Directo (Grupo II)	1 Sencillo	5%
RPAN04-01	Descarga y Carga protocolo ATRIUM + Carga y Descarga Suspjal	2 Medio	20%
RPAN04-06	Descarga de Sentencias, Demandas, etc. + Notificaciones Capital Coste	1 Sencillo	10%

8. ANEXO II – MATRIZ PRIORIZACIÓN

A continuación, se detallan los factores clave para la definición de la complejidad de los procesos a robotizar:

- **Número de aplicaciones impactadas.** No se tendrán en cuenta aplicaciones estándar como puedan ser Word, Excel, correo electrónico, etc.
- **Formato de entrada de Datos.** Es importante en la automatización de los procesos que los datos tengan en un formato estándar e inteligible para el robot. Se consideran formato estándar, por ejemplo; Word, Excel, o correo electrónico, siempre que vengan estandarizados.
- **Estandarización del proceso.** Se consideran procesos estandarizados aquellos que tienen pocas variantes y tienen pocos escenarios que contemplar. Los procesos con muchos escenarios complican los desarrollos incrementando el nivel de complejidad.
- **Estabilidad de los Sistemas.** Se consideran sistemas estables aquellos que ya están consolidados y no están sujetos a continuas modificaciones. El robot trabaja sobre las aplicaciones al igual que haría un humano, lo que implica que los fallos puntuales o bugs que puedan existir en la aplicación sobre la que trabaja, repercutirán directamente sobre el proceso.
- **Naturaleza de las aplicaciones.** Como propuesta adicional a los indicadores propuestos, se han incluido unos indicadores que en base a la experiencia de robotización y al actual modelo de desarrollo de UiPath, se ajustan de una manera más intuitiva al cálculo de la dificultad de los procesos. La naturaleza de la aplicación y su integración con UiPath, ordenada de menor a mayor por nivel de dificultad será:
 - Automatización Directa: El software es capaz de integrar directamente con las soluciones de manera automática a través de actividades, sin necesidad de simular el comportamiento humano.
 - Automatización por Selectores: No existe integración directa, lo que requiere simular el comportamiento humano, pero la automatización se puede realizar a través de selectores estables. En estos casos el robot es capaz de reconocer elementos de la aplicación lo que facilita la automatización.
 - Automatización por Imagen: No existe integración directa, ni selectores estables en los que pueda apoyarse el robot para la automatización. Esto requerirá automatizar los procesos mediante imágenes, comandos de teclado y motores OCR. Este es el modelo de automatización más costosa y menos estable. Se puede dar en aplicativos donde el robot no es capaz de reconocer el código en el que están desarrollados o entornos virtualizados, donde únicamente el robot recupera una imagen.

Adicionalmente a estos criterios de ponderación, existen unos factores de potencialidad del proceso a robotizar, relacionados con la volumetría del proceso (repetición, duración, tiempo, número de personas implicadas, etc...) y el riesgo operacional del mismo si tiene impacto en cliente interno o externo.

Con este punto de partida, se ha definido una matriz de clasificación de procesos por complejidad.



Tipo de Criterios	Criterios	Ponderación Baja	Ponderación Media	Ponderación Alta
Estabilidad y Madurez	¿Es necesario rediseñar el proceso?	No es necesario rediseñar el proceso	Pequeños cambios en el proceso	Significantes cambios en el proceso
	¿El proceso que está sujeto a cambios?	Bajo	Medio	Alto
	Automatización prevista	Bajo	Medio	Alta
	Escala de excepciones	Bajo	Medio	Alta
	Nivel de riesgo operativo	Proceso no - Core	Tiempo o negocio dependiente del proceso	Proceso crítico para el negocio
Datos estructurados y consistentes	Tipos de datos	Digital, estructurado y estandarizado	Digital, estructurado y estandarizado (no OCR)	Digital, estructurado y no estandarizado
	¿El proceso utiliza datos escritos manualmente o documentos escaneados?	Documentos escaneados	Datos escritos manualmente	Documentos escritos manualmente y escaneados
	Manejo de datos requeridos	Copiar/Pegar	Copiar, pegar, leer y modificar datos	Copiar, pegar, lectura, enriquecimiento de datos y extracción PDF
Normas	Número de aplicaciones/herramientas con las que se interactúa	Entre 1 y 2 aplicaciones	Entre 3 y 4 aplicaciones	Más de 5 aplicaciones
	Número de pantallas	Entre 1 y 4 pantallas	Entre 4 y 20 pantallas	Más de 20 pantallas
	Número de reglas lógicas	< 5 Sin flujo alternativo	5-10 Incl. Flujos alternativos	> 50 Incl. Reglas de agrupación
	Sistemas de integración	Todos los sistemas se integran directamente	Requieren de integración customizada	Requiere alto nivel de integración entre herramientas
Repetitivas y de alto volumen	¿Es el proceso repetitivo?	Bajo	Medio	Alto
	¿Consiste en un proceso con alto volumen de tareas del día a día?	Bajo	Medio	Alto
Tiempos y periodicidad	¿Cuál es la duración?	< 30 minutos	> 30 minutos y < 1 hora	> 1 hora
	¿Cuál es el volumen anual del proceso?	< 500	> 500 y < 5000	> 5000
	Número de personas dedicadas	< 5 Trabajadores	> 5 Trabajadores y < 10 Trabajadores	> 10 Trabajadores
Riesgo Operacional	¿Cuál es el riesgo asociado al proceso? Quién es el receptor del output del proceso? (e.g. Interno / Cliente externo)?	Interno	Externo	Interno y externo