Sede Social
Avda. Icaria, 133 - 135 | 08005 Barcelona
T 934 867 400
mutua@mutua-intercomarcal.com
www.mutua-intercomarcal.com

MUTUA INTERCOMARCAL

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE UNA PÓLIZA DE SEGURO DE RESPONSABILIDAD CIVIL DE CIBER RIESGOS

1. Objeto del contrato

El presente Pliego de Prescripciones Técnicas tiene por objeto regular la contratación por parte de Mutua Intercomarcal, como tomadora del seguro, de una póliza de ciberriesgo conforme a las garantías, definiciones, capitales y riesgos contenidos en el presente pliego, para cubrir los riesgos derivados de ataques informáticos que puedan afectar a la integridad de la información, la disponibilidad de la misma o a su confidencialidad, cubriendo aspectos de extorsión por cifrado de datos, pérdida de información o divulgación de datos, no disponibilidad y daños reputacionales.

El seguro contendrá, como mínimo, las indicaciones dispuestas en la Ley 50/1980, de Contratos de Seguros, en el reglamento de Ordenación del Seguro Privado y demás disposiciones reglamentarias que regulan este ramo.

El contenido de las coberturas descrito en el presente pliego tendrá carácter de mínimos, pudiendo ser ampliadas por los licitadores en sus ofertas, salvo las exclusiones, que, en ningún caso, podrán ser objeto de ampliación. En caso de duda sobre lo previsto en la póliza que pudiera llegar a emitirse, prevalecerá lo previsto en este pliego.

2. Normativa de carácter técnico

La normativa aplicable de carácter técnico aplicable es la siguiente:

-La ley 50/1980, de 8 de octubre, de Contratos de Seguros y las disposiciones legales que la amplían y/o modifican.

-Ley 20/2015, de 14 de julio, de Ordenación, Supervisión y Solvencia de las Entidades Aseguradoras y Reaseguradoras.

-Real Decreto Legislativo 6/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley de Ordenación y Supervisión de los Seguros Privados y las disposiciones legales que lo amplían y/o modifican.

-Cualquier otra disposición que regule los contratos de Seguros privados.

Esta clasificación normativa no tiene carácter restrictivo, debiendo observarse en la ejecución de los trabajos cualquier otro tipo de reglamento, norma o instrucción oficial (de carácter estatal, autonómico o municipal) que, aunque no se mencione explícitamente en este documento, pueda afectar al objeto del contrato, así como las posibles modificaciones legales que puedan afectar a las normas de aplicación.

3. Descripción del riesgo

La actividad de Mutua Intercomarcal, Mutua Colaboradora con la Seguridad Social número 39 , tiene por objeto colaborar bajo la dirección y tutela del Ministerio de Trabajo y Economía Social, en la gestión de las contingencias de accidentes de trabajo y enfermedades profesionales del personal al servicio de las empresas asociadas a ésta Mutua, así como del resto de coberturas y prestaciones contempladas al amparo de lo dispuesto en el Real Decreto

Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social, la Ley 35/2014, de 26 de diciembre, por la que se modifica el texto refundido de la Ley General de la Seguridad Social en relación con el régimen jurídico de las Mutuas de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social, así como en el Real Decreto 1993/1995, de 7 de diciembre, por el que se aprueba el Reglamento sobre colaboración de las Mutuas de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social.

4. Bases

4.1. Tomador

La Entidad tomadora de la póliza de seguro de ciberriesgos de la presente licitación será MUTUA INTERCOMARCAL.

4.2. Condiciones de ejecución

a) Condiciones de realización del servicio

La empresa adjudicataria de la presente licitación se compromete a prestar el servicio de acuerdo con lo establecido en los pliegos, utilizando para ello los medios personales, mecánicos, informáticos o de cualquier otra naturaleza que considere que mejor garantiza la finalidad perseguida y para la resolución de incidencias que surjan durante la ejecución del contrato. Los medios utilizados para la prestación del servicio serán por cuenta de la adjudicataria.

La empresa adjudicataria ofrecerá un servicio personalizado según las especificaciones indicadas en el presente pliego. En tal sentido, sin perjuicio de lo establecido en el presente documento, los niveles de servicio exigibles respecto al soporte ante una incidencia de seguridad deberán ser como mínimo:

-Tiempo de devolución de la llamada: 15 minutos.

-Tiempo para responder una llamada directa: 30 segundos.

-Tiempo de respuesta vía chat: 15 segundos desde la propia petición.

-Tiempo de respuesta vía mail: 15 minutos.

b) Gestión de reclamaciones

En caso de reclamación recibida por parte de un asegurado de un evento asegurado o que pueda dar lugar a un evento asegurado en la póliza, el asegurado debe notificar inmediatamente y por escrito al asegurador y/o sus expertos la existencia de esta reclamación.

c) Informes de seguimiento/siniestralidad

La Empresa adjudicataria deberá aportar a MUTUA INTERCOMARCAL anualmente, los datos de siniestralidad del contrato, así como cualquier otra información del desarrollo del contrato

que le sean requeridos. En caso de ser necesario para MUTUA INTERCOMARCAL disponer de esta información en otro momento, la empresa adjudicataria deberá facilitársela.

En el **Anexo I, datos de siniestralidad y de interés** del presente Pliego de Prescripciones Técnicas se reflejan los datos de siniestralidad del seguro objeto de contratación.

4.3. Carácter confidencial de los datos aportados

Toda la información que reciba la empresa adjudicataria con motivo de la celebración de la presente licitación y el posterior contrato, en virtud del cual procederá la ejecución del servicio, será considerado estrictamente confidencial y sólo será utilizada en el marco de la presente contratación. Cualquier información remitida a terceros lo será con autorización previa de MUTUA INTERCOMARCAL y en todo caso de acuerdo con las necesidades del contrato.

No se podrá utilizar ni proporcionar a terceros no interesados datos o información de carácter personal para finalidades distintas a aquellas para las que los datos hubieran sido recogidos, estando por tanto obligadas a poner todos los medios a su alcance para garantizar el carácter confidencial de esta información, así como los resultados obtenidos.

Cualquier infracción en este sentido será calificada como grave y será causa de resolución del contrato, sin perjuicio de las responsabilidades penales o de cualquier otro tipo en que pudieran incurrir.

5. Coberturas

En caso de siniestro cubierto a la entidad aseguradora le corresponderá, sin perjuicio de las especificaciones establecidas para cada cobertura y con los límites indicados, lo siguiente:

- Peritaje del siniestro: emisión de informe del incidente.

- Puesta en marcha: asistencia "in situ" y/o remotamente para la puesta en marcha del sistema afectado.

- Recuperación de datos lógicos de los sistemas de almacenamiento.

- Rescate de datos en caso de robo de información. - Certificación forense: informe técnico forense del siniestro.

- Riesgo reputacional: borrado de apariciones no deseadas.

- Costes de investigación e indagación para identificar el evento asegurado.

- Costes de gestión de requisitos reguladores.

- Costes de defensa legal. La dirección jurídica y la defensa del asegurado en los procedimientos cubiertos por la póliza serán asumidas por la entidad aseguradora, quien designará a los letrados y procuradores que hayan de representar y defender al asegurado.

- Costes de notificación y comunicación.

- Costes de comunicación y notificación a las personas afectadas por la protección de datos de carácter personal.

- Riesgo reputacional: costes de expertos o empresa de relaciones públicas en la gestión de crisis.

5.1. Alteración, pérdida o robatorio de datos

Alcance de cobertura

Por esta cobertura, el asegurador garantiza al asegurado, hasta el límite de la suma indicada para esta garantía en el presente pliego, los costes especificados en la misma cobertura como consecuencia directa de alguno de los siguientes eventos asegurados:

- la pérdida de datos en los sistemas informáticos del asegurado ocasionada directamente por un acto informático doloso, software malicioso o error humano que se produzca en el mismo sistema asegurado; o

- el robo de datos en los sistemas informáticos del asegurado; o

- la denegación de servicios en los sistemas informáticos del asegurado.

Una serie de estos eventos asegurados durante 30 días consecutivos se considera como un solo evento asegurado.

Dentro de esta garantía el asegurador debe asumir, los costes siguientes:

1. Costes de restauración y recreación de los datos perdidos o robados necesarios:

- Para recuperar, restaurar o recrear el software dañado, perdido o destruido.

- Para adquirir licencias de sustitución del software cuyo sistema físico de protección haya resultado dañado, perdido o destruido.

- En caso de que el evento asegurado afecte a un software que ya no esté disponible en el mercado, y en caso de pérdida de las copias informáticas de seguridad aplicables, se garantizan los costes generados por adaptar el nuevo software a las funciones equivalentes que se tenían con el software anterior.

- Para buscar o recopilar datos disponibles en copias informáticas de seguridad (backup), medios electrónicos u otros medios de información, incluyendo la fuente o la documentación original en la que se basaban los datos, o para volver a introducir los datos a mano o por otros medios adecuados a fin de recuperar, restaurar o recrear los datos dañados, perdidos o robados.

La obligación del asegurador para recuperar, restaurar o recrear datos está vigente hasta la fecha en que el asegurador o experto determine que no es posible recuperar, restaurar o recrear los datos.

2. Costes de descontaminación de software malicioso o código maligno informático

- Para descontaminar, limpiar y restaurar datos, copias informáticas de seguridad y medios electrónicos, incluyendo los costes de restauración de los sistemas informáticos del asegurado afectados por el software malicioso o código maligno informático.

3. Costes de investigación e indagación

- Para identificar el origen, circunstancias y limitar el impacto del evento asegurado o evaluar la cuantía de costes y gastos sostenidos respecto a un evento asegurado.

4. Costes de restauración del sistema de control de accesos

- Para restaurar el sistema de control de acceso del sistema informático del asegurado.

- Para restaurar el perímetro de seguridad en torno al sistema informático del asegurado en el estado

anterior al evento asegurado.

- Para recoger cualquier dispositivo de autenticación o token de seguridad revocado.

- Para la creación y/o actualización de las identificaciones y contraseñas.

Exclusiones

Estas exclusiones son adicionales a las exclusiones generales de la póliza:

- Cualquier pérdida como resultado de cualquier mejora, rediseño o reconfiguración de los sistemas informáticos o datos del asegurado para introducirlos en el sistema y que comporte una mejora de los sistemas del asegurado respecto a cómo funcionaban estos sistemas en el momento anterior que se produjera el evento asegurado.

- Sustitución, reemplazo o reparación de equipos de hardware y/o periféricos.

- Datos cuya fuente original no exista.

- Quedan excluidas las recuperaciones de datos que sean consecuencia de:

· Manipulación por personal no profesional.

· Incendios.

· Perdida de pistas (sobre escrituras de configuración interna del disco)

· Sobre escrituras de información (p.ej. formateo y reinstalación).

. Impactos

. Daños físicos a la superficie magnética (head crash)

- Asimismo, quedan excluidos las averías del dispositivo de soporte.

5.2. Violación de la privacidad

Alcance de cobertura

Por esta cobertura, el asegurador garantiza al asegurado, hasta el límite de la suma indicada en este pliego, los costes especificados en la misma cobertura como consecuencia directa de alguno de los siguientes eventos asegurados:

- la pérdida de datos de carácter personal confiados al cuidado, custodia y control del asegurado en los sistemas informáticos del asegurado ocasionados directamente por un acto informático doloso, software malicioso o error humano que se produzca en el mismo sistema informático del asegurado, o

- el robo o revelación a terceros no autorizados, de datos de carácter personal confiados a la cuidado, custodia y control del asegurado en medios electrónicos o en los sistemas informáticos del asegurado.

Una serie de estos eventos asegurados durante 30 días consecutivos se considera como un solo evento asegurado. Dentro de esta garantía el asegurador asumirá, a través del experto por este designado, los costes siguientes:

1. Costes de investigación e indagación

- Para identificar el origen y las circunstancias de un evento asegurado, cuando forme parte de uno procedimiento regulatorio relacionado con la protección de datos de carácter personal.

2. Costes de gestión de requisitos regulatorios

- En la gestión e interacción de procedimientos con las autoridades regulatorias y/o para acciones exigidas en un procedimiento regulatorio en relación a la protección de datos de carácter personal.

3. Costes de defensa legal

- En concepto de defensa legal cuando una autoridad reguladora lleve a cabo un procedimiento regulatorio contra el asegurado a causa de la violación de datos de carácter personal.

4. Costes de notificación y comunicación

5. Cualquier coste razonable y necesario incurrido por el asegurado para comunicar y notificar, a las personas afectadas, de forma coherente con la legislación de protección de datos sobre la violación de datos de carácter personal. Multas administrativas

6. Modificando el punto número 18 de las exclusiones generales de la póliza, se cubre cualquier sanción o multa legalmente impuesta al asegurado por la autoridad reguladora por el incumplimiento de la legislación de protección de datos personales, y se excluye cualquier multa o sanción impuesta en relación con cualquiera otra medida cautelar.

5.3. Extorsión cibernética

Alcance de cobertura

Por esta cobertura, el asegurador garantiza al asegurado, hasta el límite de la suma indicada para esta garantía en el presente pliego, cualquier extorsión cibernética real, creíble, inminente y verificable creada por un extorsionador, que amenaza con:

- La pérdida de datos confiados al cuidado, custodia y control del asegurado en los sistemas informáticos del asegurado resultante directamente de un acto informático doloso o software malicioso.

- El robo o la revelación a terceros no autorizados de datos confiados al cuidado, custodia y control de el asegurado en medios electrónicos, en los sistemas informáticos del asegurado.

- La denegación de servicios en los sistemas informáticos del asegurado.

Dentro de esta garantía el asegurador asumirá, a través del experto por este designado, los costes siguientes:

1. Costes por honorarios de expertos:

   - Para consultar la forma de proceder ante la misma extorsión cibernética sufrida.

   - Para evitar, mitigar o reducir las consecuencias perjudiciales de la extorsión cibernética.

   Asimismo, deben indemnizarse, sujeto a la autorización previa por escrito por el asegurador, los:

2. Costes adicionales en los que pueda incurrir el asegurado siempre que éstos sean asegurables por ley.

Obligaciones del asegurado

El asegurado se obliga a dar aviso inmediatamente por escrito tanto al asegurador como a la policía o a cualquier autoridad responsable del cumplimiento de la ley o autorizar al asegurador o alguno de sus representantes, a hacer el mismo aviso de cualquier extorsión cibernética sufrida. En caso de no comunicarlo en el asegurador, el asegurado pierde todos los derechos que nazcan de la póliza.

El asegurado garantiza que se mantiene la confidencialidad respecto a la existencia del seguro y de esta cobertura de extorsión cibernética, de lo contrario, el asegurador puede denegar la cobertura y dar por terminado el seguro y la cobertura de esta garantía con efecto inmediato, efectivo desde la fecha en que se haya realizado de dominio público o se haya revelado a un tercero.

Exclusiones

Estas exclusiones son adicionales a las exclusiones generales de la póliza:

- Toda extorsión perpetrada por cualquier entidad gubernamental o autoridad pública.

- Cualquier extorsión o acto voluntario, deliberado, malicioso, fraudulento o deshonesto cometido por un directivo, accionista, empleado del asegurado y/o cualquier otra persona o entidad autorizada en acceder a los sistemas informáticos del asegurado.

5.4. Responsabilidad civil contra la violación de la confidencialidad

Alcance de cobertura

Por esta cobertura, el asegurador garantiza al asegurado, hasta el límite de la suma fijada para esta garantía en las condiciones del presente pliego, los perjuicios ocasionados a terceros, de los que esté obligado legalmente a responder como consecuencia directa de las reclamaciones derivadas de alguno de los siguientes eventos asegurados: la pérdida de información confidencial confiada a la cuidado, custodia y control del asegurado en el sistema informático del asegurado causado directamente por un acto informático doloso, software malicioso o error humano; o

- El robo o revelación a terceros no autorizados de información confidencial confiada al cuidado, custodia y control del asegurado en medios electrónicos, medios de información o en los sistemas informáticos del asegurado.

- Una serie de estos eventos asegurados durante 30 días consecutivos se considera como un solo evento asegurado.

- Dentro de esta garantía el asegurador debe indemnizar:

· El abono a los perjudicados oa sus derechohabientes de las indemnizaciones a que dé lugar la responsabilidad civil del asegurado.

· Los gastos de defensa y pago de las costas y gastos judiciales o extrajudiciales inherentes al siniestro.

· La constitución de las fianzas judiciales exigidas al asegurado para garantizar su responsabilidad civil.

Exclusiones

Estas exclusiones son adicionales a las exclusiones generales de la póliza:

- Cualquier reclamación relacionada con la real o supuesta descripción inexacta, inadecuada o incompleta del precio de los bienes, productos o servicios, así como toda garantía de costes, representaciones de costes o cálculos de precios contractuales, la autenticidad de cualquier bien, producto o servicio, o la falta de conformidad de cualquier bien o servicio respecto a cualquier calidad declarada o a estándares de prestación.

- Cualquier reclamación relacionada con errores cometidos en cualquier dato financiero publicado por el asegurado, incluidos, pero no limitados al informe anual del asegurado y cuentas y cualquiera comunicación transmitida al mercado de valores.

- Cualquier reclamación relacionada con no haber retirado por parte del asegurado, publicaciones de una página de Internet después de haber recibido una queja o notificación por parte de un tercero relacionada con la publicación.

- Cualquier reclamación relacionada con cualquier publicación efectuada en cualquier página web o cuyo contenido pueda publicar cualquier persona sin registrarse, o cualquier página web o contenido que no esté directamente controlado por el asegurado.

- Cualquier reclamación relacionada con descuentos, servicios de créditos, rebajas, reducciones de precios, cupones, premios, distinciones u otro tipo de incentivos, contractuales, o no, promocionales o alicientes ofrecidos a clientes del asegurado.

- Cualquier reclamación relacionada con pagos de intereses, cargos bancarios por descubiertos y indemnizaciones por ejecuciones tardías.

5.5. Responsabilidad civil por seguridad en la red

Alcance de cobertura

Por esta cobertura, el asegurador garantiza al asegurado, hasta el límite de la suma pactada para esta garantía a las condiciones particulares de la póliza, cuyos perjuicios ocasionados a terceros esté obligado legalmente a responder como consecuencia directa de las reclamaciones derivadas de alguno de los siguientes eventos asegurados: la pérdida de datos en un sistema informático de terceros; o

- El robo de datos perpetrado en el sistema informático de terceros; o

- La denegación de servicios en el sistema informático de terceros que resulte directamente de un acto informático doloso o un software malicioso que se produzca en el mismo sistema informático del asegurado a causa del fallo o violación del entorno de seguridad del sistema del asegurado.

Dentro de esta garantía el asegurador debe indemnizar:

- El abono a los perjudicados o a sus derechohabientes de las indemnizaciones a que dé lugar la responsabilidad civil del asegurado.

- Los gastos de defensa y pago de las costas y gastos judiciales o extrajudiciales inherentes al siniestro, con excepción de las que ampara la sección I de esta póliza.

- La constitución de las fianzas judiciales exigidas al asegurado para garantizar su responsabilidad civil.

Exclusiones

Estas exclusiones son adicionales a las exclusiones generales de la póliza:

- Cualquier reclamación relacionada con descuentos, servicios de créditos, rebajas, reducciones de precio, cupones, premios, distinciones u otros tipos de incentivos, contractuales o no, promociones o alicientes ofrecidos por terceros.

- Cualquier reclamación presentada por un proveedor de servicios de TI prestados al asegurado.

- Cualquier reclamación relacionada con pagos de intereses, cargos bancarios por descubiertos y indemnizaciones por ejecuciones tardías.

5.6. Servicios en línea

El asegurado podrá acceder a la prestación de este servicio a través de una página web a disponer por el adjudicatario así como también telefónicamente sin perjuicio de otros medios puestos a disposición por el adjudicatario.

Estos servicios en línea deben permitir al asegurado ponerse en contacto con un técnico para obtener los servicios preventivos de ayuda ante cuestiones relacionadas con la seguridad de sus sistemas informáticos, el parcheo de posibles vulnerabilidades y la configuración segura del sistema, así como la resolución de dudas que tenga relativos al uso del equipo informático profesional y de las herramientas de uso más frecuente.

Generalmente, la forma de prestación de este servicio es por teléfono o chat online; el técnico puede tomar el control remoto de los equipos del asegurado cuando sea necesario. De este modo, un técnico previamente autorizado por el asegurado y siempre bajo su supervisión puede acceder remotamente a los equipos para atender la consulta o incidencia planteada. En los casos en que el asegurado no disponga de conexión a Internet o lo prefiera de esta forma, la asistencia se hará vía telefónica.

Alcance de cobertura

Los servicios online deben estar dispuestos para que el asegurado reciba soporte preventivo sobre la seguridad de sus sistemas, tanto por la propia empresa como en el hogar de sus trabajadores (en la medida en que éstos desarrollen su actividad profesional por cuenta de la empresa en régimen de teletrabajo), actualizaciones o parches sobre los siguientes sistemas y aplicaciones:

- Las vulnerabilidades detectadas en el análisis previo independientemente de sistema operativo o aplicaciones que utilice el asegurado.

- Verificación y configuración del antivirus.

- Verificación y configuración del firewall, software antiespía y software malicioso de sistema.
- Configuración segura de la red wifi del asegurado.

- Configuración de smartphones y periféricos (discos duros externos, cámaras web, etc.). - Soporte sobre aplicaciones de ofimática como Microsoft Office, Apple iWork, Acrobat y otros de uso habitual.

- Soporte sobre navegadores de internet, entre otros: Internet Explorer, Google Chrome, MozillaFirefox, Safari, Opera, etc.

- Configuración y soporte sobre cuentas de correo electrónico: Gmail, Outlook, Yahoo Mail, etc.

- Instalación de códecs necesarios para visualización en los programas multimedia.

- Compresores, entre otros: WinZIP, WinRAR.

5.7. Servicios de Seguridad y mantenimiento

Los Servicios de Seguridad de la póliza que se genere también deben ofrecer el asegurado y sus teletrabajadores, en los puntos en que resulte procedente que lo solicite los siguientes servicios:

- Revisión del sistema informático del asegurado. El asegurado puede contactar con el servicio técnico en cualquier momento para solicitar un análisis de vulnerabilidades internas, que consiste en escanear las vulnerabilidades de la red interna del sistema del asegurado, así como detectar y eliminar software malicioso, archivos temporales y servicios que ralentizan o ponen en peligro las datos o el funcionamiento de los ordenadores propiedad del asegurado cubiertos por la póliza.

- Tiene acceso al servicio de análisis de vulnerabilidades externas de la IP pública de la empresa asegurada y de la página web corporativa propiedad del asegurado, previa autorización.

- Dispone de un técnico de soporte remoto para corregir y parchear las vulnerabilidades detectadas.

- Se debe instalar una aplicación antisecuestro de información o antiransomware en los ordenadores cubiertos por la póliza para prevenir los secuestros de información.

- Recuperación de datos de discos duros o sistemas de almacenamiento de equipos tecnológicos cubiertos por la póliza que se vean afectados por rotura, secuestros de información, virus y/o software malicioso.

- Aplicación de geolocalización de smartphones, tabletas táctiles o portátiles para localizar o bloquear el dispositivo en caso de pérdida o robo. Es necesario que el asegurado active previamente este servicio con el equipo técnico para que el dispositivo quede protegido.

- Configuración de un sistema de backup online para mantener una copia de seguridad en la nube de los datos más relevantes, con una capacidad mínima de 512 GB, para disponer de los datos en caso de incidente de seguridad, pérdida o secuestro de información.

- Asesoramiento y soporte en la compra y postventa de productos tecnológicos.

- Consultas relacionadas con la seguridad del uso de internet: compras, certificados digitales, seguridad, almacenamiento en nube, etc.

- Borramiento de la huella digital, es decir, el borrado de la información pública en internet que afecte a la reputación de la marca/empresa, tanto de los buscadores como de las redes sociales y la prensa escrita.

- Ayuda en la configuración segura de los dispositivos de la empresa asegurada.

- Resolución de problemas relacionados con la seguridad de los dispositivos y aplicaciones.

Características del servicio

El Servicio en línea será aplicable a los dispositivos con las siguientes características: - Ordenadores de trabajo (PC, Mac, portátiles), periféricos (impresoras, escáneres, dispositivos de almacenamiento, etc), servidores y dispositivos móviles que formen parte del funcionamiento habitual del riesgo.

- Sistemas operativos: Windows 7/8/10/11, MAC OS X o superior, IOS 8/9/10r, Android 4/5/6/7 y Windows Server 2008/2012/ o superiores.

Exclusiones

- Este servicio no incluye el soporte a aplicaciones no estándar desarrolladas específicamente por al asegurado.

- El soporte y/o las actualizaciones del software utilizado por el asegurado que no disponga de las licencias necesarias en vigor.

- El asegurador no se hace responsable de la pérdida de información o los daños en los sistemas informáticos del asegurado como consecuencia de las actuaciones en equipos que contengan o estén infectados por virus, software malicioso, software espía o cualquier otro programa, aplicación, software o hardware que esté instalado en su ordenador teniendo conocimiento o no y que se comporte de forma maliciosa.

- Las vulneraciones de datos que no están custodiadas por el asegurado, tales como datos entregados y custodiadas por un servicio de informática en nube (cloud computing) o datos o páginas web alojadas en servidores de un tercero (servicio de hosting).

- Queda expresamente excluida la instalación de elementos de hardware si esta instalación no tiene el origen en una avería cubierta por la póliza.

- Este servicio no incluye la asistencia técnica "in situ" en el domicilio del asegurado.

6. Definiciones

Tomador del seguro: Mutua Intercomarcal, Mutua Colaboradora con la Seguridad Social n.39.

Asegurado: El tomador y sus sociedades filiales.

Asegurador: Entidad aseguradora que asume los riesgos pactados contractualmente.

Beneficiario: La persona física o jurídica que resulte titular del derecho a la indemnización.

Tercero: Cualquier persona o corporación distinta del asegurado, del representante legal del asegurado o de cualquier empleado del asegurado.

Cliente: Cualquier persona natural o entidad corporativa que solicite o compre bienes o servicios al asegurado.

Empleado: Cualquier persona natural que preste servicio o aporte trabajo al servicio y en las instalaciones del asegurado en virtud de un contrato de empleo expreso o implícito, por el que el asegurado o sus representantes legales tengan derecho a controlar los detalles de su prestación laboral. Esto engloba también el personal externo contratado por el asegurado para prestar servicios de TI trabajando dentro de la estructura operacional y bajo la autoridad funcional del asegurado. Esta definición no incluye a los representantes legales.

Expertos: Cualquier persona poseedora de un alto grado de pericia y/o conocimiento de un tema determinado, incluyendo, pero no limitándose, especialistas en TI, abogados, consultores o auditores.

Representante legal: Cualquier ejecutivo, director, miembro del equipo directivo pasado, presente o futuro del asegurado y cualquier otra persona de la plantilla del asegurado dotada de un alto grado de responsabilidad y autoridad decisoria, que tenga el derecho de representar al asegurado y actuar en su nombre.

Póliza: El documento que contiene las condiciones reguladoras del seguro. Forman parte integrante de la póliza: las condiciones generales; las particulares que individualizan el riesgo; las especiales, en su caso, y los suplementos o apéndices que se emitan para complementarla o modificarla. En cualquier caso forman parte de la póliza los presentes pliegos y demás documentación integrante de la licitación de referencia

Límite máximo de indemnización: La cantidad fijada por el tomador en cada una de las partidas que constituye el límite máximo de indemnización que debe pagar el asegurador por todos los conceptos en caso de siniestro. El límite máximo de indemnización que consta en los presentes pliegos es el límite máximo de indemnización por siniestro y por período de seguro, por lo que, en caso de siniestro indemnizable, el límite máximo de indemnización irá disminuyendo en igual medida que los siniestros indemnizados.

Evento: El conjunto de pérdidas o daños total o parcialmente indemnizables por la póliza, derivados de una misma causa no excluida, ocurrida dentro del período de vigencia de ésta.

Franquicia: La cantidad expresamente pactada, ya sea en cuantía monetaria o en período de espera, que se deduce de la indemnización que corresponda en cada siniestro.

Prima: El precio del seguro. El recibo debe contener, además, los recargos e impuestos que sean de aplicación legal.

Actos de terrorismo :Cualquier acto y/o amenaza por parte de cualquier persona o grupo/s de personas, que actúan en solitario o por encargo de o en conexión con cualquier organización/es o gobierno/s por medio del uso de sistemas informáticos, que ocasione un evento asegurado en los sistemas informáticos del asegurado, cometidos con fines políticos, religiosos, ideológicos o similares, incluida la intención de influir en cualquiera gobierno y/o provocar temor en la población o en una parte de ésta.

Acto informático doloso: Todo acto indebido llevado a cabo con la intención de causar daño o conseguir acceso ilegítimo a datos, sistemas o redes informáticos mediante el uso de cualquier sistema o red informáticos.

Archivos digitales: Cualquier almacenamiento digital a largo plazo controlado y fiable que utilice determinados procesos, políticas, medios electrónicos y software para almacenar datos y conservarlos a largo plazo, que ofrezca protección, seguridad, autenticidad y disponibilidad de los datos y defina y controle el acceso a estos datos.

Informática en nube: Cualquier servicio basado en una red informática, incluyendo pero no limitándose servidores, almacenamiento de datos y aplicaciones entregadas por ordenadores y dispositivos de un tercero a través de internet o provistas por equipos físicos (hardware) de servidor virtual y simulados por software procesado por uno o varios dispositivos reales.

Copia informática de seguridad (backup): Copia física de un archivo individual de datos o de un juego completo de archivos de datos en un medio electrónico que permite almacenar los datos en un sitio diferente y restaurarlo en un sistema informático.

Coste de defensa legal: Todos los costes, gastos y honorarios que deben pagarse a expertos, abogados y profesionales por la comparecencia ante tribunales, investigación, verificación y/o procedimientos necesarios para la defensa del asegurado en los sectores civil, comercial, administrativo y/o criminal.

Pérdida de datos: Cualquier introducción, corrupción, modificación, alteración o eliminación de datos que, al procesarlos en el sistema informático del asegurado, podrían tener como consecuencia el funcionamiento deteriorado, degradado o anómalo de los sistemas informáticos y/o la interrupción o alteraciones de las operaciones de procesamiento de datos.

Datos: Cualquier información legible, independientemente de la modalidad de uso o presentación (texto, cifras, voz o imágenes), incluido el software, transmitida o almacenada en formato digital fuera de la memoria de acceso aleatorio (RAM) propiedad del asegurado u operada por éste. El término datos también engloba el de archivos digitales.

Denegación de servicios: Cualquier ataque doloso del que resulte la privación total o parcial, la alteración y/o la falta de disponibilidad de sistemas informáticos o instalaciones de redes, incluida la alteración o destrucción del software correspondiente, mediante un alud de datos que sobrecargan sistemas informáticos con un flujo entrando de solicitudes, incluidos ataques por denegación repartida de servicios, utilizando una multitud de sistemas involucrados para coordinar un ataque simultáneo.

Proveedor de servicios: Cualquier proveedor de servicios de TI elegido por el asegurado, mediante contrato expreso por escrito, por ofrecer funciones o servicios de gestión, mantenimiento y/o desarrollo en beneficio del asegurado en un sistema informático controlado y gestionado por el proveedor de servicios de TI.

Servicios de TI: Cualquier prestación de servicios ofrecidos por un proveedor de TI, basado en el uso de tecnología de la información y en el procesamiento de datos.

Error de programación: Error ocurrido durante el desarrollo o la codificación de un software o de un sistema operativo que podría dar lugar, una vez esté operando, a un mal funcionamiento del sistema informático y/o en la interrupción de la operación y/o un resultado equivocado.

Error humano: Cualquier error de operación TI cometido por negligencia o involuntariamente, incluido un error en la elección del software a utilizar, un error de configuración o cualquier otra operación indebida llevada a término por un empleado del asegurado.

Equipos físicos: Los componentes físicos de cualquier sistema informático o dispositivo utilizado para almacenar, procesar, leer, modificar o controlar datos, incluidos medios electrónicos y dispositivos móviles de telecomunicación utilizados para transmitir y almacenar datos.

Guerra: Cualquier situación de conflicto (ya sea declarado o no) con uso de fuerzas armadas y/o de violencia por resolver una cuestión litigiosa entre dos o más estados o naciones, incluidos actos bélicos tales como invasión, insurrección, revolución o golpe militar.

Plan de reacción frente a incidencias: Cualquier incidente o plan de reacción por emergencia para afrontar y gestionar los eventos asegurados, las secuelas de una violación de seguridad TI o ataque (también conocido como incidente) y que configura el conjunto de acciones que deben ponerse en marcha después de un evento adverso que afecte a un sistema informático a una red informática de la empresa. El objetivo de un plan de reacción ante un incidente consiste en controlar la situación de forma que se limite el daño y se reduzcan el tiempo y los costes de recuperación.

Información confidencial: Toda actividad comercial sensible y cualquier información de secreto comercial de cualquier naturaleza y cualquier forma que no sea de dominio público, tanto si está marcada o estampillada como confidencial como si no.

Propiedad intelectual: Cualquier derecho que proteja la propiedad intangible, tales como productos de inteligencia y de la creatividad humana, patentes, ideas, marcas comerciales, copyrights, secretos de fabricación y secretos comerciales.

Datos de carácter personal: Cualquier información personal utilizable directa o indirectamente, por sí misma o en conexión con otra información, para identificar, contactar o localizar a una sola persona o para identificar un individuo en un contexto, incluyendo pero no limitándose a cualquier apellido paterno, el número de Seguridad Social, información médica o información protegida relativa a la seguridad, el permiso de conducir, el número de identidad fiscal, el número de tarjeta de crédito o de débito, la dirección o el número de teléfono, la referencia de

la cuenta individual o contraseña y cualquier otra identificación personal, de acuerdo con lo especificado en la legislación de protección de datos de carácter personal.

Infraestructura: Cualquier equipo telefónico, aire acondicionado, instalaciones de abastecimiento ininterrumpido de corriente, generadores independientes, unidades de inversión de frecuencia, transformadores y otras instalaciones utilizadas para el mantenimiento y funcionamiento de las instalaciones electrónicas que apoyan la operación de los sistemas informáticos y de datos.

Internet: La red pública mundial de datos que permite la transmisión de datos, incluidas intranets y redes virtuales privadas.

Intranet: La red interna de datos de una persona o entidad local privada o de acceso restringido, conectada para sus actividades privadas y destinada a ser utilizada única y exclusivamente por los empleados y determinados socios de negocio de la actividad.

Malware o software malicioso: Cualquier software hostil o intruso, incluidos virus informáticos, programas espía, gusanos, troyanos, rootkits, software de secuestro, keyloggers, dialers, adware, objetos maliciosos de ayuda del explorador y software de seguridad fraudulento, diseñados para infiltrarse en ordenadores e interrumpir las operaciones, recopilar información sensible o acceder a sistemas informáticos sin autorización.

Medios de información: Cualquier medio impreso, como diarios, cartas de información, revistas, libros y obras literarias de cualquier formato, folletos y publicaciones de todo tipo, y medios publicitarios, incluidos envoltorios, fotos y impresiones digitales.

Medios electrónicos Cualquier dispositivo de tratamiento de la información (incluyendo pero no limitándose a discos duros internos o externos, CD-ROM, DVD, cintas o discos magnéticos, lápices USB) utilizado para procesar, almacenar o registrar los datos.

Sistemas informáticos: Sistemas de tecnología de la información y la comunicación, infraestructura, software o equipamiento utilizado con fines de creación, acceso, procesamiento, protección, recuperación, visualización o transmisión de datos.

Sistemas informáticos externalizados: Sistemas informáticos controlados y gestionados por el proveedor de servicios externalizados, que sean de propiedad o estén concedidos bajo licencia o alquilados por el proveedor de servicios externalizados o por el asegurado.

Sistemas informáticos del asegurado: Sistemas informáticos controlados y gestionados por el asegurado, de su propiedad, bajo licencia o alquilados por el asegurado.

Programario: Cualquier programa digital estándar, personalizado o desarrollado individualmente, o una aplicación mantenida o procesada en un sistema informático, que comprende un conjunto de instrucciones capaces, una vez incorporadas a un medio legible por máquina, que hacer que un aparato con capacidad de procesamiento de información indique, lleve a cabo o consiga una determinada tarea o función.

Token de seguridad: Cualquier dispositivo tangible de acceso y verificación de identidad utilizado para autorizar el acceso a sistemas informáticos por medio de un número de identificación personal (PIN, por sus siglas en inglés).

Uso no autorizado: Todo uso ilegítimo de sistemas informáticos.

Virus informáticos: Software intruso u hostil o pieza de código capaz de crear réplicas de sí mismo (programas autoreplicantes) una vez integrados en otro software o en zonas interiores de sistema o que puede difundir copias de sí mismo o partes de sí mismo enviándolas a otro sistema informático. Un gusano informático es similar a un virus informático.

Reclamación: Cualquier procedimiento judicial o administrativo o una notificación escrita, comunicados por primera vez durante el período de cobertura de la póliza, por un tercero contra el asegurado o asegurador en el ejercicio de la acción directa como presunto responsable de un perjuicio amparado por la póliza.

Perjuicio: La pérdida económica como consecuencia directa de los eventos asegurados por la póliza que haya sufrido un tercero.

Red informática: Grupo de sistemas informáticos y otros dispositivos de hardware digital conectados por medio de tecnología de comunicación, que permiten que las redes de dispositivos digitales intercambien datos y otros recursos, entre ellos conexión de datos, internet, intranet o redes privadas virtuales.

Robo: Cualquier acto informático doloso de copia ilegítima o para extraer, por ejemplo, información confidencial, datos o datos de carácter personal de sistemas informáticos.

Terrorismo cibernético: Cualquier acto o series de actos de amenaza de cualquier persona o grupo de personas, ya sea actuando en solitario o en nombre de cualquier organización o en conexión con la misma mediante el uso de sistemas informáticos para destruir, perturbar o socavar sistemas informáticos, redes informáticas, infraestructuras, internet, intranet, telecomunicaciones y/o su contenido con la intención de causar daño o por razones religiosas, políticas o ideológicas, incluyendo, pero no limitándose a ello, la influencia en cualquier gobierno y/o causar miedo en la población o en una parte de ésta.

Sistema de control de accesos: Cualquier regla, derecho y privilegio requerido para el acceso legítimo a los sistemas informáticos del asegurado.

Autoridades reguladoras: Autoridad protectora, organización gubernamental u organismo estatutario en cualquier jurisdicción, autorizado para imponer obligaciones legales relativas al tratamiento o al control de la información personal de identificación.

Procedimiento regulador: Todo modo de proceder relativa a leyes formales o estatutos impuestos por la Agencia Española de Protección de datos.

Extorsión cibernética: Cualquier uso ilegal e intencionado de una amenaza dirigida por un extorsionador contra los datos de un sistema informático del asegurado o contra los sistemas

informáticos del asegurado para obtener un rescate por extorsión cibernética pagado por el asegurado a base de coerción.

Extorsionador: Cualquier tercero que cometa o instigue una extorsión cibernética o sea cómplice.

Informador: Persona que de forma secreta proporciona información sobre actividades delictivas a las autoridades policiales.

Rescate por extorsión cibernética: Cualquier cantidad de dinero, en efectivo o de otra forma, fondos o propiedades, así como bienes, productos y/o servicios que el asegurado se vea forzado a pagar o entregar al extorsionador.

Entorno de seguridad del asegurado: Medidas adoptadas y recursos utilizados por el asegurado para proteger y asegurar sus sistemas informáticos, en particular contra actos informáticos dolosos, robo de datos o información, uso no autorizado de los sistemas, software malicioso y virus informático.

7. Exclusiones

Quedan excluidas de indemnización de la póliza que derive de la presente licitación cualquier pérdida o reclamación resultante del siguiente:

1. Cualquier acto de terrorismo generado a excepción del terrorismo cibernético.

2. Guerra, guerra y operación cibernéticas. Se excluye de este contrato cualquiera:

- Pérdida, daño, responsabilidad, coste o gasto de cualquier naturaleza (en conjunto, "pérdida") causado directa o indirectamente por, contribuido por, resultante de, que surja o esté relacionado con una guerra o una operación cibernética.

A efectos de esta exclusión, se entiende por:

· Guerra: conflicto bélico que implique fuerza física (1) por un Estado soberano contra otro Estado soberano, o (2) como parte de una guerra civil, rebelión, revolución, insurrección, poder militar o usurpado, así como la incautación, la nacionalización, la requisa o la destrucción de o daños a la propiedad por o bajo el orden de cualquier gobierno o gobierno público o autoridad local; sea guerra declarada o no.

· Operación Cibernética: uso de un sistema informático por parte de la dirección o bajo la dirección o el control de un estado soberano por (1) interrumpir, negar el acceso a, o degradar la funcionalidad de un sistema informático, y/o (2) copiar, eliminar, manipular, negar el acceso a, o destruir información en un sistema informático.

Sin perjuicio de la carga de la prueba, la cual permanecerá inalterada por esta cláusula, el tomador y el asegurado deben tener en cuenta cualquier prueba disponible y objetivamente razonable para determinar la atribución de una operación cibernética a un estado soberano. Esto puede incluir la atribución formal u oficial por parte del gobierno del estado soberano (incluidos sus servicios de inteligencia y seguridad), en el que se encuentran físicamente los

sistemas informáticos afectados por la operación cibernética, a otro estado soberano o aquéllos que actúen bajo su dirección o control.

3. Cualquier huelga legal o ilegal o conflicto laboral de cualquier tipo, revuelta o disturbio civil.

4. Reacción o radiación nuclear y/o contaminación radioactiva.

5. Cualquier dispositivo que sirva para llevar a cabo fisión o fusión nuclear y/o reacciones similares o fuerza o materia radioactiva.

6. Armas químicas, biológicas, bioquímicas o electromagnéticas.

7. Mohos, hongos, esporas u otros microorganismos de cualquier tipo, naturaleza o descripción.

8. Retirada de amianto, dioxina o bifenilos policlorados.

9. Descarga, dispersión, vertido, migración, alivio o escape de sustancias peligrosas, contaminantes o poluentes de cualquier procedencia.

10. Dolo o culpa grave, comportamiento imprudente o malintencionado, conducta indebida o fraude, ya sea por omisión o por comisión del asegurado.

11. Incendio, impacto de rayo, descarga electromagnética, explosión, vendaval, granizada, inundación, daños causados por el agua, congelación, caída de objetos, peso de la nieve, hielo o aguanieve, actividad volcánica, terremotos, hundimientos, humo, aeronaves o vehículos.

12. Embargo, requisición, incautación, destrucción, daños o pérdida del sistema informático o de datos del asegurado resultantes de la aplicación de cualquier reglamento de aduanas o de cuarentena o por orden de cualquier gobierno legítimo o "de facto" o de cualquier autoridad civil o militar.

13. Uso de software ilegal o sin licencia.

14. Fallo, defecto, error u omisión en el diseño, planificación, especificación, material o mano de obra en la configuración inicial de los sistemas informáticos del asegurado de tal forma que resulten mal dimensionados para uso previsto.

15. Desgaste, disminución del rendimiento u obsolescencia de equipos electrónicos o de otros equipos utilizados por el asegurado resultante de la operación normal o del deterioro progresivo que habitualmente deberían estar cubiertas por un contrato de mantenimiento completo.

16. Llamamiento para la retirada de productos en el mercado.

17. Penalizaciones, multas o sanciones de carácter civil o penal no asegurables por ley, incluidas las fianzas que se impongan a consecuencia de éstas, a excepción de las sanciones impuestas por la Agencia Española de Protección de Datos.

18. Cualquier pérdida sufrida en el mercado financiero o en el mercado comercial, así como en la realización de transacciones financieras de fondos, dinero, valores o instrumentos negociables para o provenientes de cualquier banco o institución financiera.

19. Deuda, insolvencia, problemas financieros del asegurado o de terceros.

20. Cumplimiento de cualquier ley gubernamental, ordenanza, regulación o reglamento que regule o restrinja la construcción, la instalación, la reparación, la sustitución, el desmantelamiento, el empleo, la operación o cualquier otro uso del sistema informático del asegurado o del proveedor externo contratado por el propio asegurado, encargado de efectuar el mantenimiento o la gestión de sistema informático.

21. Tiempo de paralización planeados, cortes planeados o períodos de inactividad de sistemas informáticos o de una parte de éstos, incluyendo, pero no limitándose al cese de la producción, la operación, el servicio, entrega o recepción de bienes, que no hayan tenido lugar o se habrían podido evitar con un evento asegurado o sin él.

22. Suspensión, cancelación o caducidad de cualquier contrato, licencia o pedido cursado por clientes del asegurado, asegurado o proveedor de servicios externos.

23. Lesión corporal, daño psicológico, aflicción emocional, angustia, trauma, enfermedad, queja o muerte sufrida por una persona.

24. Robo, violación, revelación o infracción de cualquier propiedad intelectual. Espionaje real o supuesto.

25. Rescate o suma económica de extorsión exigida.

26. Fallo o interrupción ocasionado en el acceso a la infraestructura de un tercero oa la del proveedor del servicio, incluyendo telecomunicaciones, servicios de internet, satélite, cable, electricidad, gas, agua o otros proveedores públicos.

27. Error humano cometido por el proveedor de servicios externos o cualquier fallo, error u omisión generado por un tercero contratado por el propio proveedor de servicios externos.

28. Cualquier responsabilidad contractual que exceda la propia responsabilidad legal.

29. Daños materiales y personales. 30. Cualquier coste incurrido directamente por el asegurado en concepto de los trabajos efectuados por expertos designados por él.

31. La cobertura de cualquier evento asegurado ocurrido durante la prestación de servicios de TI concedidos por contrato a los proveedores de servicios externalizados.

32. Se excluyen de este contrato todos los daños y perjuicios, las responsabilidades, las reclamaciones, los costes o gastos de cualquier naturaleza que, de forma directa o indirecta, hayan sido causados por una enfermedad contagiosa, o que resulten o se deriven de una enfermedad contagiosa o que estén en ella relacionados, o del temor o de la amenaza (real o percibido) de una enfermedad contagiosa, independientemente de que cualquier otra causa o hecho cubierto por las pólizas en cuestión que haya contribuido de modo concurrente o

secuencial quedará cubierto en los términos de este contrato de seguro. Se entiende por enfermedad contagiosa cualquier enfermedad que puede transmitirse de un organismo a otro por medio de cualquier sustancia o agente cuando:

- La sustancia o agente sea, sin carácter limitativo, un virus, bacteria, parásito u otro organismo o cualquier variación de éste, tanto si se le considera vivo como si no; y

- El método de transmisión, directo o indirecto, incluya, sin carácter limitativo, la transmisión por vía aérea, la transmisión por fluidos corporales, la transmisión por o en cualquier superficie o objeto, ya sea sólido, líquido o gaseoso, o entre organismos; y

- La enfermedad, sustancia o agente pueda ser causa o amenaza de daños a la salud o al bienestar de las personas o pueda ser causa o amenaza de daños, deterioro o pérdida de valor, comerciabilidad o uso de bienes, y

- La enfermedad se enmarque en el contexto de una epidemia o pandemia, declarada como tal por la Organización Mundial de la Salud o cualquier autoridad gubernamental o sanitaria del lugar donde se haya producido el siniestro.

8. Ámbito Geográfico

La cobertura deberá amparar reclamaciones en TODO EL MUNDO.

9. Delimitación temporal

Reclamaciones presentadas contra el Asegurado por primera vez durante la vigencia de la póliza, con retroactividad ilimitada.

10. Capitales asegurados, límites de indemnización y franquicias

10. Capitales asegurados, límites de indemnización y franquicias

Las condiciones económicas y de cobertura mínimas exigidas en la presente licitación son las que se detallan a continuación. Cualquier oferta que no alcance estos mínimos será excluida del procedimiento.

10.1. Límite Máximo de Indemnización

El límite máximo de indemnización por siniestro y año para el conjunto de todas las garantías contratadas será, como mínimo, de **1.000.000 €**.

10.2. Coberturas y Sublímites Mínimos

Las siguientes coberturas deberán estar incluidas en la póliza, con los capitales y sublímites mínimos que se indican:

Cobertura	Capital / Sublímite Mínimo Exigido
Sección I: Cobertura de Datos	
Pérdida o robo de datos	Cubierto hasta el Límite Máximo de Indemnización (1.000.000 €)
Violación de la privacidad	Cubierto hasta el Límite Máximo de Indemnización (1.000.000 €)
Extorsión cibernética (incl. ransomware)	10% del Límite Máximo de Indemnización (mínimo 100.000 €)
Riesgos de reputación	10% del Límite Máximo de Indemnización (mínimo 100.000 €)
Ciber Crimen	5% del Límite Máximo de Indemnización (mínimo 50.000 €)
Sección II: Responsabilidad Civil	
Responsabilidad Civil y Constitución de Fianzas Civiles	Cubierto hasta el Límite Máximo de Indemnización (1.000.000 €)
Por violación de la confidencialidad	Cubierto hasta el Límite Máximo de Indemnización (1.000.000 €)
Por violación de la privacidad	Cubierto hasta el Límite Máximo de Indemnización (1.000.000 €)
Seguridad en la red	Cubierto hasta el Límite Máximo de Indemnización (1.000.000 €)

10.3. Franquicia

La franquicia aplicable a la cobertura de Responsabilidad Civil (Sección II) no podrá ser superior al 1% del límite máximo de indemnización por siniestro y año (es decir, no superior a 10.000 €).

No se admitirá la aplicación de franquicias para el resto de las coberturas, salvo que sean ofrecidas por el licitador como una mejora sin coste.

10.4. Servicios de Soporte Incluidos

La póliza deberá incluir, sin coste adicional y sin que su uso consuma el capital asegurado para indemnizaciones, los siguientes servicios de soporte:

11. Asistencia informática online 24 horas y descontaminación de virus.
12. Revisión informática anual.
13. Recuperación de datos y memorias.
14. Geolocalización y bloqueo de smartphone.
15. Copia de seguridad.
16. Borrado de la huella digital.
17. Aptitud para contratar y mediación de seguros

Podrán tomar parte en el procedimiento de licitación las entidades aseguradoras legalmente habilitadas para operar en el ramo correspondiente al objeto de seguro del presente pliego.

Dado que Mutua Intercomarcal no cuenta con mediador, las compañías de seguro podrán concurrir directamente o, bien, a través de la intervención de un mediador habilitado por la autoridad competente que deberá ser designado expresamente por el licitador al tiempo de presentación de la oferta.

En caso de que la entidad aseguradora se presentase mediante Mediador y resultara adjudicataria, deberá acreditar que se ha suscrito un acuerdo de mediación entre la aseguradora y una entidad autorizada como mediador, así como que la remuneración de la empresa mediadora prevista legalmente será a cargo de la aseguradora que resulte adjudicataria. Las partes se considerarán notificadas en la fecha en que la comunicación sea recibida por la entidad mediadora.

En todo caso, el mediador de seguros asignado por la aseguradora deberá ajustar su actividad a lo previsto en el Real Decreto-Ley 3/2020, de 4 de febrero, pudiendo ser rechazado por Mutua Intercomarcal si se constatara actividad irregular.

18. Duración de las pólizas

La duración de las pólizas que se suscriban como consecuencia de la presente licitación será de UN AÑO (1), con posibilidad de prorrogarlo hasta un máximo de un (1) año más estando previsto que sus vigencias comiencen a contar a partir de las 00:00 horas del día 01 de mayo de 2026.

19. Facturación

Se realizará una única factura por año, dicha factura se emitirá en el plazo máximo de 30 días al inicio de la póliza, contendrá en un solo documento y de forma detallada, el periodo de facturación y el número de expediente al que hace referencia.

ANEXO 1: Datos de Siniestralidad e información de interés

Se informa que el volumen facturación en el ejercicio 2024 fue de 358.028.226,92€ tal y como consta en las cuentas de la entidad publicadas en la página web de la Seguridad Social.

Número de empleados: 301

En los últimos cuatro años no se ha sufrido ninguna circunstancia que podría dar lugar a una reclamación amparada bajo las condiciones del presente pliego.

46581544N
ANTONIO SERRA
(R:G60328796)
FIRMA

Digitally signed by
46581544N ANTONIO
SERRA (R:G60328796)
FIRMA
Date: 2026.04.08
12:58:21 +02'00'