ACLARACIONES relativas al expediente para la contratación de una póliza de seguros de ciberseguridad para Mutua Intercomarcal, mutua colaboradora con la seguridad social número 39. (EXP. 2026/LIC/0020)

CONSULTAS Y RESPUESTAS:

Consulta 01 Recibida el 27-04-2026.

Pregunta:

Estimados Sres.,

Nos ponemos en contacto con ustedes con motivo del expediente de referencia para solicitarles que nos remitan el cuestionario adjunto cumplimentado.

Dadas las características del riesgo cyber, las compañías aseguradoras interesadas en este concurso necesitan un cuestionario de suscripción que les facilite la información básica de ciber riesgo para poder realizar el proceso de suscripción y presentar una oferta. Sin dicho cuestionario no es posible efectuar un análisis adecuado ni emitir una cotización.

Respuesta:

CUESTIONARIO

Por favor complete todas las preguntas en nombre de todos los asegurados, tomando en cuenta los servicios tecnológicos o sistemas contratados con terceros, y todos sus sistemas (red IT, red OT, dispositivos IoT, sitio web, etc.).

I. DEFINICIONES

- **Información y Sistemas críticos** se entienden como aquella información y sistemas informáticos: a) definidos como tal por el plan de contingencia o plan de recuperación ante desastres la organización, o b) que en caso de no poder acceder pasadas 48 horas comienzan a generar pérdidas.
- **Privilegios de administrador** se entienden aquellos usuarios con, al menos, derechos para instalar o desinstalar programas.
- **EPP:** Endpoint Protection Platform (antivirus tradicional)
- **EDR:** Endpoint Detection Response (antivirus de nueva generación)
- **Redes OT**: Sistemas y hardware dedicados a la gestión de procesos físicos (instrumentación, control –
  ejemplo PLC-, supervisión – ejemplo SCADA o HMI, y operación – ejemplo MES)
- **Dispositivos IoT:** objetos físicos que llevan incorporados sensores, software y otras tecnologías con el fin de conectarse e intercambiar datos con otros dispositivos (tanto en redes IT como en redes OT) y sistemas a través de Internet.

II. INFORMACIÓN GENERAL

Nombre:	Mutua Intercomarcal MCSS n39
Dirección:	Avenida Icaria 133-135 08005 Barcelona
CIF	G60328796
Seleccione aquellos que apliquen según su negocio (no incluye servicios externalizados):	☐ Venta directa a personas físicas (B2C) ☐ Venta directa a empresas (B2B) ☐ Distribución ☐ Diseño (productos o servicios) ☐ Fabricación
Describa su actividad:	Mutua Colaboradora con la Seguridad Social
Indique por favor donde tiene filiales y su porcentaje de facturación:	☑ España 100 % ☐ USA % ☐ Espacio Económico Europeo % ☐ Rusia / Bielorrusia % ☐ Latinoamérica y Caribe % ☐ Asia % ☐ Australia / Nueva Zelandia % ☐ Ucrania % ☐ Resto del Mundo %
En caso de filiales fuera del Espacio Económico Europeo por favor detallar el porcentaje de facturación por país:	
Indique los principales dominios web:	mutua-intercomarcal.com
¿Pertenece usted a un grupo de empresas?	No, no hay matriz ni filiales (unica empresa)

En caso de querer cubrir parcialmente un grupo por favor conteste a lo siguiente: NO APLICA **¿Están sus sistemas totalmente segmentados (físicamente y lógicamente) del resto de entidades del grupo que no se desea incluir en el seguro?** Si ☐ No ☐	
¿Se ha visto involucrado en alguna fusión, adquisición, venta o consolidación en los últimos 12 meses o pudiera estar involucrado en los próximos 12 meses?	Elija un elemento.
¿Cuál es el grado de homogenización de las políticas de ciberseguridad de su grupo? . Seleccione las que apliquen	
• Se gestiona a nivel central y las políticas se aplican a todas las filiales del grupo. De haber excepciones, solo es a nivel de activo (y no a nivel de filial o entidad jurídica asegurada) ☐ • Se gestiona a nivel central, pero existen excepciones para determinadas filiales o entidades jurídicas aseguradas. Los controles, tal como se describen en este cuestionario, se aplican al 98 % o más del total de los Endpoints ☐ • Se gestiona a nivel central, pero existen excepciones para determinadas operaciones o entidades jurídicas. Los controles, tal como se describen en este cuestionario, se aplican a menos del 98 % del total de los Endpoints. • Está descentralizada, pero los controles, tal como se describen en este cuestionario, se aplican al 98 % o más del total de los Endpoints.☐ • Está descentralizada, y los controles, tal como se describen en este cuestionario, se aplican a más del 50 % del total de los Endpoints, pero a menos del 98 % del total de los Endpoints ☐ • Se gestiona a nivel individual para cada filial o unidad operativa. Los controles, tal como se describen en este cuestionario, se basan en una encuesta de todas las filiales y unidades operativas ☐	

1. Dimensiones:

Importe de la cifra de negocios:

a) cerrada del último año: 348.000.000 € en el año 2025
b) estimación del año en curso: 354.000.000 € en el año 2026

Indique la actividad que mayor facturación le genere:
☐ Venta directa a personas físicas (B2C) ☐ Venta directa a empresas (B2B) Facturación online: 0 €
Número de empleados actual:
304 Número de usuarios de los sistemas: 304

Por favor adjuntar cuentas anuales consolidadas si su facturación es mayor a 50 millones.
Somos entidad semi pública y todavía no se han certificado las cuentas rendidas de 2025, se suele disponer de ellas a partir de la tercera quincena de Julio

2. Descripción general del sistema de información (selección múltiple):

X sistemas IT propios ☑ Redes OT **(ver preguntas adicionales)** X data center de terceros
X Dispositivos IoT X cloud services (SAAS) ☐ cloud services (PAAS) ☐ cloud services (IAAS)

Indique o seleccione por favor lo siguiente (en base a los sistemas seleccionados):
- el más crítico para su negocio:
- el % de sistemas críticos: ☐ <25% X ~50% ☐ >75%
- En cuanto a los sistemas en la nube por favor seleccione los proveedores de los mismos:

Microsoft Azure, Amazon Web Services, Google, Oracle, Alibaba, SalesForce, Telefónica	X
Otros con Tier III y certificados en ISO270001	X

Otros (Indicar nombre, nivel Tier y cerfiticaciones en ciberseguridad)	

3. Datos Personales (de empleados, proveedores o clientes que usted o alguien en su nombre almacena o procesa. Se requiere el número de personas, no la cantidad de información de cada uno.

	<10 mil	10 mil – 250 mil	250 mil – 1M	1M – 10M	>10M
Número de datos no sensibles:	☐	☐	☐	☑	☐
Número de tarjetas:	0	☐	☐	☐	☐
Número de datos sensibles (no incluye los de tarjeta):	☐	☐	☐	☑	☐

III. CONTROLES DE CIBERSEGURIDAD

1. ¿Dispone de un proceso para mantener un inventario de todo hardware y software de vuestro sistema de información?	Si
2. ¿Acceden los empleados únicamente a los sistemas y datos que requieren para desarrollar sus funciones (por ejemplo no todos los usuarios tienen privilegios de administrador), y siempre se elimina el acceso a éstos una vez acaban la relación laboral con usted en 24h después de su salida?	Si
3. Seleccione todas las soluciones de seguridad que dispone y en donde las tiene habilitadas	
X Antivirus / EPP en equipos X Antivirus / EPP en servidores ☐ Antivirus / EPP en red OT X EDR en equipos X EDR en servidores ☐ EDR red OT X Parcheo virtual a servidores ☐ Parcheo virtual a red OT X Parcheo virtual a equipos	
4. ¿Se ha realizado una configuración adecuada enfocada en seguridad (hardening) en los servidores?	Actualmente en proceso
5. ¿Gestiona los accesos de terceros a vuestros sistemas?	Si, otras medidas o plazos de acceso aplican
6. ¿Dispone de una Red Privada Virtual (VPN por sus siglas en inglés) habilitada en todo acceso remoto?	Si
7. En relación con el Multifactor de autenticación por favor indique donde lo tiene habilitado: Acceso VPN y servicios “on line”	
En relación con accesos remotos: X en todo acceso remoto de todos los empleados ☐ en la consola de administración de las copias de seguridad en la nube ☐ en el correo electrónico web ☐ en otras aplicaciones en la nube ☐ en todo acceso remoto de proveedores Por favor indicar excepciones: En relación con accesos dentro de instalaciones del solicitante: Para los usuarios con privilegio de administrador seleccionado: X MFA para los usuarios con privilegio de administrador ☐ MFA para todos los empleados (excepciones documentadas) ☐ en todo acceso de proveedores Por favor indicar excepciones:	

8. ¿Realiza un pre-análisis a los correos electrónicos para identificar potenciales adjuntos o enlaces maliciosos?	Si
9. ¿Qué opciones para autenticar el correo electrónico usa?	SPF
10. ¿Evalúa adjuntos a correos electrónicos en una sandbox para determinar si son maliciosos antes de su entrega?	Si
11. ¿Realiza campañas de concienciación sobre ciberseguridad para los empleados al menos anualmente?	Si, obligatorio cumplimiento
12. ¿Realiza formación obligatoria sobre ciberseguridad y protección de datos a todos sus empleados?	Si, pero solo a los nuevos
13. ¿Implementa medidas de seguridad adicionales para proteger los usuarios con privilegios de administrador? (selección múltiple)	
X PAM X Credenciales únicas de los administradores del sistemas ☐ No se permite el acceso remoto de estos usuarios X Administradores locales desactivados X No se usan los privilegios de administrador en tareas que no requieran dichos privilegios (por ejemplo, leer el mail) X He cambiado sus contraseñas por defecto X Registro de los accesos de cuentas privilegiadas ☐ Ninguna ☐ Otras:	
14. ¿Segmenta las redes de riesgo alto?	Si
15. ¿Dónde tiene desplegados cortafuegos (firewall)? Selección múltiple:	
X Workstation Red IT X Servidores IT ☑ Red OT con acceso externo X Para separar la red IT de la red OT Workstation Red OT ☐ Un WAF a nivel de acceso Internet X Dispongo de una DMZ	
16. ¿Usa sistemas sin soporte del fabricante / obsoleto?	Si, pero están totalmente aislados (de Internet y de la red)
17. En relación con las copias de seguridad por favor conteste las siguientes preguntas:	
a) ¿Dispone de un procedimiento de copias de seguridad de su información y sistemas críticos?	Si
b) ¿Cuál es la frecuencia de copias de seguridad de su información y sistemas críticos?	Diaria
c) ¿Cuál es el periodo mínimo de retención de las copias de seguridad?	30 días
d) ¿Dispone de copias desconectadas (offline) o en la nube?	Si
e) ¿Dispone de copias fuera de sus instalaciones (offsite)?	Si
f) ¿Dispone de copias de seguridad en al menos dos formatos distintos?	Si, parcialmente
g) ¿Verifica la integridad de las copias de seguridad antes de su restauración?	Si
h) ¿Cada cuánto tiempo prueba que las copias de su información y sistemas críticos pueden restaurarse correctamente?	Semestralmente
i) Únicamente pueden acceder a ellas usuarios con privilegio de administrador.	Si
j) En relación con vuestras capacidades de responder a incidentes por favor selección todas las que apliquen	
☐ SOC 24x7 X SOC 8x5 X SIEM X Gestión propia o con terceros de las alertas de varios sistemas X Auditoria de logs ☐ Se realizan ejercicios anuales de respuesta a incidentes	

18. ¿Dispone de un plan de respuesta a incidentes o protocolo equivalente para responder a los incidentes detectados?	Si
19. ¿Dispone de un plan de contingencia (BCP por sus siglas en inglés) que incluya una sección dedicada a los sistemas de la información?	Si
20. ¿Con qué frecuencia realiza pruebas a su plan de contingencia (BCP por sus siglas en inglés)?	Semestralmente
21. ¿Cuánto suele tardar en instalar las actualizaciones críticas (calificación CVSS de 8 o superior)) en sus sistemas informáticos?	No más de 14 días
22. ¿Cuánto suele tardar en instalar las actualizaciones no críticas (calificación CVSS inferior a 8) en sus sistemas informáticos?	No más de 14 días
23. ¿Qué servicios de gestión de vulnerabilidades de sus sistemas críticos usa?	
X Escaneos de vulnerabilidades** - ¿ Con qué frecuencia los realiza?: Anual X Pentesting** - ¿Con qué frecuencia los realiza?: Elija un elemento. ☐ Tenemos contratado BitSight / Security ScoreCard (o similares) **Por favor indicar si aplican al 100% de los sistemas o no: SI, 100%	

IV. RECLAMACIONES O INCIDENTES

24. ¿Ha sufrido en los últimos 24 meses alguna vulneración o destrucción de datos, fallo de seguridad (incluyendo acceso de personas no autorizadas a sus sistemas), extorsión cibernética, interrupción o caída de sus sistemas, suplantación de identidad, transferencias fraudulentas o cualquier otro incidente similar que haya dado lugar a una reclamación, procedimiento normativo o cualquier otra pérdida que hayan representado más de cinco mil euros en pérdidas?	☐ Si X No
25. ¿Ha sido objeto de algún procedimiento normativo relacionado con un incumplimiento normativo relacionado con los datos personales o privacidad?	☐ Si X No
En caso de respuesta afirmativa a alguna de las preguntas anteriores por favor facilite una descripción detallada de los incidentes, reclamaciones o procedimientos, fecha de los mismos, indicando sus consecuencias económicas y operativas, los archivos o componentes de su infraestructura tecnológica afectados, y especialmente, las medidas correctoras aplicadas. En caso de reclamaciones o procedimientos por favor indique las causas que alega el tercero, los perjuicios que reclaman y partes afectadas.	

REDES OT

En caso de disponer de condiciones de Redes OT (ver definición en el encabezado):

26. ¿Dispone de lo siguiente en relación con la seguridad de la red OT?:	
Política de seguridad OT X Si ☐ No Presupuesto de seguridad ☐ Si X No Equipo de Seguridad X Si ☐ No Comentarios / Aclaraciones:	
27. En relación con la segmentación de su red OT por favor seleccione la segmentación que aplique:	
☐ por proveedor ☐ por línea de producción X Segmentación entre IT y OT X Segmentada de Internet ☐ Por ciudad / país Comentarios / Aclaraciones:	
28. ¿Permite el acceso de empleados o terceros a su red OT?	Si, y con MFA habilitado
29. ¿Dispone de un plan de contingencia (BCP por sus siglas en inglés) que incluya in evento de restauración de la red OT en un caso de ransomware?	X Si ☐ No ☐ Parcial
30. ¿Dispone de un proceso para identificar dispositivos en la red OT con vulnerabilidades, y para parchear o actualizar esos dispositivos?	X Si ☐ No ☐ Parcial

DECLARACIÓN

El abajo firmante, como persona responsable de contratar el seguro en nombre del asegurado, tras las consultas pertinentes, confirma que no tiene conocimiento de ninguna circunstancia o incidente que, bajo su conocimiento y creencia, pudiera dar lugar a la activación del seguro de Cyber.

Firma y sello:

Director de Organización y T.I. DE Mutua Intercomarcal

46581544N

Sede corporativa
ANTONIO SERRA SERRA (R:G60328796)
Avda. Icaria 133 - 135 | 08005 Barcelona
T 934 867 400 | F 934 867 428
contratacionpublica@mutua-intercomarcal.com
www.mutua-intercomarcal.com

Consulta 02 Recibida el 27-04-2026.

Pregunta:

Buenos días. ¿Nos podrían confirmar que la prórroga contemplada en pliego es por mutuo acuerdo? Las prórrogas obligatorias limitan en gran medida la capacidad de las aseguradoras de poder aceptar el riesgo y presentar oferta. Muchas gracias.

Respuesta:

De conformidad con lo señalado en la Ley de Contratos de Sector Público (art. 29, LCSP 2017), la prórroga contemplada es de obligado cumplimiento para el adjudicatario si se cumplen las exigencias contenidas en el artículo que citamos a continuación:

La prórroga se acordará por el órgano de contratación y será obligatoria para el empresario, siempre que su preaviso se ***produzca al menos con dos meses de antelación a la finalización del plazo de duración del contrato****, salvo que en el pliego que rija el contrato se establezca uno mayor. Quedan exceptuados de la obligación de preaviso los contratos cuya duración fuera inferior a dos meses.* ***En ningún caso podrá producirse la prórroga por el consentimiento tácito de las partes.***