

Boletín de adhesión Seguro Ciber-Riesgos

Datos personales

Nombre y Apellidos/ Razón Social: _____ DNI/CIF: _____

Dirección: _____

Ciudad: _____

C.P.: _____ Email: _____

Teléfono: _____

Resumen de coberturas

- **Responsabilidad Civil derivada de la seguridad y privacidad de datos.** Se cubren las reclamaciones por incumplimiento de cualquier ley o reglamento en materia de protección de datos.
- **Servicios de respuesta por incidencias relativas a la privacidad de datos:** acceso a un panel de expertos designado para mitigar del daño causado en caso de una incidencia o fuga de datos (daños reputacionales, gastos legales, gastos de gestión de crisis y relaciones públicas, servicios de expertos informáticos, etc).
- **Defensa y sanciones.** Se pagan los gastos generados en las investigaciones de la Agencia de Protección de Datos así como las sanciones administrativas relacionadas.
- **Responsabilidad Civil derivada del contenido de la página web.** Difamación, injuria y calumnia, violación de los derechos a la privacidad de las personas, piratería y plagio, infracción en materia de copyright...
- **Multas derivadas del incumplimiento de los estándares de seguridad PCI.** Incluye costes y gastos.
- **Daños propios relacionados con la Protección de Datos.**
- **Extorsión Cibernética.** Cualquier pago por extorsión que se haya realizado bajo coacción o por cuenta del asegurado para prevenir o finalizar la amenaza de extorsión.
- **Daños por interrupción del negocio por fallos en redes o sistemas.** Pérdida de ingresos derivadas de una interrupción real y necesaria de los Sistemas Informáticos causada directamente por un fallo en el Sistema de Seguridad.
- **Franquicia 500 €**

Condiciones económicas y opciones de contratación

Prima total anual para Sociedades (según límite de indemnización elegido)

| Facturación | Límite de 100.000 € | Límite de 250.000 € | Límite de 500.000 € |
|---------------------------|--------------------------------------|--------------------------------------|--------------------------------------|
| 0 – 100.000 € | <input type="checkbox"/> 244,52 € | <input type="checkbox"/> 298,31 € | <input type="checkbox"/> 366,77 € |
| 100.001 – 500.000 € | <input type="checkbox"/> 316,47 € | <input type="checkbox"/> 386,10 € | <input type="checkbox"/> 474,72 € |
| 500.001 € - 1.000.000 € | <input type="checkbox"/> | <input type="checkbox"/> 495,84 € | <input type="checkbox"/> 609,64 € |
| 1.000.001 € - 1.500.000 € | <input type="checkbox"/> | <input type="checkbox"/> 605,58 € | <input type="checkbox"/> 744,56 € |
| Más de 1.500.001 € | <input type="checkbox"/> A consultar | <input type="checkbox"/> A consultar | <input type="checkbox"/> A consultar |

Prima total anual para Autónomos (según límite de indemnización elegido)

| Facturación | Límite de 100.000 € | Límite de 250.000 € | Límite de 500.000 € |
|-----------------------|--------------------------------------|--------------------------------------|--------------------------------------|
| 0 – 60.000 € | <input type="checkbox"/> 237,31 € | <input type="checkbox"/> 289,53 € | <input type="checkbox"/> 355,97 € |
| 60.001 – 150.000 € | <input type="checkbox"/> 253,50 € | <input type="checkbox"/> 309,28 € | <input type="checkbox"/> 380,27 € |
| 150.001 € - 250.000 € | <input type="checkbox"/> 271,50 € | <input type="checkbox"/> 331,23 € | <input type="checkbox"/> 407,24 € |
| Más de 250.001 € | <input type="checkbox"/> A consultar | <input type="checkbox"/> A consultar | <input type="checkbox"/> A consultar |

Cuestionario

Este boletín es documento vinculante de póliza si se contesta afirmativamente al apartado de “Declaración del Asegurado” y de forma negativa al apartado “Siniestros y Circunstancias”. En caso contrario deberá referirse a la Aseguradora para su confirmación.

Declaración del Asegurado

¿Realiza copias de seguridad y guarda su información (datos) importantes para el desarrollo de su trabajo en unidades externas (discos duros, pendrive) y/o en la misma red pero en otra máquina (teniendo entonces sistemas segregados o segmentados) y/o la copia de seguridad crítica no está constantemente conectada/vinculada a su entorno activo y, para todos los supuestos anteriores, comprueba con frecuencia que funcionen?

- Sí
- No. Tengo los datos en la NUBE. Si es así, ¿los datos en la NUBE están fuera de su red/entorno local o tiene que conectarse a la NUBE). Si tiene que conectarse a la NUBE, ¿utiliza la autenticación multifactor?
- Sí No

Para poder trabajar y desarrollar su actividad profesional, ¿tiene que conectarse de forma remota a algún sistema?

- Sí. Si es así, para poder conectarse de forma remota, ¿utiliza un sistema de autenticación multifactor y lo hace a través de una Red Privada Virtual (VPN)?
- Sí No
- No, trabajo con mi ordenador sin tener que conectarme de forma remota a ningún sistema ni para acceder a mi correo electrónico en la nube.

¿Es consciente del aumento de la ciberdelincuencia a nivel mundial y se forma o es consciente de medidas a tomar o señales a las que prestar atención (por ejemplo para no caer ante estafas en internet o phishing) para evitar que le pase a usted?

- Sí No

Si usted utiliza un ordenador para realizar su trabajo o como herramienta de este, ¿tiene dicho ordenador un antivirus o antimalware debidamente actualizado?

- Sí No

¿Aplicas los parches críticos y actualizas los sistemas tan pronto como sea posible, y no utiliza ningún software sin soporte y/o en el final de su vida útil (EOL, fin de vida)?

- Sí No

Analiza los correos electrónicos entrantes en busca de archivos adjuntos y/o enlaces maliciosos?

- Sí No

¿Proteges todos tus dispositivos con antivirus, antimalware y/o software de protección de puntos finales (endpoint protection software)?

- Sí No

¿Realiza/gestiona transacciones con tarjetas de crédito?

- Sí. Si es así, ¿cumple con la normativa de seguridad PCI y dichas transacciones el 25% del total de sus ingresos?
- Sí No
- No

Siniestros y circunstancias

¿Ha recibido alguna reclamación en contra del asegurado incluyendo empleados, en relación a una invasión o daño a la privacidad, robo de identidad, robo de información, Violación de las Medidas de Seguridad informática, violación de los derechos de autor, difamación o ciber extorsión?

- Sí No

¿Ha estado el Solicitante sujeto a alguna acción o investigación gubernamental y/o de la Agencia de protección de datos en relación con una presunta violación de una ley o normativa de privacidad?

- Sí No

¿ Tiene el Solicitante o algún administrador, directivo, empleado u otro Asegurado conocimiento o información de alguna circunstancia, evento u operación pasada que pueda dar lugar a una Reclamación bajo la Póliza?

Sí No

En caso afirmativo a cualquiera de las tres preguntas arriba indicadas, por favor, facilite detalles de cada Reclamación, alegación o incidencia, incluyendo los costes, pérdidas o daños incurridos o pagados y cualquier cantidad pagada bajo cualquier póliza:

Datos Bancarios

Número de cuenta bancaria: _____

Solicita más información

colegios@aon.es | 91 266 70 52

INFORMACIÓN PREVIA MEDIADORES DE SEGUROS CONFORME A LA LEY DE DISTRIBUCIÓN DE SEGUROS, POR LA QUE SE INCORPORA AL DERECHO ESPAÑOL LA DIRECTIVA 2016/97 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 20 DE ENERO DE 2016 SOBRE DISTRIBUCIÓN DE SEGUROS (en adelante "Ley de Distribución de Seguros"):

(i) Información General.

Aon Iberia Correduría de Seguros y Reaseguros, S.A.U. Sociedad Unipersonal (en adelante "AON") es un mediador de seguros en la modalidad de Correduría de Seguros. AON se encuentra inscrita en el Rº Mercantil de Madrid, Hoja M-19857, Tomo 15321, Folio 133, N.I.F. A-28109247. Asimismo, AON en su condición de sociedad de Correduría se encuentra inscrita en el Registro Especial de Sociedades de Correduría de Seguros de la Dirección General de Seguros y Fondo de Pensiones con la clave J-107 (<http://www.dgstop.mineco.es/es/Distribuidores/PUI/Paginas/pui.aspx>) y dispone de la Capacidad financiera y Seguro de Responsabilidad Civil según lo previsto en la Ley de Distribución de Seguros.

(ii) Principios de actuación de AON.

De conformidad con lo establecido en la ley de Distribución de Seguros, AON presta sus Servicios de Mediación de Seguros de manera objetiva e independiente, velando por los intereses de sus clientes y representando a éstos frente a las compañías aseguradoras.

AON facilita su asesoramiento bajo los principios de independencia frente las compañías aseguradoras, así como de análisis objetivo y personalizado a sus clientes, buscando siempre y en todo caso la cobertura que, de acuerdo con los requerimientos planteados por éstos, mejor se adapta a sus necesidades.

(iii) Servicio de quejas y reclamaciones.

En cumplimiento de la Ley de Distribución de Seguros, AON dispone de un servicio de quejas y reclamaciones en el que sus clientes puede presentar las quejas que consideren oportunas en relación con los Servicios de Mediación de Seguros prestados por AON. Para cualquier reclamación deberá dirigirse al Apartado de Correos núm. 2053, a la página web "quejasyreclamaciones.com" o bien a las propias oficinas de AON.

(iv) Remuneración.

Respecto a la remuneración que percibe AON por sus Servicios de Mediación, le informamos a continuación de los distintos sistemas de remuneración que AON tiene implementados por sus Servicios de Mediación de Seguros:

- AON pactará libremente con la compañía aseguradora la comisión que percibirá por la/s póliza/s de seguro/s intermediada/s, o, en su caso, pactará directamente con el cliente, de forma expresa y por escrito, los correspondientes honorarios profesionales, los cuales serán incrementados por los impuestos que en cada momento fueren de aplicación. Igualmente, AON podrá ser remunerado por una combinación de comisiones recibidas de la compañía aseguradora y honorarios percibidos directamente del cliente.
- En adición a lo anterior, AON podrá cobrar, junto con la prima, una cantidad adicional en concepto de gastos de administración cuyo importe será acordado con el cliente.
- Asimismo, se informa que AON puede percibir adicionalmente comisiones de las compañías aseguradoras por servicios accesorios a la Mediación de Seguros, tales como gestión de cobro de primas de seguro y otros sobre la cartera global de pólizas de seguro que intermedia con las distintas compañías aseguradoras.
- Por último, se informa que dentro del grupo AON existen otras sociedades que prestan determinados servicios a compañías aseguradoras tales como correduría de reaseguros, agencia de suscripción de seguros y/o consultoría, distintos e independientes a los Servicios de Mediación de Seguros prestados por AON, pero que pueden estar relacionados con los riesgos objeto de cobertura, pudiendo aquéllas recibir comisiones u honorarios de las compañías aseguradoras por tales servicios.
- En el caso de precisar cualquier aclaración sobre el sistema de remuneración de AON, podrá dirigirse a su interlocutor habitual en AON, quien adquiere el compromiso de facilitar cuantas aclaraciones fueran necesarias a este respecto.

(v) Resolución de conflictos de interés

El Grupo Aon dispone de una política de prevención de conflictos de interés.

(vi) Protección de Datos Personales y Derechos Digitales.

De conformidad con lo dispuesto en el Reglamento UE 2016/679 por el que se aprueba el Reglamento General de Protección de Datos ("RGPD") AON ha implantado una nueva Política de Seguridad que tiene como objetivo garantizar la aplicación de aquellas medidas de seguridad de carácter técnico y organizativo que sean necesarias, para en cada momento y teniendo en cuenta siempre el tipo de información o datos tratados, y el estado de la técnica, garantizar la seguridad, confidencialidad e integridad de los datos personales tratados. De igual modo, AON cuenta dispone de una Política de Privacidad conforme al RGPD y en la cual se detallan, entre otras cuestiones, el alcance, finalidades y base de los tratamientos de datos realizados. Ambas Políticas se encuentran disponibles en <http://www.aon.com/spain/privacidad.jsp>. La recogida y tratamiento automatizado de los datos personales, incluyendo datos especialmente protegidos (principalmente, de salud) que Ud. nos proporcione, tiene como finalidad la prestación de servicios de mediación de seguros privados, así como el mantenimiento, administración y gestión de su póliza de seguros incluyendo la gestión de siniestros. Si no se consiente el tratamiento de dichos datos para las finalidades especificadas, los servicios no podrán llevarse a cabo. Si Ud. nos proporciona datos de terceras personas físicas Ud. deberá, con carácter previo a su comunicación, informarles de los extremos contenidos en el presente documento.

Sin perjuicio de que lean detenidamente las mismas, le facilitamos a continuación la información básica del tratamiento, donde se reflejan aquellas cuestiones más relevantes de las políticas anteriormente mencionadas:

INFORMACION BASICA SOBRE PROTECCION DE DATOS





| | | |
|----------------------------|---|---|
| Responsable | AON IBERIA CORREDURÍA DE SEGUROS Y REASEGUROS, S.A.U. | |
| Finalidades y Legitimación | FINALIDADES: - Prestación de servicios de mediación de seguros privados. - Realizar análisis o estudios y promocionar y ofertar productos propios o de terceros comercializados AON. - Cumplir con nuestras obligaciones legales y regulatorias. | LEGITIMACION: - Ejecución de un contrato. - Interés legítimo. - Cumplimiento de obligaciones legales. |
| Destinatarios | Entidades Aseguradoras con las que se coticen sus riesgos y se suscriban las pólizas de seguro, gabinetes médicos, centros sanitarios, peritos y otros terceros para la gestión de siniestros. Sociedades del Grupo AON y otros terceros incluso basados en países fuera del Espacio Económico Europeo, tal y como se describe en la Política de Privacidad de AON. | |
| Derechos | Podrá ejercitar sus derechos de acceso, rectificación, supresión, portabilidad, limitación y oposición al tratamiento, mediante correo postal dirigido a AON (Calle Rosario Pino, nº 14-16, C.P. 28020) o electrónico (proteccion_datos@aon.es), acreditando su identidad. | |
| Información adicional | Puede consultar la información adicional y detallada en nuestra página web: http://www.aon.com/spain/privacidad.jsp | |




En el caso que Vds. tengan cualquier duda en relación con la presente comunicación o cualquier otro aspecto relativo a datos de carácter personal les rogamos se pongan en contacto con el Delegado de Protección de Datos de AON.

Lugar y fecha: _____

Firma del representante legal:

Requisitos de seguridad para coberturas de ciberriesgos

| 4 Requisitos de Ciberseguridad Críticos* | Información complementaria de orientación sobre los requisitos de Beazley: | Ejemplos prácticos de cómo usted o su informático podría aplicar y cumplir con este requisito: | Para más información |
|---|---|---|--|
|  <p>Con regularidad, realiza copias de seguridad de datos críticos en una ubicación "fría" o "fuera de línea" que no se vería afectada por un problema con su entorno en vivo/activo, y realiza pruebas para asegurarse de que esas copias de seguridad sean recuperables.</p> | <ul style="list-style-type: none"> Todas las empresas deben realizar copias de seguridad periódicas de sus datos y asegurarse de que estas copias de seguridad sean recientes y se puedan restaurar. Si lo hace puede asegurarse de que su empresa aún pueda funcionar después de un ataque, eliminación o borrado accidental, daño físico o robo. Además, si tiene copias de seguridad puede recuperar sus datos rápidamente y los atacantes de ransomware no lo pueden chantajear. Cuanto con más frecuencia cambie sus archivos y datos críticos para su negocio, deberá de hacer copias de seguridad de forma más regular. Es decir, si realiza muchos cambios en lo que a los datos críticos se refiere y lo hace de forma diaria, debería considerar la posibilidad de realizar copias de seguridad diarias. Si tiene pocos datos críticos y realiza pocos cambios, es posible que haciendo copias de seguridad mensuales sea suficiente. | <ul style="list-style-type: none"> Muchas plataformas tienen incorporada la función de copia de seguridad. Explora las opciones que ya tienes. Como alternativa, puedes intentarlo y explorar una solución de copia de seguridad ofrecida por terceros (por ejemplo, plataformas de copia de seguridad en la nube) o realizar tus propias copias de seguridad en unidades externas que guardes de forma segura, desconectadas de la red. | Copias de seguridad - una guía de aproximación para el empresario INCIBE |
|  <p>Utiliza autenticación multifactor (MFA) para los servicios basados en la nube (como el acceso a la cuenta de correo electrónico basada en la nube) y para todos los accesos remotos a su red.</p> | <ul style="list-style-type: none"> Las contraseñas ya no ofrecen suficiente seguridad, especialmente en el caso de los servicios disponibles en la nube (por ejemplo, Microsoft 365, Google Workspace, etc.). Los usuarios pueden elegir contraseñas fáciles de adivinar, poco seguras y tienen además el riesgo adicional de llegar a compartir sus contraseñas por medio de la ingeniería social. Disponer de MFA es importante porque hace que el robo de información de su empresa sea mucho más difícil para el delincuente medio. | <ul style="list-style-type: none"> La MFA no elimina los nombres de usuario ni las contraseñas, sino que añade una capa de protección extra al proceso de inicio de sesión. Al acceder a cuentas o aplicaciones, los usuarios proporcionan una verificación de identidad adicional, como el escaneo de una huella digital o la introducción de un código recibido por teléfono o aplicación móvil. La MFA está integrada en la mayoría de los servicios basados en la nube o en Internet, por lo que debes activarla. Otras alternativas son las que ofrecen otros proveedores como por ejemplo la posibilidad de hacer uso de MFA mediante el uso de códigos SMS, códigos únicos e incluso tokens. | Acceso seguro a los SCI: doble factor y accesos externos INCIBE-CERT Dos mejor que uno: doble factor para acceder a servicios críticos INCIBE |
|  <p>No permite el acceso remoto a su entorno de red sin una red privada virtual (VPN).</p> | <ul style="list-style-type: none"> Los atacantes escanean regularmente todos los puertos de Internet en busca de servicios de acceso remoto visibles, como el protocolo de escritorio remoto (RDP) de Microsoft. Cualquier servicio RDP abierto será rastreado constantemente en busca de debilidades, por lo que ocultar sus servicios de acceso remoto detrás de una VPN le proporcionará un buen nivel de protección contra estos ataques. | <ul style="list-style-type: none"> Al igual que con la MFA, hay muchos proveedores que ofrecen servicios de VPN. Asimismo su propia infraestructura de red (por ejemplo, los routers) también puede tener esta funcionalidad incorporada, por lo que puede que sólo sea necesario habilitarla. El requisito de una VPN es sólo para el acceso remoto a los sistemas locales. | Conéctate a tu empresa de forma segura desde cualquier sitio con una VPN INCIBE Recomendaciones de seguridad en el empleo de redes VPN INCIBE |
|  <p>Proporciona regularmente (al menos una vez al año) una formación de concienciación sobre ciberseguridad, incluida antiphishing, a todas las personas que tienen acceso a la red de su empresa o a los datos confidenciales/ personales.</p> | <ul style="list-style-type: none"> Sus empleados están en la primera línea de fuego de su empresa y están constantemente expuestos a correos electrónicos de terceros que puedan dejarlos expuestos a sus ataques. Aunque las medidas técnicas de seguridad, como las barreras de acceso al correo electrónico y el software de detección y respuesta ampliada de puntos finales (EDR), pueden ofrecer cierto nivel de protección, sigue siendo esencial que sean conscientes de los riesgos. La formación les ayudará a identificar los riesgos cibernéticos y, con suerte, a evitar que afecten a su empresa. | <ul style="list-style-type: none"> El Instituto Nacional de Ciberseguridad (INCIBE) ofrece formación gratuita sobre ciberseguridad para los empleados de las empresas muy completo. | Kit de concienciación INCIBE Políticas de seguridad para la pyme INCIBE |

| 3 Requisitos de Seguridad Importantes** | Información complementaria de orientación sobre los requisitos de Beazley: | Ejemplos prácticos de cómo usted o su informático podría aplicar y cumplir con este requisito: | Para más información |
|---|---|--|--|
|  <p>Implementa parches críticos y actualiza los sistemas tan pronto como sea posible, y no utiliza ningún software sin soporte técnico/al final de su vida útil (EOL).</p> | <ul style="list-style-type: none"> • Todo software recibe actualizaciones en forma de "parches". Algunos de ellos añaden nuevas funciones al software y/o pueden centrarse en solucionar problemas como la inestabilidad o distintas vulnerabilidades. Dado que las vulnerabilidades se descubren y corrigen constantemente, la aplicación de los parches es (y debería de ser si no es así) una tarea de seguridad rutinaria que debería de estar implementada en la empresa y en todos los niveles de la organización. | <ul style="list-style-type: none"> • La mayoría de los sistemas operativos hacen que la actualización y los parches sean muy sencillos. En el caso de otro tipo de software, consulte el sitio web del proveedor correspondiente u otros canales para asegurarse de que está al día con los parches y las versiones más importantes. Los distintos proveedores suelen anunciar cuando su software deja de ser compatible y es crucial que esté al tanto de estas comunicaciones para solventar y mejorar sus sistemas. | <p>Políticas de seguridad para la pyme: actualizaciones de software INCIBE</p> <p>Gestión de parches en sistemas de control INCIBE-CERT</p> |
|  <p>Analiza los correos electrónicos entrantes en busca de archivos adjuntos y/o enlaces maliciosos.</p> | <ul style="list-style-type: none"> • El correo electrónico sigue siendo la principal forma de comunicación electrónica para la mayoría de las empresas y, por lo tanto, no es de extrañar que también sea un objetivo principal para que los hackers lleguen a sus empleados. Las pasarelas de correo electrónico protegen a sus empleados de amenazas como el spam, los virus y los ataques de phishing, filtrando los mensajes potencialmente maliciosos para que no lleguen a ellos. | <ul style="list-style-type: none"> • Al poner los correos electrónicos maliciosos en cuarentena o bloquear esos correos o a sus remitentes, una pasarela de correo electrónico debería reducir drásticamente el número de correos maliciosos exitosos y reducir, así, la posibilidad de exposición de los datos sensibles de sus empleados. La mayoría de las plataformas de correo electrónico ofrecen un filtrado y una cuarentena básicos. Asegúrese de que están activados. Lo ideal es que también busque soluciones a través de proveedores externos especializados en pasarelas de correo electrónico. | <p>Phishing INCIBE</p> <p>Cómo identificar un correo electrónico malicioso Oficina de Seguridad del Internauta (osi.es)</p> <p>Cómo evitar incidentes relacionados con los archivos adjuntos al correo INCIBE</p> |
|  <p>Protege todos sus dispositivos con antivirus anti-malware, y/o software de protección de puntos finales (endpoint protection software)</p> | <ul style="list-style-type: none"> • Los antivirus, antimalware y EDR son tipos de software que intentan detectar, bloquear y/o eliminar el software malicioso que se ejecuta en los dispositivos. Las herramientas modernas de EDR también suelen integrarse en una plataforma de registro/acceso para que las empresas puedan observar todo su sistema y ver los patrones o tendencias que podrían indicar la presencia de un hacker en su entorno. • Estas herramientas son una parte esencial de las herramientas de ciberseguridad de cualquier empresa porque tienen como objetivo eliminar proactivamente el software malicioso, algo que herramientas como los cortafuegos no pueden hacer. | <ul style="list-style-type: none"> • Hay muchas herramientas disponibles en este sentido, y en el siguiente enlace del Instituto Nacional de Ciberseguridad (INCIBE) se ofrecen consejos sobre la selección, configuración y uso de antivirus y otros programas de seguridad en smartphones, tabletas, ordenadores portátiles y de sobremesa. | <p>Sistemas EDR: qué son y cómo ayudan a proteger la seguridad de tu empresa INCIBE</p> <p>Protege tu móvil iOS y Android con 5 consejos Oficina de Seguridad del Internauta (osi.es)</p> <p>Seguridad en la instalación y uso de dispositivos IoT: una guía de aproximación para el empresario INCIBE</p> |