**CUESTIONARIO SEGURO EMPRESAS**

[Consulta nuestra Nota Informativa](https://segurtempo.com/nota-informativa/)

[Consulta nuestra Política de Privacidad](https://segurtempo.com/politica-de-privacidad/)

|  |  |
| --- | --- |
| Tomador del seguro | **---** |
| NIF | **---** |
| Dirección | **---**  **Código Postal: -- Localidad: ---**  **Ubicación: POLÍGONO INDUSTRIAL** |
| Facturación/Presupuesto Anual | **Total: --- España: ---**  **Resto Unión Europea: --- Reino Unido: ---**  **Usa y Canadá: --- Resto del Mundo: ---** |
| Recursos Humanos | **Nº Socios/Autónomos --- Nº Empleados: ---** |
| Fecha Constitución / Inicio Actividad | **---** |
| Actividad | **---** |
| Detalle Actividad | **---** |
| Sociedades Filiales   * Actividad y Facturación | **---** |

**CIBER-RIESGO**

|  |
| --- |
| **1.- ¿Es el número de personas físicas de quien usted, o alguien en su nombre, procesa, almacena o transfiere datos sensibles\* menor a 100.000, o 50.000 en caso de ofrecer servicios de salud? SÍ**  \*Datos sensibles se entienden como: 1) DNI, número de seguridad social, número de carnet de conducir, pasaporte; 2) datos bancarios, por ejemplo números de tarjetas de crédito; 3) información sobre raza, etnia, orientación sexual, salud, genética, biométrica, de convicciones religiosas o filosóficas, opiniones o afiliaciones políticas o sindicales.  **En caso negativo, por favor indique el número de personas físicas de quienes usted o un tercero en su nombre, almacena, procesa o transfiere datos sensibles y el tipo de datos en cuestión:**  **Haga clic o pulse aquí para escribir texto.**  **2.- ¿Confirma que sus ventas online son inferiores a 25% de su facturación o en caso de superarlo, que son inferiores a 1.000.000€?**  **SÍ En caso negativo, por favor indique su facturación online: Haga clic o pulse aquí para escribir texto.** |

**3.- ¿Dispone de filiales fuera del Espacio Económico Europeo o Reino Unido? NO**

**En caso afirmativo, por favor indique donde están domiciliadas dichas filiales y cuánto factura cada una de ellas:**

**Haga clic o pulse aquí para escribir texto.**

**4.- ¿Es usted filial de un Grupo de empresas o alguna de las empresas del grupo al cual usted pertenece quedará fuera de este seguro? NO**

**En caso afirmativo, indique la facturación total del grupo; qué entidades quedarán fuera del ámbito del seguro y si comparte algún sistema o recurso tecnológico con las demás empresas del grupo no cubiertas:**

**Haga clic o pulse aquí para escribir texto.**

**5.- ¿Hace uso de programas y sistemas informáticos sin soporte del fabricante? NO**

**En caso afirmativo:**

**Qué sistemas son y para qué son usados?**

**Haga clic o pulse aquí para escribir texto.**

**Cuándos dispositivos cuentan con sistemas sin soporte del fabricante, y qué porcentaje representan sobre el total de sus equipos?**

**Haga clic o pulse aquí para escribir texto.**

**Aplica, para todos los sistemas sin soporte alguna de las medidas de mitigación detalladas abajo:**

* **todos los sistemas sin soporte están desconectados de internet y aislados del resto de la red NO**
* **dispongo de una extensión de soporte especial por parte del fabricante para todos los sistemas sin soporte NO**
* **dispongo de una solución de parcheo virtual para todos los sistemas sin soporte: NO**
  + **En caso afirmativo indique el nombre: Haga clic o pulse aquí para escribir texto.**
* **otro (por favor detallar): Haga clic o pulse aquí para escribir texto.**

**Tiene previsto remplazar todos sus sistemas sin soporte NO**

**En caso afirmativo, cuándo prevé sustituirlos por una versión con soporte? Haga clic o pulse aquí para escribir texto.**

**6.- ¿Confirma que todos sus programas y sistemas informáticos, incluyendo pero no limitado al antivirus, se actualizan máximo 30 días después del lanzamiento de sus actualizaciones? SÍ**

**En caso negativo, por favor indique qué sistemas no se actualizan cada 30 días, la frecuencia con que se actualizan, y el motivo por el cual no se garantiza la frecuencia de 30 días: Haga clic o pulse aquí para escribir texto.**

**7.-En relación con sus copias de seguridad de todos sus sistemas e información:**

* **Realiza copias de seguridad de todos sus sistemas e información al menos cada siete días? SÍ**
* **Almacena las copias de seguridad en soportes externos totalmente desconectados de sus sistemas tanto en el curso habitual de su actividad, como durante la realización de la copia; cada vez que realiza una copia lo hace en un soporte externo distinto (una sola escritura); solo se rescriben los soportes externos después de 30 días SÍ**
* **Realiza copias de seguridad en uno de los siguientes proveedores de nube (Microsoft OneDrive, Google Drive, iCloud, Microsoft Servicios de Recuperación de Microsoft Azure, Amazon WS Infrequent Access o Amazon WS Glacier) y se requiere doble factor de autenticación para acceder a la consola de copias de seguridad SÍ**

**En caso negativo:**

**Si realiza copias de seguridad en la nube, indique por favor el nombre del proveedor de nube que utiliza, si las copias son completas o incrementales, si las copias son inmutables y si tiene activado el doble factor de autenticación para el acceso a la consola de copias de seguridad en la nube Haga clic o pulse aquí para escribir texto.**

**Las copias de seguridad que ya se han realizado no son accesibles o si son accesibles, no pueden ser alteradas ni borradas a través de los sistemas de los cuales se está haciendo la copia de seguridad (por ejemplo, son inmutables, o se almacenan en modo de lectura). Así es**

**No se puede acceder a las copias de seguridad; o el acceso a las copias de seguridad debe ser controlado por doble factor de autenticación; o el acceso a las copias de seguridad no se puede hacer con el username y password que utiliza para acceder a los sistemas de los cuales se está realizando la copia (no son accesibles con permisos de dominio) Así es**

**Retiene al menos copias de seguridad semanales de los últimos 30 días Así es**

**8.- ¿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 mil Euros en pérdidas? NO**

**En caso afirmativo, por favor facilite una descripción detallada de los incidentes, fecha de los mismos, indicando sus consecuencias económicas y operativas, los archivos o componentes afectados de su infraestructura tecnológica afectados, y especialmente, las medidas correctoras aplicadas: Haga clic o pulse aquí para escribir texto.**

**9.-¿Hace uso de sistemas de correo electrónico web (por ejemplo GSuite y Office 365)? SÍ**

**En caso afirmativo, el 100% de los usuarios tienen habilitada la MFA (autentificación multi-factor) en sus cuentas de correo electrónico web? SÍ**

**¿Se requiere de dos o más personas para revisar y autorizar pagos internos o externos mayores a 5.000€ (cinco mil Euros)? SÍ**

**En caso negativo:**

* **confirma que tiene 25 o menos empleados y que sólo una persona tiene autoridad para autorizar/firmar pagos superiores a 5.000€ SÍ**
* **¿a partir de qué importe requiere de dos o más personas para revisar y autorizar pagos internos o externos mayores a 5.000€? Haga clic o pulse aquí para escribir texto.**

**10.- En caso de solicitud de cambio de los números de cuenta, ¿Se verifica con la persona contacto que dicha solicitud de cambio es legítima mediante un medio distinto al que recibió la solicitud de cambio (por ejemplo: se recibe por email y se verifica telefónicamente)? SÍ**

**11.- ¿Verifica semanalmente en sus cuentas bancarias que los movimientos de la misma (conciliación bancaria) hayan sido efectivamente realizados por usted? SÍ**

**Sólo si factura más de 10 Millones de Euros**

**12.- ¿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? SÍ**

**13.- ¿Todos los administradores de sistemas tienen dos cuentas, una con permisos de administrador, y otra sin permisos de administrador para cuando no necesiten dichos permisos (por ejemplo consultar el email? NO**

**14.- ¿Todos los usuarios con permisos de administrador de sistemas disponen de autenticación multifactor en todos los sistemas que sean accesible remotamente (incluyendo pero no limitado a GSuite, Microsoft 365, conexiones VPN, remote desktop, CRM, o cualquier solución en la nube)? SÍ**

**Sólo si factura más de 25 Millones de Euros**

**15.- ¿Todos los usuarios disponen de autenticación multifactor en todos los sistemas que sean accesibles remotamente (por ejemplo GSuite, Microsoft 365, conexiones VPN, remote desktop, CRM, o cualquier solución en la nube)? SÍ**

**16.-Confirme por favor, si usted o alguien en su nombre, aplica cifrado a la información en los siguientes momentos.**

* **Cuando está almacenada en cualquier punto de la red (incluyendo dispositivos móviles, de almacenamiento, servidores, entre otros) con un cifrado de 256 bits. SÍ**
* **Usa una red privada virtual (o VPN por sus siglas en inglés) para todos los accesos remotos a sus sistemas SÍ**

**17.-Dispone de un procedimiento de restauración de copias de seguridad que es probado anualmente SÍ**

**18.-Confirma que dispone de cortafuegos (firewall) en los siguientes puntos y equipos SÍ**

* **todos los equipos informáticos SÍ**
* **todo el perímetro de su red SÍ**
* **aplicaciones web (o ‘web application firewall’), si utiliza recursos cloud SÍ**

**19.- ¿Confirma que instala todos los parches que remedian una vulnerabilidad con una calificación CVSS (versión 3.1) de 8.0 o superior como máximo en 14 días después del lanzamiento de dichas actualizaciones? SÍ**

**CONTINUAR SÓLO SI OFRECE SERVICIOS GESTIONADOS IT O TECNOLOGÍAS OPERATIVAS OT**

**SÓLO SI OFRECE SERVICIOS GESTIONADOS IT**

PARA SERVICIOS CLOUD

**1.-¿Usa alguno de los siguientes proveedores de servicios en la nube: Microsoft Azure, Amazon Web Services, Google, Oracle, Alibaba, SalesForce o Telefónica? SÍ**

**En caso negativo, ¿Usa proveedores Tier III y certificado ISO 270001? SÍ**

**Tipo de datos sensibles y número de personas físicas de las cuales almacena o procesa (usted o un proveedor en su nombre) datos sensibles.**

**Haga clic o pulse aquí para escribir texto.**

**2.-¿Tiene activado el 2FA o MFA (dos o más factores de autenticación) para acceder usted (incluyendo el webmail, CRM o ERP) y/o sus clientes (los servicios que usted ofrece) a los sistemas correspondientes? SÍ**

**3.-¿Dispone de una DMZ en cada uno de los accesos, servicios o entornos ofrecidos a sus clientes? SÍ**

**4.-¿Dispone de WAF para sus sistemas más críticos? SÍ**

**5.-¿Tiene contratado un servicio de redundancia geográfica? En caso afirmativo por favor facilite detalles SÍ**

**Haga clic o pulse aquí para escribir texto.**

**6.-¿Ha aplicado todas las recomendaciones de seguridad aplicadas por alguno de los proveedores de nube pública (Google Security Command Center, Azure Advisor, AWZ Trusted Advisor, entre otros)? SÍ**

PARA CPD PROPIOS

**1.-En caso de ofrecer hosting a terceros clientes mediante CPD propios, necesitamos aclarar:**

* **Nivel Tier y certificación ISO27001**

**Haga clic o pulse aquí para escribir texto.**

* **2fa en accesos remotos a sus propios sistemas y cuentas con y sin privilegios para it admins SÍ**

**2.-¿Dispone de una DMZ en cada uno de los accesos, servicios o entornos ofrecidos a sus clientes? SÍ**

**3.-¿qué medidas de redundancia tiene para sus sistemas más críticos?**

**Haga clic o pulse aquí para escribir texto.**

**4.-¿Los gestiona y mantiene usted o un tercero en su nombre?**

**Haga clic o pulse aquí para escribir texto.**

**5.-¿Dispone de balanceadores? SÍ ¿están configurados en Activo – Activo o Activo - Pasivo? Activo - Activo**

SERVICIOS GESTIONADOS DE TERCEROS CLIENTES

**1.-Accede remotamente a sistemas de sus clientes? NO**

**En caso afirmativo, por favor indicar si acceden remotamente a sistemas de sus clientes para realizar al menos una de las siguientes actividades:**

1. **Gestión de copias de seguridad NO**
2. **Administración y gestión de identidad y soluciones de control de accesos, como por ejemplo Directorio Activo NO**
3. **Gestión de ciberseguridad NO**
4. **Gestión del email NO**

**Facturación que corresponde a los servicios mencionados anteriormente Haga clic o pulse aquí para escribir texto.**

**2.-¿Administra accesos (la creación, borrado o modificación de cuentas de usuario y sus privilegios), por ejemplo, mediante el uso de Directorio Activo, en nombre de uno o más de sus clientes? NO**

**3.-¿cómo controla el acceso remoto que usted tiene a los sistemas informáticos de sus clientes? Por ejemplo, mediante el uso de certificados, controles de accesos que solo son válidos temporalmente, o mediante multi-factor de autenticación? NO**

**En caso negativo, les ha recomendado a sus clientes que dichos controles deberían implementarse? SÍ**

**4.-¿Hay segmentación entre los sistemas del asegurado y las instancias de sus clientes? NO**

**5.-¿Hay segmentación entre las subredes de cada cliente para impedir movimientos laterales? NO**

**CUESTIONARIO PARA EMPRESAS QUE USAN TECNOLOGÍAS OPERATIVAS OT**

**1.-Ha implantado las medidas de protección siguientes para asegurar el acceso remoto a sus redes y sistemas de OT: (Marque todo lo que corresponda)**

|  |  |
| --- | --- |
| 1. **El acceso remoto a sus redes y sistemas de Tecnologías Operativas (OT) es posible NO** |  |
| 1. **Para el acceso remoto a estas redes y sistemas se utilizan siempre conexiones VPN seguras NO** |  |
| 1. **Se requiere una autenticación de dos factores para todos los accesos remotos NO** |  |
| 1. **El acceso remoto es controlado y de naturaleza temporal (por ejemplo, basado en el tiempo) NO** |  |
| 1. **Otros Haga clic o pulse aquí para escribir texto.** | |

**2.-¿Alguno de sus dispositivos en la red OT está conectado a internet o es accesible desde la red IT? NO**

**En caso afirmativo conteste a lo siguiente: Marque todo lo que corresponda en relación con la aplicación de parches de sus OT**

**Las OT se parchean en los 30 días siguientes a la publicación de las actualizaciones por parte del fabricante NO**

**Las OT se basan en software sin soporte y ya no cuentan con el apoyo del fabricante NO**

**3.-Existe un proceso documentado para la implantación de actualizaciones, parches y nuevos códigos, incluida la prueba de los parches en un entorno de desarrollo antes de su implantación en alguna parte de la red de OT NO**

**4.-¿Se han implantado soluciones de seguridad para endpoints en los dispositivos y sistemas de OT? En todos los dispositivos y sistemas de OT**

**Indique el tipo de solución o soluciones de punto final que se utilizan: Haga clic o pulse aquí para escribir texto.**

**5.-¿Existe una segmentación entre sus redes de IT (Tecnologías de información) y OT, y si es así, cómo se consigue? Por ejemplo, si se permite únicamente la transferencia de datos entre sus redes OT e IT (y no al revés), indíquelo también.**

**Haga clic o pulse aquí para escribir texto.**

**6.-¿Cómo se administran sus redes de IT y OT?**

**Los mismos administradores son responsables de las redes IT y OT NO**

**Las redes de IT y OT tienen sus propios administradores NO**

**Otros Haga clic o pulse aquí para escribir texto.**

**7.-Si hay diferentes administradores responsables de sus redes de IT y OT, cumplimente la pregunta siguiente:**

**¿qué administrador es responsable de lo siguiente?**

**Control de las reglas y políticas de los cortafuegos [administradores de IT y OT] Administradores de IT**

**Control de la administración de usuarios Administradores de IT**

**Auditoría de las actividades de gestión de cortafuegos Administradores de IT**

**Mantenimiento, incluida la aplicación de parches Administradores de IT**

**8.-¿Realiza copias de seguridad o documenta la configuración de sus dispositivos de OT? Sí, copia de seguridad**

**Las siguientes preguntas son exclusivas para empresas con facturación anual superior a 25.000.000€:**

**9.-¿Qué medidas toma para identificar Shadow IT dentro de su red de OT?**

**Haga clic o pulse aquí para escribir texto.**

**10.-¿Produce usted dispositivos o sensores de IoT? NO**

**11.-¿Su capacidad para generar ingresos depende de algún dispositivo o sensor de IoT? NO**

**En caso afirmativo, describa los tres tipos de dispositivos de IoT principales que se utilizan en sus instalaciones, y de qué son responsables:**

**Haga clic o pulse aquí para escribir texto.**

**12.-¿En qué red se encuentran sus dispositivos y sensores IoT? Red de TO**

**Explíquelo, especialmente si estos dispositivos y sensores se encuentran en una red pública. Indique también cómo se garantiza su seguridad:**

**Haga clic o pulse aquí para escribir texto.**

**13.-¿Es usted responsable del funcionamiento de dispositivos y sensores del IoT que pueden venderse a los clientes? NO**

**En caso afirmativo, explique a continuación. Indique también cómo se garantiza su seguridad:**

**Haga clic o pulse aquí para escribir texto.**

**Las siguientes preguntas son exclusivas para empresas con facturación anual superior a 50.000.000€:**

**14.-¿Dispone de alguna certificación pertinente en relación con las normas internacionales de su sector? Por ejemplo ISO 27001. NO**

**15.-¿Se llevan a cabo pruebas de penetración de las redes de OT y, en caso afirmativo, quién las realiza? NO**

**16.-¿Cuándo se realizó la última prueba de penetración? Haga clic o pulse aquí para escribir texto.**

**17.-¿Con qué frecuencia se realizan las pruebas de penetración? Haga clic o pulse aquí para escribir texto.**

**18.-Si la prueba de penetración identifica algún problema importante, explíquelo y proporcione información adicional sobre el modo en que se ha rectificado o se está rectificando:**

**Haga clic o pulse aquí para escribir texto.**

**19.-¿Ha realizado un análisis de la rapidez y la gravedad con las que el fallo de sus sistemas de OT afectaría a su capacidad para generar ingresos (análisis del impacto en el negocio)? NO**

**20.-¿Con qué rapidez serían afectadas las ventas de su empresa por un incidente ciber que afectara a su red de OT, incluido un incidente de fallo del sistema? 0 <8 horas**

**21.-¿Con qué rapidez puede volver a poner en marcha su red y sistemas OT tras un incidente ciber importante (por ejemplo, tras un ataque de ransomware llevado a cabo por un hacker que ha obtenido acceso remoto a sus sistemas) o un incidente de fallo del sistema? 0 <8 horas**

**22.-Si sus OT se encuentran en varias ubicaciones físicas, proporcione un resumen de cada ubicación con la actividad, las ventas y el beneficio bruto. Haga clic o pulse aquí para escribir texto.**