Ciber Protección

Formulario e información

2018

Formulario Ciber Protección

Razón social:

CIF:

Domicilio:

Actividad de la empresa:

Nº de empleados: Nº de equipos o devices:

Volumen de facturación:

Puedes consultar la ayuda pinchando encima de cada pregunta (ctrl+click) o al final del documento

Cumplimiento de la LCE o LSSI (Ley 34/2002, de 11 de julio, y Real Decreto ley 13/2012, de 30 de marzo)

1. ¿Cuántas páginas web/blog o servicios en Internet orientados a usuarios tiene la empresa? _____

2. ¿Cumples con la LCE o LSSI? ☐ Sí ☐ No
En caso de no cumplir, es necesario contestar a las siguientes preguntas:

- ¿Vendes o recoges información de tus clientes a través de tu página web? ☐ Sí ☐ No
- ¿Informas de los datos de tu empresa en la página principal de tu web? (Nombre, CIF, domicilio Social, número de Inscripción en el Registro Mercantil, etc…?) ☐ Sí ☐ No
- ¿Informas de forma accesible de qué son y qué hacen las cookies? ☐ Sí ☐ No
- ¿En los e-mails comerciales que envías a tus clientes indicas que es información comercial? ☐ Sí ☐ No
- ¿Estos e-mails se envían únicamente a destinatarios que han dado su consentimiento expreso? ☐ Sí ☐ No
- ¿En los e-mails informas de cómo puede darse de baja de la publicación? ☐ Sí ☐ No
- ¿Tus servidores, o los de tus proveedores donde se gestionan datos personales se encuentran físicamente en la Unión Europea? ☐ Sí ☐ No
- ¿Tienes autorización legal de la Agencia Española De Protección de Datos para exportar información (datos) fuera de la UE? ☐ Sí ☐ No
- ¿Informas a tus clientes del precio final, gastos de envío, impuestos y características del producto, antes de terminar una venta por internet? ☐ Sí ☐ No

3. ¿Has sido sancionado o la Administración te ha abierto algún procedimiento sancionador en los últimos tres años? ☐ Sí ☐ No

4. En caso de haber sido sancionado ¿has implementado alguna medida para evitar que se vuelvan a producir? ☐ Sí ☐ No

Cumplimiento de la LOPD (y Directiva 95/46/CE)

5. ¿Qué tipo de datos personales maneja la empresa? ☐ Básicos ☐ Medios ☐ Altos

6. ¿Cumples con la LOPD? ☐ Sí ☐ No

- ¿Se realiza cada dos años una auditoría de seguridad de los datos a tu empresa? ☐ Sí ☐ No
- ¿Los ficheros que contienen datos personales (como datos de clientes, proveedores, empleados, etc.) de la empresa están inscritos en la Agencia Española Protección de Datos? ☐ Sí ☐ No
- ¿Incluyes en los contratos u ofertas con clientes o proveedores una cláusula de cesión de datos personales? ☐ Sí ☐ No
- ¿Tiene la empresa subcontratados servicios en los que se necesite acceder a datos personales? ☐ Sí ☐ No
- En caso de subcontratar servicios que necesiten acceder a datos personales de tu empresa. ¿Tienes firmados acuerdos de confidencialidad y cesión de datos con estas subcontratas? ☐ Sí ☐ No
- ¿Tienes firmados acuerdos de confidencialidad y cesión de datos con tus empleados y han aceptado las obligaciones legales? ☐ Sí ☐ No
- ¿Los empleados de la empresa han recibido formación en materia de protección y seguridad de datos? ☐ Sí ☐ No
- ¿Facilitas el ejercicio de los derechos de acceso, rectificación o modificación, cancelación y oposición por parte de los titulares de los datos almacenados? ☐ Sí ☐ No
- ¿Borras los datos de carácter personal que ya no son necesarios? ☐ Sí ☐ No
- ¿Dispones de medidas técnicas y organizativas que garanticen la seguridad de los datos de carácter personal teniendo en cuenta la tipología de estos? ☐ Sí ☐ No
- ¿Están los servicios web de la empresa, en los que se manejan datos de carácter personal, físicamente dentro de la UE? ☐ Sí ☐ No
- Si la empresa dispone de cámaras de vigilancia ¿Guardas las imágenes o audios? ☐ Sí ☐ No

7. ¿En los últimos tres años la empresa ha sufrido algún tipo de sanción o la Agencia de Protección de Datos AGPD le ha abierto algún procedimiento sancionador? ☐ Sí ☐ No

8. ¿Tras esas sanciones, ha implementado la empresa alguna medida para evitar que se vuelvan a producir? ☐ Sí ☐ No

Infraestructura de seguridad

9. ¿La empresa hace copias de seguridad de los datos con una herramienta de backup automatizado semanalmente en un dispositivo diferente de donde están los datos originales? ☐ Sí ☐ No

10. ¿Tienes un antivirus actualizado en todos los equipos incluidos en la póliza? ☐ Sí ☐ No

11. ¿Tienes instalado algún firewall o cortafuegos? ☐ Sí ☐ No

12. ¿Actualizas el software de los equipos informáticos de acuerdo con las recomendaciones del fabricante? ☐ Sí ☐ No

13. ¿Existe en tu empresa una política de cambios de contraseñas cada 60 días? ☐ Sí ☐ No

14. ¿En caso de ataque tienes un plan de continuidad de negocio? ☐ Sí ☐ No

15. En el caso de tener servidores, ¿éstos están en una habitación con acceso restringido? ☐ Sí ☐ No

16. ¿Cuántos ataques informáticos ha sufrido la empresa en el último año? ☐ Sí ☐ No

17. ¿Tras esos ataques la empresa ha implementado medios para que no se vuelvan a producir? ☐ Sí ☐ No

Información detallada de cada pregunta

Significado de las siguientes siglas:

LOPD: Ley de Protección de Datos
AEGPD: Agencia Estatal de Protección de Datos
LSSICE: Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico

1. **¿Cuántas páginas web/blog o servicios en Internet orientados a usuarios tiene la empresa?**
   Una página web o blog es es un documento o información electrónica capaz de contener texto, sonido, vídeo, programas, enlaces, imágenes, que puede ser accedida mediante un navegador web que suele estar en formato html.

2. **¿Cumples con la LCE o LSSI?**

   - **¿Vendes o recoges información de tus clientes a través de tu página web?**
     En el caso de comercializar productos o servicios a través de internet, o simplemente para poder contactar con clientes, es necesaria la recopilación de sus datos personales, como son su nombre, dirección, nº de tarjeta de pago etc.

   - **¿Informas de los datos de tu empresa en la página principal de tu web? (Nombre, CIF, domicilio Social, número de Inscripción en el Registro Mercantil, etc…?)**
     Una página corporativa o un portal de comercio electrónico, deben cumplir una serie de normas establecidas por la LSSICE, como es la publicación de:
     - Su nombre
     - Domicilio (indicando al menos, la localidad y provincia de residencia)
     - Dirección de correo electrónico.
     - Número de Identificación Fiscal (NIF).
     - Cualquier dato que permita establecer una comunicación directa y efectiva, como podría ser, por ejemplo, un teléfono o un número de fax.
     - Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

   - **¿Informas de forma accesible de qué son y qué hacen las cookies?**
     Las «cookies» permiten almacenar y recuperar datos que los usuarios tienen almacenados en sus equipos, de manera que el sitio web puede saber cuál es la actividad o hábitos de navegación de este usuario y agilizar búsquedas posteriores. Cuando se emplean cookies se debe obtener el consentimiento y se ha de informar a los usuarios de su utilidad y uso.
     Por ejemplo: cuando pones tus contraseñas de acceso al correo electrónico y te pide guardarlas, en siguientes ocasiones que entres en tu correo, esa cookie que se ha generado, hace que no la tengas que volver a poner.

   - **¿En los e-mails comerciales que envías a tus clientes indicas que es información comercial?**
     En las comunicaciones comerciales enviadas a clientes actuales o potenciales sobre noticias de la entidad, ofertas promocionales o concursos, ya sea vía email o usando otros medios como SMS, MMS, etc., Se debe indicar de una manera clara que se trata de información comercial.

- **¿Estos e-mails se envían únicamente a destinatarios que han dado su consentimiento expreso?**

  Según la LSSICE Estas newsletters o email comerciales únicamente se han de enviar a los destinatarios que han dado su consentimiento expreso.

- **¿En los e-mails informas de cómo puede darse de baja de la publicación?**

  Tal como menciona la LOPD, en estos e-mails, debe informarse claramente como poder darse de baja de esta publicación, ya sea a través de un link a una página web, correo electrónico, correo postal, tf, etc…

- **¿Tus servidores, o los de tus proveedores donde se gestionan datos personales se encuentran físicamente en la Unión Europea?**

  Las comunicaciones comerciales, enviadas por correo electrónico, se envían a través de servidores de correo electrónico, si estos servidores se encuentran fuera de la UE, se necesita una autorización por parte de la AEPD, para poder exportar los datos personales de los destinatarios fuera de la UE.

- **¿Tienes autorización legal de la Agencia Española De Protección de Datos para exportar información (datos) fuera de la UE?**

  Para poder exportar datos personales (es decir, si utilizas proveedores que utilicen esos datos, nombre, correo etc…, y que tengan sus servidores fuera de la UE), y usarlos para el envío de las newsletters fuera de la Unión Europea se necesita la autorización de la Agencia de Protección de Datos. Esta autorización debe ser solicitada para esos ficheros.

- **¿Informas a tus clientes del precio final, gastos de envío, impuestos y características del producto, antes de terminar una venta por internet?**

  En caso de realizar ventas a través de internet, se debe proporcionar al comprador, toda la información relativa al producto, precio, impuestos y gastos de envío, además de cualquier otra información necesaria para el cliente.

3. **¿Has sido sancionado o la Administración te ha abierto algún procedimiento sancionador en los últimos tres años?**

   En caso de haber incumplido alguna de las normas señaladas por la Administración, o Agencia de Protección de Datos, puedes ser sancionado o multado, estas multas tienen cuantías que varían en función de la gravedad del incumplimiento y pueden llegar a 600.000€, a partir de Mayo de 2018 con la nueva regulación serán de hasta 20 Millones de € o un 4% de la facturación anual.

4. **En caso de haber sido sancionado ¿has implementado alguna medida para evitar que se vuelvan a producir?**

   A raíz de las sanciones administrativas, has estudiado e implementado mejoras para impedir que las causas de las sanciones no se vuelvan a producir.

5. **¿Qué tipo de datos personales maneja la empresa? Básicos, Medios o Altos?**

   Según la ley LOPD se definen unos tipos de datos. Se catalogan en tres niveles en función de su grado de privacidad

   Básico: Ejemplos: Nombre, domicilio, teléfono, DNI, número de afiliación a la seguridad social, fotografía, firmas, correos electrónicos, datos bancarios, edad, fecha de nacimiento, sexo, nacionalidad, etc.

   Medio: Ejemplos: Datos de personalidad, hábitos de consumo, hábitos de carácter, datos de seguridad social, solvencia patrimonial y crédito, antecedentes penales, sanciones administrativas, pruebas psicotécnicas, currículos, etc.

   Altos: relativos a ideología, afiliación sindical y política, religión y creencias, origen racial, salud, alimentación, bajas laborales, vida y práctica sexual, etc.

6. ¿Cumples con la LOPD?

- **¿Se realiza cada dos años una auditoría de seguridad de los datos a tu empresa?**

  La LOPD estipula la realización de una auditoría de cumplimiento de la ley cada 2 años, en caso de que la empresa maneje datos de carácter personal de nivel medio o alto.

- **¿Los ficheros que contienen datos personales (como datos de clientes, proveedores, empleados, etc.) de la empresa están inscritos en la Agencia Española Protección de Datos?**

  Están obligados a notificar la creación de ficheros y a su vez inscribirlos el Registro General de Protección Datos (RGPD), aquellas personas físicas o jurídicas, de naturaleza pública o privada, u órgano administrativo, que creen ficheros con datos de carácter personal.

- **¿Incluyes en los contratos u ofertas con clientes o proveedores una cláusula de cesión de datos personales?**

  Es necesario obtener el consentimiento de clientes o proveedores siempre que realicemos un tratamiento de sus datos personales, para tratar con sus datos, por ello es importante incluir esta cláusula en los contratos u ofertas comerciales.

- **¿Tiene la empresa subcontratados servicios en los que se necesite acceder a datos personales?**

  Es habitual para las empresas trabajar con terceros que tengan acceso a datos de tu titularidad, como por ejemplo, la gestoría que elabora las nóminas de los empleados; las empresas de mantenimiento informático que tienen acceso a sus aplicaciones en las que almacenan bases de datos, empresas de almacenamiento externo y destrucción de documentación, empresas de seguridad y vigilancia, imprentas que etiquetan sobres para mailing, etc…

- **En caso de subcontratar servicios que necesiten acceder a datos personales de tu empresa. ¿Tienes firmados acuerdos de confidencialidad y cesión de datos con estas subcontratas?**

  En caso de subcontratar esos servicios, deberán estar regulados mediante un contrato por escrito que permita acreditar su celebración y contenido, es muy importante que se asegure que el correspondiente contrato de prestación de servicios refleje todos los condicionantes indicados en el artículo 12 de la LOPD.

- **¿Tienes firmados acuerdos de confidencialidad y cesión de datos con tus empleados y han aceptado las obligaciones legales?**

  La LOPD regula también las obligaciones que tienen los empresarios para proteger los datos personales de sus trabajadores así como el deber de secreto y confidencialidad que deben cumplir los empleados. El contrato de trabajo constituye un medio adecuado para ofrecer información de este tipo.

- **¿Los empleados de la empresa han recibido formación en materia de protección y seguridad de datos?**

  Las empresas deben disponer de un protocolo que regule los procesos, responsabilidades, etc. de los trabajadores para con la empresa y viceversa, en materia de protección de datos , siendo la empresa la responsable de informar y formarlos para que sepan que riesgos corren y a que sanciones quedan sujetos.

- **¿Facilitas el ejercicio de los derechos de acceso, rectificación o modificación, cancelación y oposición por parte de los titulares de los datos almacenados?**

  La LOPD reconoce a los interesados unos derechos sobre sus datos personales, que obliga a las empresas, como responsables de dichos datos, a atender los siguientes derechos:

  - Derecho de acceso a los datos de carácter personal en poder de las compañías y sometidos a tratamiento.
  - Derecho de rectificación de aquellos datos que sean incorrectos, inexactos o incompletos.
  - Derecho de cancelación de los datos cuando no sean necesarios, o resulten inadecuados o excesivos.
  - Derecho de oposición, total o parcial, a solicitar que no se traten sus datos.
  - Si desea ejercitar sus derechos de acceso, rectificación, cancelación y oposición sobre sus datos.

- **¿Borras los datos de carácter personal que ya no son necesarios?**

  La LOPD establece que:

  - Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
  - Si los datos de carácter personal resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados.
  - Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

- **¿Dispones de medidas técnicas y organizativas que garanticen la seguridad de los datos de carácter personal teniendo en cuenta la tipología de estos?**

  La LOPD impone al propietario de los datos personales adoptar medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, que variarán en función de la naturaleza y nivel de la información tratada.

- **¿Están los servicios web de la empresa, en los que se manejan datos de carácter personal, físicamente dentro de la UE?**

  Un servicio web es una tecnología que sirve para intercambiar datos entre aplicaciones o redes de ordenadores como Internet.

  Si estos servidores están ubicados físicamente fuera de la Unión Europea, la LOPD técnicamente considera el tránsito de datos como una transferencia internacional, y exige que el país en el que esté físicamente el servidor posea un nivel de protección de datos de carácter personal equiparable al contemplado en dicha norma

- **Si la empresa dispone de cámaras de vigilancia ¿Guardas las imágenes o audios?**

  Estas imágenes no deberían estar guardadas más de 30 días, solo se deberán guardar en casos excepcionales cuando se solicite aporte de pruebas por autoridad competente.

7. **¿En los últimos tres años la empresa ha sufrido algún tipo de sanción o la Agencia de Protección de Datos AGPD le ha abierto algún procedimiento sancionador?**

   En caso de haber incumplido alguna de las normas señaladas por la Administración, o Agencia de Protección de Datos, puedes ser sancionado o multado, estas multas tienen cuantías que varían en función de la gravedad del incumplimiento y pueden llegar a 600.000 €, que a partir de Mayo de 2018 con la nueva Regulación serán de hasta 20 Millones de € o un 4% de la facturación anual.

8. ¿Tras esas sanciones, ha implementado la empresa alguna medida para evitar que se vuelvan a producir?

Es muy importante la prevención. El ciberriesgo se puede cubrir y además se pueden aplicar medidas de prevención para evitar medidas sancionadoras.

9. ¿La empresa hace copias de seguridad de los datos con una herramienta de backup automatizado semanalmente en un dispositivo diferente de donde están los datos originales?

Consideramos una herramienta de backup o copia de backup cuando tiene las siguientes características:

- la copia es realizada por herramientas automáticas
- el resultado de las copias no es el propio equipo físico donde están los datos a copiar
- el sistema de realización de copias debe ser automático
- la realización de la copia debe realizarse de una manera periódica
- Y por supuesto, a partir de esas copias se pueden restaurar los ficheros o datos guardados.

10. ¿Tienes un antivirus actualizado en todos los equipos incluidos en la póliza?

Un antivirus es un software que tiene las siguientes características:

- Detección de virus
- Eliminar los virus
- Actualización de su base de datos de virus con la que realiza las detecciones
- Creación de copias de ficheros infectados evitando su propagación o ejecución

11. ¿Tienes instalado algún firewall o cortafuegos?

Un firewall o cortafuegos son programas informáticos que controlan el acceso de los ordenadores a la red y de elementos de la red a los ordenadores, por motivos de seguridad, pudiendo denegar el acceso en caso de peligro.

12. ¿Actualizas el software de los equipos informáticos de acuerdo con las recomendaciones del fabricante?

En su empresa, se realizan actualizaciones periódicas de software (sistema operativo y aplicativos) teniendo sus equipos actualizados según las recomendaciones del fabricante. Estas actualizaciones de los programas se llaman parches y son actualizaciones ya sea con nuevas funcionalidades o mejoras que arreglan problemas de dichos programas. Cada cierto tiempo los proveedores sacan estos parches aconsejando que se instalen en los sistemas de esas compañías.

13. ¿Existe en tu empresa una política de cambios de contraseñas cada 60 días?

Se deben cambiar las contraseñas regularmente. Dependiendo de la criticidad de los datos puede ser con más frecuencia.

1. La longitud de las contraseñas no debe ser inferior a ocho caracteres. A mayor longitud más difícil será de reproducir y mayor seguridad ofrecerá.
2. Construir las contraseñas con una mezcla de caracteres alfabéticos (donde se combinen las mayúsculas y las minúsculas), dígitos e incluso caracteres especiales (@, ¡, +, &).
3. Usar contraseñas diferenciadas en función del uso (por ejemplo no debe usarse la misma para una cuenta de correo que la usada para acceso a servicios bancarios).
4. Un buen método para crear una contraseña sólida es pensar en una frase fácil de memorizar y acortarla aplicando alguna regla sencilla.

14. ¿En caso de ataque tienes un plan de continuidad de negocio?

Un plan de continuidad de negocio es un plan escrito donde están recogidos los pasos uno por uno y de manera pormenorizada necesarios en caso de que ocurra un incidente que ocasione que la empresa no realice correctamente su función.

15. En el caso de tener servidores, ¿éstos están en una habitación con acceso restringido?

El acceso físico a los servidores/ordenadores está restringido y controlado. Por ejemplo, los ordenadores y servidores están en una habitación con una puerta cerrada con llave y esta llave solo la tienen ciertas personas.

16. ¿Cuántos ataques informáticos ha sufrido la empresa en el último año?

Consideramos como ataque informático, cuando a través de medios informáticos se intenta tomar el control, desestabilizar o dañar el sistema informático de la empresa. En este grupo se consideran los virus, pérdida de datos, indisponibilidad de servicios, etc.

17. ¿Tras esos ataques la empresa ha implementado medios para que no se vuelvan a producir?

Es muy importante la prevención. El ciberriesgo se puede cubrir y además se pueden aplicar medidas de prevención para evitar medidas sancionadoras.