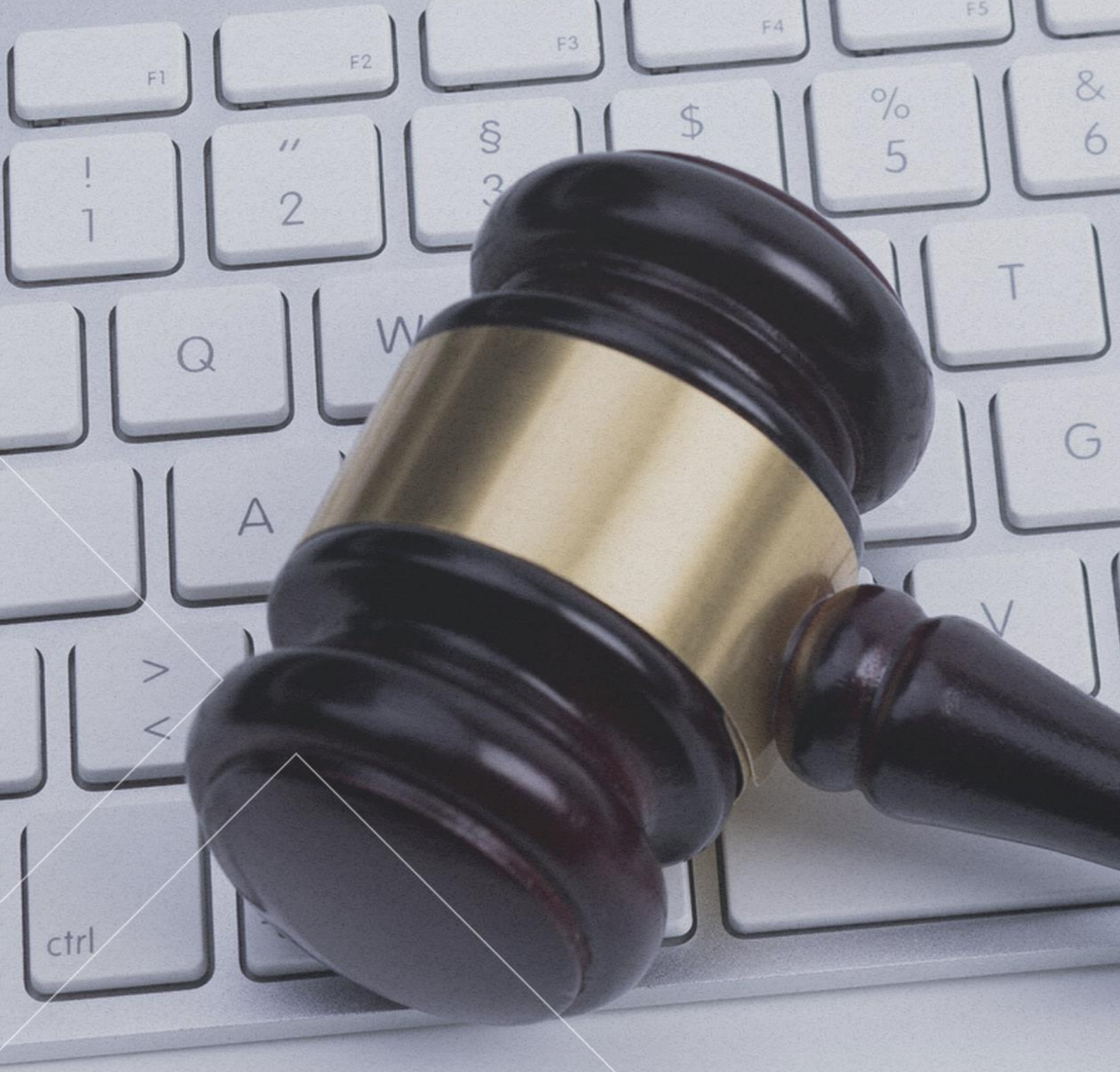

Cumplimento legal

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. CUMPLIMIENTO LEGAL

1.1. Antecedentes

Las empresas han de cumplir las leyes de los países en los que están establecidas o en los que ofrecen servicios y productos. Hoy en día utilizamos la tecnología para desarrollar nuestra actividad y establecer relaciones comerciales. Lo hacemos a través de internet, utilizando correo electrónico, tiendas online, redes sociales o apps para móviles; por ello las empresas debemos conocer las responsabilidades de cumplimiento legal [1] derivadas del uso de estos desarrollos tecnológicos.

Las leyes regulan aspectos de ciberseguridad en muchos ámbitos: las telecomunicaciones, los servicios de los operadores, las relaciones comerciales entre empresas y las relaciones con las administraciones. También protegen a los usuarios [18] en las redes regulando por ejemplo: la privacidad de las personas, los derechos de los consumidores en el comercio electrónico, la firma electrónica y la identidad digital o la propiedad intelectual.

En un mundo globalizado y en constante cambio las leyes están en continua revisión para adaptarse a los nuevos escenarios que plantea la realidad tecnológica: nuevos modelos de negocio (consumo colaborativo, *freemium*), *cloud*, *big data*, ciudades inteligentes, internet de las cosas, etc.

Estas son algunas de las leyes que tenemos que conocer:

- LOPD (Ley Orgánica de Protección de Datos) [2] y el nuevo reglamento europeo de protección de datos RGPD [16], para proteger la vida privada de las personas y sus datos en las comunicaciones electrónicas;
- LSSI-CE (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico) [3] que regula los aspectos jurídicos de las actividades económicas o lucrativas del comercio electrónico, la contratación en línea, la información y la publicidad y los servicios de intermediación;
- LPI (Ley de Propiedad Intelectual) [4], que regula los derechos relativos a las creaciones literarias, artísticas o científicas, en formatos tradicionales (fotografía, pintura, literatura,…) y en formatos digitales (imágenes, videos, contenido multimedia, libros digitales …), incluido el software;
- Leyes de Propiedad Industrial [5], que protegen diseños industriales, marcas y nombres comerciales, patentes y modelos de utilidad;
- Reglamento europeo de identificación electrónica y servicios de confianza en el mercado interior [6], para reforzar la confianza en las transacciones electrónicas entre ciudadanos, empresas y las AAPP en el marco del Mercado Único Digital Europeo.

El incumplimiento de la legislación puede tener como consecuencia sanciones penales y económicas, con el consiguiente daño de imagen y la pérdida de confianza de nuestros clientes.

1.2. Objetivos

Asegurarnos del **conocimiento y cumplimiento** por parte de nuestra empresa de las obligaciones legales en materia de seguridad de la información.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al **cumplimiento legal**.

Los controles se clasificarán en dos niveles de **complejidad**:

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
A	PRO	**Definir y documentar la manera de cumplir con todos los requisitos legales** Detallas los procedimientos a seguir para cumplir con la legislación aplicable a tu empresa en materia de ciberseguridad.	☐
B	PRO	**Garantizar el cumplimiento de los derechos de propiedad intelectual de terceros** Controlas la adquisición y uso del software de tu empresa y de cualquier otro activo que está bajo la protección de leyes de propiedad intelectual.	☐
B	PRO	**Garantizar el cumplimiento de los derechos de propiedad intelectual propios** Revisas que se respetan los derechos sobre las obras de tu empresa.	☐
B	PRO	**Comprobar si tu empresa realiza una actividad comercial en la UE o trata datos personales en la UE o sobre personas que se encuentren en la UE**. Compruebas si existe alguna actividad de la empresa que necesite gestionar datos de carácter personal. Cumples las normas de seguridad en base a un análisis de riesgos si manejas este tipo de información.	☐
B	PRO	**Determinar las responsabilidades para gestionar la protección de datos personales.** Designas un responsable del tratamiento de datos y un DPD si lo necesitaras. Revisas los contratos con los encargados y con el DPD si los hubiera.	☐

NIVEL	ALCANCE	CONTROL	
B	PRO	**Revisar el cumplimiento del deber de informar y que los interesados puedan ejercitar sus derechos según el RGPD.** El Responsable ha de informar sobre el tratamiento; obtener el consentimiento adecuado; permitir a los interesados ejercitar sus derechos; y notificar a las autoridades y a los interesados en caso de brechas.	☐
A	TEC	**Realizar una evaluación de impacto si haces tratamientos de alto riesgo para la privacidad.** Son tratamientos de alto riesgo los que tratan datos de categorías especiales o a gran escala.	☐
B	PRO	**Llevar un Registro de actividades de tratamiento.** Si tienes más de 250 empleados o los tratamientos que realizas son de alto riesgo, realizas el registro de actividades según el RGPD.	☐
B	PRO	**Establecer un procedimiento para notificar en caso de brecha de seguridad.** Si una brecha pone en riesgo la privacidad, actualizas tus procedimientos para notificar en un plazo máximo de 72 horas a las autoridades y sin dilación a los interesados.	☐
B	PRO	**Aplicar las medidas organizativas para adecuarse al RGPD.** Defines los procedimientos necesarios para asegurar que cumples los principios del RGPD, ofreces las garantías para que los interesados puedan ejercer sus derechos; y proporcionas formación adecuada los empleados si van a participar en el tratamiento de datos personales.	☐
B	PRO	**Aplicar las medidas técnicas de seguridad adecuadas según el análisis de riesgos para la privacidad**. Determinas dónde están ubicados los datos, los clasificas según su criticidad, monitorizas su uso, conoces quién accede, cuándo se borran y los cifras cuando sea necesario. Garantizas la confidencialidad, integridad y disponibilidad de los tratamientos y datos personales. Permites que las autoridades puedan verificarlo.	☐
B	PRO	**Revisar si tu empresa realiza comunicaciones comerciales que obliguen al cumplimiento de la LSSI** Cumples con lo establecido en la LSSI garantizando la seguridad en las comunicaciones comerciales.	☐
B	PRO	**Comprobar los requisitos de la LSSI y la LOPD si tu empresa dispone de comercio electrónico o realiza transacciones online** Muestras la información requerida por la LSSI en tu web. Asimismo, informas de la política de cookies de tu web.	☐
B	PRO	**Garantizar el cumplimiento de los derechos de propiedad industrial y marcas propias y de terceros** Revisas que se respetan los derechos sobre diseños industriales, marcas y patentes tanto de terceros como propios.	☐

NIVEL	ALCANCE	CONTROL	
B	PRO	**Otras regulaciones** Tienes en cuenta la existencia de cualquier limitación legal que afecte a la seguridad de la información de tu empresa.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Definir y documentar la manera de cumplir con todos los requisitos legales.** Para cumplir de manera eficiente con la legislación vigente tenemos que definir los procedimientos a seguir para garantizar los requisitos legales, regulatorios, estatutarios o contractuales que afectan a la actividad de nuestra empresa. Además, analizaremos qué información será necesaria para este propósito y cómo tendrá que ser registrada.
- **Garantizar el cumplimiento de los derechos de propiedad intelectual de terceros.** Para cumplir con los derechos de propiedad intelectual [4] debemos concretar y detallar los siguientes aspectos:
    - como debemos adquirir, usar, copiar y eliminar software legalmente;
    - disponer de un registro con los activos que estén bajo la protección de leyes de propiedad intelectual y los contratos mercantiles que nos faculten para el uso de dichos activos;
    - documentar y notificar a nuestro personal las sanciones y las responsabilidades por el uso de software ilegal o no autorizado.
- **Garantizar el cumplimiento de los derechos de propiedad intelectual propios.** Debemos garantizar como empresa los derechos sobre nuestras propias creaciones o sobre las de los propios empleados en virtud de su relación contractual reflejada por escrito.
- **Comprobar si tu empresa realiza una actividad comercial en la UE o trata datos personales en la UE o sobre personas que se encuentren en la UE**. Es importante determinar si existe alguna actividad de nuestra empresa que necesite gestionar datos de carácter personal [16]. Un dato personal es cualquier dato que identifique o que pueda ser asociado a una persona identificada o identificable [17]. El RGPD nos obliga a cumplir ciertas normas de seguridad [8] en base a un análisis de riesgos si manejamos este tipo de información. Si es así has de hacer un análisis de riesgos de privacidad [16], tomar las medidas adecuadas y verificar que puedes demostrar que garantizas la privacidad.
- **Determinar las responsabilidades para gestionar la protección de datos personales** [24]**:**
    - El **responsable del tratamiento** de datos en el RGPD es «la persona física o jurídica […] que sólo o junto con otros, determine los fines y medios del tratamiento; […]».
    - El **encargado del tratamiento** es «la persona física o jurídica […] que en el ejercicio de su actividad trata datos de carácter personal que son responsabilidad del responsable del tratamiento.» La relación entre responsable y encargado debe formalizarse en un **contrato o acto jurídico vinculante** siguiendo las Directrices para la elaboración de contratos entre responsables y encargados del tratamiento [19] de la AEPD.
    - Si realizas tratamientos a gran escala de forma sistemática o con datos especiales será necesario nombrar a un DPD (Delegado de Protección de Datos). El DPD puede formar o no parte de la empresa y puede serlo a tiempo completo o no. Es una figura que además de **cooperar y ser el punto de contacto** con la autoridad, **informa, coordina y asesora** al responsable o al encargado en todo lo relativo al cumplimento del RGPD.

- **Revisar el cumplimiento del deber de informar y que los interesados puedan ejercitar sus derechos según el RGPD.** Según la Guía del RGPD para Responsables del tratamiento [16], el Responsable ha de:
  - **informar** de forma visible, accesible, sencilla y transparente sobre el tratamiento;
  - obtener el **consentimiento** inequívoco o expreso según las categorías de datos del tratamiento;
  - permitir a los interesados **ejercitar sus derechos** de forma sencilla, transparente y en los plazos previstos en el RGPD;
  - **notificar** a las autoridades y a los interesados en caso de violaciones de seguridad que puedan afectarles.
- **Realizar una evaluación de impacto si haces tratamientos de alto riesgo para la privacidad.** Son tratamientos de alto riesgo los que tratan datos de categorías especiales o a gran escala. Las empresas que hacen este tipo de tratamientos deben realizar una Evaluación de Impacto en la protección de datos personales [16].
- **Llevar un Registro de actividades de tratamiento si tienes más de 250 empleados o los tratamientos que realizas son de alto riesgo**. Este registro contendrá la identificación del Responsable, los fines del tratamiento, la descripción de las categorías de los datos, las categorías de destinatarios, las transferencias internacionales si se realizan, los plazos se supresión y la descripción de las medidas de seguridad. En la Guía de Análisis de Riesgos de la AEPD [16], en su anexo, puedes encontrar modelos para Responsable y Encargado.
- **Establecer un procedimiento para notificar en caso de brecha de seguridad que ponga en riesgo la privacidad.** Actualiza tus procedimientos para notificar, en un plazo máximo de 72 horas a las autoridades y sin dilación a los interesados.
- **Aplicar las medidas organizativas para adecuarse al RGPD.** Para garantizar el cumplimiento del RGPD definiremos los procedimientos necesarios. Entre ellos nos aseguraremos de que:
  - se cumplen los principios del RGPD [20];
  - se ofrecen las garantías para que los interesados puedan ejercer sus derechos; y,
  - los empleados reciben formación adecuada si van a participar en el tratamiento de datos personales.

  Se recomienda consultar las guías y documentos de la Agencia Española de Protección de Datos [16] y el apartado de la web de Incibe: RGPD para pymes [21] [24].
- **Aplicar las medidas técnicas de seguridad adecuadas según el análisis de riesgos para la privacidad**. Para ello tendremos que determinar dónde están ubicados los datos, clasificarlos según su criticidad, monitorizar su uso, conocer quién accede, cuándo se borran y cifrarlos cuando sea necesario. Estas son algunas de las medidas técnicas que pueden necesitarse según los casos:
  - Aplicar en fase de desarrollo técnicas de privacidad por diseño y por defecto en base al Análisis de impacto. Utilizar mecanismos de anonimización y seudoanonimización si procede.
  - Implantar controles de acceso, archivo, auditoría y custodia a los ficheros. Utilizar soluciones de prevención de fuga de información [22].

- Instalar herramientas antimalware y antifraude, activarlas y mantenerlas actualizadas.
- Evitar accesos no autorizados y restringir el acceso a los datos aplicando principios de mínimos privilegios mediante sistemas de gestión de identidad y autenticación.
- Tener controlados todos los dispositivos y soportes con herramientas que nos permitan hacer inventarios de los mismos y del software instalado verificando a su vez que sea legítimo y esté actualizado.
- Implantar una gestión de soportes y almacenamiento.
- Proteger las comunicaciones tanto por cable como inalámbricas con equipos específicos, y en particular con cortafuegos, para evitar que puedan estar accesibles a terceros no autorizados. Igualmente tendremos que asegurar las comunicaciones con redes privadas virtuales o VPN u otros mecanismos que cifren la comunicación y permitan autenticar los extremos.
- Planificar y realizar periódicamente backups y copias de respaldo.
- Cifrar los datos con herramientas de cifrado. El cifrado garantiza la confidencialidad e integridad, reduce el riesgo de sanciones y evita que tengamos que informar a los usuarios en caso de brecha de seguridad.
- Implantar una adecuada gestión de incidentes [23].

- **Revisar si tu empresa realiza comunicaciones comerciales que obliguen al cumplimiento de la LSSI.** Si realizamos comunicaciones comerciales a través de la red, deberemos cumplir con la LSSI garantizando la seguridad y la protección de datos en las comunicaciones comerciales (publicidad, envíos masivos,…).
- **Comprobar los requisitos que obliguen al cumplimiento de la LSSI si tu empresa dispone de comercio electrónico o realiza transacciones online.** Si realizas actividades comerciales a través de internet por medio de la web [14] o de una publicación online, deberemos mostrar obligatoriamente la siguiente información:

  - denominación social, NIF, domicilio social, dirección de correo electrónico de contacto y datos de inscripción registral;
  - cuando existan o sean necesarios: códigos de conducta a los que estamos adheridos, datos de colegiación o titulación académica;
  - si vendemos productos: los precios de los productos, especificando claramente los impuestos aplicados y los gastos de envío.

  Si además nuestra web permite la contratación de servicios online [15] deberemos informar sobre:

  - los tramites que se deben seguir para celebrar el contrato;
  - si vamos a registrar electrónicamente el documento del contrato y si este estará disponible;
  - los medios técnicos que permitan corregir los datos erróneos durante la contratación;
  - las lenguas en las que podrá formalizarse la contratación;
  - las condiciones generales del contrato.

  Tendremos en cuenta también que si nuestra web utiliza cookies debemos informar al usuario para que nos permita su instalación en su equipo. Indicaremos asimismo que son las cookies, el propósito de las mismas y quién es el instalador (si son propias o de terceros) [9]. Las cookies están también reguladas en el nuevo RGPD para incluir un consentimiento más explícito por parte del usuario, por lo que recomendamos consultar los documentos de la AEPD [16].

- **Garantizar el cumplimiento de los derechos de propiedad industrial y marcas propias y de terceros.** Estos derechos hacen referencia a las siguientes creaciones inmateriales:
  - diseños industriales;
  - marcas, logotipos y nombres comerciales;
  - patentes y modelos de utilidad;
  - topografías de semiconductores.

  Debemos garantizar que nuestra empresa no hace un uso fraudulento de dichas creaciones cuando son de terceros, del mismo modo, si la creación es propia debemos solicitar nuestros derechos de propiedad a través de la Oficina Española de Patentes y Marcas. Pondremos especial énfasis en proteger las creaciones que determinan nuestra identidad digital.
- **Otras regulaciones.** Revisaremos permanentemente la existencia de algún otro tipo de limitación legal que afecte a nuestra empresa, como pueden ser:
  - restricciones nacionales o internacionales en el uso o adquisición de hardware o software de encriptación;
  - gestión de nombres de dominio;
  - certificados digitales [10] [11];
  - adaptación a ciertos estándares tecnológicos como PCI-DSS [12].

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – ¿Qué te interesa? – Cumplimiento Legal https://www.incibe.es/protege-tu-empresa/que-te-interesa/cumplimiento-legal

[2]. BOE – Ley Orgánica Protección de Datos de Carácter Personal http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750 y BOCG - 24/11/2017 el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal http://www.congreso.es/backoffice_doc/prensa/notas_prensa/57631_1518684517278.PDF

[3]. LSSICE – Ley de Servicios de la Sociedad de Información y Comercio Electrónico http://www.lssi.gob.es/paginas/Index.aspx

[4]. BOE – Texto refundido de la Ley de Propiedad Intelectual https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930

[5]. BOE, Colección Códigos electrónicos. Propiedad industrial http://www.boe.es/legislacion/codigos/codigo.php?id=67&modo=1&nota=0&tab=2

[6]. EUR-Lex – Reglamento UE 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014R0910

[7]. Incibe – Protege tu empresa – Blog -¿Cómo beneficiará a las empresas la reforma de la protección de datos europea? https://www.incibe.es/protege-tu-empresa/blog/beneficios-reforma-proteccion-datos-europea

[8]. Incibe – Protege tu empresa – Blog – Dime qué nivel LOPD tienes y te diré que controles necesitas https://www.incibe.es/protege-tu-empresa/blog/nivel-lopd-controles-necesitas-ciberseguridad-empresas

[9]. Incibe – Protege tu empresa – Blog -¿Qué debe aparecer en la política de cookies de mi web? https://www.incibe.es/protege-tu-empresa/blog/politica-cookies-web-empresas

[10]. Incibe – Protege tu empresa – Avisos de seguridad – El certificado SILCON de la TGSS, dejará de ser válido para su uso en el Sistema RED https://www.incibe.es/protege-tu-empresa/avisos-seguridad/silcon_deja_de_ser_valido

[11]. Incibe – Protege tu empresa – Avisos de seguridad – La FNMT se adelanta a la normativa europea y emite el nuevo certificado de representante https://www.incibe.es/protege-tu-empresa/avisos-seguridad/fnmt_certificado_representante

[12]. Incibe – Protege tu empresa – Avisos de seguridad – Empieza la cuenta atrás para adecuarse a PCI DSS v3.2 https://www.incibe.es/protege-tu-empresa/avisos-seguridad/cuenta-atras-adecuaresPCIDSSv32

[13]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Aplicaciones permitidas https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[14]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Protección de la página web https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[15]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Comercio electrónico https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[16]. AGPD – Reglamento General de protección de datos http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php

[17]. Incibe – Protege tu empresa – Blog – Primeros pasos para cumplir el nuevo reglamento RGPD https://www.incibe.es/protege-tu-empresa/blog/primeros-pasos-cumplir-el-nuevo-rgpd
[18]. Incibe – Protege tu empresa – Blog – La privacidad de clientes y empleados: un valor en alza https://www.incibe.es/protege-tu-empresa/blog/privacidad-clientes-y-empleados-valor-alza
[19]. AGPD – Directrices para la elaboración de contratos entre responsables y encargados del tratamiento http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricescontratos.pdf
[20]. Incibe – Blog – El RGPD da el pistoletazo de salida para su aplicación https://www.incibe.es/protege-tu-empresa/blog/el-rgpd-da-el-pistoletazo-salida-su-aplicacion
[21]. Incibe – Protege tu empresa – RGPD para pymes https://www.incibe.es/protege-tu-empresa/rgpd-para-pymes
[22]. Incibe – Protege tu empresa – Cómo gestionar una fuga de información. Una guía de aproximación al empresario https://www.incibe.es/protege-tu-empresa/guias/guia-fuga-informacion
[23]. Incibe – Juego de Rol - Cuestionario inicial de respuesta a incidentes https://www.incibe.es/sites/default/files/contenidos/JuegoRol/juegorol_cuestionarioinicialrespuestaincidentes.pdf
[24]. Incibe – Protege tu empresa – Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario https://www.incibe.es/protege-tu-empresa/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD