PROTEGE TU WEB

Colección

PROTEGE TU EMPRESA

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

Hoy en día, disponer de una **página web** es una necesidad de casi cualquier negocio: nos permite tener presencia en Internet y ofrecer nuestros servicios de manera global. Además puede servir para solucionar dudas de potenciales clientes y convertirse en un medio adicional de comunicación con ellos.

El incremento del **comercio electrónico** durante los últimos años juega un papel vital en la importancia de las páginas web de nuestras corporaciones. La seguridad de este medio ha adquirido una especial relevancia, tanto por las implicaciones económicas como de reputación e imagen.

El número de compras a través de tiendas virtuales va en aumento conforme los clientes van adquiriendo más confianza en los mecanismos de pago. Para ello es importante que las empresas responsables de las tiendas online, dispongan de mecanismos de **pago seguro**.

Otro aspecto que debemos considerar para mejorar la confianza de nuestros clientes es la utilización de **certificados digitales** y el **cifrado de las conexiones**, al igual que **mostrar la información sobre nuestro comercio** de la manera más detallada y accesible posible. No hay nada que genere más recelos en un posible cliente que una página web donde no podemos localizar la información referente al propietario, ya que eso tiende a transmitir una sensación de inseguridad y desconfianza al usuario que nos visita.

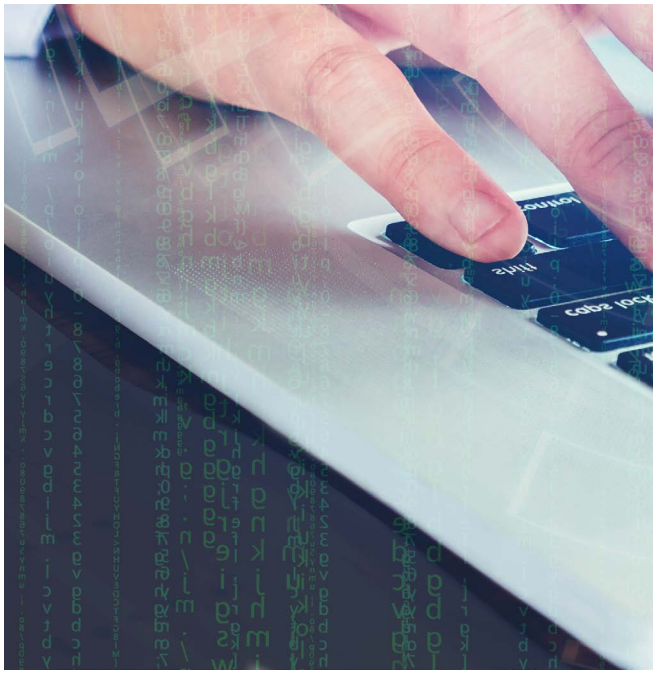
A la hora de poner en marcha una página web podemos **alojarla bien en nuestra propia organización bien en un proveedor externo**. Tanto en un caso como en el otro, la responsabilidad última de la información publicada en la página web y disponible para nuestros clientes es nuestra, y en caso de que ocurra un incidente de seguridad, las repercusiones legales, económicas y de reputación impactarán sobre nuestra organización. Por tanto, no son aspectos que podamos dejar libremente a criterio del proveedor.

1.1. ¿CÓMO PROTEGER NUESTRA WEB?

¿CÓMO PROTEGER NUESTRA WEB?

Para proteger adecuadamente nuestra página web, independientemente de si la alojamos en un proveedor externo o en nuestra propia organización, debemos tener en cuenta las siguientes consideraciones desde cuatro puntos de vista diferentes:

- **aspectos técnicos;**
- **métodos de pago online;**
- **certificados digitales;**
- **cumplimiento legal y normativo.**



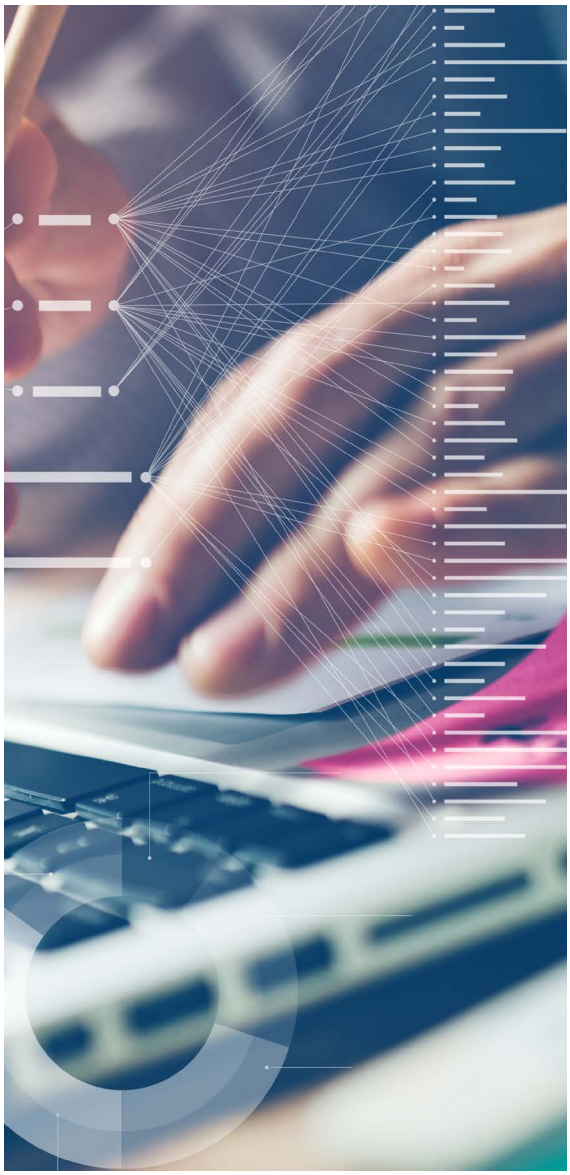
2. ASPECTOS TÉCNICOS

Existen ciertos **riesgos** que debemos **identificar y evitar** para que la página web cumpla correctamente su función. Una de las primeras decisiones que debemos tomar es sobre quién realizará la gestión de la página web, que podemos ser nosotros mismos o externalizarla. Es conveniente evaluar los pros y contras de cada opción, y determinar cuál de ellas nos conviene.

Independientemente de quién realice la gestión y mantenimiento de la página web, existen determinadas **consideraciones y aspectos** a tener en cuenta para garantizar su protección y seguridad, sí que nos ayudarán a evitar riesgos como:

- La sustracción de la base de datos de clientes de nuestra web o de documentos privados de la extranet (si disponemos de ella).
- La alteración de nuestro portal para insertar un *phishing* (cambiando el aspecto de nuestra web para simular a otra empresa) o algún tipo de *malware*.
- La manipulación o modificación de los contenidos del portal web, por ejemplo los precios, la descripción de productos, los medios de pago, los datos bancarios para realizar la transferencia o los datos de contacto de nuestra empresa.

Para que ninguno de los escenarios anteriores llegue a materializarse en la web de la organización, es necesario valorar los siguientes aspectos y aplicar medidas de seguridad adecuadas.



2.1. USO DE SISTEMAS *CAPTCHA*

Si nuestra página web **permite realizar comentarios** o cualquier tipo de **interacción con el usuario** (sistema de valoración de productos o servicios, sugerencias o reclamaciones, etc.), debemos valorar el uso de sistemas *captcha*. Estos sistemas impiden que una máquina pueda actuar como si fuera un usuario introduciendo comentarios, valoraciones o reclamaciones de forma automática. Comentarios que pueden incluir ***spam* malicioso o publicitario**.

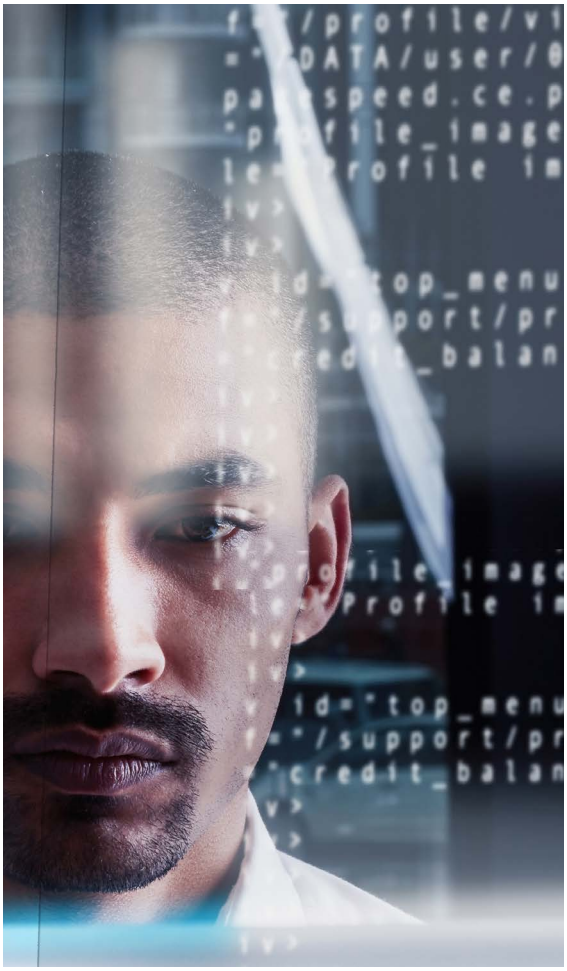
Para ello un *captcha* presenta un contenido que difícilmente puede ser interpretado por una máquina y nos pide que sea tecleado, de esa manera que se asegura que es un humano el que está al otro lado.

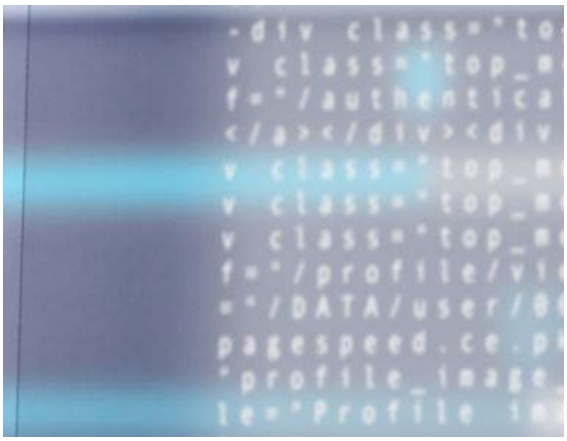
Tanto si la gestión de la página web la llevamos nosotros como un tercero, debemos valorar la conveniencia del uso de estos mecanismos, según el contenido de nuestra página web.

2.2. ELIMINACIÓN DE METADATOS

Si vamos a publicar documentos descargables como folletos, manuales u otra documentación en formatos ofimáticos, es importante que utilicemos alguna herramienta para eliminar los metadatos que estos documentos guardan, ya que pueden proporcionar **información** a un posible atacante **sobre nombres de usuarios, equipos, directorios, etc.** Actualmente los principales productos de ofimática incorporan funcionalidades para realizar esta tarea.

Nosotros mismos, como generadores de los documentos a publicar en nuestra web, debemos ser los que revisemos la correcta eliminación de metadatos antes de su publicación, independientemente de quien sea el encargado de la gestión de la página web.





2.3. ACTUALIZACIÓN DEL GESTOR DE CONTENIDOS

Es habitual que actualmente las páginas web estén basadas en los llamados **gestores de contenidos (CMS)**, como Joomla!, Drupal, Wordpress, etc. Se trata de herramientas que facilitan enormemente el proceso de creación y actualización y mantenimiento de una página web. Si este es nuestro caso es fundamental que mantengamos el gestor de contenido correctamente actualizado.

Cuando se descubre una vulnerabilidad nueva en un CMS, los ciberdelincuentes realizan sondeos mediante sistemas automáticos en busca de páginas con esas versiones vulnerables.

Además, el gestor de contenidos (CMS) puede hacer uso de algún **complemento (o *plugin*)**. Es conveniente que dichos complementos sean ampliamente utilizados en internet, lo que garantiza su soporte y frecuente actualización frente a posibles incidencias de funcionalidad y seguridad.

Tanto si la gestión de la página web la llevamos nosotros como un tercero, **la actualización del gestor de contenidos** y sus complementos, además de la **actualización del software del servidor** deberán ser algunas de las tareas periódicas a realizar. Por otra parte es conveniente estar suscrito a un servicio de avisos de seguridad del propio fabricante del gestor de contenidos y de otro software que utilicemos.

2.4. CONTRASEÑAS ROBUSTAS Y SEGURAS

Independientemente del gestor, debemos asegurarnos de que **las claves que dan acceso al panel de control** de la página web mediante el que creamos y actualizamos los contenidos se generan cumpliendo unos criterios mínimos de seguridad (al menos 8 caracteres y mayúsculas, minúsculas, números o símbolos). También es importante que estas contraseñas sean cambiadas regularmente.

Este punto es particularmente importante, ya que existen programas automáticos que detectan el gestor de contenidos que utilizamos y comprueban si la clave de acceso es la que viene establecida por defecto. Es recomendable cambiar las contraseñas de todos los usuarios por defecto de los gestores de contenidos e incluso deshabilitarlos si no se van a utilizar. Además de las contraseñas es recomendable también **modificar los nombres de los usuarios** que vienen por defecto, como por ejemplo el caso de los administradores.

2.5. GUARDADO DE REGISTROS *(LOGGING)*

Para poder **investigar** cualquier **incidente** relacionado con nuestra página web o incluso poner los registros a disposición judicial si se diera el caso, es necesario **guardar un registro de cualquier interacción con la página web.** Cualquier servidor web dispone por defecto de ésta funcionalidad, por lo que su activación es sencilla.

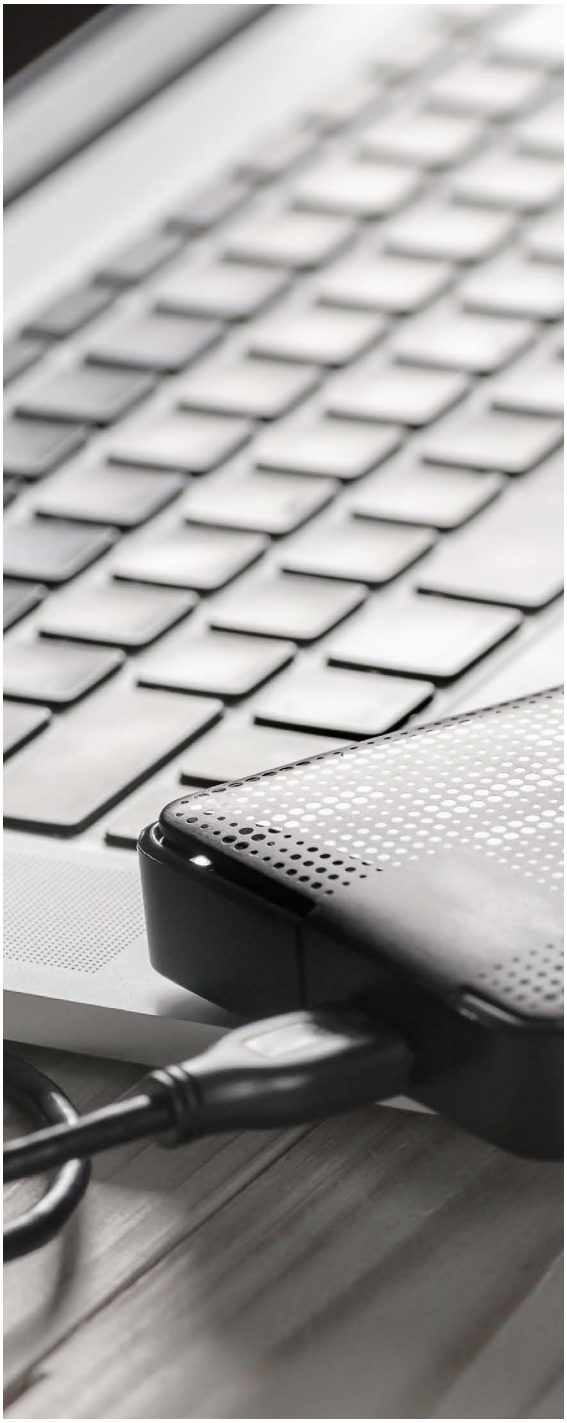
Si la gestión del servidor la llevamos nosotros, seremos nosotros los responsables de guardar esos registros durante un período de tiempo conveniente. Si por el contrario, la gestión del servidor es externa, este aspecto deberá estar reflejado en nuestro contrato con el proveedor, especificando el tipo de registros que se guardan, durante cuánto tiempo y la forma de acceso a dichos registros.

2.6. COPIAS DE SEGURIDAD

Como cualquier elemento de nuestra organización, y más si nuestra página web presta servicios críticos para nuestro negocio (comercio electrónico, medio de contacto habitual con clientes, catálogo de productos, tarifas, etc.), debemos diseñar e implementar **una política de copias** de seguridad que salvaguarde toda la información de nuestra página web.

Si la página web la gestionamos nosotros mismos, deberán incorporarse a la política de copias de seguridad todos los elementos que permitan el funcionamiento del portal web y no olvidándonos de las bases de datos asociadas si las hubiera. Las copias de seguridad deben guardarse en **un lugar diferente** al origen de los datos y verificar puntualmente que se realizan correctamente y que se pueden recuperar los datos.

Si la página web es gestionada por un tercero, debemos incluir la realización de copias de seguridad periódicas de todos los elementos que conforman nuestro servicio web como parte de nuestro contrato con el proveedor.



2.7. ENTORNOS DE PRODUCCIÓN Y PRUEBA

Si tenemos página web con una alta complejidad, puede ser importante disponer de dos **entornos diferenciados** que suelen recibir los nombres de producción y pruebas (o preproducción). Se trata de dos entornos iguales, con los mismos contenidos y la misma configuración. Esto nos permitirá **aplicar parches** (en el entorno de pruebas) y comprobar el correcto funcionamiento de las nuevas **modificaciones** y **funcionalidades** antes de aplicar los cambios sobre la página web visible para los usuarios (el entorno de producción).

Si la página web la gestionamos nosotros, seremos nosotros los responsables de montar y gestionar ambos entornos. Mientras que si la página web la gestiona un tercero, será responsabilidad de nuestro proveedor cumplir con los requisitos de gestión de ambos entornos.

En el caso de que tengamos externalizada nuestra página web, no debemos delegar totalmente la seguridad del portal en el proveedor, puesto que el impacto de cualquier problema de seguridad recaerá siempre sobre nuestra organización.

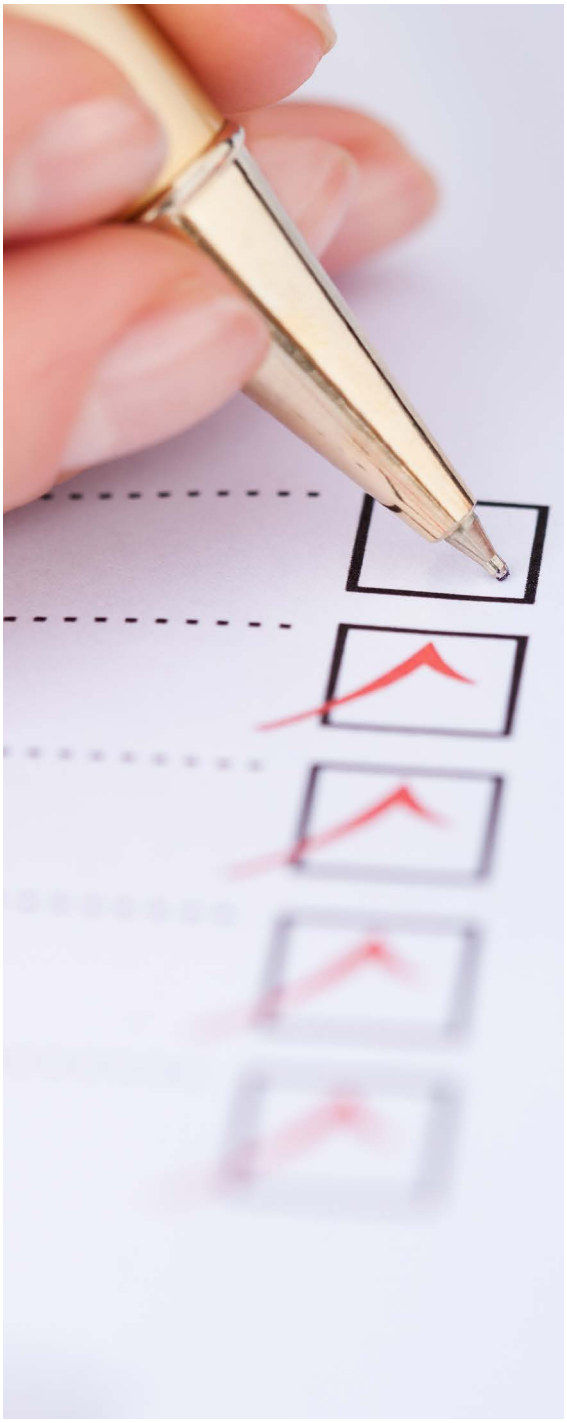
PRUEBAS

PRODUCCIÓN

2.8. METODOLOGÍA DE DESARROLLO SEGURO

Debemos ser capaces de integrar el ámbito de la seguridad a la hora de desarrollar nuestra página web, tanto si lo hacemos nosotros como si contratamos este servicio a un tercero. Es necesario hacer hincapié en aspectos de seguridad tan importantes como los funcionales y debemos **establecer unos requisitos** previos en el campo de la **seguridad**. Este ámbito es aún más importante si vamos a gestionar datos de nuestros clientes a través de la página web.

Utilizando metodologías de desarrollo seguro a la hora de construir nuestra página web nos aseguramos de que nuestra página web cumple con unos requisitos mínimos en cuanto a seguridad de la información. Un ejemplo de estas metodologías de desarrollo seguro es el proyecto **OWASP [1]**, una metodología accesible que se encuentra muy bien documentada.



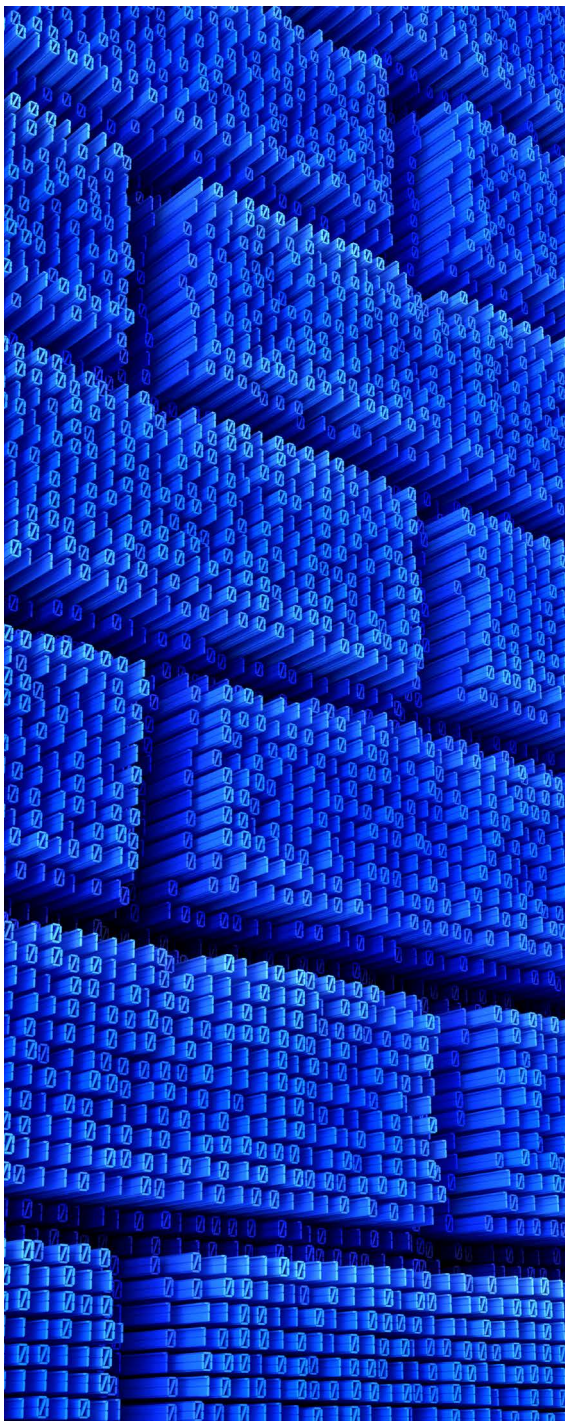
2.9. UBICACIÓN DE LA PÁGINA WEB DENTRO DE NUESTRA RED

Si el alojamiento de nuestra página web es interno, en instalaciones bajo nuestro control, debemos ubicar el servidor web en una subred aislada del resto de servidores internos de nuestra empresa. Para esto necesitamos crear una subred accesible desde el exterior y separada de nuestra red interna mediante segmentación de red. A esta subred se le llama DMZ o **zona desmilitarizada.**

Desde la DMZ no debe haber visibilidad de la red interna de nuestra organización. Es decir, si nos conectamos físicamente a un servidor alojado en la DMZ no podremos acceder a un sistema de la red interna de la empresa. De esta manera, en caso de que nuestra página web sea atacada, no será posible que este ataque afecte al resto de la organización.

Para conseguirlo el tráfico entre la DMZ y la red interna de la empresa debería ser filtrado mediante un **cortafuegos**.

Si la página web es alojada por un tercero, su ubicación no es un riesgo para el resto de nuestra infraestructura, ya que ésta estará albergada en la red de nuestro proveedor y no tendrá ninguna conexión directa con nuestra red corporativa.



2.10. CONEXIONES HACIA EL EXTERIOR

Es posible que nuestra página web requiera conectarse a Internet para realizar sincronizaciones con otras páginas, redes sociales o por cualquier otra razón. Esto supone que la página web tendrá que establecer conexiones «hacia el exterior».

Este tipo de comportamiento y de conexiones debe mantenerse bajo control, para así evitar que si el servidor que aloja la página web se ve comprometido, el atacante no será capaz de establecer conexiones al exterior, realizar ataques a otras empresas o utilizar nuestro sistema o nuestra página para fines ilegales.

Tanto si la gestión de la página web la llevamos nosotros como si la lleva un tercero, las conexiones hacia el exterior desde nuestra página web deberán estar administradas y controladas por una política de conexiones apropiada en el firewall correspondiente, idealmente mediante una **política de lista blanca** (permitiendo sólo aquellas conexiones autorizadas).

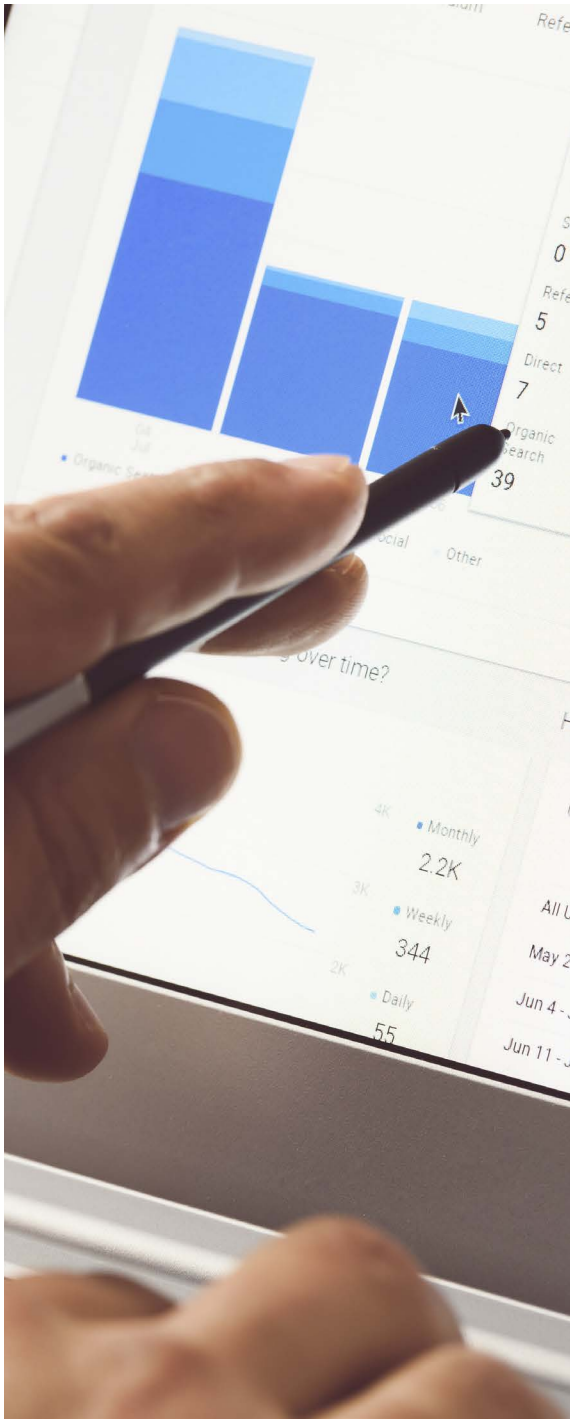
2.11. MONITORIZACIÓN DEL TRÁFICO

Para la detección de cualquier tipo de ataque que nuestra web pueda sufrir, es una buena práctica la **monitorización tanto del tráfico recibido como del tráfico generado**. De este modo no sólo se pueden detectar posibles ataques sino también otras situaciones en las que la web haya sido comprometida.

Si la página web la gestionamos nosotros mismos, es necesario instalar en nuestra red (si no las tenemos aún) ciertas herramientas como un **sistema de detección de intrusos o IDS**. Este sistema de seguridad revisa el tráfico que se transmite a través de la red, identificando posibles comportamientos sospechosos: tráfico con patrones que responden a ataques, incremento excesivo de las comunicaciones o búsqueda de vulnerabilidades propias de los entornos web.

Además, es muy recomendable instalar un cortafuegos de aplicación web o ***Web Application Firewall (WAF)***. Estos cortafuegos son sistemas de seguridad específicos para los servidores de aplicaciones que funcionan detrás de algunas páginas web. Su función es prevenir y detener ataques específicos que no son detectados como tales por un cortafuegos de red.

Si la página web es gestionada por un tercero, debemos incluir ésta monitorización y supervisión del tráfico de red de nuestra página como parte del contrato de nivel de servicio con el proveedor.



2.12. SISTEMA DE RESPALDO

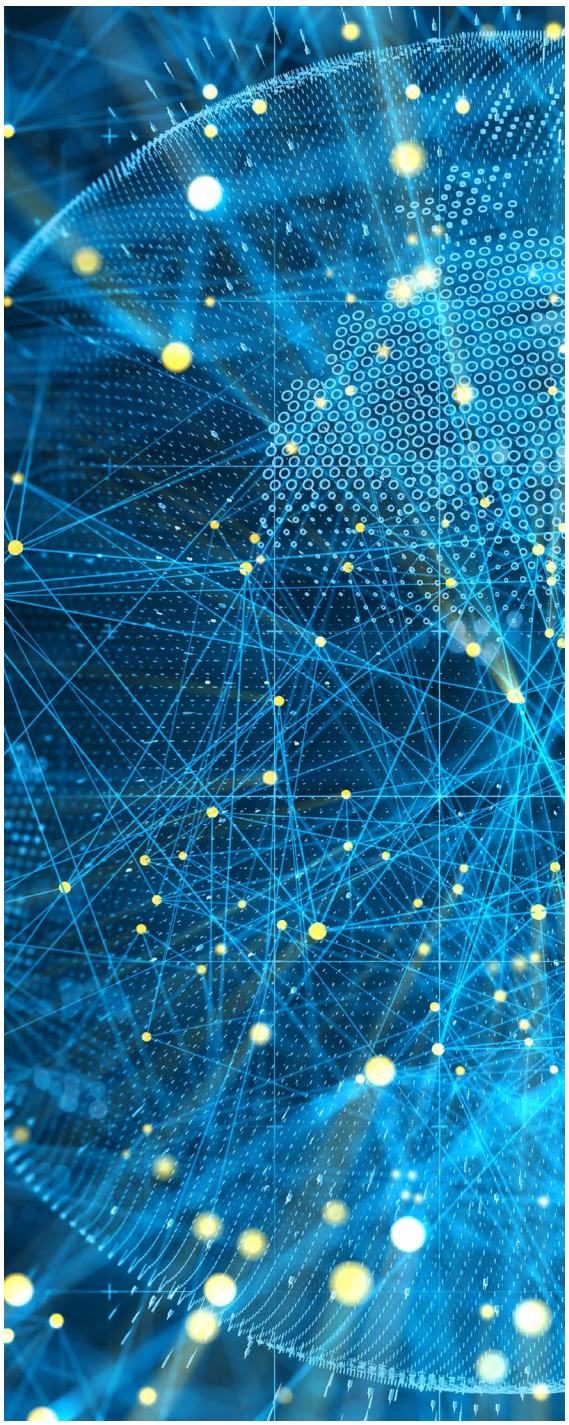
Para evitar que un **incidente** nos deje sin página web, podemos disponer de un sistema de respaldo de nuestra página web que nos permita ofrecer al usuario un conjunto de funcionalidades mínimas en caso de que falle la página web principal.

Si la página web la gestionamos nosotros, podemos consultar con un proveedor externo o habilitar un servidor con menor potencia que se mantenga en modo pasivo hasta que sea necesario. Este **servidor de respaldo** no tiene que cubrir todas las funcionalidades del portal central, pero sí aquellas que nos permitan dar una respuesta y un punto de contacto con nuestros clientes.

Es recomendable que dicho servidor **no comparta la infraestructura principal** del servidor principal, dado que en casos como la caída del suministro eléctrico o la red, ambos sistemas se verían afectados.

Si la página web la gestiona un tercero, este aspecto y sus particularidades deberán estar recogidos en el acuerdo de servicio con el proveedor.

No debemos olvidar que todos los aspectos de seguridad a los que el proveedor se comprometa, así como muchos otros, deben figurar en el documento de contratación.



2.13. AUDITORÍA TÉCNICA

Es recomendable que antes de publicar nuestra página web en Internet llevemos a cabo un **análisis técnico de seguridad o auditoría técnica, tanto de nuestra página web como del servidor** que la contiene. Esto es especialmente importante si nuestra página web no es meramente informativa, sino que va a gestionar datos de nuestros clientes.

Como parte de esta auditoría técnica, se deben llevar a cabo una serie de pruebas que incluyen, entre otras:

- **Análisis de visibilidad externa:** Se comprueban las funcionalidades accesibles desde el exterior a nivel de servidor, el gestor de contenidos usado y los complementos utilizados. Se evalúa si es necesario que dichos complementos y funcionalidades estén habilitados y si no lo es, se deshabilitan para evitar que posibles atacantes puedan aprovecharlas en su beneficio.
- **Contenido del directorio web:** Cualquier archivo o información almacenados en el directorio de nuestra web, es susceptible de ser accedido desde Internet, aunque no esté directamente enlazado desde nuestra página web.

  Es recomendable que el contenido del directorio donde se aloja nuestra página web, ya sea propio o de un tercero, sea revisado frecuentemente y que se evite almacenar en él cualquier información sensible.

- **Búsqueda de vulnerabilidades** propias de los entornos y lenguajes de programación utilizados para crear la página web. A la hora de realizar esta búsqueda de vulnerabilidades, se puede utilizar la **metodología OWASP [1]** entre otras. Entre las posibles vulnerabilidades que puede tener un portal, las más típicas son:

  - ***Cross-Site Scripting o XSS:*** La ejecución de un ataque de XSS, consiste en el envío de un código malicioso como parte de una petición aparentemente legítima. Los puntos de entrada más habituales son los formularios en línea. Una vez ejecutado el XSS, el atacante puede ser capaz de cambiar configuraciones de usuarios, secuestrar cuentas, envenenar *cookies*, exponer conexiones seguras, acceder a sitios restringidos y hasta instalar publicidad en la web víctima del ataque.

  - **Inyección de SQL:** Un ataque de inyección de SQL consiste en la ejecución de un comando malicioso de acceso o modificación de una base de datos como parte de una petición a una página web. Una deficitaria validación de los datos de entrada en la web puede permitir la realización de consultas no autorizadas a la base de datos.

Estos análisis técnicos deben ser realizados por profesionales de la seguridad en sistemas informáticos y es recomendable que los lleve a cabo una empresa independiente que no haya participado en los procesos de desarrollo y gestión de nuestro sitio web.

3. MÉTODOS DE PAGO ONLINE

En el caso de que nuestra página web incorpore la posibilidad de vender productos, es importante seleccionar un sistema de pago adecuado para que nuestros clientes se sientan cómodos y seguros con la compra.

Disponemos de varias soluciones de pago *online* para nuestra página web: pago a contra-reembolso, transferencia bancaria, pago con tarjeta de crédito o a través de entidades intermedias entre las que destaca Paypal aunque existen otras como Google Wallet o Amazon Payments. Cada una de estos sistemas tiene sus ventajas y particularidades tanto para nuestro cliente como para nosotros:

- Aunque el pago **contrarrembolso** no es una forma de pago online como tal, ya que el producto se abona en mano cuando llega el pedido, sí es una forma de pago que se ofrece habitualmente en Internet.

La ventaja para el usuario de este sistema es que le garantiza que sólo pagará por el producto si lo recibe y que no es necesario que envíe sus datos bancarios por Internet.

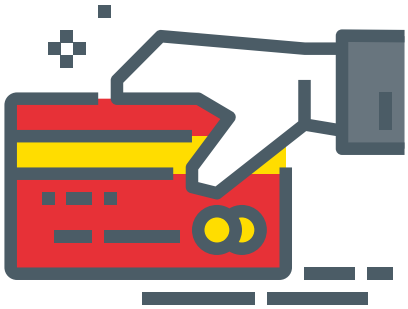
Sin embargo, nosotros como vendedores debemos tener en cuenta la posibilidad de que un cliente decida rechazar un producto que ha comprado y tengamos que hacer frente a los costes de mensajería, inventario, etc. Por ello puede ser necesario establecer un pequeño coste adicional, que nos cubra ante este tipo de imprevistos.

- Mediante la **transferencia bancaria** el comprador hace el pago directamente a través de su banco mediante una transferencia a una cuenta bancaria que le facilitamos.

Debemos tener en cuenta que algunos usuarios son reticentes a este tipo de pagos, imposibles de cancelar una vez se ha asentado el apunte en la cuenta destinatario. El plazo suele ser un día y además

puede tener un coste asociado. El cliente puede ponerse en contacto con nosotros para recuperar el dinero por lo que debemos valorar sus ventajas e inconvenientes para nuestra estrategia de venta.

- El **pago con tarjeta** es actualmente la opción más utilizada y traslada al cliente sensación de seguridad siempre que se realice mediante la pasarela de pago de una entidad bancaria. De este modo, nosotros nunca accederemos a los datos de la tarjeta, sino que dicha información será proporcionada exclusivamente al banco.



Para poder cobrar de esta forma debemos contactar con una entidad bancaria para la instalación de una plataforma segura de pago. Las comunicaciones de estos terminales de punto de venta o TPV virtuales van siempre cifradas (a través del protocolo TLS o Seguridad de la Capa de Transporte, de sus siglas en inglés *Transport Layer Security*) e incorporan medidas de seguridad adicionales proporcionadas por el banco, como tarjeta de coordenadas o código de confirmación por **SMS** al móvil (*Short Message Service*).

Otra ventaja es que para el cliente es la forma más fácil y rápida de pagar ya que el pago es aceptado al instante.

- El pago mediante **entidades intermediarias** es una opción cada vez más utilizada y aceptada por los clientes, siempre que se trate de entidades reputadas como Paypal o asociadas a grandes empresas como Google.

En este caso, el cliente realizará el pago a través de la entidad intermediadora y ésta nos lo remitirá a nosotros. Este tipo de servicios tienen un coste para el vendedor, por lo que deberá analizarse su conveniencia en función del volumen de ventas.

4. CERTIFICADOS DIGITALES

Los casos de intento de **fraude en Internet** se incrementan a la vez que aumenta el uso de este medio para realizar compras o acciones donde se tengan que facilitar datos confidenciales, especialmente bancarios.

Para que estos intentos de fraude no sean exitosos hay que tomar medidas y además, generar la confianza necesaria para que los visitantes y clientes sientan que su información está a salvo. Siempre que en la visita esté implicada una compra, es necesario que el cliente perciba que protegemos la confidencialidad y autenticidad de las comunicaciones mediante los elementos característicos de una conexión segura: «candado» visible en la página, dirección «https», textos informativos, etc.

Todos estos elementos de conexión segura los aporta un **certificado digital**: una herramienta que identifica inequívocamente un sitio web, igual que un DNI identifica a un ciudadano español. Los certificados digitales son **emitidos por entidades internacionales de prestigio** que certifican que el sitio al que accedemos es auténtico y legítimo. Dichas entidades se denominan **Autoridades de Certificación**. Un certificado digital nos aporta también la ventaja de que toda las comunicaciones entre el usuario y nuestro servidor están cifradas mediante una clave de cifrado única asociada al certificado. Por ello, es fundamental la instalación de este tipo de certificados **en cualquier página de comercio electrónico.**

Un ejemplo de una página con un certificado confiable es el siguiente:

Ilustración 1
Ejemplo de certificado confiable

Podemos comprobar que es una página web que va cifrada (ya que el protocolo es https://) y que dispone de un certificado digital de confianza. Esto lo reconocemos porque aparece el **candado** y el nombre de la identidad verificada coincide con la del dominio. Pulsando sobre el candado podemos obtener la información sobre el certificado:

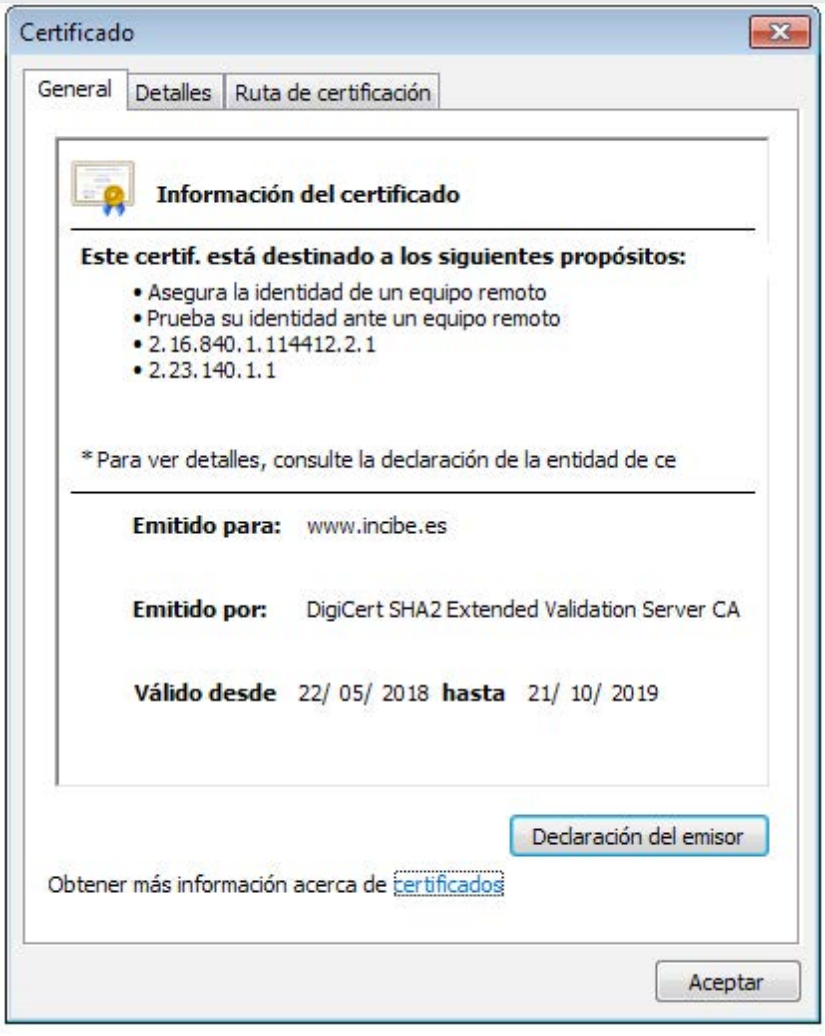


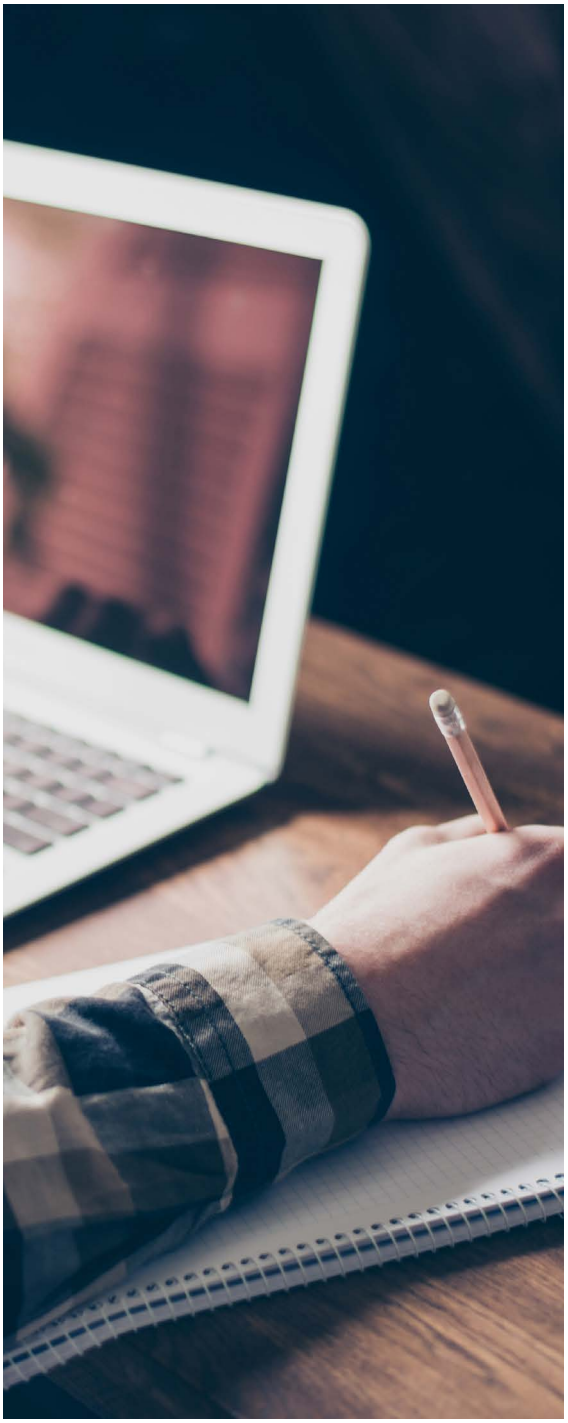
Ilustración 2
Información del certifido

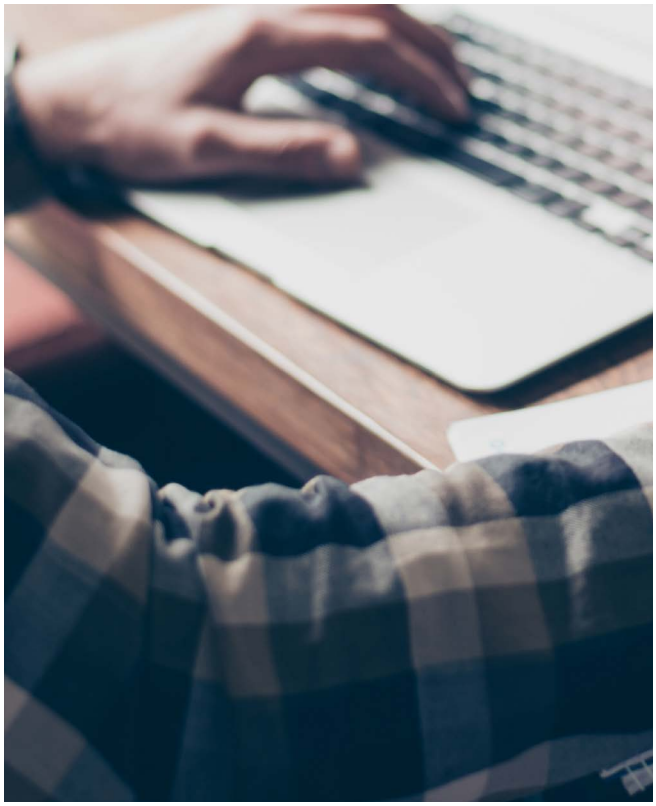
5. CUMPLIMIENTO LEGAL Y NORMATIVO

En cualquier página web, el cumplimiento legal y normativo tiene un papel especialmente importante, ya que en este caso no se trata de recomendaciones sino de imperativos legales.

Nuestra web deberá contener al menos:

- normativa de uso del sitio web;
- aviso legal;
- política de privacidad.





5.1. NORMATIVA DE USO DEL SITIO WEB

La normativa de uso es la información que el propietario de la página aporta al usuario respecto a:

- el contenido del portal web que visita;
- la finalidad del sitio;
- tratamiento de datos correspondiente;
- uso de cookies en el sitio web.

Esta información cumplirá, en el caso de que se realicen actividades económicas, lo indicado en la LSSI-CE (Ley 34/2002) **[3]**.

En cuanto al contenido del portal, se debe incluir el tipo de licencia y la información de derechos de autor **[5]** de la información contenida. Estos aspectos le indican al usuario qué derechos tiene sobre el contenido web. Los tipos de licencia más comunes son *Creative Commons, Copyleft y Copyright.*

- ***Copyright:*** Esta licencia es la más conocida porque es la que se usa en la mayoría de libros, películas y discos. Con esta licencia sólo el autor puede utilizar la obra creada y si un tercero desea utilizarla sólo podrá hacerlo con consentimiento del creador. Una vez adquirida la obra no se podrá distribuir, pues esta licencia sólo permite disponer de la obra para uso personal.
- ***Copyleft:*** Este tipo de licencia permite el uso, la modificación y distribución del contenido de nuestra web, siempre que mantenga las mismas condiciones de utilización y difusión en las obras que se creen a partir de la original.
- ***Creative Commons (CC)*** **[6]**: Hay diferentes tipos de licencias dentro de la CC pero todas ellas permiten la reproducción y distribución con la obligación de mencionar al autor de la obra. Según el tipo de CC usada se puede especificar entre otras cosas si se permite el uso comercial o crear un trabajo derivado del original.

5.2. AVISO LEGAL

El aviso legal es otra información que debemos ofrecer al usuario de nuestra página web, si esta tiene fines comerciales, en cumplimiento con la LSSI-CE **[3]**. Esta ley aplica a las actividades que se realicen por Internet u otros medios telemáticos y persigan un fin económico, es decir, cuando el responsable del portal recibe ingresos, directos (por prestar un servicio o por la venta de un producto) o indirectos (publicidad mostrada en el sitio).

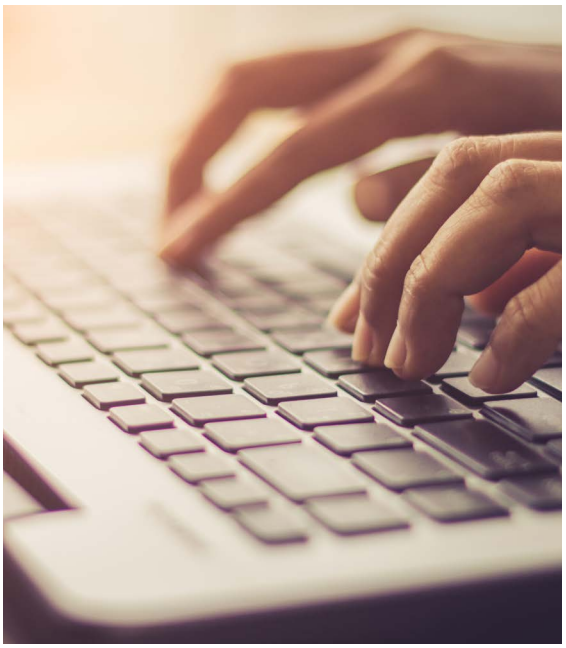
La ley indica que en el aviso legal debe constar, de una forma sencilla, directa y permanente la siguiente información de nuestra empresa:

- denominación social;
- código de Identificación Fiscal (CIF) o Número de identificación fiscal (NIF);
- domicilio y dirección de correo electrónico;
- los datos de inscripción del registro mercantil si fuese el caso.

No necesariamente en el aviso legal, pero también debemos indicar el precio de los productos o servicios con indicación de los impuestos y gastos de envío si los hubiese.

Por último, en el caso de que se lleven a cabo contratos online, se debe también informar, en un paso previo al proceso de contratación, de:

- los trámites que deben seguirse para contratar online;
- si el documento electrónico del contrato se va a archivar y de si será accesible;
- los medios técnicos para identificar y corregir errores en la introducción de datos;
- los idiomas en que podrá formalizarse el contrato.



5.3. POLÍTICA DE PRIVACIDAD

Nuestra página web, si desde ella tomamos datos personales, deberá contener una política de privacidad para cumplir con el RGPD **[2]**. Esta política tendrá además de información sobre los responsables del sitio web:

- La existencia de un tratamiento de datos de carácter personal. Por ejemplo, «Clientes online».
- La finalidad de la recogida de éstos. Por ejemplo, realizar compras online.
- La identidad y dirección del responsable del tratamiento, en este caso nuestra empresa.
- Si existe alguna cesión de esos datos, para lo que es necesario recabar el consentimiento del usuario.
- Dónde ejercer los derechos de ser informado, derecho de acceso, derecho de rectificación, derecho a supresión (derecho al olvido), derecho a la limitación del tratamiento, derecho a la portabilidad, derecho de oposición (o a la exclusión voluntaria) y el derecho a no someterse a la toma de decisiones automatizadas incluyendo la elaboración de perfiles.

Toda esta información debe quedar claramente reflejada, ser comprensible para nuestros visitantes, y estar accesible en la página web.

Para cumplir con el RGPD no basta con informar en la política de privacidad de lo indicado anteriormente, debemos cumplir con las medidas de seguridad recogidas en dicho Reglamento **[2]**.

5.3.1. COOKIES

Un aspecto particular a tener en cuenta es la normativa de *cookies* **[4]**.

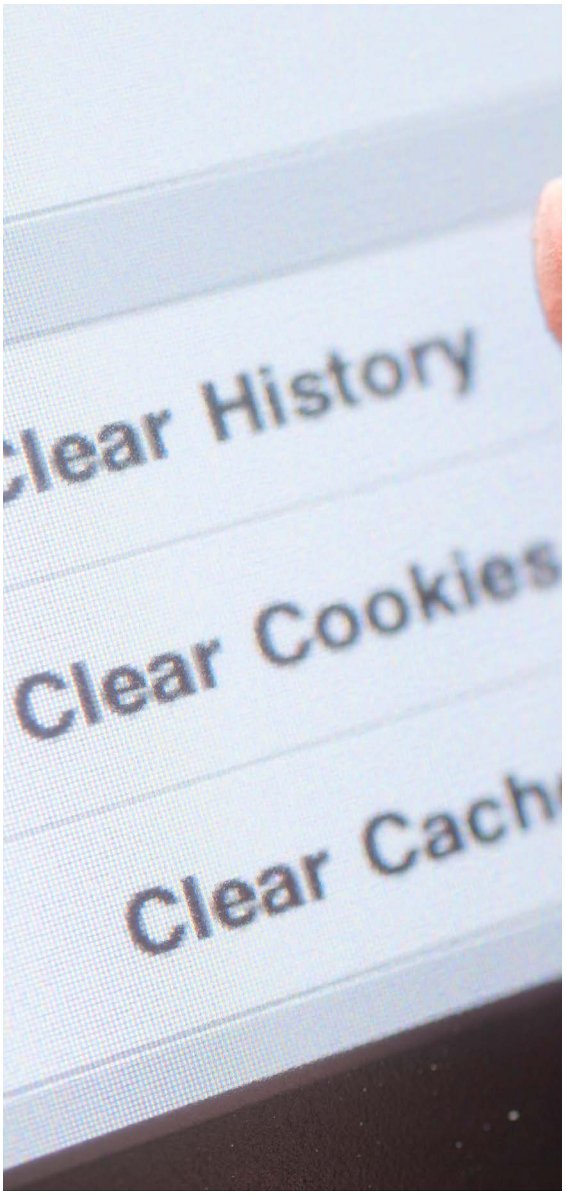
Si las *cookies* son utilizadas para la comunicación entre el equipo del usuario y la red, o son utilizadas para prestar un servicio solicitado por el usuario, es suficiente con mencionar dicho aspecto en la política de privacidad o en el aviso legal.

Si utilizamos las *cookies* para realizar **estadísticas de navegación**, para analizar la **actividad** de los usuarios o para **fines publicitarios**, debemos aplicar el artículo 22 de la LSSI **[3]**.

En estos casos es necesario incluir la siguiente información:

- qué son las *cookies*;
- para qué se utilizan en la página web;
- quién las instala y gestiona;
- cómo pueden ser rechazadas por el usuario, indicando algunos pasos explicativos para que el visitante sepa rechazarlas en el navegador que utilice.

De nuevo toda esta información se debe facilitar al visitante de forma clara y visible, y debe ser aceptada por el usuario. Es suficiente con pedir el consentimiento en la primera visita. En cualquier caso, siempre que se haya informado convenientemente, se asume que da el consentimiento si el usuario sigue navegando.



6. REFERENCIAS

[Ref - 1]. **Open Web Application Security Project, OWASP -** https://www.owasp.org/

[Ref - 2]. **INCIBE, Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario -** https://www.incibe.es/sites/default/files/contenidos/guias/doc/

[Ref - 3]. **BOE, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico -** https://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf

[Ref - 4]. **AEPD, Guía sobre el uso de las cookies -** https://www.aepd.es/media/guias/guia-cookies.pdf

[Ref - 5]. **BOE Legislación. Códigos. Propiedad Intelectual -** https://www.boe.es/legislacion/codigos/codigo.php?id=87&modo=1&nota=0&tab=2

[Ref - 6]. **Licencias Creative Commons -** https://creativecommons.org/licenses/?lang=es_ES


GOBIERNO
DE ESPAÑA
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL


incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD


protege
tuempresa