
# Protección de la página web

## Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# ÍNDICE

**1. Protección de la página web ..... 3**

1.1. Antecedentes ..... 3
1.2. Objetivos ..... 3
1.3. Checklist ..... 4
1.4. Puntos clave ..... 6

**2. Referencias ..... 9**

# 1. PROTECCIÓN DE LA PÁGINA WEB

## 1.1. Antecedentes

Tener presencia en internet mediante una página o portal web es una necesidad para la mayoría de empresas. Esto permite ofrecer servicios de manera global, una comunicación más estrecha con el cliente, ahorro de recursos, publicidad constante, posibilidad de venta *online*, etc.

Una página web es un servicio que ofrecemos desde un equipo conectado a internet, con un software específico (servidor web). Los contenidos de la web los administramos a través de un gestor de contenidos o CMS (Drupal, Joomla o Wordpress por ejemplo), donde está desarrollada la página. Todas las combinaciones son posibles: tener todo en nuestras instalaciones, hacernos una página básica con nuestros medios o con herramientas online (Wix, Weebly, Jimdo,..), contratar el servicio de alojamiento (servidor y CMS) a un proveedor y contratar el diseño de nuestra web.

A la hora de contratar o diseñar la web corporativa debemos tener en cuenta, y exigir a nuestros proveedores en su caso, los siguientes aspectos de seguridad:

- garantías de seguridad, auditorías, sellos, ;
- utilizar metodologías de desarrollo seguro a la hora de construir la web, como por ejemplo la metodología OWASP [1];
- garantizar un acceso seguro al panel de control del sitio web;
- si se trata de una web de venta *online* tendremos que contratar medios de pago seguros;
- realizar copias de seguridad periódicas de todos los elementos que conforman nuestro servicio web;
- mantener el gestor de contenidos (CMS) siempre actualizado;
- guardar registros de la actividad generada en el servidor;
- cumplir con la legislación marcada por la LOPD [2], LSSI [3] y la LPI [4];
- disponer de un certificado digital que garantice la seguridad del sitio web.

Con las medidas de seguridad anteriores podremos evitar posibles ataques a la web o sus consecuencias, tales como:

- denegación de servicio;
- la modificación de los contenidos del portal web (*defacement*), como cambios no autorizados en los precios, descripción de productos, medios de pago, etc.;
- la sustracción de la base de datos de clientes de la web o de información confidencial;
- la manipulación del portal para realizar ataques de *phishing* o de almacenamiento y distribución de malware.

## 1.2. Objetivos

Proteger nuestra página web o tienda *online* de posibles ataques, cumplir con la legislación y garantizar a los usuarios de nuestra web la protección de sus datos personales.

## 1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a la **protección de la página web**.

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/TEC | **Certificado web**<br>Proteges los canales por los que se transmite información sensible (correo electrónico, página web, etc.) mediante el cifrado de las comunicaciones, adquiriendo un certificado web de confianza. | ☐ |
| A | PRO/TEC | **Información del usuario (LOPD)**<br>Aplicas las normas de seguridad exigidas por la LOPD para los datos personales de los clientes. | ☐ |
| B | PRO/TEC | **Desarrollo de terceros**<br>Tienes en cuenta criterios de seguridad en los desarrollos llevados a cabo por terceros. | ☐ |
| B | TEC | **Cumplimiento legal**<br>Cumples con los aspectos legales contemplados en la legislación nacional (LSSI y LPI). | ☐ |
| A | TEC | **Alojamiento en servidor propio**<br>Disponen de medidas de seguridad en los sistemas de alojamiento propio. | ☐ |
| A | TEC | **Alojamiento en servidor externo**<br>Te aseguras que el alojamiento contratado al proveedor disponga de las medidas de seguridad adecuadas y pactadas. | ☐ |
| B | TEC | **Administración por terceros**<br>Mantienes un registro de la actividad de los administradores externos. | ☐ |
| A | TEC | **Configuración del CMS**<br>Aplicas medidas de seguridad al gestor de contenidos. | ☐ |

| NIVEL | ALCANCE | CONTROL | |
|---|---|---|---|
| B | TEC | **Acceso al panel de control**<br>Aseguras que las claves de acceso al panel de control sean fuertes y cumplan los criterios de seguridad. | ☐ |
| A | TEC | **Limitación de accesos**<br>Los servidores web se han configurado con un límite de accesos concurrentes para evitar ataques de denegación de servicio. | ☐ |
| B | TEC | **Usuarios por defecto**<br>Eliminas los usuarios por defecto de las herramientas y software que soporta la web. | ☐ |
| B | TEC | **Guardado de registros (*logging*)**<br>Guardas un registro de cualquier interacción con la página durante un período de tiempo conveniente. | ☐ |
| A | TEC | **Comercio electrónico**<br>Si la web dispone de comercio electrónico elaboras una normativa de seguridad que sigue las pautas indicadas en la política de comercio electrónico. | ☐ |
| A | TEC | **Sellos de confianza**<br>Dispones de un sello de confianza que acredita la seguridad del sitio web. | ☐ |
| B | TEC | **Copias de seguridad**<br>Realizas copias de seguridad periódicas de la web. | ☐ |
| A | TEC | **Auditorias**<br>Se realizan auditorías externas para verificar la seguridad. | ☐ |
| B | TEC | **Software actualizado**<br>Actualizas periódicamente el gestor de contenidos, sus complementos y el software del servidor donde se aloja la web. Estas suscrito a un servicio de avisos de seguridad del fabricante del CMS así como de cualquier otro software que utilices. | ☐ |
| B | TEC | **Protección frente al malware**<br>Instalas antivirus en equipos y servidores. | ☐ |

**Revisado por**: _____ **Fecha:** _____

## 1.4. Puntos clave

Los puntos clave [5] de esta política son:

- **Certificado web.** Si tenemos usuarios que hacen *login* en nuestra página o pueden interactuar con ella de alguna forma (formularios, comentarios,…), es necesario proteger los canales por los que se transmite información mediante el cifrado de las comunicaciones, adquiriendo un certificado web de confianza [12].
- **Información del usuario (LOPD).** Si la web recoge información del cliente, la LOPD [6 y 7] obliga a tomar estas medidas de seguridad:
    - no recabar más datos de los necesarios;
    - tomar las medidas de seguridad adecuadas a los datos (autenticación, control de accesos, control de incidencias, gestión de soportes, copias de seguridad,…);
    - solicitar el consentimiento explícito del usuario, en un lenguaje claro y conciso, para tratar sus datos personales [17];
    - contar con una política de cookies [8]
    - garantizar, indicando cómo ejecutarlos en el Aviso Legal, los derechos:
        - ARCO: acceso, rectificación, cancelación y oposición;
        - y otros derechos: limitación del tratamiento, portabilidad de los datos y a no ser objeto de decisiones individualizadas automatizadas, incluida la elaboración de perfiles.
- **Desarrollo de terceros.** Si contratamos el desarrollo de la web a un tercero, al solicitar el desarrollo debemos incluir requisitos de seguridad como: autenticación y cifrado de credenciales, cumplimiento legal, copias de seguridad, privacidad por diseño y por defecto, y solicitar que se utilicen metodologías de desarrollo seguro [1].
- **Cumplimiento legal.** La página web debe cumplir, además de con la LOPD, con otra legislación vigente [6]:
    - si la utilizamos con fines lucrativos, la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI), indicando con claridad:
        - las condiciones de contratación o las condiciones de uso
        - lo relativo a las comunicaciones comerciales
    - si utilizamos contenidos de terceros, la Ley de Propiedad Intelectual (LPI)
- **Alojamiento en servidor propio.** Si tenemos un servidor web para la página web en nuestras instalaciones, comprobaremos que:
    - se encuentran en la DMZ corporativa [9];
    - dispone de medidas de seguridad perimetrales: cortafuegos y sistemas de prevención y detección de intrusiones (IDS/IPS);
    - dispone de medidas de seguridad contra malware;
    - se han deshabilitado los servicios innecesarios (transferencia de ficheros, mantenimiento remoto,…);
    - el/los administradores utilizan dispositivos y canales seguros para administrar los servidores.
- **Alojamiento en servidor externo** [10]**.** Si la web está alojada en un proveedor revisaremos que el contrato:

- incluye cláusulas de confidencialidad;
- estipula quién es el encargado del tratamiento de datos si fuera necesario;
- incluye acuerdos de nivel de servicio con responsabilidades de seguridad (copias de respaldo, actualizaciones, auditorías,…);
- establece la propiedad del código fuente.

- **Administración por terceros.** Si la web la administra un tercero, debe existir un registro de la actividad de los administradores que podamos consultar y obtener en caso de fraude o de incidentes de seguridad.
- **Configuración del CMS.** Tanto si lo administramos nosotros como si lo hace un proveedor para proteger el gestor de contenidos se deben aplicar y verificar las siguientes medidas de seguridad:

  - deshabilitar los módulos que no se utilicen;
  - eliminar el directorio de instalación;
  - cambiar el nombre del usuario «admin» y el prefijo de la base de datos;
  - utilizar CAPTCHA en los formularios (evitar spam);
  - eliminar metadatos de los documentos e imágenes;
  - vigilar los cambios en los contenidos y los accesos al panel de control;

- **Acceso al panel de control.** Independientemente del gestor de contenidos utilizado, debemos asegurar que las claves de acceso al panel de control se generan cumpliendo los criterios de seguridad [11]. Es recomendable:

  - cambiar los nombres y las contraseñas de todos los usuarios por defecto y deshabilitarlos si no se van a utilizar;
  - proteger al administrador (contraseñas fuertes y cambios frecuentes de contraseña, doble factor de autenticación,…);
  - utilizar comunicaciones seguras para administradores y usuarios;

- **Limitación de accesos.** Los servidores web se deben configurar (tanto en nuestras instalaciones como en las del proveedor) con un límite de accesos concurrentes para evitar ataques de denegación de servicio.
- **Usuarios por defecto.** Tendremos que eliminar o comprobar que se han eliminado los usuarios por defecto de las herramientas y software que soporta la web (servidores web, gestores de contenidos,…).
- **Guardado de registros (*logging*).** Para poder investigar cualquier incidente relacionado con nuestra 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. Si la gestión del servidor la lleva el técnico de la empresa será él quien guarde esos registros durante un período de tiempo conveniente. Si la gestión del servidor es externa, este aspecto deberá estar reflejado en el contrato con el proveedor, especificando el tipo de registros que se guardan, durante cuánto tiempo y la forma de acceso a dichos registros.
- **Comercio electrónico.** Si la web se utiliza para tener una tienda online se debe elaborar y cumplir una normativa específica de seguridad para prevenir el fraude y proteger a los clientes online con las pautas indicadas en la política de comercio electrónico [16].
- **Sellos de confianza** [12]**.** Si la web es una tienda online, es recomendable que este acreditada con un sello que garantice la seguridad del sitio. Los mejores sellos son los que auditan nuestra web periódicamente.

- **Copias de seguridad.** Tendremos que realizar copias [13] periódicas de la web, incluida la BBDD, tanto si está alojada en un servidor propiedad de la empresa como si está en un servidor externo.
- **Auditorias** [14]**.** También se realizará auditorías externas para verificar la seguridad de la web.
- **Software actualizado.** La actualización del gestor de contenidos y sus complementos, además de la actualización del software del servidor deben ser algunas de las tareas periódicas o puntuales a realizar tanto si la gestión de la página web se desarrolla en la empresa como si la realiza un tercero. Por otra parte se considera conveniente estar suscrito a los servicios de avisos o alertas de seguridad del propio fabricante del gestor de contenidos, así como de cualquier otro software que utilicemos que nos indicará de la existencia de actualizaciones puntuales.
- **Protección frente al malware** [15]. Instalaremos un antivirus en todos los equipos y servidores de la empresa, que sirva tanto para el correo electrónico como para la navegación web. Lo actualizaremos periódicamente o puntualmente cuando sea necesario, configurándolo y comprobando que está activo.

# 2. REFERENCIAS

[1]. *Open Web Application Security Project* https://www.owasp.org/
[2]. BOE – Ley Orgánica de Protección de Datos de Carácter Personal http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750
[3]. BOE – Ley de servicios de la sociedad de la información y de comercio electrónico https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
[4]. BOE – Códigos – Propiedad intelectual https://www.boe.es/legislacion/codigos/codigo.php?id=87&modo=1&nota=0&tab=2
[5]. Incibe – Protege tu empresa – ¿Qué te interesa? – Protege tu web https://www.incibe.es/protege-tu-empresa/que-te-interesa/protege-tu-web
[6]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Cumplimiento legal https://www.incibe.es/protege-tu-empresa/herramientas/politicas
[7]. AEPD– Reglamento general de protección de datos https://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php
[8]. AEPD – Guía sobre el uso de las cookies http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf
[9]. Incibe – Protege tu empresa – Blog – La importancia de separar la información pública de interna mediante zonas desmilitarizadas (DMZ) https://www.incibe.es/protege-tu-empresa/blog/segmentacion-dmz
[10]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Relación con proveedores https://www.incibe.es/protege-tu-empresa/herramientas/politicas
[11]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Contraseñas https://www.incibe.es/protege-tu-empresa/herramientas/politicas
[12]. Incibe – Sellos de confianza – Comercio electrónico · https://www.incibe.es/protege-tu-empresa/sellos-confianza/comercio-electronico
[13]. Incibe – Guías – Almacenamiento seguro de la información. Una guía de aproximación para el empresario https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad.pdf
[14]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Auditoría de sistemas https://www.incibe.es/protege-tu-empresa/herramientas/politicas
[15]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Antimalware https://www.incibe.es/protege-tu-empresa/herramientas/politicas
[16]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Comercio electrónico https://www.incibe.es/protege-tu-empresa/herramientas/politicas
[17]. Incibe – Protege tu empresa – Blog – Primeros pasos para cumplir el nuevo RGPD https://www.incibe.es/protege-tu-empresa/blog/primeros-pasos-cumplir-el-nuevo-rgpd



INSTITUTO NACIONAL DE CIBERSEGURIDAD