

Guía de **Ciberseguridad**

PARA MANTENER TU WEB Y TU PYME SEGURAS





En dinahosting llevamos en esto desde 2001, siendo diferentes, ilusionándonos y aprendiendo. Nuestras ganas de hacer comunidad nos han llevado a apoyar grupos de ciberseguridad, Software Libre, WordPress, marketing... así como a patrocinar los eventos tecnológicos más importantes del Estado. También hemos introducido cambios en la parte técnica: la evolución en el hardware, los mejores sistemas de caché, la securización de nuestras herramientas, el apoyo a WordPress como plataforma de ecommerce... y un largo etcétera al que sumaremos todas tus aportaciones.

Todos nuestros servidores trabajan bajo distribuciones propias en las que hemos cuidado cada detalle para optimizar el rendimiento, asegurando una plataforma polivalente que posibilite el uso de diferentes tecnologías. La fiabilidad de nuestros partners de hardware y red se unen a la capa de innovación que hemos aportado mediante desarrollos propios: CMS autoinstalados, Panel de Control exclusivo, email con entorno groupware gratuito, etc. son nuestra aportación para ayudarte a superar los retos que tengas en cada momento.

No te olvides de que también somos registradores de primer nivel para casi todos los dominios del mercado.

¿Te queda alguna duda? Siempre nos tendrás a un solo chat o llamada de distancia las 24 horas del día, los 7 días de la semana. Sin contestadores, sin formalismos, sin esperas... Cuéntanos tu proyecto y haremos todo lo posible por echarle una mano.

Si quieres seguirnos en [Facebook](#), [Twitter](#), [Instagram](#), [LinkedIn](#) o [YouTube](#) también estaremos encantados de ayudarte.

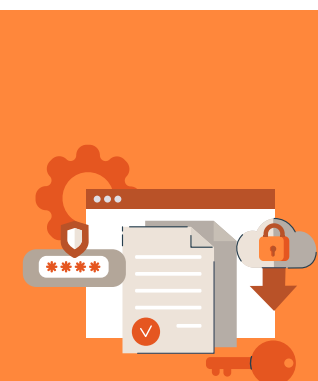
Guía de Ciberseguridad

PARA MANTENER TU WEB Y TU PYME SEGURAS



1. Consejos y recomendaciones de seguridad para ti y para tu negocio

- [1.1. 20 Consejos de ciberseguridad para protegerte](#)
- [1.2. La seguridad de una página web es esencial. ¿Apruebas este checklist?](#)
- [1.3. 6 Tips para un teletrabajo seguro](#)
- [1.4. 10 Consejos de ciberseguridad para pymes](#)
- [1.5. Herramientas para monitorizar la seguridad de tu pyme](#)
- [1.6. Consejos para almacenar información de forma segura](#)
- [1.7. 10 Consejos para mejorar tu seguridad en Windows](#)
- [1.8. Consejos de seguridad para tu marca en redes sociales](#)
- [1.9. Protocolo SSH: ¿qué es y para qué sirve?](#)
- [1.10. Cómo crear contraseñas seguras: consejos y herramientas](#)
- [1.11. Recomendaciones de seguridad en IoT](#)
- [1.12. Cómo y por qué borrar la caché en Chrome, Firefox y Safari](#)
- [1.13. ¿Qué es un CAPTCHA?](#)
- [1.14. Implementar Google ReCAPTCHA en un formulario PHP](#)



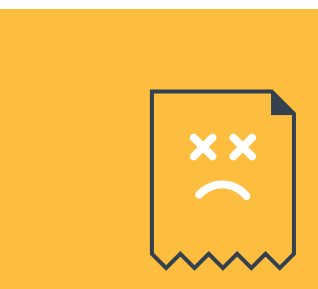
2. Tus servicios más seguros en dinahosting

- [2.1. 13 Medidas para securizar aún más tu Panel y servicios](#)
- [2.2. Por qué necesitas una copia de seguridad diaria de tu hosting](#)
- [2.3. ¿Cómo funciona el servicio de Backups?](#)
- [2.4. La seguridad de nuestros Hosting Linux](#)
- [2.5. Consejos de seguridad para tu correo electrónico](#)
- [2.6. ¡Que no suplanten tu identidad! Activa el registro SPF en tu dominio](#)
- [2.7. ¿Qué son los registros SPF, DKIM y DMARC?](#)
- [2.8. Autenticación en 2 pasos: qué es y qué herramientas necesitas para activarla](#)
- [2.9. ¿Qué es y para qué sirve Firewall DNS?](#)
- [2.10. ¿Alojamiento web en España o en Estados Unidos?](#)



3. Seguridad WordPress

- [3.1. Seguridad para tu WordPress: primeros pasos](#)
- [3.2. Cómo securizar tu WordPress: buenas prácticas y algunos plugins](#)
- [3.3. Cómo recuperar tu contraseña en WordPress](#)
- [3.4. 6 Plugins de seguridad en WordPress](#)
- [3.5. Plugins de protección de datos en tu tienda en WooCommerce](#)
- [3.6. Proteger tu WordPress mediante .HTACCESS: 5 consejos](#)
- [3.7. Qué son wp-admin y wp-login.php de WordPress](#)
- [3.8. Cómo añadir Google reCAPTCHA a tu WordPress](#)



4. Errores HTTP

- [4.1. Soluciona los errores HTTP de tu web con estos tips](#)
- [4.2. Error 403 "Forbidden": qué es y cómo solucionarlo en tu web](#)
- [4.3. HTTP error 404: ¿qué es? ¿Cómo lo soluciono?](#)
- [4.4. HTTP error 500. Qué es y cómo solucionarlo en tu web](#)
- [4.5. Qué es un error 502 y cómo solucionarlo](#)
- [4.6. ¿Qué es el error 503? Causas y soluciones](#)
- [4.7. Cómo arreglar el error 504 Gateway Timeout](#)

Guía de Ciberseguridad

PARA MANTENER TU WEB Y TU PYME SEGURAS



5. Certificados SSL

- [5.1. ¿Tu web no tiene HTTPS? Google dice que no es segura](#)
- [5.2. Por qué debes instalar ya un certificado SSL en tu web](#)
- [5.3. Certificados SSL Let's Encrypt: seguridad para tu web gratis](#)
- [5.4. Nuevos certificados SSL GlobalSign](#)



6. Protección de datos

- [6.1. Checklist RGPD: ¿tu web cumple esta normativa?](#)
- [6.2. Protección de datos en tu tienda online: cómo cumplir con la normativa](#)
- [6.3. ¡Que no te sancionen! Pon tu web al día con la Ley de Cookies](#)
- [6.4. ¿Qué textos legales necesita tu web o ecommerce?](#)
- [6.5. 4 Criterios legales en la elección de tu hosting](#)



7. Amenazas online

- [7.1. Protege tu pyme: las 10 amenazas online más frecuentes](#)
- [7.2. ¿Qué es el email phishing?](#)
- [7.3. ¿Qué hacer si has recibido un correo phishing?](#)
- [7.4. Phishing con fraude en bitcoins](#)
- [7.5. Cuidado donde compras: ojo al phishing en ecommerce](#)
- [7.6. Ransomware: qué es y cómo combatirlo](#)
- [7.7. ¿Qué es el SPAM? ¿Cómo defendernos de él?](#)

GUÍA DE CIBERSEGURIDAD

1. Consejos de seguridad para ti y tu negocio

[1.1. 20 Consejos de ciberseguridad para protegerte](#)

[1.2. La seguridad de una página web es esencial. ¿Apruebas este checklist?](#)

[1.3. 6 Tips para un teletrabajo seguro](#)

[1.4. 10 Consejos de ciberseguridad para pymes](#)

[1.5. Herramientas para monitorizar la seguridad de tu pyme](#)

[1.6. Consejos para almacenar información de forma segura](#)

[1.7. 10 Consejos para mejorar tu seguridad en Windows](#)

[1.8. Consejos de seguridad para tu marca en redes sociales](#)

[1.9. Protocolo SSH: ¿qué es y para qué sirve?](#)

[1.10. Cómo crear contraseñas seguras: consejos y herramientas](#)

[1.11. Recomendaciones de seguridad en IoT](#)

[1.12. Cómo y por qué borrar la caché en Chrome, Firefox y Safari](#)

[1.13. ¿Qué es un CAPTCHA?](#)

[1.14. Implementar Google ReCAPTCHA en un formulario PHP](#)





1.1 20 CONSEJOS DE CIBERSEGURIDAD PARA PROTEGERTE

Compartimos contigo **20 consejos de ciberseguridad** muy sencillitos, pero que aplicándolos todos juntos te ayudarán a mantener tu correo, web u otros equipos ultra protegidos.

Esperamos que te sean de utilidad y que comiences a ponerlos en práctica desde ahora.

1. Aumenta tu seguridad auditando tus contraseñas

Asegúrate que tus contraseñas tengan una combinación de caracteres fuerte y actualízalas constantemente.

Evita las contraseñas comunes tipo 1234, abcde, password, etc. y siempre que puedas, utiliza claves diferentes en tus dispositivos y cuentas.

¿Sin ideas para crear contraseñas seguras? ¿Cómo memorizarlas y guardarlas? [Echa un ojo a este capítulo.](#)

2. Actualiza los navegadores

Cuando todo va bien nos olvidamos de las tareas más básicas, como es tener **actualizados nuestros navegadores y sistemas antivirus**. Eso sí, cuando actualices tus navegadores hazlo desde la página oficial del proveedor.

3. Evita usar WI-FI públicas

Seguro que más de una vez te has conectado a una red **Wifi pública y gratuita** en algún viaje, aeropuerto o cafetería. Al usarlas estamos exponiendo nuestros datos, tráfico e identidad.

Si no te queda más remedio que usar una, a la hora de conectarte indica que esa **conexión es una red pública** (y no de trabajo o doméstica) y así evitarás que tus carpetas o recursos estén a disposición de cualquier usuario. E intenta en la medida de lo posible **no acceder a cuentas bancarias**, correo o redes sociales usando Wifi.

4. Tapa la webcam

Si no vas a usar tu webcam tápala con un protector, estarás protegiendo tu intimidad. **Pero no solo la cámara es vulnerable, sino también el micrófono o incluso el teclado**. Desactívalos siempre que no los uses.

Si has estado en alguno de nuestros eventos, seguro que ya tienes tu tapa de webcam :) Y si todavía no la tienes, sigue nuestra ruta en redes. ¡Pronto volveremos!

5. Adjuntos con malware o ransomware

A los ciberdelincuentes les encanta **ocultar malware o ransomware en archivos como documentos o presentaciones**. Al descomprimirlos o abrirlos estarás dándole libre acceso a tu información a los hackers.

Recientemente estamos recibiendo correos con el asunto **Enfermedad de Coronavirus (Covid-19)**. Dentro del email los usuarios verán información relacionada, pero el problema del correo es que incluyen un archivo ejecutable llamado CURE.exe o similar que introduce una amenaza en nuestro sistema.

Lo mejor que puedes hacer es fijarte en el remitente, en el cuerpo del mensaje y en el nombre del archivo. Ante la mínima duda, borra el correo.

6. ¿Sabes detectar el phishing?

Muy relacionado con el punto anterior está el phishing. Y es que seguro que en más de una ocasión has recibido un **correo en el que se intentaba suplantar la identidad de una empresa** u organización, y te pedían datos sensibles como tu número de cuenta bancaria.

Como claves para detectar el phishing fíjate en el saludo del mensaje, en el correo del remitente o la firma. Échale un vistazo al [capítulo 7](#) para saber más sobre esta estafa.

7. Protege y actualiza tus sistemas operativos

Más reciente es sinónimo de más resistente. Si llevas semanas postergando esa actualización del sistema operativo, no lo dejes pasar más tiempo.

- **Vigila el estado de actualización** de tus sistemas operativos de forma regular. Márcate una fecha en el calendario para hacerlo cada 15 días, por ejemplo.
- Opta por las **actualizaciones automáticas** para mayor comodidad.
- En cuanto salga una actualización, hazla ya y no lo postergues. Corres el riesgo de que se te olvide.
- Acude a la **página oficial**.
- Si el sistema operativo está obsoleto y no te ofrece las mayores garantías, no lo uses.

8. Actualiza tu smartTV

También son muy importantes las **actualizaciones de nuestros dispositivos como la televisión**, ya que suponen una puerta de entrada a nuestros datos personales.

Una smartTV debe tener el mismo mantenimiento que tu móvil u ordenador, ya que cuentan con sistema operativo propio, tienda de aplicaciones o puertos de entrada.

La tele es uno de los electrodomésticos más usados. Te recomendamos que revises las actualizaciones del sistema y elimines las APP dudosas que puedan poner en jaque tu seguridad.

9. Revisa los logs de tu correo o redes

Los logs son los encargados de explicarnos el comportamiento de nuestros sistemas o programas. Analizando los registros de actividad podrás detectar **fallos de rendimiento, mal funcionamiento, errores e intrusiones**.

Por ejemplo, si recibes un correo notificándote de que se ha bloqueado un intento de inicio de sesión, primero comprueba la actividad y si no has sido tú, cambia inmediatamente la contraseña para proteger tu información.

10. Activa alertas antifraude en tu banco

Ser preventivos es la arma más eficaz contra el fraude y el mejor consejo que te podemos dar. Por ello te recomendamos que te subscribas a los sistemas de alertas para recibir un informe de los movimientos realizados en tus tarjetas o cuentas, y así detectar al momento si te han hecho un cargo sospechoso.

11. Desactiva el bluetooth u otras conexiones

¿A qué no te dejas el grifo de agua abierto cuándo no lo necesitas? Pues con el bluetooth debería pasar lo mismo. Si lo usas para conectar tu móvil al coche, asegúrate de desconectarlo al finalizar tu viaje.

12. Usa una VPN

Una de las herramientas de seguridad más importantes y totalmente imprescindible para teletrabajar es la instalación de una **VPN, o red Privada Virtual**, en nuestro portátil.

La VPN se usa especialmente para acceder a información confidencial de nuestra empresa de manera remota, y es especialmente necesaria cuando la red que usamos no ofrece las mejores condiciones de seguridad.



Para más información
Mira el vídeo
¿Qué es una VPN?

13. Configura métodos de verificación en dos pasos

La verificación en 2 pasos (2-Step Verification) es un sistema adicional de seguridad que se intercala en el login de tus servicios proporcionándoles **una nueva capa de control**. La premisa en la que se basa es que para poder acceder a tu servicio debes combinar algo que sabes y algo que tienes:

- **Algo que sabes:** tu contraseña.
- **Algo que tienes:** un número de 6 dígitos generado automáticamente cada 30 segundos en tu aplicación móvil.

Sin esta combinación de ambos elementos no se permite el acceso.

Podrás configurar la verificación en dos pasos en nuestro [Panel de Control](#) o [Webmail](#) de forma muy fácil. [Echa un ojo a este contenido para saber cómo activarlo.](#)

14. Instala un certificado SSL en tu web

Los [certificados SSL](#) son un must para dar más seguridad y confianza a los usuarios de tu web. Si todavía no tienes uno, ahora es un buen momento para activarlo.

En dinahosting disponemos de [5 certificados diferentes](#) y ajustados a tus necesidades.

Este tipo de certificados activan el protocolo HTTPS en tu web, cifrando las comunicaciones que se produzcan en el sitio y marcándola como segura para los posibles visitantes.

Por este mismo motivo, también es recomendable y más seguro que navegues por webs que tengan este certificado.

15. Controla los permisos de tus aplicaciones

Muchas de las aplicaciones que nos instalamos acceden a nuestra lista de contactos, cámara de fotos, micrófono o ubicación. Todo esto es información muy sensible. Echa un ojo a todas las aplicaciones que tienes en tu móvil y **reconfigura sus permisos para protegerte**.

16. Ojo con lo que publicas online

Todo lo que pones en la red es susceptible de que lo vea cualquier persona o bot. En la medida de lo posible, evita publicar información personal o sensible que puedan utilizar terceros en tu contra tanto si es tuya como de otros.

Nunca subas fotos de documentación importante, reveles tu dirección o pongas los datos de tu tarjeta, por ejemplo, en redes sociales, foros, comentarios de blogs, etc. **Siempre puede haber alguien espiando.**

17. Desinstala programas que no utilices

Muchas veces instalamos aplicaciones o programas en nuestros equipos para probar alguna funcionalidad y luego nos olvidamos de ellos. **Si no tienes pensando volver a usar un programa lo mejor es que lo desinstales.**

Piensa que los programas son como pequeñas puertas que acceden a nuestros equipos o datos. Mejor cierra esas puertas desinstalándolos. Revisa y borra complementos de los navegadores, plugins de los CMS, addons de correo, aplicaciones... Previene amenazas y además ahorrarás espacio.

18. Descarga solo lo necesario

Si no tienes por qué descargar algo, no lo hagas. Como te comentábamos en el punto 5, es habitual que los hackers escondan malware en los adjuntos de correo, pero también puedes descargarte algo que no debes online.

En la red hay infinidad de sitios fraudulentos que utilizan diferentes técnicas para que los usuarios piquen y descarguen sin saberlo virus o troyanos que infectan sus equipos.

Las páginas de descargas ilegales de películas, libros, música... están plagados de ellos. Pero también puedes descargarte un virus de una página disfrazada de legal.

No realices descargas innecesarias de fuentes dudosas no seguras ni por supuesto, ilegales.

19. Si sospechas actúa con precaución

Si algo te parece sospechoso como un correo, una alerta, una web, un link... Antes de clicar o realizar alguna acción sobre el elemento analiza la situación y actúa con precaución.

Trata de informarte antes o pide consejo a tus colegas o al responsable de ciberseguridad si no sabes como proceder.

Si por ejemplo, crees que alguien ha accedido a tu cuenta, cambia la contraseña. O si recibes un enlace o archivo sospechoso analízalo con tu antivirus u otras herramientas ([VirusTotal](#), [Metadefender](#) o [VirSCAN](#)) antes de abrirlo.

¿Sabes qué en dinahosting realizamos auditorías de seguridad? Es uno de los servicios ofrecidos en nuestra área de [Asesoría Técnica](#).

20. Mantente informado

Casi tan importante como actualizar el software es estar uno mismo al tanto de las últimas noticias en ciberseguridad.

Si estás enterado de que se ha producido un ataque online de una determinada forma es mucho más difícil que caigas en la trampa. También es importante estar informado por si surgen nuevas formas de mantenerte protegido en la red.

Presta atención a las noticias de sobre ciberseguridad para estar al día y minimizar los riesgos.



1.2 LA SEGURIDAD DE UNA PÁGINA WEB ES ESENCIAL. ¿APRUEBAS ESTE CHECKLIST?

La seguridad de una página web es muy importante no solo para ofrecer una excelente experiencia de usuario, sino también para la reputación online de tu negocio.

Razones para hacer tu página más segura

Mejor posicionamiento y reputación en buscadores

Si tu web no dispone de un buen certificado de seguridad, puede ser un blanco fácil de ataques informáticos.

Google penaliza aquellas páginas que son hackeadas y peligrosas para sus visitantes, lo que afectará a tu posicionamiento en buscadores. [Cuidar el SEO de tu web](#) es esencial para situarte en lo más alto.

¡No te olvides!

Además, un hackeo o advertencia de que tu web no es segura perjudica tu reputación online. **Cuando la reputación online se ve afectada, se tardan años en poder recuperarla.**

Aumento de las conversiones en tu web

Y ahora piensa en cómo te comportas como usuario. Entrás en una web de ropa y te topas con contenido no seguro. Inmediatamente cierras la página sin efectuar ninguna acción. **¡Eso son menos ventas para tu ecommerce!**

Existen múltiples conversiones, como suscribirse a una newsletter, enviar un formulario o efectuar una compra, y todas ellas son esenciales para incrementar la tasa de conversión de tu web.

Incremento del tráfico y ventas en tu web

El aumento del tráfico y la seguridad de una página web van estrechamente ligados. **Cuanto más segura y robusta sea una web, más visitas recibirá**, y por lo tanto, más posibilidades de que tus clientes efectúen una compra con total tranquilidad.

Checklist para mejorar la seguridad de una página web

Si tu web ha sufrido un hackeo o prefieres prevenir, estos consejos te ayudarán a mantener tu web segura.

1. Empieza por el hosting

Que tu hosting **pueda con todo, sea seguro y transmita fiabilidad** es tu mejor inversión de presente y futuro. A la hora de elegir un hosting para tu web, fíjate en que la plataforma sea estable, que el [centro de datos esté en España](#), en el Panel de Control que te ofrece y las copias de seguridad para tu web, por ejemplo.

Repasa estos post en los que te damos [consejos para elegir el mejor hosting](#) y [las series que publicamos anteriormente](#).

2. Usa contraseñas seguras

Si usas autoinstalables en tu web como WordPress, Joomla o PrestaShop, te recomiendo que las contraseñas que elijas sean seguras.

En este capítulo te daba una serie de claves, tanto para [crear contraseñas indescifrables](#) como para recordarlas.

3. Confía en un buen equipo técnico

En dinahosting, contamos con un equipo de Soporte especializado, que te ayudará a mantener [tu hosting seguro y optimizado](#). Dispones de **auditorías de seguridad**, modificación de rutas, entorno de staging, servicio de backups... Además de un servicio de desinfección en caso de que tu hosting tenga alguna vulnerabilidad.

4. Actualiza, actualiza, actualiza

Como te comentábamos en el punto dos, si tu web está montada con un autoinstalable como WordPress, WooCommerce o Joomla, mantenlos actualizados. **No pierdas ojo de las actualizaciones** que publiquen, como nuevas versiones de plugins o plantillas, y actualízalos a la última versión.

5. Haz backups diarios y de forma automática

Ante la inmensa cantidad de información que almacenamos diariamente, es indispensable contar con un buen servicio de backup, ya que de producirse un incidente, podrás seguir accediendo a todos los datos de tu empresa.

Desde tu [Panel de Control](#) de dinahosting puedes restaurar tu web, bases de datos o correo a un estado anterior. O simplemente disponer de una copia de seguridad de tu web por si en un futuro la necesitas. Consulta este post de ayuda en el que te explicamos paso a paso [cómo realizar o programar backups](#).

6. Contar con un buen certificado de seguridad en tu web

Tal y como mencionamos al principio, un buen certificado es vital para la seguridad de una página web. **Google ya está marcando como no seguras aquellas webs que no disponen de HTTPS**, por eso debes hacerte cuanto antes con un [certificado SSL](#) si no lo tienes.

La seguridad de una página web es vital tanto para tus clientes como para tu negocio. Esperamos que estos consejos te sean de utilidad,.

Ven a dinahosting

Contamos con soluciones a la medida de cada proyecto





1.3 6 TIPS PARA UN TELETRABAJO SEGURO

Si a ti también te ha tocado llevarte la oficina a casa, no bajes la guardia y sigue estas recomendaciones básicas de ciberseguridad. Seguro que muchas de ellas ya te suenan, pero nunca está de más recordarlas para garantizar el **intercambio seguro de información en tiempos de teletrabajo**.

1. Usa el cable de red

Conectando tu equipo físicamente por cable las comunicaciones serán más rápidas y seguras. Si no te queda más remedio y tienes que usar la wifi, evita redes públicas o de terceros.

En una wifi pública cualquiera con mínimos conocimientos de hacking podría estar analizando el flujo de tráfico. Si se da el caso y envías información no cifrada, va a ser muy fácil interceptarla y hacerse con esos datos.

Fíjate bien en que tu wifi te solicite una contraseña a la hora de conectarte. Eso quiere decir que tu conexión está cifrada.

2. Mantén tu equipo de trabajo en un lugar seguro

No lo dejes al alcance de cualquiera. Parece una obviedad, sí, pero te sorprendería lo poco conscientes que somos a veces. Además, todos conocemos la predilección de los gatos por los teclados ajenos.

Tampoco te ausentes temporalmente sin bloquear la pantalla al levantarte. Aunque creas que estás en casa, lejos de cualquier peligro, tu hijo pequeño podría hacer de las tuyas mientras te levantas al baño. También está de más recordarte que tu PC debe estar protegido con contraseña.

3. Usa un gestor de contraseñas

Lo de guardar las contraseñas en un archivo de texto en el escritorio o en un post-it a la vista de todo el mundo no es para nada seguro. En un gestor de contraseñas tienes toda esa información crítica centralizada y protegida.

Te damos algunos ejemplos de gestores: [Bitwarden](#), [KeePassXC](#), [1Password](#), [LastPass](#), etc. Y anótate estos [consejos para crear contraseñas](#) difíciles de descifrar, a la vez que te resulten fáciles de recordar.

4. Tapa la webcam

Asegúrate de que la cámara solo funciona cuando tú quieres. Lo mismo para el micrófono, desactívalo siempre que no lo estés utilizando.

Si alguien consigue acceder a tu equipo no sería muy complicado encender la webcam sin que tú te dieras ni cuenta. Lo que viene después ya lo sabes.

5. Permanece alerta ante correos de phishing

En los últimos meses ha habido un fuerte repunte de campañas de malware vía email, por lo que a no ser que sea meramente imprescindible evita abrir documentos y archivos adjuntos que tengan relación con temas candentes, como lo fue el COVID-19.

Presta mucha atención a los documentos que descargas y a los links a los que accedes.

En la mayoría de los casos, se tratará de ciberdelincuentes que se hacen pasar por instituciones sanitarias o financieras, organismos de la administración, etc. [Aquí te damos algunos trucos para que detectes al momento un intento de suplantación de identidad por phishing.](#)

Por otro lado, si te demandan urgentemente el pago de una factura o la transferencia de una cantidad de dinero significativa, piénsalo dos veces antes de completar la acción. Muchos estafadores se aprovechan de este sentimiento de urgencia para que no confirmes bien que esa persona es quien dice ser. Para asegurarte, es tan fácil como hacer una llamada a tu jefe y comprobar que no se trata de un engaño.

6. Si puedes, usa una VPN

Una VPN (del inglés, Virtual Private Network) o Red Privada Virtual es una de las herramientas de seguridad más importantes para teletrabajar. Funciona como **una extensión de la red de la oficina**, por lo que es un canal 100 % seguro mediante el que envías la información cifrada.

Siempre que puedas, evita utilizar servicios de acceso remoto que dependan de un tercero. Si todavía no cuentas con acceso por VPN, es importante que lo solicites.

Como ves son medidas muy sencillas de aplicar pero imprescindibles para garantizar un teletrabajo seguro. Basta con no bajar la guardia y securizar tu equipo de trabajo con lo básico.

Igual de importante que trabajar con seguridad es hacerlo en un entorno cómodo y que favorezca la productividad. En este post tienes unos cuantos [consejos básicos para favorecer tu rendimiento en situación de teletrabajo](#). ¡No te los pierdas!

6 TIPS para un TELETRABAJO SEGURO

- 

1 USA EL CABLE DE RED

Si usas WIFI evita redes públicas o de terceros

4 TAPA LA WEBCAM

Desactívala junto con el micrófono cuando no los estés utilizando



2 MANTÉN TU EQUIPO DE TRABAJO PROTEGIDO

No lo dejes al alcance de cualquiera ni te ausentes temporalmente sin bloquear la pantalla





5 PERMANECE ALERTA ANTE CORREOS DE PHISHING

Presta mucha atención a los documentos que descargas y a los links a los que accedes.



3 USA UN GESTOR DE CONTRASEÑAS

Así tienes toda la información crítica centralizada y protegida

6 SI PUEDES, USA UNA VPN

Una Red Privada Virtual envía la información cifrada y es 100% segura



 Si lo prefieres
Mira el vídeo online



1.4

10 CONSEJOS DE CIBERSEGURIDAD PARA PYMES

Si tienes un negocio y quieres mantenerlo protegido en la red empieza por aplicar estos 10 consejos de ciberseguridad para pymes.

Con el auge de las nuevas tecnologías también han ido en aumento los ataques online y el malware. Es por eso que hay que extremar las precauciones para evitarlos y prevenirlos siempre que sea posible.

Sabemos que la seguridad en la red o ciberseguridad es un factor muy importante para cualquier empresa. Especialmente en los pequeños negocios o pymes suele ser más complicado llevar a cabo medidas de protección eficaces dado sus recursos más limitados.

Es por eso que te echamos un cable con una serie de **consejos básicos de seguridad** que puedes comenzar desde ya a aplicar en tu pyme.

Amenazas online más frecuentes

Antes de nada, aclaremos cuáles son las amenazas más comunes que puedes encontrarte por la red:

- **Malware:** con este término nos referimos a cualquier tipo de software o programa malicioso.
- **Virus:** malware que infecta o altera el funcionamiento de programas y dispositivos con fines dañinos o ilícitos.
- **Spyware** o troyano: programas de apariencia normal o que se ocultan en otros para robar información.
- **Phishing:** es la suplantación de identidad a través de correo electrónico con el objetivo de obtener información sensible.
- **Ransomware:** software que infecta los equipos y desde el que se coacciona a los usuarios para que faciliten información o entreguen dinero.

Ten en cuenta que existen muchos más peligros online. Las formas y tipos de estas amenazas van evolucionando constantemente por eso es tan importante que agudices las medidas de ciberseguridad de tu pyme.

Mantén tu pyme segura con estos 10 consejos

Siguiendo estos 10 consejos de ciberseguridad para pymes tu negocio o proyecto estará mucho más protegido y a salvo de posibles amenazas.

1. Activa el antivirus

Muchos negocios todavía no tienen ningún sistema de detección y bloqueo de malware en sus equipos, ¡evita cometer este mismo error!

Instalar un buen antivirus es uno de los primeros pasos que debes realizar en todos tus dispositivos para mantenerlos protegidos.

Algunos de los más utilizados son Avast, Kaspersky, Bitdefender o Norton. Casi todos cuentan con una versión gratuita o planes adaptados a todos los bolsillos.

Windows Defender es el servicio de antivirus de Microsoft Windows. Se incluye y se activa por defecto en Windows 8 y versiones que le siguen para evitar que el malware entre en tu dispositivo.

Una vez hayas elegido e instalado uno recuerda que **es igual de importante mantenerlo actualizado** para que funcione correctamente. Puedes activar la actualización automática o periódica así como bloquear la desinstalación del programa para que se mantenga siempre activo y funcionando.

2. Actualiza tanto el software como el hardware

La ciberseguridad, como te comentábamos antes, va evolucionando a medida que cambian también las amenazas. Por este motivo, los programas se van actualizando incorporando avances para afrontarlas.

Cuando dejas de actualizar cualquier tipo de software estás cerrando la puerta a las posibles mejoras y soluciones de bugs que haya realizado el equipo de desarrollo del programa.

Actualiza a la última versión tus programas y herramientas de trabajo para que sea mucho más complicado para los hackers y virus acceder a ellas.

Lo mismo con el hardware. Si tus equipos son muy antiguos posiblemente cuenten con sistemas obsoletos que pueden ser fácilmente asaltados, además puede que no soporten las versiones más modernas y actualizadas de los programas.

Cambia y actualiza tu hardware con una periodicidad moderada para que el nivel de seguridad de los mismos sea mayor.

3. Vigila las contraseñas

Crea en tu negocio unas políticas de contraseñas para que tanto tú como tu personal utilicéis claves lo más seguras posibles.

El uso de contraseñas débiles o inseguras es una de las causas que más propicia los accesos indeseados.

Estas son algunas de las premisas que debéis seguir en la creación de contraseñas:

- Crea contraseñas fuertes que sean largas y combinen letras y caracteres
- Evita las claves obvias o las que vienen por defecto
- No compartas la misma contraseña en diferentes dispositivos o programas
- Utiliza un gestor de contraseñas

De forma adicional a las contraseñas seguras, es conveniente también que habilites un sistema de [Autenticación en dos pasos](#) **para que los accesos o logins sean mucho más seguros.**

4. Limita las instalaciones

Otra opción para mejorar la ciberseguridad en tu pyme sobre todo si tienes empleados a tu cargo, es habilitar usuarios con permisos limitados. Es decir, que **solo el personal autorizado tenga permisos para instalar programas, descargarse archivos** o realizar cambios en la configuración del sistema.

Esto evitará que aquellos usuarios sin conocimientos o no autorizados puedan provocar brechas de seguridad o instalar software malicioso queriendo o sin querer.

En el caso de que no puedas limitar las descargas, otra recomendación que puedes aplicar tú mismo o transmitir a tu equipo es que se descarguen solamente archivos de fuentes confiables.

Si vas a actualizar o descargar un programa revisa que sea siempre desde su página oficial, evita webs de terceros o dudosas.

5. Ojo a los adjuntos y links sospechosos

En línea con el anterior punto, una medida básica pero efectiva es avisar de que no se abran enlaces o archivos sospechosos que lleguen por correo.

El email es una de las puertas de entrada por las que llegan más virus y se producen más intentos de hackeo. Es muy habitual que lleguen enlaces disfrazados en comunicaciones de todo tipo o incluso archivos adjuntos con extensiones raras.

Si el link es de origen desconocido o no sabes que archivo te están mandando, mejor no lo abras.

Antes de abrir nada dudoso, mejor consulta a tus compañeros o intenta solicitar más información al contacto.

Presta especial atención también a los remitentes que envían la información (revisa que el correo sea el habitual) y que el diseño y tono del correo sea el apropiado. Si el correo transmite urgencia y te solicita datos sensibles ¡sospecha! Puedes estar ante una [suplantación de identidad o ataque de phishing](#).

6. Usa redes seguras

Las conexiones a internet tienen que ser seguras y cifradas. Los routers que utilices deben estar provistos de cortafuegos y actualizados (punto 2 del post ;)). También puedes **activar reglas para limitar el acceso a la conexión** por dispositivos o IP.

Si estás teletrabajando utiliza mejor una VPN. Este tipo de redes virtuales ofrecen una conexión más segura que usar simplemente la red doméstica.

Tanto a nivel usuario como corporativo mejor **nunca utilices redes abiertas desconocidas para conectarte a internet**. Desde redes wifi públicas puedes compartir datos y exponer información sensible a usuarios desconocidos.

7. Bloquea equipos y cierra sesiones

Si no estás utilizando tu ordenador o algún programa concreto bloquéalos o cierra la sesión. Dejar el equipo desbloqueado o las sesiones abiertas facilita y mucho que puedan acceder a donde no queremos.

Así mismo, desactiva o desinstala cualquier aplicación o programa que no sea necesario para el funcionamiento de tu negocio. De esta forma también minimizas los posibles riesgos.

8. Realiza backups

Si se produce cualquier fallo o brecha de seguridad es muy importante estar cubiertos y **disponer de backups o copias de los datos para restablecer el sistema**.

Habilita una copia de seguridad periódica en los equipos y dispositivos que utilices tanto online como externamente (disco duro o memoria USB). Así los datos de tu negocio estarán a salvo y serán recuperables en el caso de que sean borrados o dañados por algún malware.

¿Sabías que en dinahosting **realizamos copias de seguridad diarias en nuestros Servicios Administrados?** Mantenemos tu web o proyectos online seguros guardando los datos de tus hostings y servidores con nuestros [Backups Selfservice](#).

9. Crea un plan de prevención y acción

El clásico más vale prevenir. Una correcta formación en ciberseguridad tanto para ti como para tus empleados puede ahorrarte muchos disgustos.

Crea un plan con la política o recomendaciones que debe seguir cada miembro del equipo para mantener tu pyme segura. Incluye reglas básicas de detección de amenazas y cómo actuar en caso de que se produzca un ataque o haya una sospecha. Una actuación rápida en caso de darse la brecha de seguridad puede salvarte de un aprieto.

Ayudar a tu equipo a interiorizar unas reglas básicas de protección puede ayudarte y mucho a que la ciberseguridad en tu pyme sea mucho mejor y más fácil de mantener.

Si no sabes por donde empezar, puedes valerte de los [recursos que facilita el INCIBE](#), Instituto Nacional de Ciberseguridad.

10. Sentido común

Por último y más importante, en cualquier pyme debe imperar el sentido común en ciberseguridad.

Evitar entrar en sitios no seguros, no facilitar datos sensibles a terceros, no descargar archivos dudosos... todo ello son pequeñas acciones que pueden evitar males mayores.

Si algo te da mala espina, mejor analiza y revisa el caso cuidadosamente.

Si la posible amenaza se escapa a tu comprensión no arriesgues, mejor contacta con un profesional en ciberseguridad para mantener tu pyme protegida.

Esperamos que estos consejos de ciberseguridad para pymes te ayuden a mantener tu negocio a salvo de virus y amenazas online.



Evitar entrar en sitios no seguros, no facilitar datos sensibles a terceros, no descargar archivos dudosos... todo ello son pequeñas acciones que pueden evitar males mayores.

1.5

HERRAMIENTAS PARA MONITORIZAR LA SEGURIDAD DE TU PYME

Monitorizar la seguridad es fundamental para mantener tu negocio o pyme a salvo de posibles amenazas online. Vemos la mejores herramientas Open Source para realizar esta tarea.

Cuando tienes tu propia empresa uno de los puntos cruciales que deben figurar en tu hoja de ruta es la ciberseguridad.

Al igual que se utilizan cámaras para controlar lo que sucede físicamente, a nivel online existen también diferentes herramientas para vigilar la actividad de un sistema. Estas son las herramientas de monitorización de seguridad online.

¿Qué es la monitorización de seguridad?

Se trata del seguimiento, análisis y control de las posibles [amenazas online](#) que pueden afectar a una empresa a través de sus sistemas y redes.

La monitorización es un proceso mediante el cual se vigila y se avisa de cualquier fallo de seguridad, actividad extraña o intrusión dentro de un sistema. De esta forma, los responsables de IT pueden actuar sobre ellos y evitar que se repitan. Además, también facilitan llevar a cabo diferentes acciones preventivas para minimizar riesgos.

Es por ello que las herramientas de monitorización resultan muy útiles para aumentar la seguridad online de tu pyme.

Herramientas de monitorización de seguridad Open Source

Ten en cuenta que estas herramientas son libres y puede utilizarlas quien quiera. Aunque principalmente están pensadas para el uso de administradores de sistemas o responsables de ciberseguridad.

Para utilizarlas correctamente y sacarle todo el partido a sus funcionalidades más avanzadas son necesarios conocimientos técnicos.

Si no cuentas con estos conocimientos y quieres que tu empresa se mantenga segura y lo más protegida posible ante amenazas online, nuestra recomendación es que contrates los servicios de un profesional.

Wazuh

[Wazuh](#) es una **plataforma de seguridad gratuita** Open Source que permite detectar vulnerabilidades, monitorizar la seguridad y responder a incidentes. Además, también facilita la aplicación de los diferentes estándares de seguridad y tratamiento de datos.

Su principales ventajas son:

- Gran abanico de funcionalidades de ciberseguridad

- Paneles intuitivos y sencillos de utilizar
- Comunidad muy activa y desarrollo constante
- Despliegue rápido con contenedores

Suricata

Suricata es un **sistema de alto rendimiento para el monitoreo de seguridad** de red que permite detectar (IDS, Intrusion Detection System) y prevenir intrusiones (IPS, Intrusion Prevention System).

Con esta herramienta podrás ver y revisar qué pasa en tu red en tiempo real. Estas son sus ventajas:

- Compatible con Unix, Linux, Windows y macOS
- Seguimiento en tiempo real en aplicaciones de red como HTTP, FTP o SMB
- Módulo de scripting incorporado
- Se integra bien con otras herramientas de terceros

OpenVAS

OpenVas es un **escáner de vulnerabilidades de código abierto**. En la actualidad se encuentra incluido dentro de los paquetes comerciales ofrecidos por Greenbone Networks, y aquí puedes ver el [proyecto en GitHub](#).

De esta herramienta destacamos:

- Cuenta con interfaz web y aplicación cliente
- Completo listado de vulnerabilidades actualizado constantemente
- Permite realizar pruebas autenticadas y no autenticadas
- Sin limitación de número de máquinas

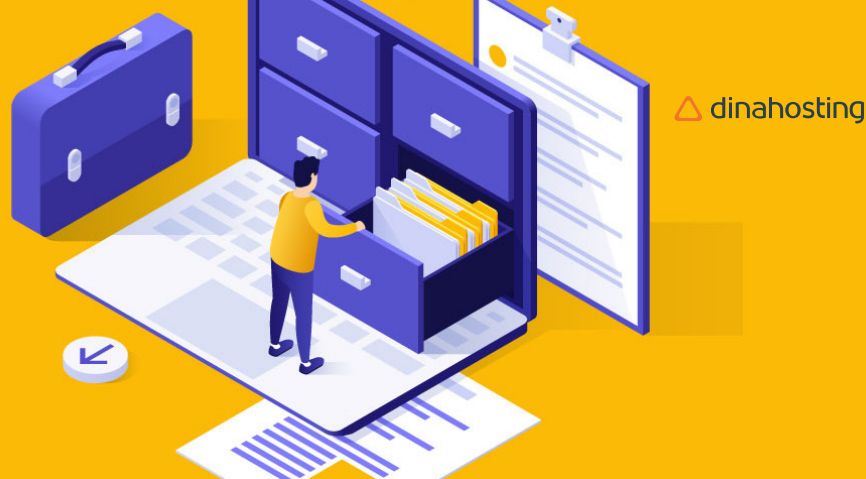
pfsense

pfsense es un **firewall libre** desarrollado por la empresa Netgate. Las iniciales pf de su nombre se refieren al filtrado de paquetes (packet filter) que es la tecnología que utiliza para monitorizar la actividad. Sus principales ventajas son:

- Software libre y fácil de usar
- Realiza un filtrado dinámico de paquetes
- Cortafuegos flexible, sencillo de personalizar
- Con soporte para WireGuard

ASESORÍA TÉCNICA PARA TU HOSTING

*Contrata nuestros servicios de seguridad
Mantenemos tu hosting libre de malware*



1.6

CONSEJOS PARA ALMACENAR INFORMACIÓN DE FORMA SEGURA EN TU NEGOCIO

En este post veremos una serie de consejos y recomendaciones sobre cómo debes almacenar información para asegurar una buena integridad de todos los datos de tu negocio.

Si gestionas un negocio seguro que consideras muy importante toda la información y datos relacionados con el mismo.

Desde las facturas y cuentas de la empresa, hasta los datos personales de empleados, pasando por todo tipo de documentos corporativos y de trabajo... Generalmente, da igual el tipo de negocio que tengas, la información que se genera en el día a día suele ser bastante grande y mucha de ella muy importante. Por todo esto es clave cómo se guarda y almacena.

Existen diferentes tipos de información que según su importancia deberemos de tratar de una u otra forma:

Tipo de información

- **Confidencial:** se trata de la información sensible o clasificada de la empresa. Solamente un personal limitado puede tener acceso a ella y en ningún caso se puede compartir sin autorización expresa. En esta categoría entrarían por ejemplo los datos personales de empleados y clientes.
- **Interna:** son todos los documentos y datos que se utilizan para llevar a cabo los diferentes funciones del negocio. Metodologías de trabajo, normas de comportamiento, políticas de seguridad, etc. Por norma general son solo para utilizar y compartir entre empleados y no se pueden transmitir a terceros o sacar de la empresa.
- **Pública:** toda información que sea para uso comercial o informativo, como la que ponemos en nuestra web, redes sociales, comunicaciones por correo, etc.

Como puedes deducir, el rango de seguridad varía en función del tipo de datos que guardes siendo la información confidencial la que precisa un mayor nivel de seguridad y la pública la que menos. Por supuesto, dependerá también de los criterios de protección de datos que apliques en tu empresa.

Según el nivel de protección que quieras para cada uno de tus archivos, estas son algunas de las formas en las que puedes almacenarlos:

Cómo almacenar de forma segura los datos de tu pyme

Tanto si almacenas tus archivos en local como en red, estas son algunas de las precauciones que puedes tomar para asegurar que tus datos están seguros y no caen en las manos incorrectas:

Establecer políticas de almacenamiento y guardado de datos

Si se establecen unas pautas de guardado y almacenamiento entre los compañeros que forman el equipo de trabajo es más sencillo implantar medidas de seguridad para proteger los datos.

De esta forma se pone sobre aviso de las normas de guardado previniendo errores a la vez que se establecen unos criterios que a la larga optimizan los tiempos y facilita la gestión.

Ejemplo genérico de Política de almacenamiento y guardado de datos:

- **Almacenamiento en local:** utilizar las carpetas X del equipo para guardar archivos, borrar archivos almacenados que no sean relevantes cada cierto tiempo...
- **En la red:** seguir el criterio de ordenación y nomenclatura, guardar en el área correspondiente, borrado de archivos limitado a responsables, guardar solamente archivos de formatos específicos...
- **Relativo a los dispositivos externos:** se desaconseja el uso de dispositivos externos. En caso de que no quede más remedio que utilizarlos para almacenar información, revisar que funcionan correctamente, etc.

Cada empresa debe establecer su criterio de guardado basándose en los medios que ponga a disposición de los empleados para tal fin y al tipo de información que suela almacenar.

Carpetas protegidas

En los sistemas operativos y gestores de archivos tanto online como locales existen varias opciones para proteger las carpetas o documentos donde se guarda la información. Estas son las más habituales:

- **Establecer contraseñas:** asignamos una clave que será necesario introducir para poder abrir o editar la carpeta.
- **Cifrado de contenido:** se encripta el contenido para que solo aquel que lo activó o que disponga del certificado de cifrado pueda abrirlo.
- **Ocultar:** esta opción hace que la carpeta no se muestre de primeras en el explorador de archivos. Deberás activar la opción de Mostrar archivos ocultos para poder verla.

En Windows las opciones están disponibles en el menú de Propiedades > Avanzadas. En Mac puedes acceder al cifrado desde Apple > Preferencias del sistema > Seguridad y privacidad > FileVault.

También contamos en dinahosting con una solución en el [Panel](#) para la **protección de carpetas de tu hosting**. En este vídeo te explicamos como funciona:



Mira el vídeo

Para qué sirve la Protección de carpetas en tu hosting

Permisos de usuario

En casi cualquier sistema operativo o explorador de archivos existe la opción de asignar permisos a carpetas, documentos e incluso programas y herramientas para que solamente aquellos que establezcamos puedan acceder a ellos o editarlos.

Normalmente, los permisos están ligados a diferentes roles como por ejemplo: usuario con rol de Administrador > permiso: Control total, usuario con rol Editor > permiso Escritura, etc.

La nomenclatura puede variar en función del programa que utilicemos, pero los permisos más utilizados que se pueden asignar son:

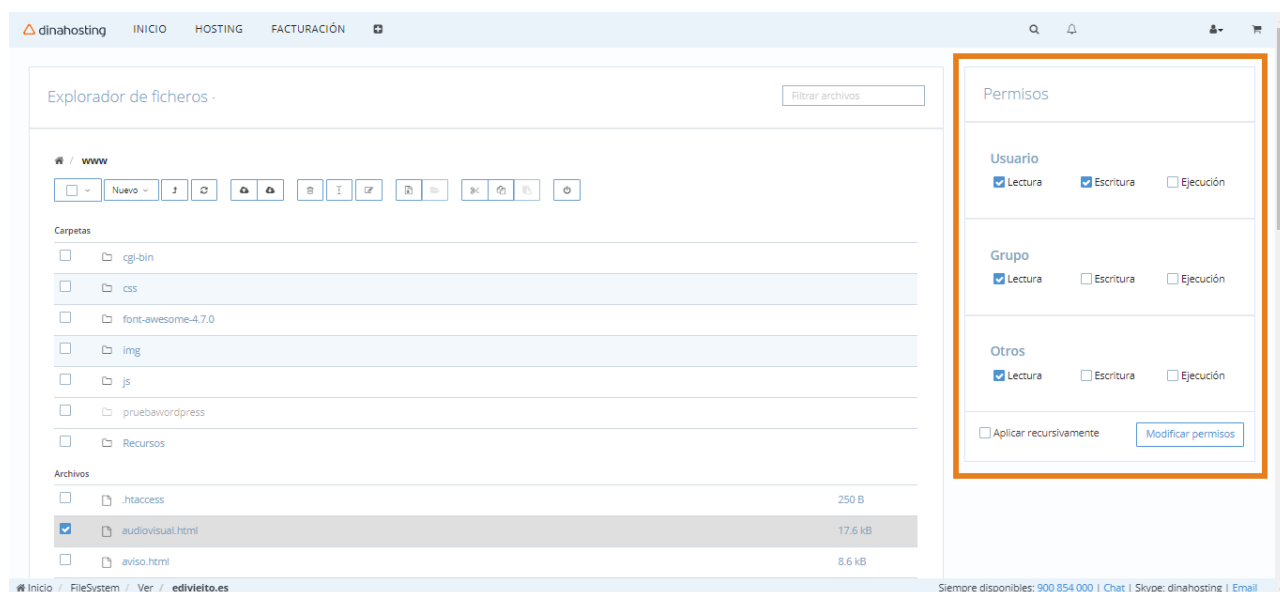
- **Control total:** generalmente se le da a los dueños o administradores de los equipos, ya que esto permite hacer cualquier edición y abrir o ejecutar todo.

- **Modificar/Escritura:** permite hacer cambios sobre los archivos.
- **Lectura:** solo permite abrir los archivos y verlos pero no hacer modificaciones.
- **Ejecutar:** permiso para abrir algún programa.

En Windows puedes establecer permisos para las diferentes usuarios de un equipo desde Configuración > Cuentas o establecer permisos para documentos y carpetas desde el menú de Propiedades > Seguridad > Permisos.

En MacOS si pulsamos CMD+I sobre una carpeta, accedemos a sus opciones. Entre ellas está la de Compartir y permisos en la que podemos añadir usuarios y asignarles diferentes niveles de acceso.

Y así se ven los permisos en el Explorador de Ficheros de dinahosting:



Almacenamiento en la nube seguro

Los servicios para almacenar información o datos en la nube deben **contar con unas buenas medidas de seguridad que garanticen la privacidad e integridad de los datos**.

Los principales **requisitos para elegir una buena nube** o plataforma donde guardar los datos son los siguientes:

- **Medidas de seguridad:** debe contar como mínimo con un cifrado (HTTPS y otros), un firewall propio y copias de seguridad.
- **Control de accesos y movimientos:** el acceso a nuestros datos debe estar restringido. Los usuarios que accedan deben hacerlo desde plataformas de login con controles de acceso seguro.
- **Normativa vigente:** es clave conocer bajo que normativa son guardados los datos. Según dónde se almacenen los archivos la ley es diferente, tal y como te contamos en el capítulo [¿Alojamiento web en España o en Estados Unidos?](#)
- **Condiciones de uso y contratación:** lee la letra pequeña para confirmar que efectivamente estás de acuerdo con las condiciones que se establecen en la nube.

Por supuesto, en dinahosting cumplimos con todos estos requisitos. Todos los archivos que guardas en nuestros servidores están a buen recaudo, en cumplimiento con la normativa vigente española y con las más altas medidas de seguridad.

¿Quieres conocer más sobre nuestra infraestructura? [Descubre más sobre nuestro Centro de Datos](#) y todas las soluciones que utilizamos para garantizarte la mayor conectividad y seguridad de tus datos.

Copias de seguridad

No hay mejor medida de seguridad que prevenir, y para eso están las copias de seguridad.

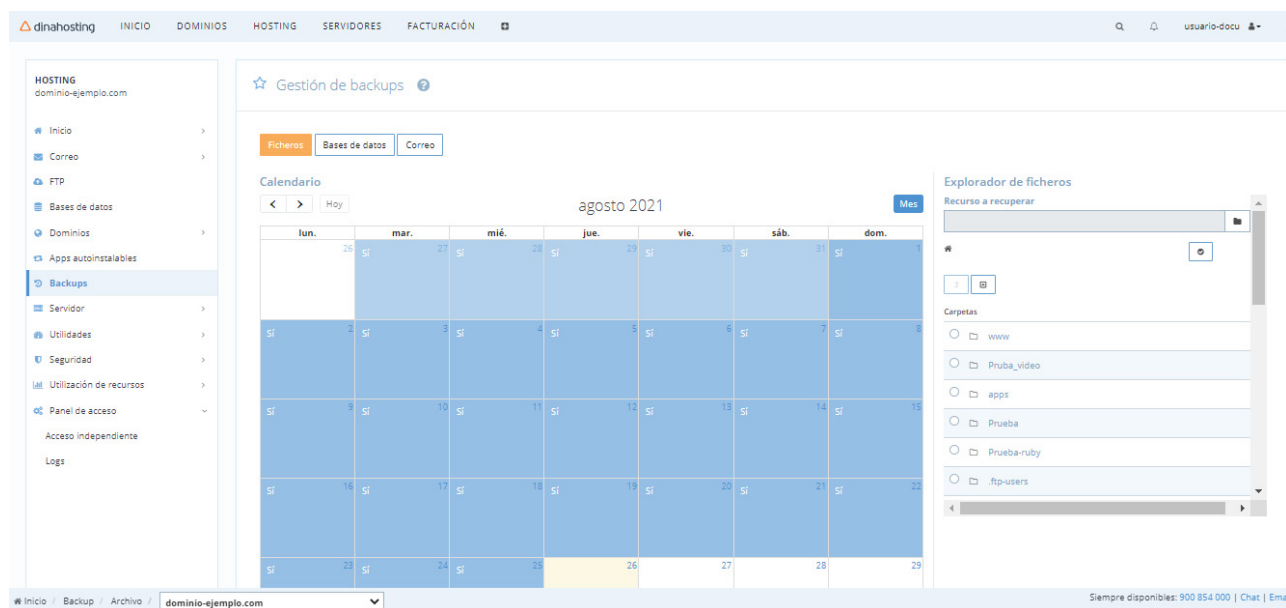
Cuando algo falla, nos equivocamos al almacenar información o borramos por error algún archivo es imprescindible contar con una backup o copia de seguridad que nos permita recuperarlo.

Es por eso que debemos establecer tanto en los equipos locales como en red diferentes tareas de copia periódicas, para que ninguno de nuestros datos se pierda.

Ten en cuenta que es recomendable realizar las copias de seguridad en discos o servidores diferentes a los que se utilicen para el guardado, para que sean accesibles en caso de un fallo crítico que no nos permita acceder.

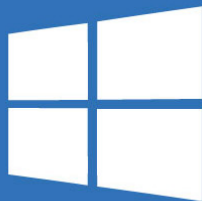
En Windows puedes configurar copias de seguridad desde Panel de Control > Sistema de Seguridad > Copias y restauración. En MacOS puedes seguir estas [recomendaciones de su Soporte](#) según el tipo de copia que quieras hacer.

En dinahosting contamos con un servicio de **Backups Selfservice incluido en todos nuestros [planes de Hosting y Servidores Administrados](#).**



Con ellas puedes recuperar los datos de tu web, el correo o las bases de datos que tengas guardadas o simplemente acceder a la información de un día en concreto.

Hasta aquí nuestras recomendaciones para almacenar información de forma segura.



1.7

10 CONSEJOS PARA MEJORAR TU SEGURIDAD EN WINDOWS

Si trabajas con Windows, tanto a nivel usuario como en tu empresa, es muy importante que tengas en cuenta los consejos de seguridad que te damos en este post.

Los ataques informáticos están a la orden del día, por eso es básico tomar ciertas precauciones. Verás que mantener tu sistema securizado no es para nada difícil.

Qué puedes hacer como usuario

Lo primero, lo que puedes hacer tú desde tu casa como usuario de Windows para garantizar tu seguridad y privacidad cuando uses Windows y navegues por Internet.

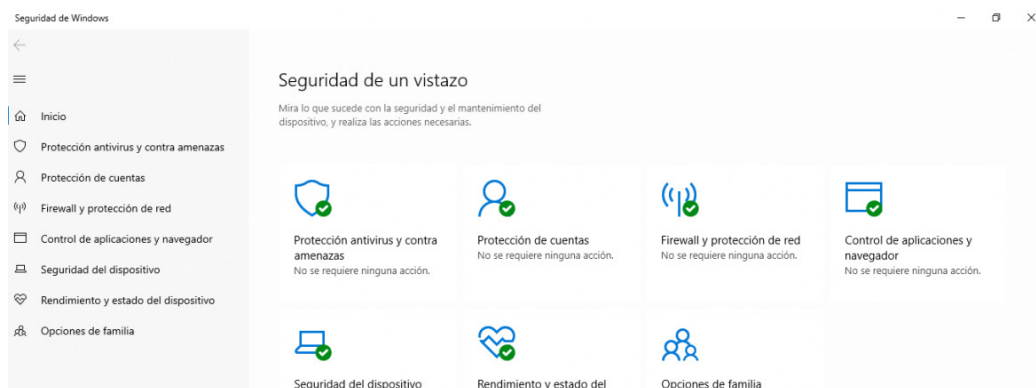
Activa las opciones de seguridad de Windows

Dentro de Windows hay diferentes áreas de protección en las que puedes trabajar. Es fundamental que estas tres las tengas en cuenta:

- **Antivirus:** Windows Defender es el servicio de antivirus de Microsoft Windows. Se incluye y se activa por defecto en Windows 8 y versiones que le siguen para evitar que el malware entre en tu dispositivo. Incluso puedes activar la opción de protección en tiempo real si quieres. Si hay algún elemento que te interese excluir del antivirus, también puedes hacerlo.
- **Protección contra ransomware:** para proteger tu dispositivo frente a amenazas de ransomware y poder restaurarlo en caso de ataque. El ransomware actúa bloqueando tu dispositivo y reclamando después un pago online para restaurarte el acceso a él.

Desde aquí también puedes controlar el acceso a determinados archivos o carpetas de tu equipo para impedir cambios no autorizados de aplicaciones malintencionadas.

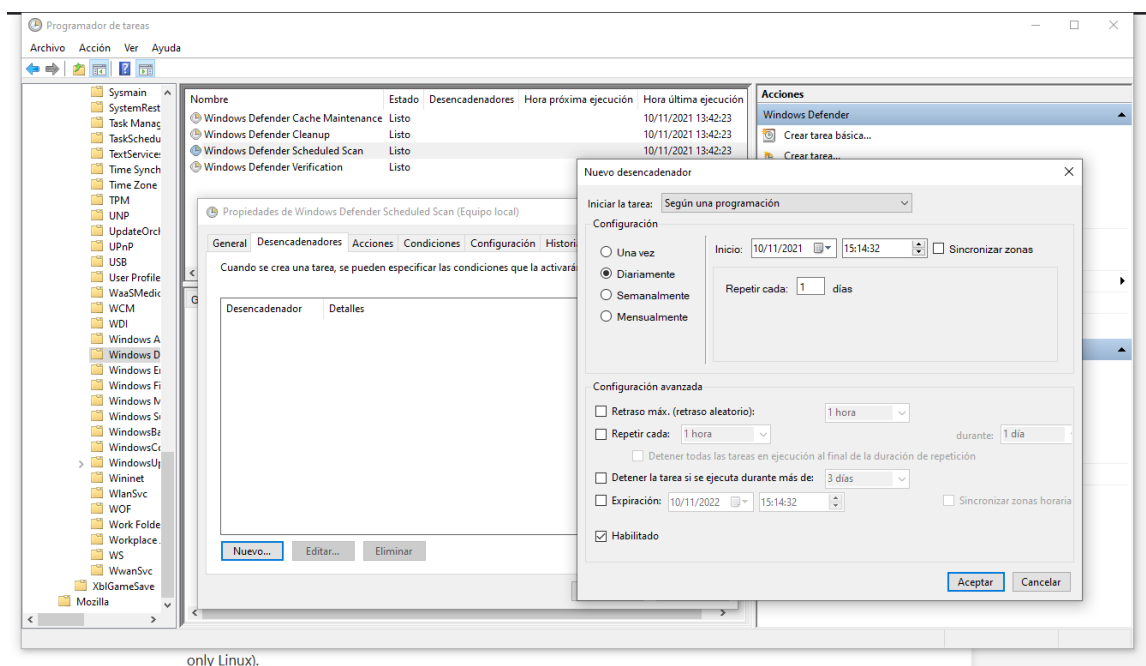
- **Firewall y protección de red:** importantísimo. Actúa como un escudo que filtra qué y quién puede tener acceso a tu red.



Programa escaneos periódicos del antivirus

Si te interesa que Windows Defender haga escaneos periódicos de seguridad en tu equipo en busca de virus. Se trata de un **análisis completo de todo tu equipo**, no solo de los procesos y servicios en ejecución, sino de los ficheros que tengas almacenados en el sistema, descargas que no has llegado a finalizar, etc.

Para ello tienes que utilizar el programador de tareas de Windows. Accede a él y dirígete a la Biblioteca > Microsoft > Windows > Windows Defender. Entre las opciones que te aparecen elige Windows Defender Scheduled Scan. Clic en ella y luego ve a Desencadenadores > Nuevo. Ahora te toca elegir la periodicidad con la que quieres que se haga el escaneo. También puedes fijarle una hora concreta.

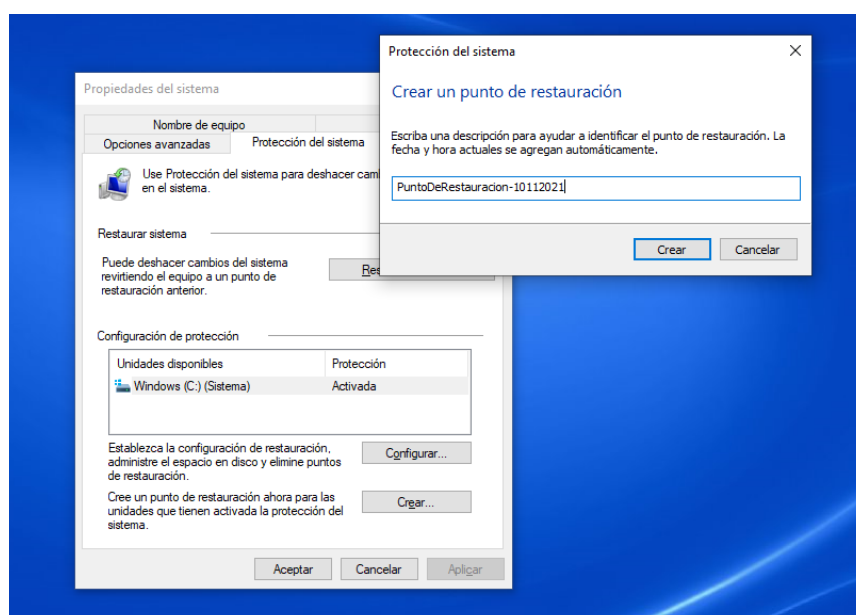


Habilita la restauración del sistema en caso de desastre

Este punto es fundamental para que puedas restaurar el sistema en caso de catástrofe.

Para contar con esta opción, tienes que **crear un punto de restauración del sistema**. Haz esta misma búsqueda ("Crear un punto de restauración") en el buscador de Windows. Accederás a Propiedades del sistema > Protección del sistema. Una vez ahí, haz clic en Crear.

Lo primero que tienes que hacer es ponerle un nombre. Para que te sea intuitivo, puedes incluir en él la fecha. Por ejemplo: PuntoDeRestauración-10112021. Haces clic en Crear y listo.



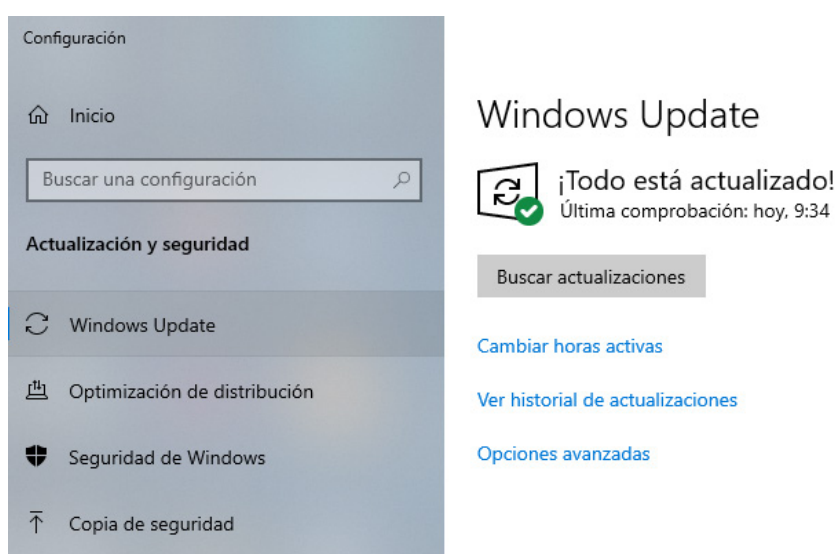
Lleva al día las actualizaciones

Como sabes, las actualizaciones sirven para reparar errores de seguridad detectados previamente, y que han sido fuente de ataques informáticos.

Si no te preocupas por llevar al día las actualizaciones que te proporciona tu sistema operativo, te vas a quedar atrás y tendrás más posibilidades de sufrir vulnerabilidades.

Además, [las versiones más antiguas de Windows carecen de servicio de soporte](#), lo que implica que ya no reciben actualizaciones de seguridad periódicas. Si aún tienes Windows Server 2008, por ejemplo, tendrás muchas más posibilidades de ser víctima de un ataque.

En conclusión: mantén Windows y los programas que uses siempre al día. **Lo más sencillo es que utilices el asistente Windows Update.** Configúralo para que las actualizaciones se instalen automáticamente.



Usa cuentas locales en lugar de login en la nube

La desventaja de usar cuentas en la nube para hacer login en tu equipo es que los cambios que hagas en esa cuenta quedarán reflejados en el resto de equipos y servicios que la usen, como el correo electrónico.

Por ejemplo, si cambiaras la contraseña en el login de tu equipo, la estarías cambiando también en tu correo, lo que significa que si alguien accede a tu equipo y te cambia la contraseña, podrías perder el acceso a tu cuenta de email.

En caso de que uses una cuenta de usuario local, los **cambios estarán acotados al equipo que estés usando en ese momento**. Sin duda es la opción más segura.

Piénsalo dos veces antes de instalar drivers

Un driver es el **intermediario entre Windows y el hardware de tu PC**. Lo necesitarás para poner en funcionamiento una impresora o un escáner, por ejemplo.

Nuestra recomendación es que si no eres un usuario con conocimientos en la materia no instales ningún driver por tu cuenta y dejes esta tarea en manos de un experto. De hacerlo, fíjate bien en que lo descargas desde la **página web del fabricante** y de que estás bajando la última versión disponible (por lo que te comentábamos anteriormente de trabajar con versiones actualizadas).

Los drivers suelen ir actualizándose con el tiempo para corregir sus defectos. De nuevo es importante tener siempre su **versión más reciente**.

Cuidado con la descarga de aplicaciones

A la hora de descargar aplicaciones en Windows (juegos, redes sociales, softwares específicos...) lo ideal es que lo hagas o bien desde [Microsoft Store](#), que siempre te va a ofrecer más garantías de seguridad, o desde una fuente oficial.

Hay muchas páginas disponibles por ahí desde las que puedes hacer descargas, pero no todas estarán libres de virus. Por lo tanto, **no te quedes con el primer resultado de búsqueda que te ofrece Google**, puesto que podría ser una versión pirata que introduzca malware en tu equipo.

No te conectes a redes wifi abiertas o públicas

En una wifi abierta o pública tienes muchas más posibilidades de ser hackeado que en una wifi que te solicite contraseña a la hora de entrar.

Cada vez hay más redes de wifi públicas en restaurantes, hoteles, aeropuertos, bibliotecas... por lo que si te ves obligado a usarlas, intenta entrar solo en páginas web que tengan un certificado SSL activado. También te recomendamos desactivar la wifi durante el tiempo que no la estés usando, para minimizar el riesgo de ataque.

Si entras a la plataforma de trabajo de tu empresa, es indispensable que cuentes con una [VPN](#).

Qué puedes hacer cómo empresa

Si usas Windows en tu trabajo, además de aplicar todas las medidas que te acabamos de detallar, puedes sumar estas dos recomendaciones.

Encripta el disco con BitLocker

En caso de pérdida o robo de tu equipo, necesitas tener la seguridad de que un posible atacante no pueda acceder a tus ficheros fácilmente. Una de las formas más sencillas de hacerlo sería quitando el disco duro de tu equipo, pero si lo tienes encriptado con BitLocker ya se lo estarás poniendo difícil.

BitLocker es el **sistema de cifrado** que Microsoft implementa por defecto en sus sistemas empresariales. La encriptación del disco te permitirá **evitar fugas de datos**, pues en caso de intento de acceso fraudulento a tu disco, sería necesario que el atacante introdujese antes una clave de descifrado.

Para activarla, tan solo tendrías que irte a la barra de búsqueda de Windows y buscar "Administrar BitLocker". A continuación haz clic en Activar Bitlocker y sigue las instrucciones que te da el asistente. Te pedirá que indiques el lugar en el que quieres guardar tu clave: en tu cuenta de Microsoft, en un USB, obtenerla impresa, etc. Piensa cuál sería el método más seguro para ti, y adelante.

Recuerda que esta opción solo está disponible en los entornos profesionales de Windows, por ser en ellos donde se producen más intentos de robos de datos.

Activa el arranque seguro

Su función es que cuando inicies tu equipo se ejecute solo software seguro, de forma que si alguien intenta ejecutar código peligroso en el proceso de arranque no lo consiga.

Puedes **activarlo en la BIOS** (del inglés, Basic Input Output System, o lo que es lo mismo, Sistema básico de entrada y salida) de tu PC. Generalmente, los equipos usan la tecla F10 o la de escape (Esc) para acceder a la BIOS, pero en función de la marca de tu PC la tecla puede variar.

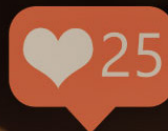
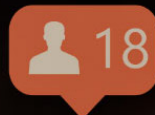
Si pulsas la tecla correspondiente durante el arranque de tu equipo, accederás a la configuración del BIOS. Ahí tendrás la opción de activar el arranque seguro.

¡Y esto es todo! Esperamos que le saques mucho partido a este decálogo de seguridad en Windows.

Añade un **Certificado SSL** a tu web

*Comunicaciones cifradas y seguras
Mejora tu posicionamiento SEO*





1.8

7 CONSEJOS DE SEGURIDAD PARA TU MARCA EN REDES SOCIALES

¿Te acuerdas de cómo era el mundo antes de las Redes Sociales? Tanto han evolucionado que ya no solo se usan a nivel personal. Desde hace unos años muchos negocios y particulares las emplean como herramienta de promoción de sus marcas. Por eso, **cuidar la seguridad de una marca en las Redes Sociales** es básico para que el negocio no se vea comprometido.

Crea contraseñas de acceso seguras

Las contraseñas son el primer filtro de acceso a tus redes sociales. Es importante que crees contraseñas robustas, que sean difíciles de descifrar.

Es decir, todo lo contrario a 123456, password, qwerty, abc123... Este tipo de contraseñas son de lo más inseguras y las aplicaciones que las usan son vulneradas a diario. Otro error habitual: si tu empresa se llama "miempresaelmejor", no puedes caer en la trampa de usar tu propio nombre como contraseña.

Habilita la doble autenticación

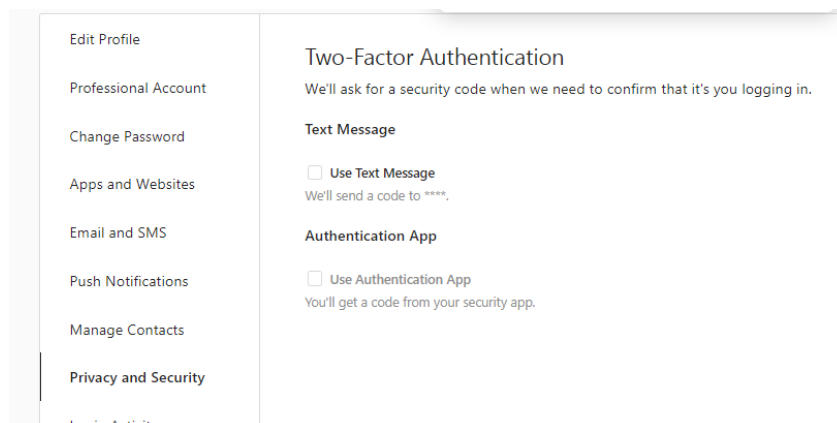
Cada vez es más común que para acceder a las aplicaciones en las que entras a diario, ya sean las Redes sociales, la banca electrónica o el Panel de Control de dinahosting, tengas la posibilidad de añadir una doble autenticación.

Lo que te permite este sistema es que, además de introducir tu usuario y contraseña, tengas que **añadir a mayores algún otro elemento que indique que eres tú** quien verdaderamente está intentando acceder.

En el caso del Panel de dinahosting, por ejemplo, la autenticación o verificación en 2 pasos la hacemos a través de una aplicación externa como Authy, que te genera un número aleatorio que caduca pasados unos segundos y que tú tienes que introducir para terminar de hacer login.

Siempre que las Redes Sociales te lo permitan, añade esta doble autenticación y multiplica por dos la seguridad de tu marca.

A continuación, te ponemos un ejemplo de cómo lo hace Instagram, vía mensaje de texto o mediante aplicación de autenticación, lo que prefieras:

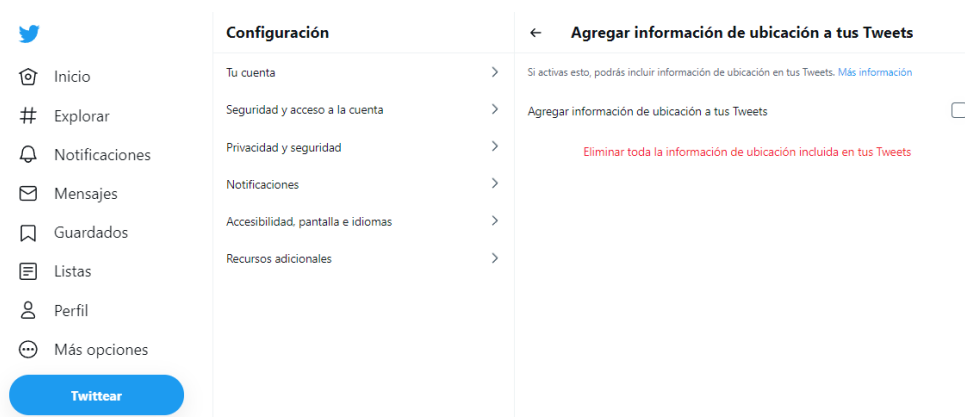


Opciones de Autenticación de Instagram

Desactiva la geolocalización

Como ya sabes, entre las opciones de configuración de los perfiles de Redes Sociales hay un punto llamado localización o geolocalización. Es lo que las Redes Sociales utilizan para saber dónde te encuentras y hacerte recomendaciones basándose en esos datos. Por ejemplo, mostrándote anuncios de empresas de las áreas geográficas por las que te mueves.

Desactivar la geolocalización te vendrá bien **para que no sepan dónde estás en cada instante**. Por ejemplo, en Twitter existe una pestaña dentro de su configuración de privacidad desde la que puedes eliminar la información de ubicaciones de tus tweets. Imagínate que estás publicando algo desde tu casa en el perfil de la empresa... Seguro que no te interesa que tu ubicación se comparta:



Geolocalización en Twitter

Establece una buena configuración de privacidad

Todas las Redes Sociales tienen una configuración de privacidad, que puede ser más fuerte o más débil en función de lo restrictivo que quieras ser. Cuando hablamos de Redes Sociales de una marca, **lo mejor es que revises bien todas las opciones de privacidad de las que dispones**.

En Twitter puedes decidir si quieres que todos tus tweets sean públicos o estén protegidos -por ejemplo, si no es apto para menores-. Otra cosa que puedes hacer es bloquear a usuarios que estén generando contenido indeseado y con los que prefieras no tener contacto (eso sí, piénsalo dos veces antes de hacerlo porque puede volverse en tu contra).

Otro punto fundamental son los roles. Puede que en un determinado momento te interese **darle acceso a tus redes a un tercero** (por ejemplo, un colaborador externo). Recuerda eliminar ese permiso en cuanto vuestra relación termine. También puedes **crear diferentes roles** dentro de tu red social.

Por ejemplo, en Facebook: no es lo mismo un rol de Administrador (tiene permiso para hacer todo lo que quiera dentro de la página), que uno de editor (puede publicar contenido, pero no administrar roles y hacer cambios en las configuraciones del perfil) o de anunciante (solo puede crear anuncios y consultar estadísticas). Crea los roles estrictamente necesarios y fijándote bien a quién se los asignas.



Roles en Facebook

Cuidado con los enlaces y los adjuntos

Ya te hemos hablado largo y tendido de lo que es el [phishing](#) y lo mucho que han crecido los ataques de usurpación de identidad vía email en los últimos tiempos. Estos ataques no se producen solo a través del correo electrónico, sino también mediante las Redes Sociales.

Ten cuidado con los links y los documentos a los que accedes desde las Redes, pues pueden comprometer la seguridad de tu negocio. **Fíjate bien en que procedan de perfiles que están activos**, que tienen un buen número de seguidores, que muestran imágenes de perfil y portada actualizadas, etc. Todos estos detalles te dan pistas de si estás ante un perfil verdadero o falso.

Y por supuesto, en caso de que desde cualquier Red se te redirija a una página en la que se te pidan datos personales, información bancaria, etc. desconfía. Fíjate bien en si el sitio en el que has entrado corresponde verdaderamente a la marca, y en si tiene un [certificado SSL de seguridad](#) activado. Lo verás en aquellas páginas que tienen HTTPS en vez de HTTP.

Forma a tus empleados

Básico para mantener la seguridad en tus Redes Sociales. ¿Sabías que **los errores humanos son la principal fuente de brechas de seguridad**? La gestión de Redes no es algo que deba hacer cualquiera.

Si no vas a externalizar la gestión de las Redes y os vais a encargar de esta tarea desde dentro, es fundamental que los empleados sepan cómo manejarse en el mundillo. Conciéncialos sobre los riesgos de ciberseguridad en el uso de las tecnologías y enséñales trucos y consejos para aplicar en el día a día.

Sentido común por encima de todo

Como siempre en estos casos, tu mejor aliado es el sentido común. No está de más recordar que publicar cualquier tipo de información confidencial, como cuentas de correo privadas, documentos identificativos, etc. es un peligro en Redes.

Por ejemplo, si haces un tutorial de uso de tus servicios y en la captura de pantalla tienes que introducir un usuario y contraseña, preocúpate de que los datos que añadas estén pixelados o sean de usuarios que usas exclusivamente para hacer este tipo de pruebas.

Tampoco es recomendable que desde perfiles corporativos publiques noticias de dudosa veracidad, o entres en debates que no llevan a ningún sitio. Mantener la neutralidad es lo mejor para evitar ser víctima de ataques online.

¡Y esto es todo! Esperamos que le saques mucho partido a estos consejos de seguridad en Redes Sociales.



CONSEJOS DE SEGURIDAD EN REDES SOCIALES



3 DESACTIVA LA GEOLOCALIZACIÓN

Dejarán de llegarte anuncios de tu zona pero también no sabrán donde estás en cada instante.

1 CREA CONTRASEÑAS SEGURAS

Las contraseñas son el primer filtro de acceso a tus redes sociales. Mejor utiliza contraseñas robustas, que sean difíciles de descifrar.



4 CONFIGURA TU PRIVACIDAD

Revisa bien todas las opciones de privacidad de las que dispones en las redes en las que estés. Decide con quién quieres compartir tu contenido, asigna roles, etc.





2 USA LA DOBLE AUTENTICACIÓN

De esta forma sumas una capa extra de seguridad para acceder a tus redes a la vez que verificas tu identidad por otra vía.



5 SENTIDO COMÚN

Publicar cualquier tipo de información confidencial, como cuentas de correo privadas, documentos identificativos, etc. es un peligro en Redes Sociales



1.9 PROTOCOLO SSH: ¿QUÉ ES Y PARA QUÉ SIRVE?

Administra tu servidor en remoto y de forma segura mediante el protocolo SSH. Te contamos los detalles de este sistema cifrado para habilitar conexiones protegidas entre usuario y servidor.

Para cualquier empresa que gestione servidores en remoto es primordial contar con sistemas que permitan niveles óptimos de ciberseguridad. El protocolo SSH es una de las herramientas más útiles para garantizar la seguridad a la hora de realizar este tipo de conexiones remotas.

¿Qué es el protocolo SSH?

SSH o Secure Shell es un programa o protocolo que permite conectarte a un servidor de manera remota y segura. Su principal ventaja es que cifra todas las comunicaciones entre el equipo del usuario y el servidor, por lo que es mucho más seguro que otras opciones.

Antes de que apareciese SSH, se utilizaban otros protocolos como Telnet que realizaban la misma función, pero no encriptaban las comunicaciones. Esto podía provocar que se interceptasen y se realizasen usos fraudulentos de la información más fácilmente, y es por eso también que se desaconseja su uso.

Mediante SSH puedes realizar cualquier gestión o tarea en un servidor remoto, casi como si estuvieras allí pero de manera incluso más segura.

Las acciones más habituales que podrás realizar a través del protocolo SSH son:

- Gestionar carpetas y archivos en el servidor
- Transferir archivos
- Editar el contenido de los archivos del servidor
- Administrar permisos y accesos
- Realizar labores de mantenimiento

Y cualquier otra acción que requiera una conexión directa y segura entre un ordenador y un servidor remoto.

¿Por qué es seguro el protocolo SSH?

Cualquier conexión que realices mediante este protocolo está completamente encriptada. Por lo que es mucho más difícil, por no decir imposible, que haya una brecha de seguridad.

SSH utiliza 3 capas diferentes de cifrado:

Cifrado simétrico

Se trata de una **clave secreta compartida entre ambos dispositivos** que codifica los mensajes que se envían entre ellos.

Toda comunicación durante la conexión SSH es cifrada con este sistema que se acuerda entre ambos equipos nada más inicias la sesión.

Esta clave se obtiene con un algoritmo de manera independiente en cada equipo, de ahí que sea muy difícil de obtener. A cualquier persona que desconozca esta clave le será imposible descifrarlo.

Cifrado asimétrico

Este sistema utiliza dos claves distintas, en lugar de una como el simétrico. **Una clave pública para el cifrado y otra, la privada, para el descifrado.** La privada debe permanecer en secreto, ya que funciona como decodificador de los mensajes generados usando la clave pública.

Las claves son totalmente independientes y, aunque estén relacionadas entre sí, no se puede generar una a partir de la otra. Este tipo de cifrado se utiliza durante la autenticación del usuario y cada clave pública-privada se crea para una única máquina.

Hashing

Consiste en que los mensajes ya cifrados se pasan por un **algoritmo llamado "hash" que crea un valor alfanumérico para cada mensaje.**

Este valor es único y regular, es decir, es diferente en cada caso pero tiene la misma longitud, por lo que no se puede trazar un patrón a partir del mismo que permita obtener los mensajes.

Si alguien modifica cualquier información del mensaje el hash variará, por lo que el receptor sabrá si se ha alterado el mensaje. Este sistema es conocido por ser indescifrable.

¿Cómo activo el SSH en mi Hosting?

En primer lugar debes [habilitar el acceso SSH](#). Puedes hacerlo de manera muy sencilla desde tu [Panel](#) activando la casilla Permitir SSH en el menú principal de tu [Hosting Linux](#).

Para establecer la conexión puedes acceder desde Utilidades > SSH.

En dinahosting ponemos a tu alcance otras muchas opciones para que trabajes en un entorno más seguro. Te las contamos aquí: [13 medidas para securizar aún más tu Panel de Control y tus servicios](#).

En Mac y Linux también puedes establecer la conexión SSH directamente desde su terminal, ya que vienen con el cliente instalado por defecto.

En Windows puedes hacerlo a través de programas como [Putty](#). Se trata del cliente SSH externo más utilizado, muy sencillo de utilizar y es de código abierto.

1.10 CÓMO CREAR CONTRASEÑAS SEGURAS: CONSEJOS Y HERRAMIENTAS

¿Cuántas aplicaciones web usas que necesitan contraseña para entrar? ¡Seguro que la mayoría! En este capítulo te enseñaremos cómo crear **contraseñas seguras y difíciles de descifrar** para mantener a buen recaudo tus datos online.

123456, password, qwerty, abc123, 111111... son, aunque no lo creas, algunas de las contraseñas más usadas, y también algunas de las más inseguras. Todavía hay usuarios que usan combinaciones como estas para proteger el acceso a aplicaciones en las que entran a diario, como su correo electrónico, alguna red social, o incluso su cuenta en el banco.

A todos nos gusta que nuestra contraseña sea fácil de escribir y recordar, pero esto no es incompatible con que sea segura. ¿Quieres tomarte tus contraseñas en serio antes de que sea demasiado tarde? Sigue leyendo.

Consejos a la hora crear tus contraseñas seguras

Cuando te pidan una contraseña en cualquier aplicación no puedes ir a lo fácil, ni tampoco poner lo primero que se te venga a la cabeza. Así que, ¡atiende bien a esto!

- **No conserves la contraseña que te da el sistema por defecto.** Lo mejor es que crees una tú, que seguro te resultará mucho más fácil de recordar.
- **Huye de las claves obvias** como tu nombre, fecha de nacimiento, número de teléfono, dirección, nombre de tu mascota... O cualquier otro dato que esté público en alguno de tus perfiles sociales o que sea de sobra conocido por tu entorno.
- **Las palabras o frases comunes no son una buena idea.** Piensa que cualquier tipo de fórmula popular o predefinida es de sobra conocida por los atacantes.
- **No compartas la misma clave** para diferentes dispositivos, correos, redes sociales... Es especialmente importante que tengas contraseñas concretas para aplicaciones de banca y webs de compras online.
- **¡Memoriza tus claves o usa un gestor de contraseñas!** Dejarlas por escrito no es muy seguro. Más abajo tienes unas cuantas alternativas.

Además de crear contraseñas fuertes, puedes doblar tu seguridad utilizando el sistema de verificación en 2 pasos, que ya está presente en muchas aplicaciones del mercado. En dinahosting, por ejemplo, puedes usarlo [tanto en el acceso a tu Panel de Control como en el Webmail](#).

Trucos para crear y memorizar tus contraseñas seguras

Recordar tus contraseñas seguras puede ser una auténtica pesadilla (¡a la altura de memorizar las tablas de multiplicar del cole!). Para facilitarte el asunto, te damos algunos truquillos:

Crea patrones de teclado y reemplaza números por letras

Escoge, por ejemplo, los 5 primeros dígitos de tu número de identidad y combínalos con las letras del teclado que tiene justo debajo. Supongamos que tu número es el 65897, con las letras quedaría: 6t5r8u9i7y. Ahora alterna caracteres en mayúscula y minúscula y añádele símbolos. Así quedaría: &6t5€R8U9i/7Y.

Escoge una frase, una letra de canción o un proverbio para tu contraseña segura

¡Y crea una contraseña segura! Te contamos cómo hacerlo...

Fíjate en este ejemplo de un proverbio: “más vale pájaro en mano que ciento volando”.

- Toma la primera letra de cada palabra: mvpemqcv.
- Alterna caracteres en mayúscula y minúscula: mVPemQcV.
- Inserta algunos números y símbolos entre las letras: #mVP?1emQ6cV.

¡Y listo!

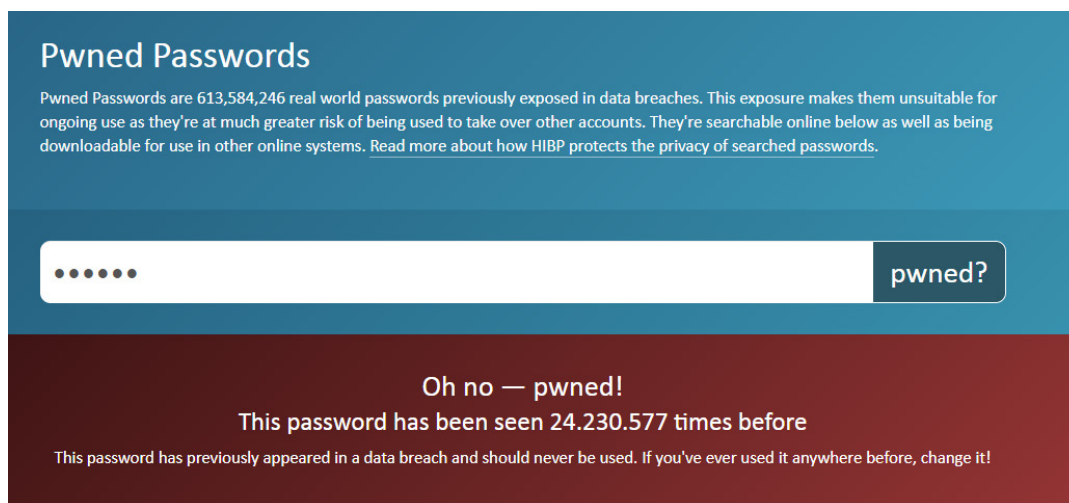
Si te gustan los sudokus, ¡a dibujar!

Pinta una cuadrícula con números escritos al azar o usa uno ya hecho. Ahora piensa en un patrón como el que usas para desbloquear tu móvil. Los números por los que pasa tu trazado formarán parte de tu contraseña. Ahora solo añádele letras y símbolos, ¡y ya lo tienes! Lo bueno de este sistema es que te sirve para crear infinitas contraseñas.

Comprueba si tu contraseña es vulnerable

Una vez tengas tu contraseña, te recomendamos que compruebes en la herramienta Pwned Passwords si es segura o ha sido vulnerada antes. Es tan fácil como introducir tu contraseña en el buscador y te dirá si debes o no usarla.

Para que lo veas con un ejemplo, hemos probado a meter la contraseña 123456, y este es el resultado:



Como era de esperar, nos dice que la contraseña ya ha sido usada y vulnerada, y que la cambiemos por otra más segura.

3 herramientas de gestión de contraseñas

Anotar tus contraseñas en un papel es un peligro (podrías perderlo o que alguien te lo viese). Guardarlas todas en un documento más de lo mismo (sería un regalo para cualquier ciberdelincuente que consiguiese acceder a tu equipo). ¿Qué puedes hacer entonces para no depender en exclusiva de tu memoria? **Utilizar gestores de contraseña.**

- **Son mucho más seguros que cualquier otro método tradicional**, puesto que reduce los errores humanos, tanto a la hora de crear malas contraseñas como de memorizarlas y teclearlas.
- **Son un dos en uno**: te recuerdan contraseñas, pero también te proponen nuevas si quieres.
- **Te lo ponen muy fácil**: tú solo necesitas recordar una “contraseña maestra” para acceder a tu gestor.

Bitwarden

Bitwarden **guarda todas tus contraseñas de forma cifrada (AES-256 bits) y sincronizada** para que puedas acceder a ellas desde cualquiera de tus dispositivos. Aparte de contraseñas, te permite también guardar notas y tarjetas de crédito.

Incorpora además un generador de contraseñas, por si no quieres perder tiempo en configurar una segura.

Su software es 100 % de código abierto y puedes usarlo gratis. Está disponible en Windows, Linux y Mac, y también tanto en Android como en iOS.

Puedes acceder a él desde el navegador web, incorporándolo como extensión en Chrome, Firefox, Safari... o instalándolo de forma nativa como aplicación de escritorio.

LastPass

LastPass te proporciona un espacio seguro en el que guardar tus contraseñas, notas, archivos, tarjetas de crédito... Te ofrece sincronización automática entre tus dispositivos, y también incluye un generador de contraseñas aleatorias y seguras cuando te registres en un sitio nuevo o quieras cambiar una contraseña antigua.

Tienes un mes de prueba gratis con su versión de pago, por si te interesa disfrutar de opciones avanzadas. Si pasado ese mes decides seguir con la versión gratuita, todos los datos que hayas guardado se seguirán manteniendo en tu cuenta.

El cifrado que utilizan es el AES de 256 bits.

Una característica interesante de LastPass es que, si en algún momento pierdes la “contraseña maestra” te ofrece un **método de recuperación del acceso a tu cuenta**.

Puedes instalarlo en los principales navegadores, tanto en Windows como en Mac y Linux. Si quieres también puedes descargar su versión móvil para iOS y Android.

Dashlane

A diferencia de Bitwarden y LastPass, que te ofrecen contraseñas ilimitadas gratis, con Dashlane tienes **hasta 50 contraseñas disponibles**. Luego tendrás que pasarte a un plan de pago.

La propia versión gratuita incluye **alertas de seguridad personalizadas**, en caso de que una cuenta que guardes en el gestor se viese afectada por una violación de datos.

Es compatible con Windows, Mac, iOS y Android, y con los principales navegadores: Chrome, Firefox, Safari y Edge.

Su principal desventaja es que en el plan gratuito podrás **conectarte desde un único dispositivo**. Si te interesa un plan de pago, podrás probarlo antes gracias a su versión de prueba gratis.

Esperamos que estos consejos y herramientas te sean útiles a la hora de crear y gestionar tus contraseñas seguras. En seguridad online cada detalle cuenta, ¡así que ponte manos a la obra!

1.11 RECOMENDACIONES DE SEGURIDAD EN IOT

Seguramente te hayas comprado alguna vez un termostato inteligente, una Smart TV, una cámara IP, una alarma... Pues no te fíes de lo bonitos que son y de lo cómodo que es poder controlarlo todo desde el teléfono...Hablamos sobre IoT (Internet of Things) y las peculiaridades de estos dispositivos.

La cámara IP

Estas cámaras permiten ver lo que ocurre en casa desde un smartphone o cualquier ordenador. A algunas cámaras se accede introduciendo en la web del fabricante el ID de la cámara y la contraseña. El **ID es un número aleatorio de 6 dígitos y en algunos casos se guarda la clave por defecto (ej. 123)**. Esto no solo nos preocupa porque sea simple, sino porque se repite para las miles de cámaras de ese modelo que se han puesto en el mercado.

¿Con estos datos que te doy se te ha encendido la bombilla? ¿Todavía no? Te ayudo: ¿que pasaría si entras en la web del fabricante (desde la que se accede a la cámara), pones un número de 6 cifras (aleatorio, el primero que se te ocurra) y luego la clave 123? Nos podemos encontrar con dos escenarios:

- Un usuario consciente de la importancia de la seguridad que haya cambiado la clave
- Puede que empecemos a ver la casa donde está la cámara

Lo primero que tienes que hacer es establecer una contraseña más robusta que la que trae por defecto. Aunque tu modelo de cámara tenga una contraseña más difícil, es posible que sea para todas las cámaras la misma.

La alarma inteligente

Están muy bien estas alarmas, ya que por unos 50 o 100 € podemos tener un sistema de seguridad en casa y sin pagar un mantenimiento mensual a una empresa de seguridad.

Tienen una centralita que controla los distintos sensores, enciende/apaga la alarma... Incluso algunas tienen un botón de pánico para hacer saltar la alarma en caso de peligro. **Muchas de estas alarmas funcionan en la frecuencia de los 433 MHz** (la misma que utilizan algunos mandos de coches y portales de garaje).

Lo más habitual es que solo el emisor y receptor conozcan el contenido del mensaje, pero como es una onda de radio y se extiende por el espacio, cualquiera puede capturar esa señal para un posterior procesamiento.

Entonces, ¿qué ocurriría si alguien con malas intenciones (y mucho tiempo libre) captura todos los mensajes que se emiten en esa frecuencia? Podría encender y apagar la alarma, desactivar un sensor, encender una lámpara, abrir la puerta del garaje...

Comentarte que esta no es más que una prueba de concepto. Aunque el rango de funcionamiento de estos emisores/receptores se puede extender, por defecto no alcanza más que unos pocos metros, algo que juega a nuestro favor si no deseamos que nos capturen estas señales.

Buenas prácticas en IoT

Puede que seamos conservadores con la tecnología y rechacemos utilizar dispositivos de IoT, pero viendo los [datos que se manejan acerca de la expansión de estos dispositivos](#), no tardaremos mucho en caer en la tentación.

Una práctica muy habitual en algunos fabricantes es lo que se llama Seguridad por oscuridad, por la que se intenta **ocultar el secreto de diseño, de implementación, etc. para asegurar la seguridad del desarrollo**. Pero esta no es del todo una buena práctica, puesto que cualquier persona con conocimientos de programación o entusiasta de esta tecnología podría encontrar agujeros de seguridad.

Entonces, **¿como consumidores qué podemos hacer?** Lo mejor es comprar productos testados y garantizados, que tengan una buena empresa respaldándolos. Y sobre todo, recordar que **cuando son muy baratos posiblemente sea porque hayan ahorrado costes en el desarrollo y producción de sus componentes**.



TU **HOSTING** DE ALTO RENDIMIENTO

Más espacio gratis
Garantía de reembolso: 30 días
Pruébalo gratis y paga al publicar tu web

1. Recomendaciones de seguridad en IoT | 38



1.12

CÓMO Y POR QUÉ BORRAR LA CACHÉ EN CHROME, FIREFOX Y SAFARI

¿Alguna vez has necesitado borrar la caché en Chrome o en otro navegador? Su función es almacenar cookies y otra información relevante sobre los sitios web que visitas a diario. A veces, hay que limpiarla para optimizar el funcionamiento de tu navegador.



Si lo prefieres
Mira el vídeo
¿Qué es la caché?

¿Qué es la caché del navegador?

La memoria caché es un **almacenamiento temporal de las cookies y otra información de los sitios webs** a los que entras, como elementos HTML, CSS, JS o imágenes. Al utilizar la versión en caché de una página, se **acelera considerablemente su velocidad de carga** y se reduce mucho la cantidad de peticiones enviadas al servidor que contiene los archivos.

Además, te permite establecer tus **preferencias de navegación** en ese browser (ubicación, idioma, etc.) y las recuerda cada vez que accedas.

Por qué borrar la caché del navegador

Al limpiar la caché de tu navegador, todos los datos que hayas almacenado en local hasta ese momento se eliminan. Como no existe una copia en caché de los mismos, el servidor web correspondiente se pone a funcionar para entregar de cero los recursos de la web, lo que conlleva un mayor tiempo de carga.

Aunque visto así parezca contraproducente, con el paso del tiempo te encontrarás con situaciones en las que sí necesitarás borrar la Caché de tu navegador. Te ponemos tres ejemplos:

- Estás haciendo **tareas de mantenimiento en tu web** y quieres comprobar que los cambios que has implementado se visualizan correctamente. Cuando accedes al navegador, te encuentras con que lo que te carga es una versión antigua de tu página. Por eso, si quieres dejar de ver contenido caducado y que te muestre correctamente las últimas actualizaciones, necesitas limpiar la caché del navegador. En este caso, también podría interesarte deshabilitarla temporalmente, pero acuérdate siempre de activarla después.
- Si **tu memoria caché lleva almacenando recursos durante mucho tiempo**, tu navegador tendrá que buscar entre un montón de archivos y cookies cada vez que le hagas una petición. Para evitar que se sobrecargue y que funcione más lento de lo normal, es conveniente borrar la caché cada cierto tiempo.
- Si **has modificado tus preferencias de navegación** (idioma, aspecto, opciones de privacidad y seguridad...), puede que los recursos obsoletos dentro de la memoria caché sigan sirviéndote la versión antigua de tu navegador. Limpia la caché y carga de nuevo.

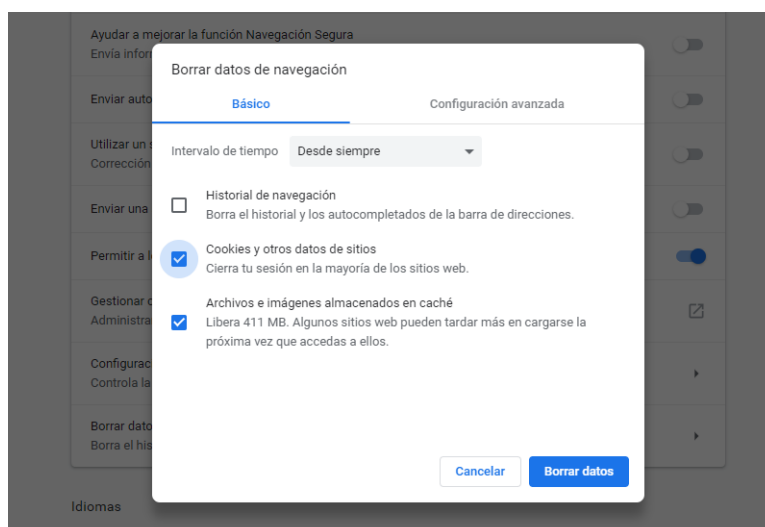
Cómo borrar la caché en Chrome, Firefox y Safari

Borrar la caché es una tarea sencilla y que no te llevará mucho tiempo. Te explicamos cómo se hace en los principales navegadores:

Google Chrome

Si te ayudas de los atajos de teclado, Ctrl + F5, Ctrl + R o Ctrl + Mayúsculas + R son los más utilizados. Si lo haces desde el menú lateral -los tres puntos verticales de la esquina superior derecha de Chrome-, clicas en Más herramientas > Borrar datos de navegación, selecciona el intervalo de tiempo durante el que te interesa eliminar la caché y marca las casillas de Cookies y otros datos de sitios y Archivos e imágenes almacenados en caché.

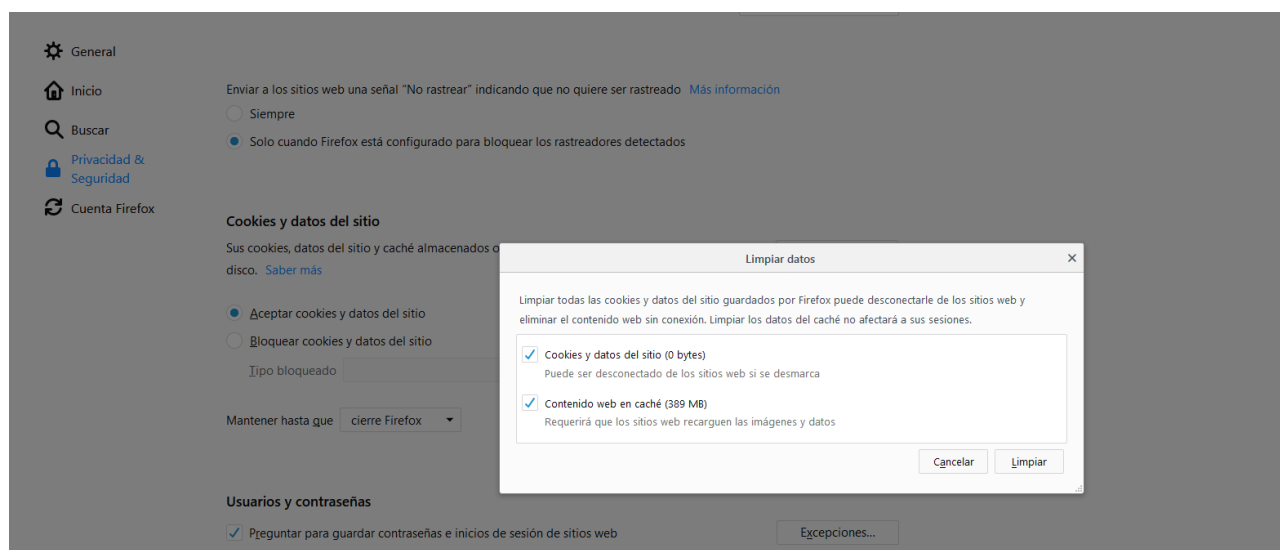
En la pestaña de configuración avanzada tienes otras opciones de borrado que también puedes activar si te interesa.



Cómo borrar la caché en Chrome

Mozilla Firefox

Usa los comandos Ctrl + F5 o Ctrl + Mayús + R. Si quieres establecer una configuración más avanzada, accede de nuevo a la esquina superior derecha del navegador, luego elige Opciones > Privacidad y seguridad > Cookies y datos del sitio > Limpiar datos. Marca las opciones Cookies y datos del sitio y Contenido web en caché, y ya lo tienes.



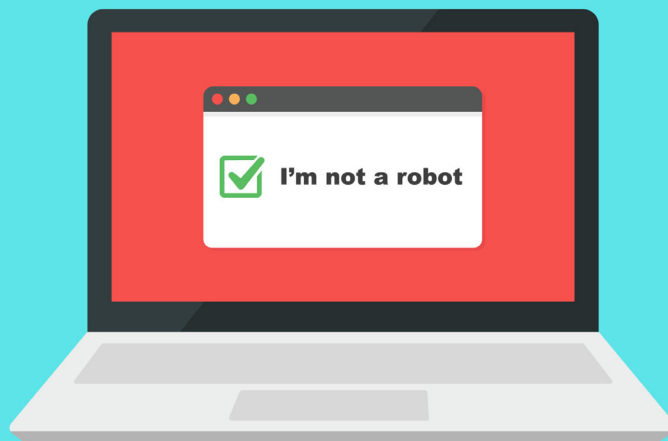
Cómo borrar la caché en Mozilla Firefox

Firefox también te da la opción de mantener las cookies y datos del sitio solo hasta que cierres el navegador. Puedes activarla para que cuando Firefox se cierre la caché se limpie de forma automática.

Safari

Puedes borrar la caché rápidamente combinando las teclas Comando + Alt + E. Desde el navegador, accede a la rueda situada en la parte superior derecha. Luego selecciona Restaurar Safari > Vaciar Caché y Eliminar cookies > Restaurar. ¡Reinicia y listo!

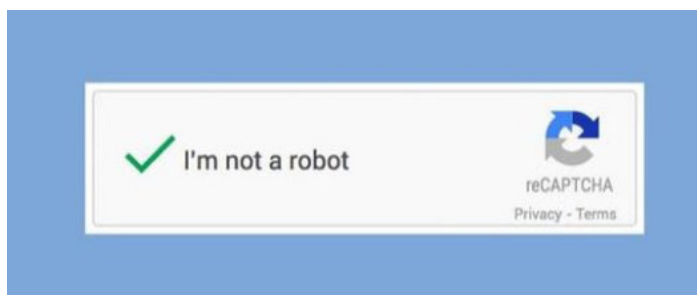
Ya ves que en general el proceso es sencillo, y si borras la caché en el momento oportuno, tu experiencia de navegación puede mejorar mucho.



1.13

¿QUÉ ES UN CAPTCHA?

El término CAPTCHA (test de Turing público y automático para **distinguir a los ordenadores de los humanos**, del inglés *Completely Automated Public Turing test to tell Computers and Humans Apart*) se utiliza para definir un **sistema de seguridad de tipo pregunta-respuesta** que demuestra que la persona que está interactuando con la web es un humano, excluyendo con ello cualquier interacción en la web por parte de robots o scripts automatizados.



Las principales funcionalidades de los CAPTCHA son las siguientes:

- Prevenir la publicidad (SPAM) en los blogs
- Evitar la creación masiva de usuarios falsos en el registro de la web
- Prevenir que bots puedan ver la dirección de correo electrónico del contacto de tu web
- Proteger encuestas en línea
- Prevención de ataques por fuerza bruta
- Prohibir el acceso a motores de búsqueda

¿Por qué debo poner CAPTCHA en mi web?

Es cada vez más común encontrar robots buscadores de internet que se dedican a buscar vulnerabilidades en las webs, con el fin de buscar formularios desprotegidos donde poder colocar comentarios de SPAM, localizar un acceso de usuario sin protección para lanzar un ataque de fuerza bruta, buscar un módulo o plugin desactualizado que permita cualquier tipo de vulneración y muchas otras tareas sospechosas. Los sistemas de CAPTCHA te ayudan a disuadir en cierta medida a estos robots buscadores y a mejorar la seguridad de la web.

Pero, ¿por qué mi web?

En este caso no se trata de nada personal contra tu web, estos robots maliciosos que buscan vulnerabilidades en las webs, van de una web a otra buscando posibles brechas. Por ello, nuestra recomendación es tener sistemas de CAPTCHA en cualquier formulario, apartado de comentarios o acceso de la web.

¿Qué tipos de CAPTCHA existen?

Existen múltiples tipos de CAPTCHA. Decantarse por utilizar uno u otro dependerá de la persona que administre la web, teniendo en cuenta el tipo de usuarios que frecuentan la página y la facilidad de implementación del mismo.

A continuación describimos algunos de los tipos de CAPTCHA más comunes:

Google ReCAPTCHA

Ha sido creado por Google y está funcionando desde el año 2014. Este sistema determina si un usuario es robot o humano presentando una simple tarea. Normalmente **se indica al usuario que haga clic en una casilla** que indica “No soy un robot”. Este CAPTCHA rastrea el movimiento del ratón, el clic y las cookies del usuario, además de otros parámetros, y determina si el usuario es un robot o no. Incluso, si este sistema no fuese capaz de determinar si se trata de un humano, mostrará una segunda prueba que consiste en escribir una serie de números y letras o seleccionar unas imágenes en concreto.

El [reCAPTCHA](#) está ampliamente aceptado y muchas webs confían en él para mantener a los robots alejados.

ReCAPTCHA invisible

Es una mejora del sistema de Google reCAPTCHA anterior. Su ventaja es que la experiencia de usuario no se ve afectada, pues no requiere que el usuario haga clic en el botón “No soy un robot”. Simplemente **monitorea los patrones de navegación**, y con ello consigue diferenciar a un humano de un bot sin que el usuario tenga que interactuar.

Sweet CAPTCHA

Este sistema **solicita al usuario realizar algún tipo de tarea sencilla** que solo un humano sería capaz de completar, como por ejemplo, mover una barra de desplazamiento hasta un punto en concreto, o arrastrar un elemento de la pantalla hasta un destino concreto. Se basa en que la prueba no pueda ser ejecutada con precisión por un robot.

El Sweet CAPTCHA ha demostrado ser muy efectivo, pero puede resultar frustrante para los usuarios menos hábiles.

CAPTCHA basado en tiempo

Este sistema **registra el tiempo que le lleva a un usuario completar un formulario**. Normalmente, cualquiera tardaría entre 2 y 3 minutos, mientras que un robot lo completaría de forma casi instantánea.

Es un buen sistema para implementar por ejemplo en un WordPress.

Honeypot

Consiste en **añadir múltiples campos ocultos en pantalla**. El objetivo de este CAPTCHA no es engañar al humano, sino al robot. Los bots pueden ver estos campos e intentar rellenarlos, confirmando con ello que quien está accediendo a la web no es un humano. Consecuentemente, se deniega o bloquea su acceso a la web.

El mayor beneficio de este sistema es que la experiencia del usuario en la página no se ve afectada en ningún momento.

Iniciar sesión en redes sociales

Una manera sencilla de verificar que el usuario no sea un robot es hacer que inicie sesión con su cuenta de Google, Facebook, Instagram u otras redes sociales. De este modo, el usuario no necesitará introducir ninguna información adicional.

La ventaja es que el usuario no precisa crear nuevos usuarios o perfiles en la web. La contrapartida es que existen usuarios que son reacios a vincular su información personal al sitio.

CAPTCHA matemático

Una forma popular de CAPTCHA es **añadir un sencillo problema matemático**. Por ejemplo, un usuario debe resolver e ingresar el resultado de un problema matemático como puede ser “2+2”.

No es tan sofisticado como otros sistemas de CAPTCHA, no obstante, es sencillo de implementar y puede ser perfecto para una web personal en WordPress o HTML.

CAPTCHA de palabras

Similar al caso anterior, este CAPTCHA consiste en una sencilla **prueba de palabras que el usuario debe descifrar**. Por ejemplo, se puede solicitar al usuario que escriba una palabra concreta en mayúsculas, escribir la última palabra de una frase, o responder a una sencilla pregunta.

Puede resultar excelente para usuarios con discapacidad visual o que tengan dificultades para resolver problemas más visuales.

¿Cómo instalar un CAPTCHA en un formulario?

Si quieres instalar ReCAPTCHA en un formulario de contacto o en los comentarios de tu blog personal, debes empezar por [conseguir las claves de Google reCAPTCHA](#) ¡es muy sencillo!

Dependiendo si trabajas con WordPress, PrestaShop o si tienes una web diseñada a medida, deberás seguir diferentes pasos.

En el vídeo te contamos Cómo añadir Google reCAPTCHA en tu WordPress.

Y a continuación, te explicamos paso a paso Cómo introducir Google reCAPTCHA en un formulario PHP.



Mira el vídeo

Google reCAPTCHA
en tu WordPress



SERVIDORES DEDICADOS

*Configura tu Servidor Dedicado a medida
El mejor Dedicado con IP española*



1.14

IMPLEMENTAR GOOGLE RECAPTCHA EN UN FORMULARIO PHP

Vamos a explicarte como implementar Google ReCAPTCHA en un formulario PHP enviado por POST, tanto para la versión de V2 como para la versión V3.

Normalmente si trabajas con WordPress, PrestaShop o cualquier CMS, dispones de plugins o módulos para facilitarte esta tarea, sin embargo, **en una web a medida tendrás que añadirlo de forma manual a tus formularios.**

El proceso es sencillo teniendo una pequeña base de programación PHP. Se añaden unas líneas de código adicional en el formulario y en el proceso de validación para la implementación de Google ReCAPTCHA V3 y el proceso es el mismo para Google ReCAPTCHA V2 añadiendo además una librería que Google pone a nuestra disposición y que puedes descargar desde [aquí](#).

Antes de empezar asegúrate de tener tus [claves Google ReCAPTCHA](#), ten en cuenta que son diferentes según la versión

Implementando ReCAPTCHA V2

Descarga la librería `recaptchalib.php` que indicamos anteriormente y súbela a tu hosting.

Edita tu formulario PHP y añade la siguiente línea al principio del código, justo después de “<?php”

```
require_once "recaptchalib.php";
```

Puedes subir esta librería al mismo directorio donde está tu formulario, sin embargo puedes colocarla donde desees y cambiar la ruta en el script para llamar a esta librería.

Ahora añade el siguiente script entre las etiquetas <head> y </head>

```
<script src="https://www.google.com/recaptcha/api.js?hl=es" async defer></script>
```

Coloca el siguiente código donde quieras que sea visible el cuadro de validación de Google ReCAPTCHA.

```
<div class="g-recaptcha" data-sitekey="CLAVE PUBLICA"></div>
```

Debes cambiar la palabra CLAVE PÚBLICA de este código por la clave pública o también llamada clave de sitio que te facilita Google.

En el fichero que hace la validación de los datos de formulario añade el siguiente código:

```
require_once "recaptchalib.php";  
$secret = "CLAVE PRIVADA";  
$response = null;  
// Verificamos la clave secreta
```

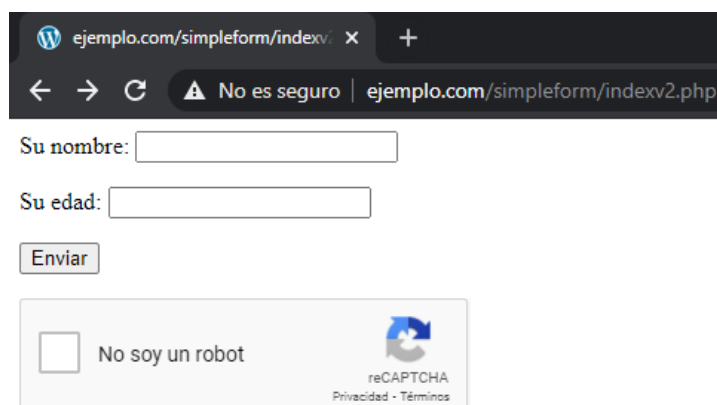
```
$reCaptcha = new ReCaptcha($secret);
if ($_POST["g-recaptcha-response"]) {
    $response = $reCaptcha->verifyResponse(
        $_SERVER["REMOTE_ADDR"],
        $_POST["g-recaptcha-response"]
    );
}

if ($response != null && $response->success) {
    // Añade aquí el código que desees en el caso de que la validación sea correcta
} else {
    // Añade aquí el código que desees en el caso de que la validación no sea correcta o muestra
}
```

Debes cambiar la palabra CLAVE_PRIVADA de este código por la clave privada o también llamada clave secreta que te facilita Google.

Con esto podremos ver el campo de verificación de Google ReCAPTCHA v2 en nuestro formulario.

*Formulario PHP con
Google ReCAPTCHA V2*



Implementando ReCAPTCHA V3

El primer paso es añadir el siguiente script entre las etiquetas <head> y </head> del formulario de tu web

```
<script src='https://www.google.com/recaptcha/api.js?render=CLAVE_PÚBLICA'>
</script>
<script>
    grecaptcha.ready(function() {
        grecaptcha.execute('CLAVE_PÚBLICA', {action: 'ejemplo'})
        .then(function(token) {
            var recaptchaResponse = document.getElementById('recaptchaResponse');
            recaptchaResponse.value = token;
        });
    });
</script>
```

Debes cambiar la palabra CLAVE PÚBLICA de este código por la clave pública o también llamada clave de sitio que te facilita Google. También puedes cambiar el valor action para hacer un seguimiento de tus formularios en el administrador de Google ReCAPTCHA

A continuación inserta el siguiente contenido dentro del código de formulario:

```
<input type="hidden" name="recaptcha_response" id="recaptchaResponse">
```

En el fichero que hace la validación de los datos de formulario añade el siguiente código.

```
$recaptcha_url = 'https://www.google.com/recaptcha/api/siteverify';
$recaptcha_secret = 'CLAVE_PRIVADA';
$recaptcha_response = $_POST['recaptcha_response'];
$recaptcha = file_get_contents($recaptcha_url . '?secret=' . $recaptcha_secret . '&response=' . $recaptcha_response);
$recaptcha = json_decode($recaptcha);
if($recaptcha->score >= 0.7){
    // Añade aquí el código que desees en el caso de que la validación sea correcta
}else{
    // Añade aquí el código que desees en el caso de que la validación no sea correcta
}
```

Debes cambiar la palabra CLAVE_PRIVADA de este código por la clave privada o también llamada clave secreta que te facilita Google.

Modifica el valor score del código por el que desees entre 0 y 1. Este valor indica cuál es la probabilidad de que el usuario que está accediendo al formulario sea una persona y no un robot, en función de eso podrás definir si bloqueas esa petición o no.

Con este código tendrás funcionando el sistema de validación sin interacción del usuario Google reCAPTCHA v3.

TU HOSTING MÁS RÁPIDO Y SEGURO

Con discos NVMe ¡hasta 6 veces más rápidos que los SSD tradicionales!

Certificado SSL preinstalado

GUÍA DE CIBERSEGURIDAD

2. Tus servicios más seguros en dinahosting

[2.1. 13 Medidas para securizar aún más tu Panel y servicios](#)

[2.2. Por qué necesitas una copia de seguridad diaria de tu hosting](#)

[2.3. ¿Cómo funciona el servicio de Backups?](#)

[2.4. La seguridad de nuestros Hosting Linux](#)

[2.5. Consejos de seguridad para tu correo electrónico](#)

[2.6. ¡Que no suplanten tu identidad! Activa el registro SPF en tu dominio](#)

[2.7. ¿Qué son los registros SPF, DKIM y DMARC?](#)

[2.8. Autenticación en 2 pasos: qué es y que herramientas necesitas para activarla](#)

[2.9. ¿Qué es y para qué sirve Firewall DNS?](#)

[2.10. ¿Alojamiento web en España o en Estados Unidos?](#)





2.1 13 MEDIDAS PARA SECURIZAR AÚN MÁS TU PANEL Y SERVICIOS

Como bien sabes, la seguridad se ha convertido en una de las principales preocupaciones de los usuarios de cualquier web o aplicación online. En este post te hacemos un resumen de las posibilidades que tienes a tu alcance para hacer que el acceso y la gestión de tu Panel de Control y de tus servicios en dinahosting sean todavía más seguros.

1. Mantén el email de contacto actualizado

Asegúrate de que el email de contacto que nos facilitas está actualizado. Es muy importante, porque es a través de este correo que puede modificarse la contraseña y recuperar el acceso al [Panel de Control](#) principal.

Puedes revisar tu información de contacto en el apartado Mi Cuenta > Contacto.

2. Activa la notificación de logins incorrectos

Con la notificación de logins incorrectos recibirás un correo cada vez que se produzca un login erróneo con tu usuario. Esto te permite detectar si hay alguien que no seas tú intentando entrar en tu cuenta.

Activa esta opción en tu [Panel](#) de dinahosting, desde Mi Cuenta > Preferencias > Seguridad.

3. Mantén tu hosting libre de malware

¿Conoces el detector de malware? Es una herramienta genial para comprobar si tu hosting tiene algún tipo de virus.

Entra a tu [Panel de Control](#), al hosting correspondiente, y luego a Seguridad > Antivirus web.

El antivirus web **escanea tu alojamiento en busca de cualquier software malicioso**, haciendo un análisis rápido y gratuito de tu alojamiento y comprobando si está limpio. Al terminar la herramienta te proporciona un informe detallado con los resultados obtenidos por el antivirus, que puedes descargar en PDF. Si el hosting tiene algún virus, puedes solicitarnos su desinfección bajo presupuesto también desde el propio Panel.

Además, también es fundamental que los equipos o dispositivos desde los que te conectes al Panel estén libres de malware, virus, etc. Esto favorecerá también la seguridad.

El malware puede redundar no solo en un bajo rendimiento de tu equipo, sino en el bloqueo de determinadas aplicaciones. Incluso **puede llegar a actuar en un segundo plano, intentando capturar todo tipo de datos personales**, como las contraseñas de acceso que introduzcas a diario.

4. Activa la Verificación en 2 pasos

La Verificación en 2 Pasos es un sistema de seguridad que se intercala en el login de tus servicios proporcionándoles una capa de protección adicional.

En cuanto la actives, para acceder a tu Panel no bastaría tan solo con conocer la contraseña, sino que además sería necesario estar en posesión de un código de 6 dígitos que se genera automáticamente mediante una APP en tu móvil. Aquí te explicamos al detalle [cómo funciona la Verificación en 2 pasos](#).

Además de en el Panel de Control, puedes configurar este mismo sistema de [verificación en tu webmail de dinahosting](#).

5. Proporciona accesos secundarios

Los [accesos o usuarios secundarios](#) son útiles cuando quieres autorizar a terceras personas a realizar una determinada acción en tu Panel (mantenimiento de los hostings, hacer gestiones administrativas, llevar la contabilidad, etc.), pero sin que puedan acceder al resto de secciones. Así cada persona entrará exclusivamente a los servicios relacionados con su área.

En la creación de las credenciales para los usuarios secundarios, **intenta siempre que las contraseñas que generes sean fuertes y diferentes entre los usuarios que tengas**. También es recomendable que cambies las contraseñas con las que acceden de forma periódica.

6. Configura permisos de acceso a tus Bases de datos

La de Bases de datos es una sección sensible dentro de tu hosting por toda la información que almacena, por eso en nuestro Panel puedes crear usuarios secundarios con permisos limitados para cada una de las bases de datos que tengas. **Hablamos tanto de permisos de acceso como de privilegios de uso:** lectura, escritura, ambas, o privilegios personalizados según los parámetros que tú quieras.

Accede al [Panel](#) de dinahosting y luego a Hosting > Bases de datos. En la tabla inferior donde se listan las bases de datos que tienes, haz clic en el "+" de la columna Usuarios secundarios.

Créalos desde ahí y asígnales los permisos que te interesen.

7. Crea restricciones de entrada al Panel por continente, país o IP

Restringir el login por continente, país o IP es básico para evitar accesos maliciosos a tu cuenta desde una IP o zona geográfica determinada.

Tan solo tienes que acceder al apartado Mi Cuenta > Preferencias > Seguridad y configurar el acceso con tu usuario desde ahí.

Este tipo de restricciones puedes aplicarlas también a carpetas concretas dentro de tu hosting para que solo tú puedas entrar a ellas. Para habilitar esta utilidad, entra al Panel y luego a Hosting > Seguridad > Protección de carpetas. **Si eliges la opción de IP, asegúrate de que la tuya no cambie recurrentemente.**

Además, desde tu Panel de dinahosting también puedes crear **restricciones de acceso a cuentas de correo por IP**. El funcionamiento es sencillo.

Entras en el [Panel de Control](#), al hosting que quieras, y luego a Correo > Seguridad > Restricciones IP.

Seleccionas la cuenta en el desplegable, indicas las IP o rangos de IP que podrán acceder a la cuenta separados por comas, ¡y listo!

8. Deshabilita FTP y SSH cuando no lo uses

Para la transferencia segura de archivos entre tu PC y el servidor en el que esté alojado tu hosting, en dinahosting contamos con FTPS, que usa los mismos comandos que FTP pero recurre a los protocolos SSL o TLS para cifrar la transferencia de datos.

Para evitar ataques por fuerza bruta desde múltiples IP, se recomienda desactivarlo siempre que no se tenga previsto subir o descargar ficheros del hosting.

Puedes hacerlo desde tu [Panel](#), en la sección Hosting > FTP.

SSH es un protocolo de administración que te permite gestionar tus servidores en remoto: copiar o mover ficheros en tu hosting, exportar o importar bases de datos, crear directorios, etc.

En tu [Panel de Control](#), Hosting > Utilidades > SSH tienes acceso a una consola SSH para conectarte a tu hosting Linux.

SSH utiliza técnicas criptográficas que garantizan que las comunicaciones entre cliente y servidor se lleven a cabo mediante cifrado. Si no vas a necesitarlo, recuerda también desactivarlo por la seguridad de tu hosting.

9. Protégete del hotlinking

Seguro que te suena el término hotlinking. Se produce **cuando un tercero usa imágenes tuyas en sus contenidos, pero en vez de subirlas a su hosting las enlaza desde un URL de tu web**. Por lo tanto, cada vez que esas imágenes se carguen estarán llamando al servidor de tu web y consumiendo sus recursos.

Piensa que si el sitio que te enlaza es súper popular tu servidor incluso podría llegar a caerse por una sobrecarga derivada del exceso de peticiones.

Es genial que compartan tus contenidos, pero cuando se trata de imágenes hay que tener cuidado con este tipo de prácticas.

Para proteger tu hosting del hotlinking ante dominios concretos, entra a tu [Panel de Control](#) y luego Hosting > Seguridad > Bloqueo accesos.

Puedes bloquear el acceso a audios, vídeos, imágenes, documentos o archivos ZIP, RAR, etc. para que solo sean accesibles desde tu web.

10. Define filtros y reglas para eliminar el spam antes de que llegue a tu buzón

Para filtrar los correos recibidos para tu dominio, tienes la opción de definir reglas y filtros antispam.

Entra al [Panel](#), al hosting que quieras, y luego ve a Correo > Reglas y filtros.

Desde ahí puedes diseñar toda una configuración de parámetros que reduzcan la recepción de spam en la bandeja de entrada de tu correo. Aquí te dejamos unos cuantos [ejemplos muy sencillos de implementar](#).

11. Activa el Correo TLS

TLS es un protocolo criptográfico que cifra tus comunicaciones por email para que si un tercero intercepta tus mensajes no pueda descifrarlos fácilmente.

Puede que TLS no te suene, pero seguro que SSL sí. Pues TLS no es más que una versión más reciente de SSL, que corrige algunas vulnerabilidades de seguridad, además de mejorar la velocidad del cifrado entre cliente y servidor.

Para activar TLS en tu correo, te vas a tu hosting y luego a Correo > Sobre este correo. Marca con un check la opción Correo TLS y ya estaría.

12. Usa DKIM y SPF para proteger tu identidad en el correo

Los registros o protocolos de autenticación SPF y DKIM te van a ser útiles a la hora de proteger tu identidad.

DKIM te vendrá bien para autenticar y firmar tus correos electrónicamente, de forma que tu destinatario sepa que el email se envió desde tu servidor y no desde otro no autorizado.

Podrás crear registros SPF para evitar suplantaciones de identidad vía email, lo que se conoce como phishing. Lo que hace es **certificar desde qué IP se pueden mandar un correo** utilizando un determinado dominio.

Aquí tienes [información más detallada sobre DKIM y SPE](#), con ejemplos prácticos de uso.

13. Activa las alertas de renovación y traslado de servicios

Ya sabes que en tu Panel de Control puedes personalizar la periodicidad con la que quieres recibir los avisos relacionados con el alta, renovación o traslado de tus servicios.

Tienes esta opción en el apartado de Facturación > Preferencias del [Panel de Control](#).

Nuestra recomendación cuando se trata de servicio que te interesa mantener en el tiempo es que lo mejor es no arriesgarse y activar la renovación automática del mismo, así te olvidas de tener que renovarlo manualmente periódicamente. Aquí te explicamos [cómo activar una renovación automática](#) paso a paso.

PROGRAMA DE **RESELLERS**

*Ideal para agencias y empresas de desarrollo
Disfruta de grandes descuentos por volumen*



2.2 POR QUÉ NECESITAS UN BACKUP O COPIA DE SEGURIDAD DIARIA DE TU HOSTING

Ante la inmensa cantidad de información que almacenamos diariamente, un buen servicio de backup en tu hosting te da la tranquilidad de que, en caso de incidente, podrás seguir accediendo a toda la información relativa a tu web: ficheros, bases de datos y correo.

En este capítulo profundizamos en qué es un backup o copia de seguridad, y qué opciones tienes en dinahosting para recuperar tus backups cuando lo necesites.

¿Qué es hacer un backup?

Un backup o copia de seguridad es el **proceso de copia y almacenamiento de la información que acumulas en tu hosting**: ficheros, bases de datos y correo.

Con la llegada de un virus o cualquier tipo de malware, problemas con el hardware, si te has despistado y borrado algún contenido que necesitabas... tener una copia de seguridad **evita que pierdas información sensible o valiosa para tu proyecto web**.

Por ejemplo, imagínate que acabas de actualizar tu tienda online en WordPress a la última versión del CMS. Resulta que la actualización no ha salido como esperabas, y necesitas restaurar tu web a un estado anterior para evitar así perder ventas. En este caso, tener un backup es la forma más rápida de solucionar el conflicto.

Fundamentalmente, las ventajas de disfrutar de backups en tu hosting son dos:

Seguridad

En dinahosting **monitorizamos tu hosting las 24 horas al día**. Nuestro equipo de Soporte Técnico está preparado para enfrentarse a cualquier tipo de incidencia, aunque con tu servicio de backups tú mismo puedes recuperar la información que necesites.

Automatización

Tú no tienes que hacer nada, **la copia de seguridad se genera automáticamente**. El **proceso de restauración**, tal y como te explicamos a continuación, también es **automático**.

Aún así, si quieres asegurarte todavía más, puedes guardar por tu cuenta un backup en tu equipo o en cualquier dispositivo de almacenamiento, como una memoria USB. Puedes hacer este tipo de backups fuera de línea cada cierto tiempo para mayor tranquilidad.



2.3

¿CÓMO FUNCIONA EL SERVICIO DE BACKUPS?

Un backup es una **copia de seguridad de tu web o también llamado respaldo**, se trata de una versión reciente de la información que contenía tu alojamiento. Los backups nos permiten volver a un estado anterior del hosting.

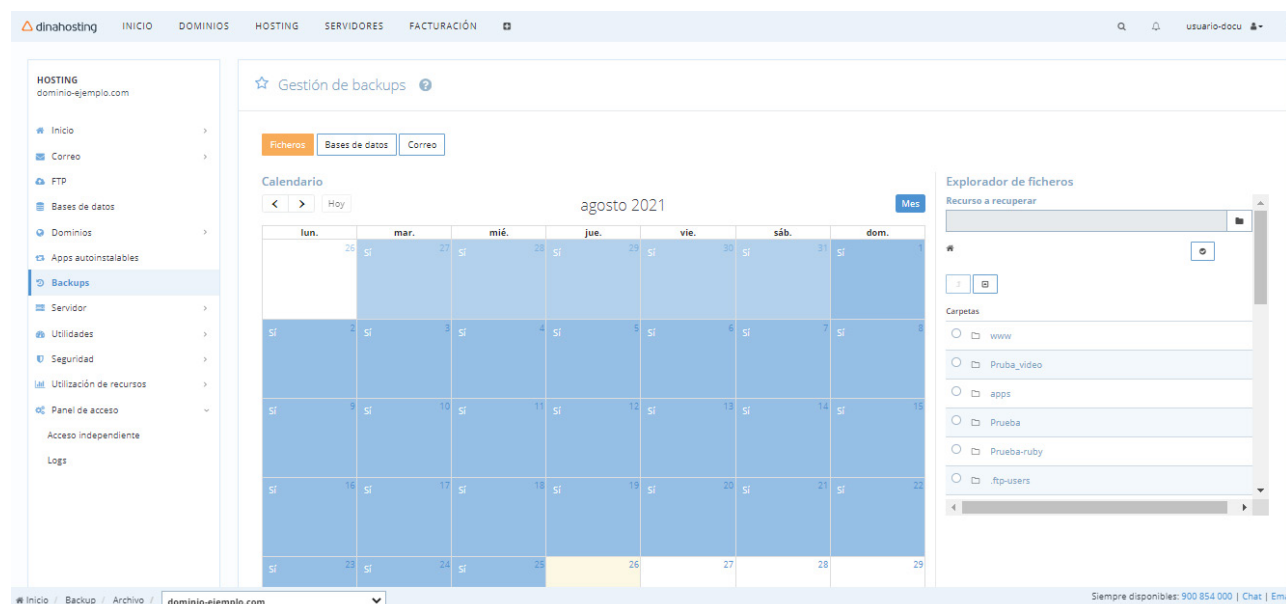
En el caso de que exista un problema en tu web, base de datos o necesites restaurar correo, puedes usar la herramienta de backups de tu panel de control de hosting y volver a una fecha donde no tenías problemas.

Por ejemplo, suele ser común que tengamos que hacer alguna actualización de contenidos en nuestra web o simplemente actualizar WordPress o nuestra tienda online. Tener un backup a mano es la forma más rápida de restaurar el sitio en caso de que el proceso no termine de la forma esperada.

La principal ventaja de los backups es **tener un plan de acción** ante cualquier problema en el hosting y poder recuperar la información de forma rápida y tener la tranquilidad de que si algo sale mal siempre podemos contar con la copia de seguridad.

Cómo realizamos los Backups

Dinahosting realiza copias de seguridad de todos los Servicios Administrados. Nuestro sistema de Backups hace una **copia incremental cada día**, de madrugada, y además **una copia completa durante el fin de semana**. El backup completo de tu hosting se realiza de sábado a domingo.



The screenshot displays the 'Gestión de backups' (Backup Management) section of the Dinahosting control panel. The interface includes a sidebar with navigation options like 'Inicio', 'Correo', 'FTP', 'Bases de datos', 'Dominios', 'Apps autoinstalables', 'Backups', 'Servidor', 'Utilidades', 'Seguridad', 'Utilización de recursos', 'Panel de acceso', 'Acceso independiente', and 'Logs'. The main area shows a calendar for August 2021 with a grid of backup status (SI for success, NO for failure). The 'Ficheros' (Files) tab is selected. On the right, there's a file explorer showing a list of folders like 'www', 'Prueba_video', 'apps', 'Prueba', 'Prueba-ruby', and 'ftp-users'.

Panel de Backups de dinahosting

Desde la aplicación de Hosting de tu [Panel de Control](#), entrando al apartado Backups, accedes a todas tus copias de seguridad diarias de una forma facilísima.

En caso de que te surja algún problema con tu web o base de datos, o necesites restaurar tu correo, desde esta interfaz del Panel puedes volver atrás sin problemas, simplemente eligiendo la fecha que te interese.

Estas copias son almacenadas durante un mes. Esto quiere decir que puedes restaurar, si lo necesitas, los contenidos correspondientes a los 30 días anteriores. Solo tienes que acceder a tu Panel de Control y [restaurar cualquier contenido o guardar una copia de seguridad](#).



Mira el vídeo

Qué es y cómo restaurar un backup de ficheros, correo y base de datos

En cualquier caso y como recomendación adicional, siempre es conveniente que guardes un backup fuera de línea, en tu equipo, o en una memoria USB y revises que funciona correctamente, de esta forma, en caso de emergencia dispondrás de una tranquilidad extra.



**LOS VPS
MÁS RÁPIDOS
Y SEGUROS**

Ahora con más espacio, ¡gratis!

*Discos NVMe: máxima
velocidad y rendimiento*



2.4 LA SEGURIDAD DE NUESTROS HOSTING LINUX

Te hace falta un **Hosting Linux**, hay un mundo de características que quieres revisar antes de contratarlo y no sabes por dónde empezar. Te vamos a dar una pista: fíjate en la seguridad. Necesitas un [hosting seguro](#) y que tu plataforma no se caiga a la primera de cambio.

En un proyecto online **la seguridad es fundamental**. Una web inestable deja de tener visitantes, posiciona peor en los buscadores y los datos privados que acumula se vuelven vulnerables, lo cual es un problema. Y como no queremos que esto pase, en dinahosting nos tomamos el asunto muy en serio.

Antes de meternos de lleno en la seguridad de nuestros hosting Linux, hay **dos cosas que nos gustaría que supieras**. Una: llámanos/escríbenos cuando quieras (a cualquier hora, los 365 días del año), que además, te vamos a atender en tu idioma (español, catalán, gallego, euskera o inglés). Dos: prueba nuestros productos con la tranquilidad de saber que tienes 30 días de reembolso. ¡Sabemos que al final te vas a quedar en dinahosting!

Ventajas de seguridad

Nuestros [planes de Hosting Linux](#) tienen algunas ventajas que (¡haznos caso!) vas a apreciar mucho cuando te hagan falta.

Servicio de Backup

Hacer **copias de respaldo de tus datos** es un básico en seguridad. Aunque algo falle, vas a poder recuperar rápidamente tus ficheros, bases de datos y correos sin perder nada por el camino.

¿Qué condiciones te ofrecemos? En Hosting Compartido, el sistema se encarga de realizar una **copia incremental diaria**, una completa cada semana y de mantener todo almacenado **durante 30 días**. Puedes acceder a ellas desde la aplicación de Hosting de tu [Panel de Control](#).

Si tienes un Servidor en exclusiva para ti: si es Administrado, contrata nuestro servicio de backups para trabajar en tu proyecto con toda la seguridad; si es No Administrado, haz tus copias por tu cuenta, cuando y como quieras.

Limpieza de malware

Como ya sabrás, el malware es un tipo de software maligno que ojalá no se infiltre nunca en tu sistema. ¿Cómo reaccionamos ante él? Desde [Google Safe Browsing](#) recibimos información sobre las amenazas que afectan a las IP alojadas en nuestros servidores. Luego, alertamos del problema a los usuarios afectados.

Además, si tienes un hosting Administrado te proporcionamos un **detector de malware** con el que puedes escanear tu hosting en busca de virus completamente gratis. Entra a tu Panel de Control, al hosting correspondiente, y luego a Seguridad > Antivirus web, y solicitas el escaneo. Al finalizar te proporcionamos un informe de resultados, por lo que de haber malware puedes contratar nuestro **servicio de limpieza de bajo presupuesto** que te deja el hosting limpio como una patena. Hazlo desde esa misma sección del Panel.

ModSecurity

Otra de las ventajas de seguridad de nuestros Hosting Linux. [ModSecurity](#) es un firewall de aplicaciones web (WAF) que filtra las peticiones HTTP antes de pasarlas al servidor, y está activo en todos nuestros servidores Linux por defecto. Funciona mediante el uso de reglas a través de las que se generan acciones (rechazar, ignorar...). Entre los ataques que puede filtrar están los fallos conocidos de aplicaciones, las anomalías en protocolos, los troyanos, los robots maliciosos...

Lo que hacemos en dinahosting es desarrollar **reglas propias** para ModSecurity, en función del tipo de incidencias que sufran nuestros clientes, para reforzar aún más la protección de su web y mantener tu hosting seguro.

Correo

Desde aquí **monitorizamos los accesos** a la cuenta de correo que tengas con tu alojamiento. Si detectamos que se entra al mismo desde países poco comunes para nuestros clientes los avisamos de que, posiblemente, su cuenta haya sido hackeada. ¿Te suena eso de “hemos detectado un acceso a tu cuenta desde la IP... Si no has sido tú...”? Pues te enviaremos un aviso de este tipo para que cambies los datos de tu cuenta cuanto antes.

Además, también aplicamos **antispam y antivirus en tiempo real** a las cuentas que tengas.

Panel de Control

En [nuestro Panel](#) te proporcionamos unas cuantas medidas para mantener tu hosting más seguro. ¡Échales un ojo y empieza a aplicarlas!

- Activa la notificación de logins incorrectos
- Activa la Verificación en 2 pasos
- Proporciona accesos secundarios
- Configura permisos de acceso a tus Bases de datos
- Crea restricciones de entrada al Panel por continente, país o IP
- Deshabilita FTP y SSH cuando no lo uses
- etc.

[Aquí](#) te explicamos a fondo estas y otras funcionalidades para que tu el acceso y la gestión de tus servicios en dinahosting sean de lo más seguros.

Y además...

...tres buenas razones para alojar tu web en dinahosting:

- **Escala de plan de hosting** de forma sencilla. Añade recursos o migra a un plan superior conforme tu proyecto vaya creciendo.
- **Muévete de una a otra versión** a través de [Migrar de servidor](#). Incluso puedes cambiar de versión de PHP sin cambiar de servidor.
- **Tráete tu web a dinahosting** sin esfuerzo. Está mal que lo digamos, pero tenemos una herramienta de portabilidad que va muy bien. Pero si lo prefieres, nos encargamos de todo y [migramos tus webs completamente gratis](#).

2.5

CONSEJOS DE SEGURIDAD PARA TU CORREO ELECTRÓNICO

Mejorar la seguridad de tu correo es una tarea a la que debes prestar mucha atención. Seguramente ya estés habituado a la palabra Phishing o malware. A día de hoy el email sigue siendo una puerta de entrada enorme a timos y ataques fraudulentos, es por ello que en el post de hoy te hablaremos sobre **como securizar tu email al máximo**.

Los delitos de estafas por Internet **han aumentado al menos en un 70 %**, en un momento en el que la gente está más conectada que nunca. Los cálculos de la Guardia Civil estiman que este aumento está provocado aprovechando la crisis del coronavirus. Algunas organizaciones como la [Interpol](#) han publicado artículos con recomendaciones para evitar ser objetivos de estos delitos. Si tienes curiosidad por conocer cuáles fueron las principales estafas del año pasado (muy vigentes este año también), no te pierdas [este artículo](#) de la empresa de seguridad Kaspersky.

Sentido común para mejorar la seguridad de tu correo

Aún llevando todas las normas y recomendaciones a rajatabla nadie está exento de sufrir una estafa a través correo electrónico. Cada día están más al alcance de los ciberdelincuentes herramientas para realizar [phishing](#) con muy poco esfuerzo. Por ello es primordial que prestemos especial atención a cualquier correo que pueda llegarnos de un remitente importante (banco, tesorería general, Ayuntamiento...).

Algunas acciones no requieren de ningún tipo de herramienta adicional, únicamente ser cautelosos en la lectura y uso de nuestro correo electrónico.

Cuidado con los enlaces

La mayor parte de los correos contienen enlaces. En los correos de Phishing estos enlaces están orientados a páginas que te pueden introducir cookies maliciosas u otro tipo de software en tu ordenador. Antes de hacer clic en un enlace echa un vistazo a la dirección a la que te reenvía, verificando que tiene una URL confiable.

Cuidado con los adjuntos

Algo tan inofensivo como una imagen o un archivo .txt adjunto puede esconder un troyano o un virus. Si tienes la mínima duda del remitente del mensaje nunca descargues y abras estos adjuntos. Si realmente te interesa ver lo que viene en ese correo, la acción a seguir podría ser: descargar en tu equipo el archivo y antes de abrirlo, pasarlo por algún antivirus, de forma que corrobore que no existan problemas con el adjunto.

Atención a los remitentes y los asuntos

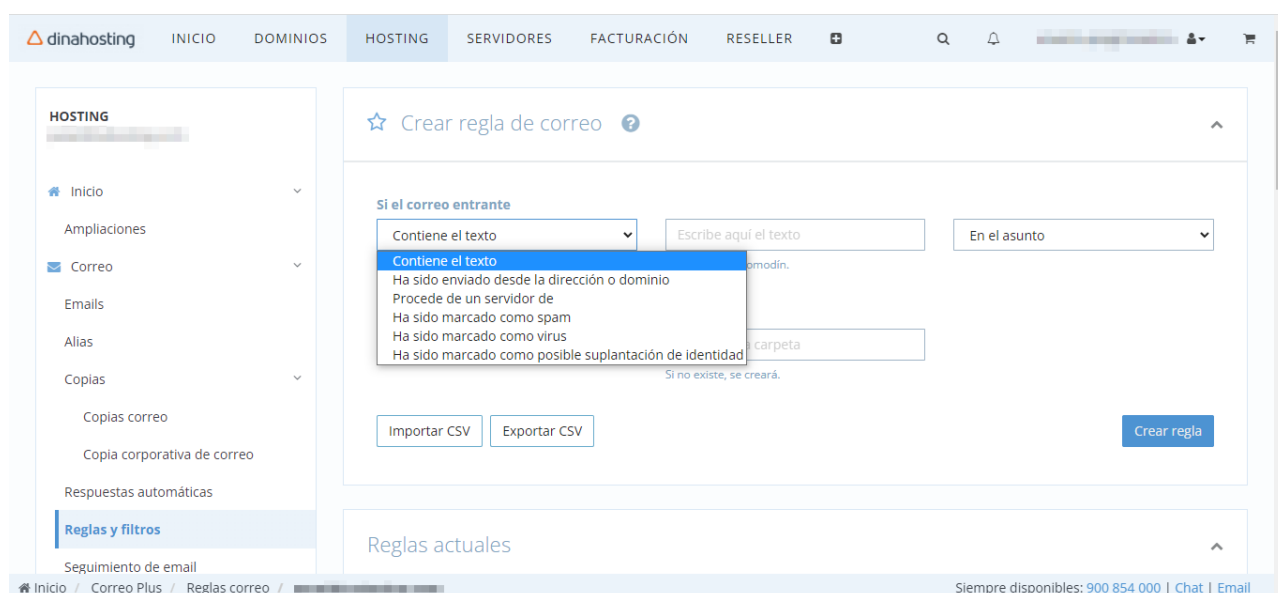
En muchas ocasiones, solamente con ver el remitente o el asunto ya podemos hacernos una idea de la seguridad de es correo. Mejor pecar de precavido que de curioso. Presta especial cuidado a asuntos con faltas de ortografía, mal redactados o aspecto de ser una mala traducción. Hoy en día casi cualquier empresa tiene una persona encargada de la comunicación, que presta especial atención a estos detalles.

Herramientas de seguridad para tu correo

Además del sentido común, casi todos los gestores de correo poseen herramientas Antispam y filtros para automatizar las cuestiones de seguridad en tu bandeja de entrada. Nos vamos a concentrar en las que ofrecemos en dinahosting. En caso de que no dispongas de las mismas recuerda que nuestro [hosting correo](#), viene por defecto con todas ellas y además, tendrás tu **email con dominio propio**.

Creación de reglas

El sentido común es algo que puede “automatizarse”, por ejemplo, si en un asunto vemos la palabra “dinero gratis”, ya nos da pistas de que ese correo puede ser fraudulento. En lugar de estar revisando todos los emails de la bandeja de entrada, podremos crear reglas para que por ejemplo cuando detecte el texto “dinero gratis” lo mueva a una carpeta específica (SPAM, papelería o la que decidamos). De esta manera evitaremos poder equivocarnos un día por cansancio, que omitamos las reglas de seguridad sobre correo aprendidas y acabemos abriendo ese email.



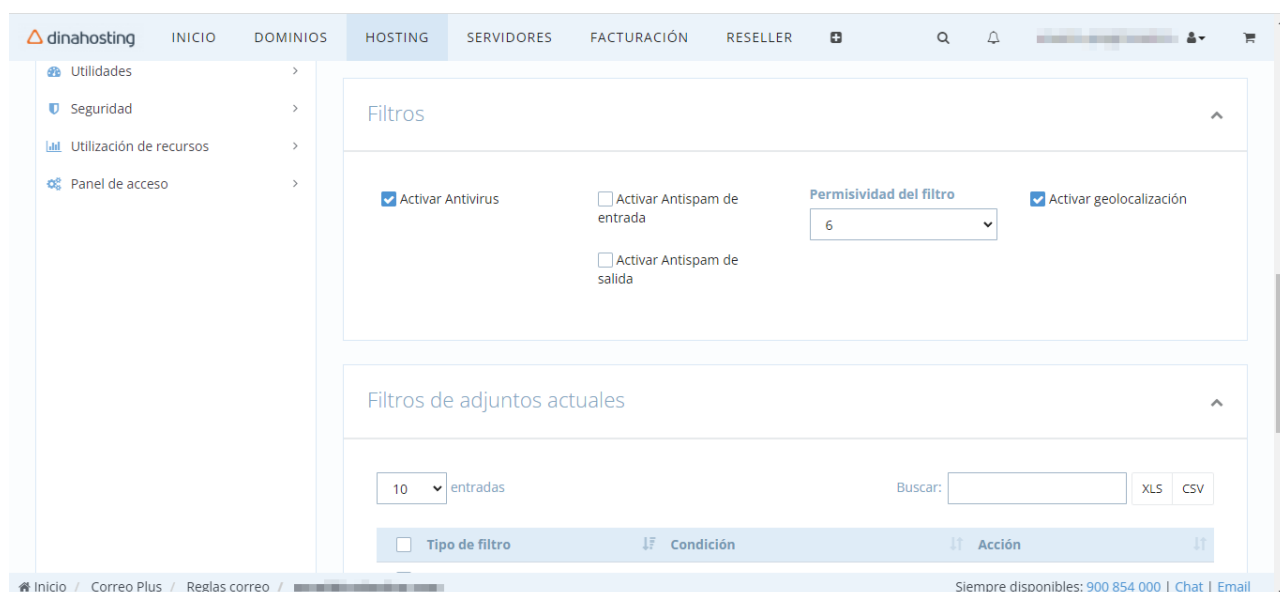
Reglas de correo

En el apartado de correo de dinahosting pueden crearse reglas para:

- **Contiene el texto:** nos ayuda a discriminar correos analizando la búsqueda de cadenas de texto.
- **Ha sido enviado desde la dirección o dominio:** tan pronto conozcamos que un remitente o dominio es fraudulento, podemos añadir una regla para que los correos que nos envíen no aparezcan en la bandeja de entrada.
- **Procede de un servidor de:** en internet cuando se sufren ataques de phishing, muchas veces informan sobre los datos del servidor. De esta manera podremos también discriminar mensajes que provengan de ese servidor.
- **Ha sido marcado como spam,** ha sido marcado como virus, ha sido marcado como posible suplantación de identidad: si por cualquier motivo se etiqueta un email de esta forma, podemos evitar que salga en nuestro correo de entrada.

Filtros de seguridad para tu correo

Podemos activar el antivirus en nuestro servidor de correo, de forma que escanee toda nuestra bandeja de entrada y salida y mejore la seguridad del correo electrónico. Además, podemos adaptar la permisividad del mismo, para evitar que posibles emails que sí nos interese recibir no los etiquete como spam. También es posible activar la geolocalización para saber de dónde proceden.



Filtros de correo

Existe dentro de nuestro Panel, la opción de escanear todos los archivos adjuntos para corroborar que no tengan virus, o directamente para denegar su recepción.

En dinahosting siempre estamos pendientes de tu seguridad, creando hostings seguros, haciendo backups de tus productos y cuidándote con herramientas que te faciliten la vida. En caso de que prefieras que alguien se encargue de parametrizar todas estas cosas, disponemos de un servicio [Auditoría de Seguridad](#), que analizará lo vulnerable que eres a ataques y configurará todo para protegerte al máximo.



CORREO PROFESIONAL CON TU PROPIO DOMINIO

*Personaliza tu dirección de email y
destaca tu marca*

*Webmail dinahosting: tu entorno
colaborativo*

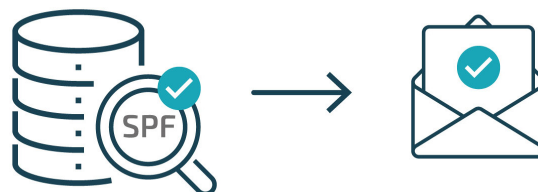


2.6 ¡QUE NO SUPLANTEN TU IDENTIDAD! ACTIVA EL REGISTRO SPF EN TU DOMINIO

Seguro que recibiste más de un correo de identidades sospechosas o claramente falsas. Para evitarlos existen medidas como el registro SPF, que comprueba que el servidor que envía el correo es ciertamente quien indica el dominio.

La suplantación de identidades (spoofing) y las técnicas como el phishing son de los fraudes más habituales que pueden llegar a nuestro buzón de correo.

Para protegernos de estas amenazas, además de ser cautelosos y de fijarnos en el contenido del correo, podemos comprobar el registro SPF.



¿Qué es el registro SPF?

El registro SPF o Sender Policy Framework es un protocolo de seguridad que **identifica los servidores de correos autorizados para enviar mensajes** desde un determinado dominio.

Es decir, con este registro **evitas que otras personas o máquinas envíen correos en tu nombre**.

Si realizas email marketing activar el registro SPF en tus comunicaciones es casi un requisito imprescindible para que tus correos lleguen a todos los destinatarios. Si utilizas un proveedor externo de correo, asegúrate de que cuenta con el registro SPF de sus IP para que tu correo no acabe en la carpeta de SPAM.

Autenticar los correos que envías dará un plus de confianza al destinatario que los reciba.

Ahora bien, es el servidor de la persona que los recibe el que comprueba si los dominios de los correos entrantes están autorizados, por lo que está en su mano poner las medidas para bloquear o realizar las acciones que considere con los que no lo estén.

¿Cómo lo activo en dinahosting?

En dinahosting, el registro SPF es una de las [zonas DNS que se activan por defecto](#) en tu dominio al dar de alta un hosting con cualquiera de nuestros [Planes](#).



Si quieres saber más
Mira el vídeo
¿Cómo creo un Registro
SPF en mi dominio?

Para crear un registro nuevo, puedes acceder desde tu Panel de Control al apartado Zonas DNS > Quiero hacer un... > Registro SPF. [Aquí](#) puedes consultar todos los registros DNS que puedes configurar en tu dominio dinahosting.

Frente a los ciberataques, toda protección es importante. **Activando en tu correo el registro SPF aportas mayor seguridad y confianza**, que nunca sobran, al destinatario que lo reciba.



2.7 ¿QUÉ SON LOS REGISTROS SPF, DKIM Y DMARC?

Los registros o protocolos de autenticación SPF, DKIM y DMARC nos pueden ayudar a evitar que se manden correos suplantando nuestra identidad, una actividad conocida como phishing. También sirven para dar más seguridad a los servidores de destino de nuestros correos y así evitar, dentro de lo posible, que sean marcados como SPAM.

A continuación te explicamos en qué consiste cada registro y te mostramos unos ejemplos de cada uno de ellos.

SPF

Como te adelantamos en el capítulo anterior, el Sender Policy Framework, o SPF, se encarga de certificar qué IP pueden mandar correo utilizando el dominio en cuestión. Este registro es eficaz contra los ataques de phishing. También ayuda a que los servidores de destino tengan más confianza y no cataloguen correos legítimos enviados por ti como SPAM.

Un ejemplo de SPF básico:

```
v=spf1 a mx ~all
```

Con la letra “a” indicamos que la IP del dominio está autorizada a enviar correos.

Con “mx” permitimos enviar correos desde las IP de los registros mx del dominio.

El carácter “~”, llamado softfail, indica que puede ser que alguna vez se mande correo desde otra IP no especificada. El correo se acepta, pero posiblemente como no deseado.

SPF con varias IPs:

```
v=spf1 a mx include:127.0.0.1 ~all
```

include: 127.0.0.1 Con esto autorizamos una IP para que pueda enviar correos bajo este dominio, en este caso la 127.0.0.1.

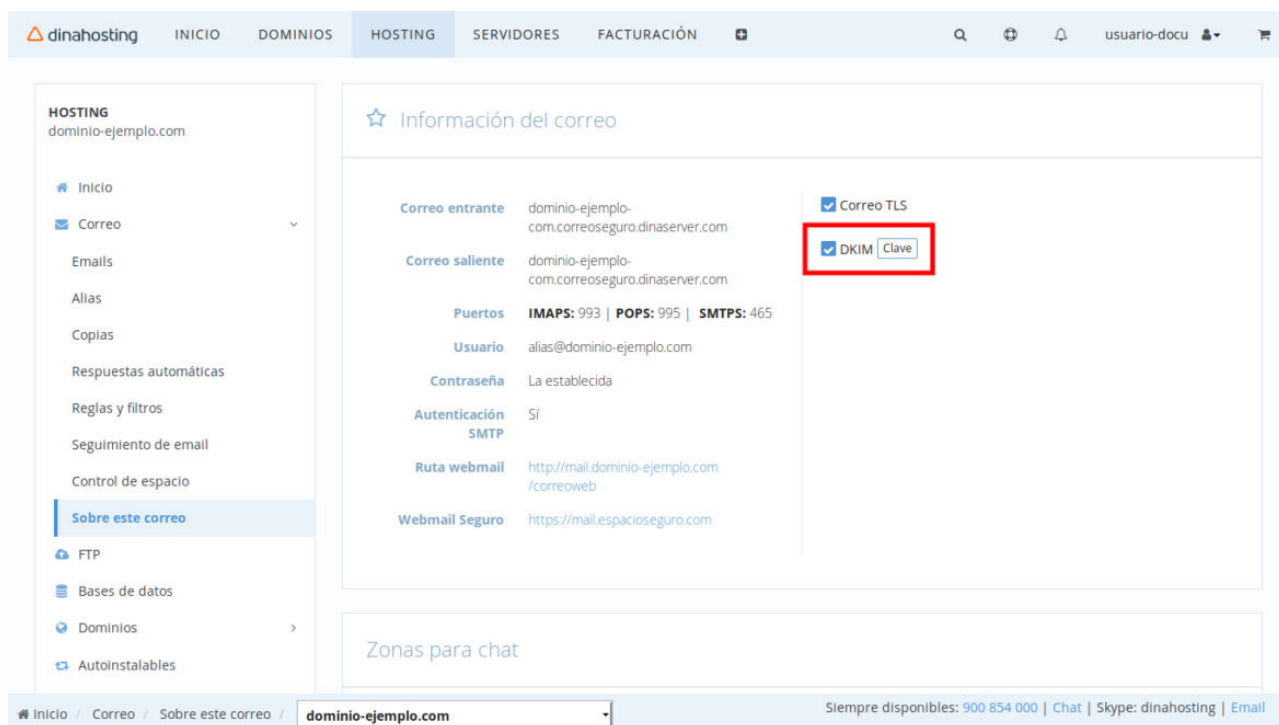
SPF para denegar todos los correos:

```
«v=spf1 -all»
```

“-” significa “fail”. Rechaza todos los correos de IP no indicadas en el registro. Al no indicar ningún valor, rechaza todos los correos.

DKIM

El *DomainKeys Identified Mail*, o DKIM, es un registro que permite firmar el correo con tu dominio mediante claves públicas indicadas en las zonas de tu dominio. De este modo, el destinatario está seguro de que el correo ha sido enviado desde tu servidor y no ha sido interceptado y/o reenviado desde otro servidor no autorizado.



Este registro se puede activar fácilmente desde el [Panel de Control](#). Solo tendrías que acceder al apartado Hosting > Correo > Sobre este correo y hacer clic en el checkbox de DKIM:

DMARC

El *Domain-based Message Authentication, Reporting and Conformance*, o DMARC, que complementa al SPF y DKIM. Este registro indica qué hacer cuando dan error los registros anteriores, para así poder tomar las medidas necesarias lo antes posible. Se crea como un registro TXT desde el apartado de zonas DNS, de la siguiente forma:

- Tipo TXT
- Host: _dmarc
- Ejemplo de cadena de texto:

```
v=DMARC1; p=quarantine; rua=mailto:info@dominio-ejemplo.com; ruf=mailto:info@dominio-ejemplo.com
```

Recuerda seleccionar Subdominio en el desplegable para poder agregar el host _dmarc

- **v=** es el nombre del registro. En este caso DMARC1.
- **p=** Indicamos qué quieres que se haga con nuestros correos. Podría ser: reject, quarantine o none.
- **reject:** rechaza todos los correos que no cumplen las comprobaciones del DMARC.
- **quarantine:** los correos que fallan se pondrán en cuarentena. Irán a la carpeta de correos no deseados/SPAM.
- **none:** se supervisan los resultados, sin tomar medidas para los mensajes que fallan.
- **rua/ruf=** referencia la forma en la que se solicita que se envíen los reportes de errores detectados.
- **rua:** se utiliza cuando necesitamos un reporte general.
- **ruf:** se emplea cuando queremos recibir los mensajes completos que fallan.

2.8 AUTENTICACIÓN EN DOS PASOS: QUÉ ES Y HERRAMIENTAS QUE NECESITAS PARA ACTIVARLA

Ante un posible ciberataque, correo de phishing, intento de acceso no autorizado... la autenticación o verificación en dos pasos o de doble factor es una técnica de seguridad imprescindible para proteger tu cuenta de usuario en un determinado servicio: correo electrónico, perfil de redes sociales, etc.



Si quieres saber más

Mira el vídeo

¿Qué es la verificación en dos pasos?

¿Tienes claro qué es y cómo puedes activarla? A continuación te explicamos en detalle en qué consiste y qué herramientas puedes utilizar para proteger tu presencia digital.

¿Qué es la autenticación en 2 pasos?

La autenticación en dos pasos añade una segunda capa de seguridad o de verificación para que solo tú puedas acceder a tu cuenta de usuario de un determinado servicio.

Su funcionamiento es muy sencillo, puesto que se basa en algo que ya sabes y en algo que ya tienes:

- **Lo que sabes:** tu contraseña.
- **Lo que tienes:** un número de 6 dígitos generado automáticamente cada 30 segundos desde una aplicación móvil, como Google Authenticator y Authy, de las que te hablamos más abajo.

Sin esta combinación de ambos elementos no podrás acceder a tu cuenta en una determinada plataforma, por ejemplo, el [Panel de Control de dinahosting](#) o el [servicio de webmail](#). Ya ves que a menos que te hayan robado el móvil, tus accesos estarán mucho más seguros.

La ciberseguridad cobra cada vez un papel más importante en Internet. Muchos usuarios usan **contraseñas poco seguras y fáciles de descifrar**, por lo que es habitual que existan filtraciones. Por eso, la autenticación en dos pasos es una manera de comprobar que quien efectivamente está intentando acceder al servicio eres tú, y no alguien que se ha adueñado de tus claves. [Aquí](#) te dejamos unos cuantos trucos para crear contraseñas robustas.

El único inconveniente que tiene este sistema de autenticación es que vas a tardar unos segundos más en acceder a tu aplicación. También es cierto que puede resultar incómodo tener que depender de tu móvil, pero a la larga lo agradecerás.

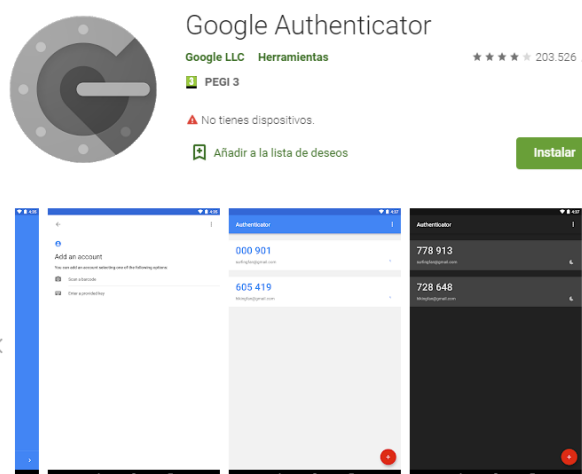
Herramientas de autenticación: Google Authenticator y Authy

Ahora que ya sabes lo importante que es tener activada la autenticación en dos pasos para proteger tus cuentas de los ciberdelincuentes, te hablamos de un par de servicios gratuitos desde los que generar los códigos de seguridad para verificar tu identidad.

Google Authenticator

Como su nombre indica, [Google Authenticator](#) es una aplicación desarrollada por Google y disponible tanto para Android como para iOS. Es muy fácil de utilizar:

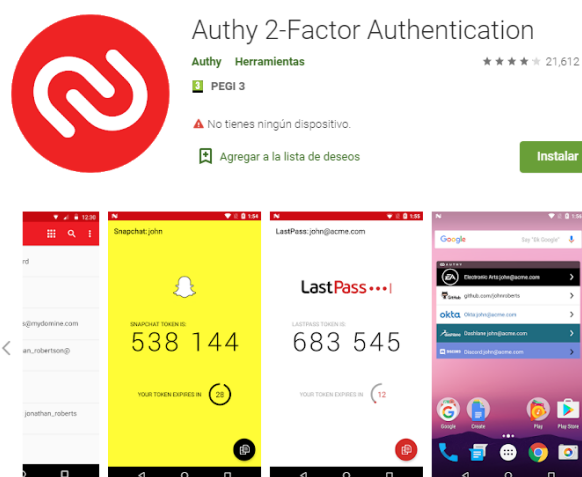
1. Instala la APP en tu móvil.
2. Activa la autenticación en dos pasos en tu cuenta de usuario de una determinada plataforma y localiza el código QR que incluye toda la información de la cuenta y su configuración.
3. Configura en Google Authenticator la cuenta del servicio que quieres proteger, escaneando el código QR del que te hablamos en el punto anterior.
4. Inicia sesión en tu cuenta con tu usuario y contraseña e introduce el código numérico que se muestra en Google Authenticator.



Authy

Es otra de las herramientas para la autenticación en dos pasos más populares. Para utilizarla sigue los mismos pasos que te planteábamos para Google Authenticator: escaneas el código QR de la cuenta e introduces el código de dígitos que te proporciona [Authy](#), y listo.

1. Instala Authy en tu smartphone.
2. Activa la verificación en dos pasos en los servicios que te interesen.
3. Una vez obtengas el código QR correspondiente, ve a Authy y añade una cuenta para el servicio que vas a proteger.
4. Inicia sesión en las cuentas de usuarios configuradas con tu usuario y contraseña e introduce a mayores el código que Authy generará por ti.



Existen otras aplicaciones de este estilo, como [LastPass Authenticator](#) o [Microsoft Authenticator](#) que pueden funcionar igual de bien.

También hay **otras formas autenticación** que seguro que te suenan. Por ejemplo, las entidades bancarias suelen trabajar mucho con el SMS: recibes el código por mensaje y lo introduces en la aplicación que sea para iniciar sesión.

Lo mismo ocurre con el email. Hay muchas redes sociales que te piden que accedas a tu correo para confirmar tu identidad cuando te estás logueando. Quizá este método sea el menos seguro, puesto que es mucho más probable que alguien se haya hecho con tu contraseña de correo que con tu teléfono móvil.

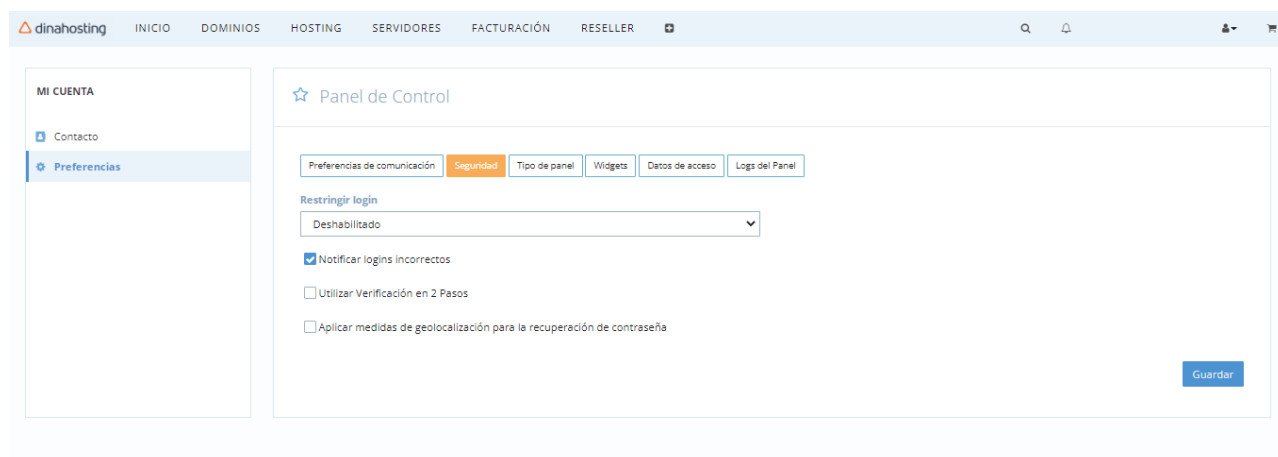
Autenticación en dos pasos en tus servicios en dinahosting

Si no lo has hecho todavía, es importante que actives la autenticación en dos pasos en los servicios que utilizas a menudo en dinahosting. Aquí te explicamos:

Cómo activar la Verificación en dos pasos en tu Panel

Primero, instala Authy u otra aplicación similar en tu smartphone.

Luego, accede a Mi Cuenta, arriba a la derecha > Preferencias > Seguridad en tu Panel de Control. Una vez allí podrás configurar tu protocolo personalizado de seguridad y, entre otras cosas, activar la 2-Step Verification. Por defecto te aparecerá desmarcada, tal y como ves a continuación. Selecciónala.



A continuación agrega tu acceso al Panel a Authy, escaneando el código QR con la APP o ingresando manualmente la llave. No te olvides de comprobar su correcta activación después.

Y listo! Ya tienes la Verificación en 2 Pasos activada. A partir de este momento, **cuando vayas a acceder a tu cuenta se te pedirá —además de tu contraseña habitual— el código de 6 dígitos generado en tu APP para ese preciso momento. ¡Seguridad doble!**

Configura tu propio protocolo de seguridad

La Verificación en 2 Pasos es solo una de las opciones del “mix” con el que puedes conformar tu propio sistema de seguridad. En dinahosting también te ofrecemos:

- **Restringir login por continente, país o IP:** para evitar accesos maliciosos a tu cuenta desde una IP o zona geográfica determinada.
- **Notificar logins incorrectos:** recibirás un correo cada vez que se produzca un login erróneo con tu usuario. Esto te permite detectar si hay alguien intentando entrar en tu cuenta.
- **Aplicar medidas de geolocalización para la recuperación de contraseña:** para eliminar la posibilidad de recuperar contraseña si te encuentras en alguna de las áreas geográficas a las que has restringido el login.



¡Y un último apunte! Cuando una nueva cuenta se activa, se proporciona también una contraseña de un solo uso que te permitirá acceder a tu Panel de Control en caso de que hayas perdido el móvil. **Imprímela o guárdala en un lugar seguro.**

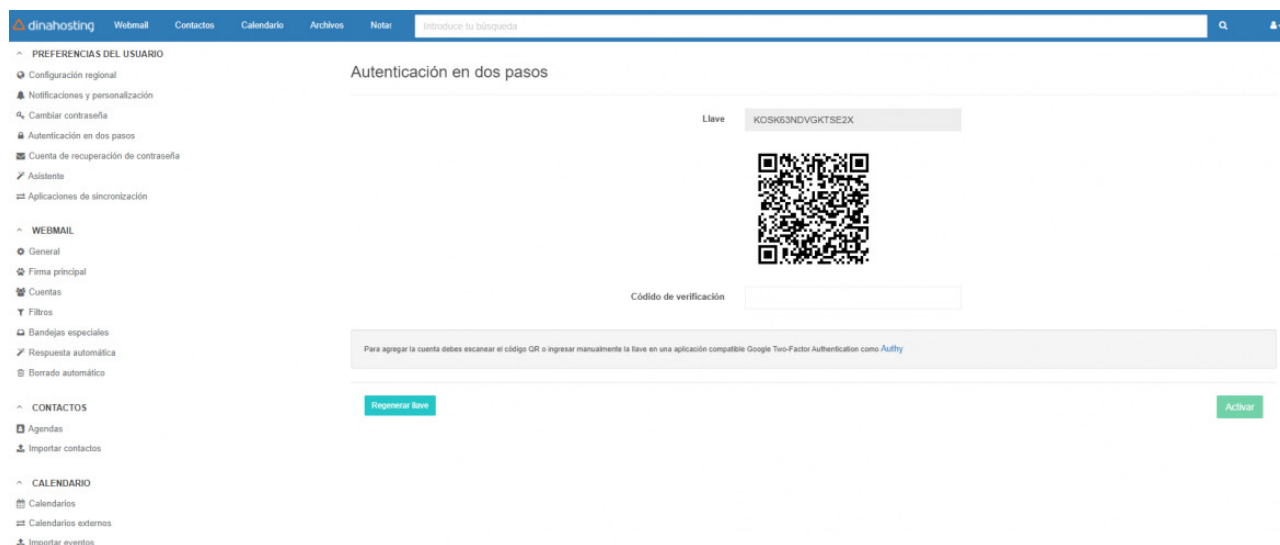
Cómo activar la Verificación en dos pasos en el webmail

Te explicamos paso a paso cómo poner a funcionar la autenticación en dos pasos en tu Webmail:

Primero, instala Authy u otra aplicación similar en tu smartphone.

Luego, accede a tu Webmail en dinahosting, y una vez en él a Configuración > Preferencias del usuario > Autenticación en dos pasos.

A continuación agrega tu cuenta de Webmail a Authy, escaneando el código QR con la APP o ingresando manualmente la llave. Luego haz clic en Activar.



Finalmente, cuando entres a tu Webmail de nuevo, además de tu usuario y contraseña tendrás que añadir el código generado automáticamente por Authy para completar el login.

De esta manera evitas cualquier tipo de login sospechoso, como un intento de iniciar sesión desde una ubicación o un dispositivo distinto de los habituales.

Una vez tengas la autenticación en 2 pasos activada, puedes desactivarla en cualquier momento siguiendo los mismos pasos (Configuración > Preferencias del usuario > Autenticación en dos pasos) y haciendo clic en Desactivar.

Recuerda que también puedes **activar la autenticación en tus redes sociales** (Twitter, Facebook, Instagram...), en tu cuenta de Google, en tu cuenta de Amazon... A día de hoy, la mayoría de sitios web en los que tienes que iniciar sesión disponen de esta opción. La encontrarás en el apartado de seguridad que hay en las opciones de configuración.

Es un procedimiento súper sencillo y que te permitirá respirar mucho más tranquilo. ¡No esperes más!

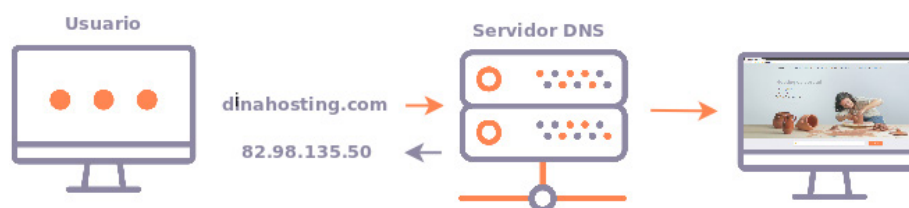
2.9

¿QUÉ ES Y PARA QUÉ SIRVE FIREWALL DNS?

El sistema DNS es uno de los componentes en los que se basa el funcionamiento de Internet. Sin él, no existiría tal y como lo conocemos hoy en día. Sus siglas se corresponden con **Domain Name System (Sistema de Nombres de Dominio)**.

Cuando un ordenador está conectado a Internet se le asigna una dirección IP, que es algo así como un número de teléfono que cada dispositivo tiene asociado a la red, para que puedan conectarse unos con otros. Tienen el siguiente formato: 82.98.135.78.

Cuando accedemos a una página web, dinahosting.com por ejemplo, realmente nos estamos conectando a su dirección IP 82.98.135.50. El sistema DNS **es el encargado de traducir los nombres de dominio a estas direcciones IP**.



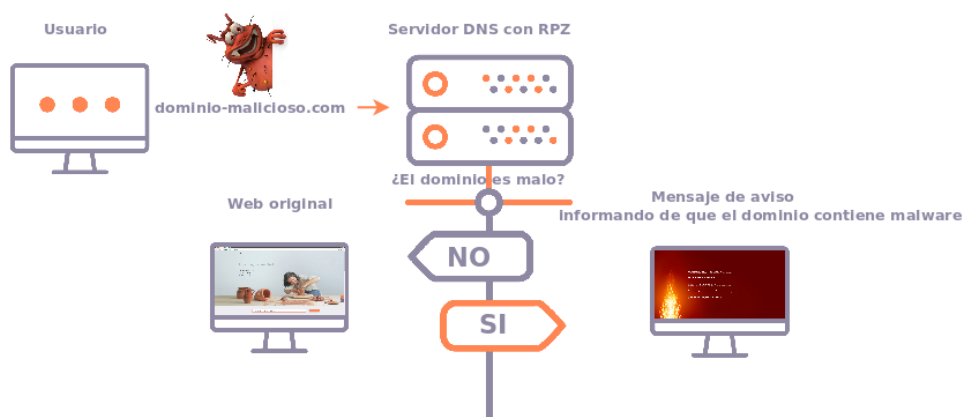
Este sistema se gestó porque **es mucho más sencillo recordar nombres de dominios que direcciones numéricas**.

Las ventajas de la protección de Firewall DNS

Un **DNS recursivo** con una configuración estándar responde con la IP que tiene asociada, sin hacer ninguna comprobación adicional. **En un servidor con Firewall DNS**, técnicamente llamado RPZ (Response Policy Zone), **se comprueba que el dominio que intentamos resolver no sea un “dominio malo”**. Esto se hace mediante listados de dominios que tuvieron actividad maliciosa en el pasado, es decir, que alojaron virus, páginas de phishing y otro malware.

También hay otros métodos más avanzados para saber si el dominio es peligroso. Cuando un usuario intenta acceder a uno de ellos usando un DNS con RPZ, **el servidor le puede responder con un NXDOMAIN (dominio no existente), o redirigiéndolo a otra página** para informarlo de que está intentando acceder a un dominio malicioso.

Con esta protección evitamos, por ejemplo, que si un virus te llega por correo en el enlace “http://dominiomalo.com”, no pueda acceder a esta dirección y así no se introduzca directamente en tu PC.

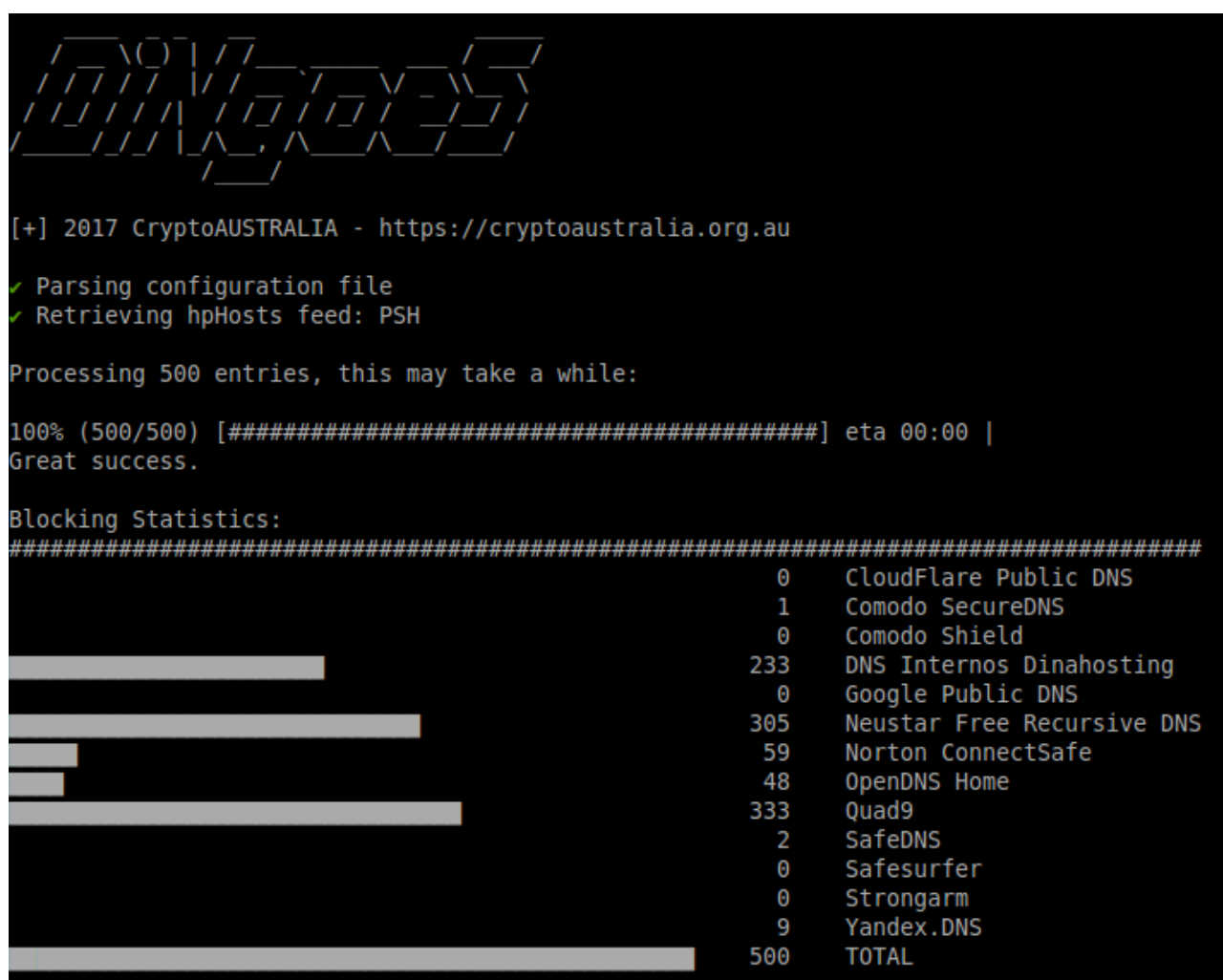


¿Qué hacemos en dinahosting?

En nuestros DNS recursivos internos contamos con esta protección de Firewall DNS. **Estos DNS son los usados por todos los servicios Administrados y por muchos de los No Administrados.**

Para comprobar la efectividad de nuestro Firewall DNS hicimos una **comparativa con otros proveedores** que ofrecen este servicio de manera abierta.

Hemos utilizado [esta herramienta](#). Primero, esta descarga una lista de dominios conocidos por su actividad maliciosa. A continuación, intenta resolver cada dominio con cada proveedor de DNS y almacena si se produjo un bloqueo o no. Finalmente, genera un informe con los resultados obtenidos.



Como puedes comprobar, nuestros DNS internos quedan en el tercer puesto, con **233 bloqueos en 500 peticiones**, justo por debajo de los DNS de IBM y Neustar.

2.10

¿ALOJAMIENTO WEB EN ESPAÑA O EN ESTADOS UNIDOS?

La ubicación es crucial a la hora de elegir un buen hosting. Te contamos los pros y contras de elegir alojamiento web en España o en Estados Unidos.

Si estás creando tu web y te toca buscar hosting seguramente ya te hayas topado con muchas opciones tentadoras de diferentes países.

El mercado del hosting es un sector muy globalizado, ya que al tratarse de un servicio online es relativamente sencillo ofrecer tus productos desde cualquier parte del mundo.

Es especialmente en EE. UU. donde este mercado es más competitivo, dado que allí se encuentran las mayores proveedoras.

Antes de decidir dónde dar de alta tu hosting te recomendamos que tengas en cuenta los siguientes factores.

Factores a tener en cuenta para elegir hosting en España o en EE. UU.

Precio

La competencia entre las grandes compañías de hosting estadounidenses hace que los precios sean en general más económicos del otro lado del charco.

O por lo menos esa era la percepción hasta ahora. Si comparas y echas un vistazo a distintas proveedoras, verás que la diferencia es de apenas unos céntimos. [Mira los descuentos que tenemos](#) y verás que **el hosting español de calidad también está a buen precio.**

IP geolocalizada

Como ya te contamos [en el siguiente post](#), tener tu IP localizada en el país donde vas a vender tus productos es muy recomendable para tu web.

Por un lado, **ganas en velocidad de respuesta**, ya que al estar en tu mismo país se elimina la latencia derivada de conectarse con el extranjero.

Y por otro lado, **mejoras el posicionamiento de tu web en Google**. La ubicación es un factor clave para optimizar tu SEO y escalar posiciones en las búsquedas locales.

Elige mejor un hosting en España si tu público está en el mercado español.

Protección de datos

Para que aplique la normativa europea en protección de datos **el servidor que aloja los datos debe estar ubicado dentro de la Unión Europea** o en un país autorizado. Estados Unidos no está entre estos países autorizados.

Esto no quiere decir que en EE. UU. tus datos vayan a quedar desprotegidos. Si no que al tener tus datos allí tendrías que aplicar una normativa diferente y que, obviamente, esta no tendría las garantías que se presuponen dentro de la normativa de la Unión Europea.

Trato cercano y en tu idioma

Sobre todo cuando algo falla, quieres una respuesta lo antes posible y sin complicaciones. **Es por eso que contar con un equipo de personas que te entiendan en tu idioma es tan importante.**

También los horarios pueden afectar a los tiempos de respuesta a la hora de gestionar algo en tu web. Por eso, mucho ojo a las diferencias horarias con el extranjero.

En dinahosting eso no será un problema, [te atendemos durante las 24 horas](#), todos los días del año y en tu idioma ;)



VENTAJAS DE TENER TU HOSTING CON IP ESPAÑOLA

1

MEJOR POSICIONAMIENTO SEO

Si tu web se orienta al mercado nacional, disponer de IP española te ayudará a escalar posiciones en las búsquedas locales, ya que Google y otros buscadores priorizan las páginas alojadas en el mismo país.



2

MAYOR VELOCIDAD EN TU WEB

Nuestros servidores están en España. Cuanto más cerca esté el servidor, menores serán los tiempos de latencia y tu web se cargará mucho más rápido. Una mayor velocidad repercutirá en una mejor experiencia de usuario.



3

CUMPLIMOS CON EL RGDP

Nuestra infraestructura cumple con la normativa europea en protección de datos. Nos aseguramos de que tu información y la de tus clientes esté totalmente protegida, por lo que ganas en seguridad y confianza.



4

SOPORTE TÉCNICO 24/7 EN TU IDIOMA

En dinahosting hablamos tu idioma y no utilizamos contestadores automáticos para atenderte. Trabajamos en tu mismo horario, por lo que te resultará más sencillo programar tareas o realizar el mantenimiento de tu web.



Si lo prefieres
**Mira el vídeo
online**

GUÍA DE CIBERSEGURIDAD

3. Seguridad en WordPress

[3.1. Seguridad para tu WordPress: primeros pasos](#)

[3.2. Cómo securizar tu WordPress: buenas prácticas y algunos plugins](#)

[3.3. Cómo recuperar tu contraseña en WordPress](#)

[3.4. 6 Plugins de seguridad en WordPress](#)

[3.5. Plugins de protección de datos en tu tienda en WooCommerce](#)

[3.6. Proteger tu WordPress mediante .HTACCESS: 5 consejos](#)

[3.7. Qué son wp-admin y wp-login.php de WordPress](#)

[3.8. Cómo añadir Google reCAPTCHA a tu WordPress](#)





3.1 SEGURIDAD PARA TU WORDPRESS: PRIMEROS PASOS

Seguro que una de tus principales preocupaciones a día de hoy si tienes una [página web en WordPress](#) es su seguridad. Protegerla contra ataques y malware es algo de lo que debes estar muy pendiente.

Ejemplos de ataques contra la seguridad de tu web

Existen muchos tipos de ataques que puede sufrir tu web en WordPress, entre los que podríamos mencionar:

- **Puertas traseras:** como su propio nombre indica, los malos no intentan acceder a tu WordPress desde tu página de login, sino que se buscan formas para llegar a ella por otros métodos.
- **Fuerza bruta:** en este caso el significado no es tan literal, no van a ir con un mazo a donde se encuentre tu página. Los ataques de fuerza bruta son ataques por repetición. Introducen miles de contraseñas mediante un bot, hasta que da con la contraseña adecuada.
- **Cross-Site Scripting:** es una de las razones por las cuales siempre tienes que instalar plugins y temas de WordPress desde su página oficial. Si no es así, puede que estés ejecutando en tu web un código que en gran parte de los casos comparte las cookies de información de tus usuarios.
- **DoS:** consiste en inundar de peticiones (como por ejemplo, en el login) hasta lograr colapsar el servidor y que tu web se caiga. Aunque en este caso el principal objetivo es hacer caer tu web, es muy importante protegerte en la medida de lo posible, para que no pierdas posibles ganancias.

En este capítulo hablaremos sobre los primeros pasos a seguir para mejorar la seguridad de tu sitio web en WordPress, sin perder de vista cómo pueden afectar a su rendimiento las modificaciones que realices.

¿Plugins sí o plugins no?

Si no tienes conocimientos en desarrollo seguramente utilices [plugins para solventar muchos problemas de tu web](#), pero debes saber que estos consumen recursos de tu servidor y pueden derivar en que tu web vaya más lenta.

En la medida de lo posible, es importante **medir muy bien la capacidad de respuesta y el uso que le vas a dar a cada plugin**. ¿Es realmente necesario? ¿Ralentiza mucho mi web? A veces nos obcecamos e instalamos plugins de manera indiscriminada, cuando no son realmente necesarios.

Por ello, te aconsejamos que antes de instalar cualquier plugin valores sus pros y contras, haciendo una pequeña auditoría:

- Revisa las valoraciones de los usuarios en la propia página del plugin.
- Busca reviews externas sobre el plugin en blogs especializados.
- Instálalo y mide la respuesta de tu web con y sin el plugin (puedes ayudarte de [Google PageSpeed](#)).

Y cuando lo tengas todo claro, ¡adelante con el plugin para mejorar la seguridad de tu WordPress!

Configuraciones básicas de seguridad en WordPress

1. Revisa las actualizaciones

Los hackers siempre están estudiando formas de piratear webs y entrar en la administración de tu sitio. Por eso, lo que hoy es completamente seguro, mañana quizás no lo sea. Es muy importante que mantengas tu sitio al día (temas, plugins, core del propio WordPress...) pero sin olvidarte de que las actualizaciones requieren de un tiempo de testeo para averiguar si son realmente efectivas y seguras.

Nuestro consejo: mantén tu sitio actualizado pero sin estar siempre en la cresta de la ola, así te evitarás muchos quebraderos de cabeza.

2. Mejora el acceso y la autenticación

Aún siendo un CMS cuyo acceso requiere autenticación, WordPress no está al margen de ataques externos. Intenta ponérselo difícil a los intrusos siguiendo estos consejos:

URL de acceso

Evita que tu URL de acceso sea nombredetusitio.com/wp-admin, pues un simple bot podría generar contraseñas aleatorias hasta dar con la tuya. Con la ayuda de WPS Hide Login podrás personalizar la URL a tu manera.

Doble autenticación

Si eres lector habitual de nuestro blog ya sabrás de lo que hablo. La [autenticación en dos pasos](#) es una barrera más de seguridad en el login. Puedes seguir estas instrucciones [para implementarla en WordPress](#) o ayudarte del plugin [Duo Two-Factor Authentication](#).

3. Añade un firewall

Un firewall o cortafuegos sirve para filtrar el tráfico hacia nuestra web, lo que permitirá **evitar ataques recurrentes desde un mismo dispositivo o IP**.

Si buscamos un plugin para implementar una regla de firewall en WordPress, podemos hacerlo con [Ninja Firewall](#). Es uno de los más usados, ya que es muy ligero y realizan actualizaciones constantemente sobre él.

4. Evita el SPAM

Además de ser muy molesto, el SPAM es un consumidor de espacio y recursos de tu alojamiento. Lo primero es intentar mantener tu WordPress limpio de comentarios de SPAM y publicitarios no deseados.

Si tu página tiene pocas visitas, es sencillo gestionar los mensajes y comentarios de SPAM. Sin embargo, **en sitios con muchos usuarios o visitas esto ya comienza a ser una tarea más laboriosa**. Para ayudarnos está el archiconocido plugin [Akismet](#), pero si te apetece probar algo más alternativo te recomendamos [Spam protection](#), que ya viene con normas de firewall. ¡Dos en uno!

Me han hackeado. ¿Qué hago?

Si aún siguiendo todas las recomendaciones han conseguido vulnerar la seguridad de tu WordPress, una opción es acceder a un backup o copia de seguridad de tu base de datos desde el [Panel de Control](#). Así podrás recuperar una versión anterior de la web en la que no haya todavía errores.

Siempre es mejor que optes por un [hosting seguro](#) para evitar males mayores. Si aun así has tenido problemas con tu web, recuerda que en dinahosting ofrecemos además un servicio de [Asesoría técnica](#), que incluye **servicio de desinfección y reportes de seguridad gratis**.



3.2 CÓMO SECURIZAR TU WORDPRESS: BUENAS PRÁCTICAS Y ALGUNOS PLUGINS

Te presentamos algunas ideas de lo más efectivas para **securizar tu WordPress**. La seguridad es un requisito obligatorio para cualquier web, desde un simple blog a un gran portal. **WordPress por sí solo ya es un sistema con directrices de seguridad en su núcleo**, sin embargo, hay más cosas que podemos (y debemos) hacer para ampliar ese alcance e impedir eventuales dolores de cabeza.

Mantener tu WordPress bien seguro es mucho más fácil de lo que te pueda parecer. Presta atención porque en unos minutos tendrás tu WordPress preparado para (casi) todo lo que venga.

Actualizaciones de WordPress, plugins y temas

WordPress se actualiza constantemente. Esto significa que se corrigen errores y se añaden recursos. Muchas de las correcciones pueden estar relacionadas con problemas de seguridad, por lo tanto, mantén siempre tu instalación actualizada.

Tampoco te olvides de mantener tus temas y plugins en su última versión. **Es muy recomendable que actives las actualizaciones automáticas**, que aparecerán en tu área administrativa de WordPress ;)

Otra de las causas para que las webs sean atacadas es la “basura”. **Borrar los plugins y temas que no uses** es una muy buena forma de securizar tu WordPress, dejando solo el contenido necesario para que funcione tu web.

Define los privilegios de las personas usuarias

Crea un perfil para la administración de tu web y utilízalo solo cuando necesites hacer tareas de mantenimiento. Recuerda que en muchos blogs con WordPress este perfil es “Admin”. **Lo recomendable es crear un nuevo perfil con otro nombre y darle permisos de administración** para evitar ataques de fuerza bruta. Después inicia tu sesión con el nuevo perfil y borra el antiguo “Admin”.

Para escribir, utiliza un perfil con permisos de “Editor”, tendrás acceso a todas las funciones de edición, creación y exclusión de artículos pero sin acceso a las herramientas administrativas.

Si quieres mayor seguridad puedes crear un **perfil “Autor”**, para personas que colaboren en tu web. Así, solo tú podrás alterar, editar o excluir tus artículos.

Securizar tu WordPress con una contraseña segura

Para hacer que tu web sea segura, lo recomendable es **que tu contraseña sea fuerte**, con dos o más palabras, números y caracteres especiales. Por ejemplo: Dcs@rÑH37. [En este capítulo](#) te contábamos algunos tips para que tu contraseña sea más segura.

Refuerza la seguridad de la zona de login

Instala algún sistema de bloqueo temporal de login para intentos de acceso fallidos. Un plugin [“Limitador de intentos de login”](#) te dará buen resultado.

Utilizar captcha en el área de login es una buena manera de securizar tu WordPress. El objetivo del captcha es que el sistema sepa distinguir a una máquina de un ser humano, y de este modo impedir que los robots accedan, por eso previenen estupendamente de los ataques de fuerza bruta, porque siempre están hechos por bots. Uno como el que provee el plugin [Captcha](#) es válido y no tienes ni que configurarlo.

Los captcha también previenen de comentarios automáticos como SPAM. **Ten en cuenta que los captchas visuales dificultan la accesibilidad** a personas con dificultades visuales así que evita en lo posible su uso. «La Web no solo conecta máquinas, conecta personas», recuerda. Akismet es un muy buen plugin para evitar el SPAM en los comentarios de tu blog.

Si tienes una IP que no cambia, puedes **restringir el acceso al área de administración desde IP determinadas**. Haciendo esto conseguirás que solamente tú puedas acceder al área de administración. Actívalo desde el [Panel de Control](#) accediendo desde Hosting > Seguridad > Protección de carpetas.

También podrás **proteger con doble contraseña el login del WordPress**. Cuando accedes al área de administración de tu WordPress, nos pedirá el usuario y clave. Para aumentar la seguridad establece otra contraseña a nivel directorio wp-admin.

Otra buena opción es **restringir archivos tipo wp-uploads para evitar hackeos**. Para ello debes crear un archivo .htaccess dentro de la carpeta wp-content para establecer las reglas de acceso, añadiendo simplemente este código:

```
Order deny,allow
Deny from all
<Files ~ “.(xml|css|js|jpe?g|png|gif|pdf|docx|rtf|odf|zip|rar)$”>
Allow from all
</Files>
```

Plugins WordPress que pueden ayudarte con la seguridad

Te comentamos algunos plugins que pueden ayudarte a proteger tu web:

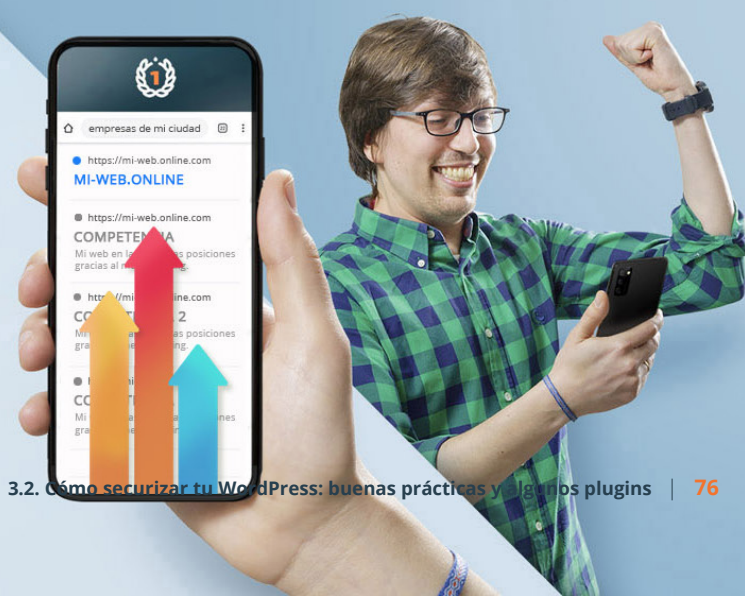
- [Wordfence Security](#): uno de los mejores plugins para la seguridad de WordPress. Incluye un servidor de seguridad, escaner anti-virus, sistema de autenticación en dos pasos mediante token (móvil), análisis de enlaces maliciosos y tráfico en tiempo real incluyendo rastreadores.
- [Security Audit Log](#): este plugin genera un informe de todas las actividades de tu web, desde registros de personas usuarias, intentos de login y actualizaciones, las configuraciones modificadas o nuevos post publicados.
- [WP Security Scan](#): detecta vulnerabilidades en tu instalación y realiza el cambio de prefijo de la base de datos automáticamente.
- [Clef](#): un plugin de verificación en dos pasos, que tras la instalación de una simple app te permite loguearte en tus webs desde tu smartphone.

Cuida tu web, ¡vale más prevenir que remediar!

Si quieres una web con WordPress en dinahosting te ofrecemos [alojamiento 100 % compatible](#) donde puedes crear tu sitio en un clic. Echa un vistazo a nuestro [Hosting App](#), para crear una página sencilla o decídate por un [Hosting Profesional](#), si necesitas programación. **Todos nuestros planes administrados te permiten crear planes específicos de WordPress.**

POSICIONA TU WEB CON UN **HOSTING DE MÁXIMO RENDIMIENTO**

*Ahora al 60 % y con más espacio gratis
Garantía de reembolso: 30 días
Pruébalo gratis y paga al publicar tu web*



3.3

CÓMO RECUPERAR TU CONTRASEÑA EN WORDPRESS

Te mostramos algunas opciones para recuperar la contraseña de tu página web en WordPress de la manera más sencilla.

Hoy en día manejamos tantas contraseñas que es muy fácil que olvidemos alguna de vez en cuando. También puede darse el caso de que hayas arrancado el proyecto de un amigo o seas el webmaster de un cliente y este te pida ayuda porque no recuerda sus claves. ¿A qué te ha pasado más de una vez?



Si lo prefieres
Mira el vídeo
Cómo recuperar tu
contraseña en WordPress

Primera opción: Llamar a Soporte

Si la informática no es tu fuerte, o tienes miedo de hacer algún estrepicio, casi mejor dejarlo en manos de los profesionales. Recuerda que en dinahosting tenemos [servicio de Soporte 24/7](#) y estaremos encantados de ayudarte con cualquier duda que te surja durante el proceso. Llámanos o escríbenos un chat y solucionaremos tu incidencia lo antes posible.

Segunda opción: Recuperar tu contraseña en WordPress

Sí, tienes razón. Es algo obvio y seguramente ya lo has probado... pero es necesario enumerarlo. En WordPress, como en muchos otros sistemas de registro, te dan la opción de crear una nueva contraseña. Para ello **es necesario que recuerdes, al menos, tu email de usuario**.

Los pasos a seguir son muy sencillos. En el panel de acceso, normalmente [www.nombredetuweb.com/wp-admin](#), encontrarás un enlace con la leyenda *¿Has olvidado tu contraseña?*





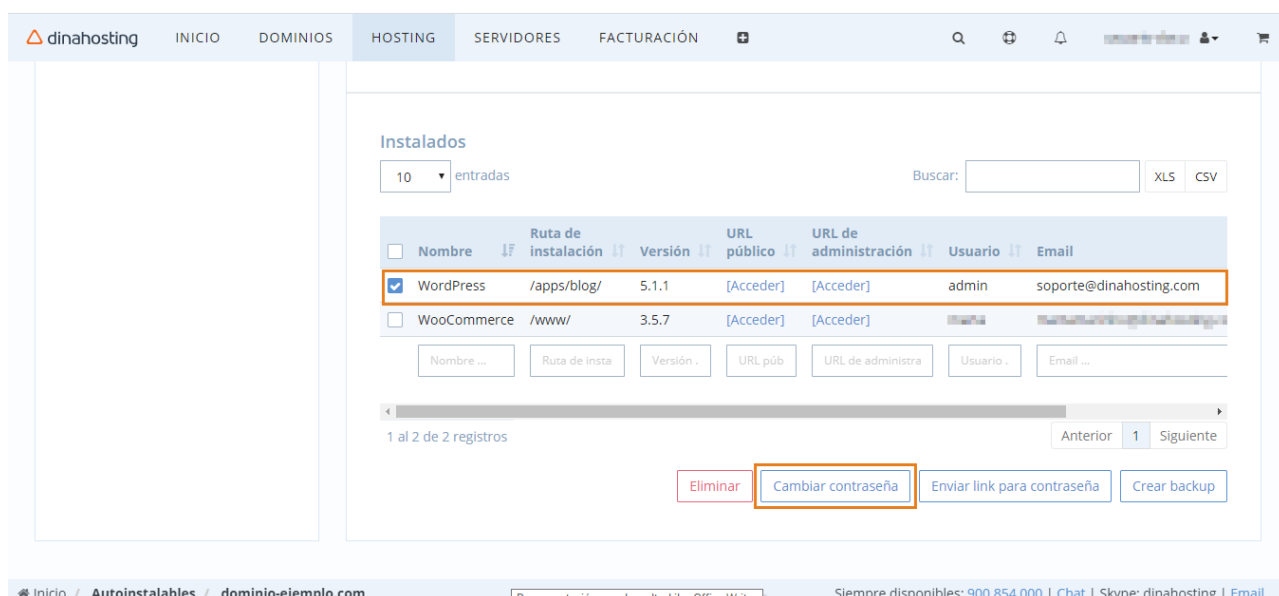
Si haces clic te redireccionará a otra ventana donde introducir tu email de usuario y generar una nueva contraseña.

Solo te queda seguir los pasos que se te han enviado a tu correo electrónico y ya podrás recuperar tu contraseña de WordPress.

Tercera opción: Desde nuestro Panel de Control

En dinahosting sabemos que lo de olvidar usuario y contraseña es algo muy común, por ello te ofrecemos una opción de recuperación súper directa. Pasos a seguir:

1. Entra a tu [Panel de Control](#), al apartado Hosting de tu Hosting WordPress.
2. Luego ve a Autoinstalables > Autoinstalables instalados. Ahí tienes un botón para cambiar la contraseña.



En un par de clics contraseña cambiada. ¡Ventajas de ser de dinahosting!

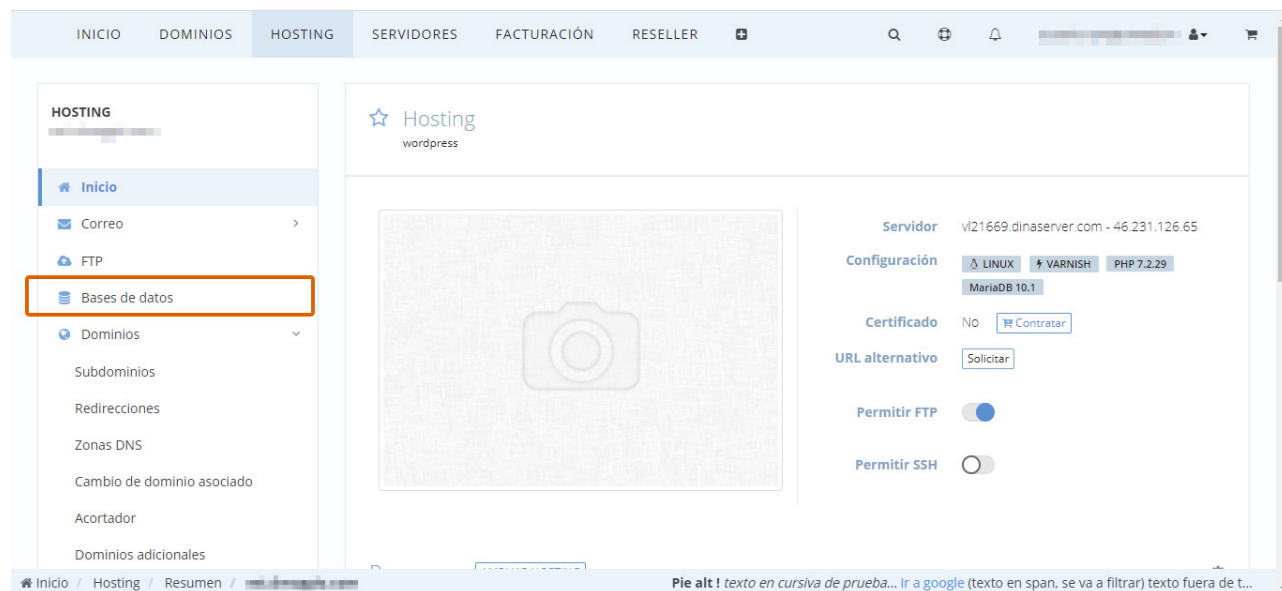
Cuarta opción: Desde tu base de datos

Si has llegado hasta aquí es seguramente porque ninguna de las opciones anteriores te han funcionado. Posiblemente sea porque aún no eres cliente de dinahosting.

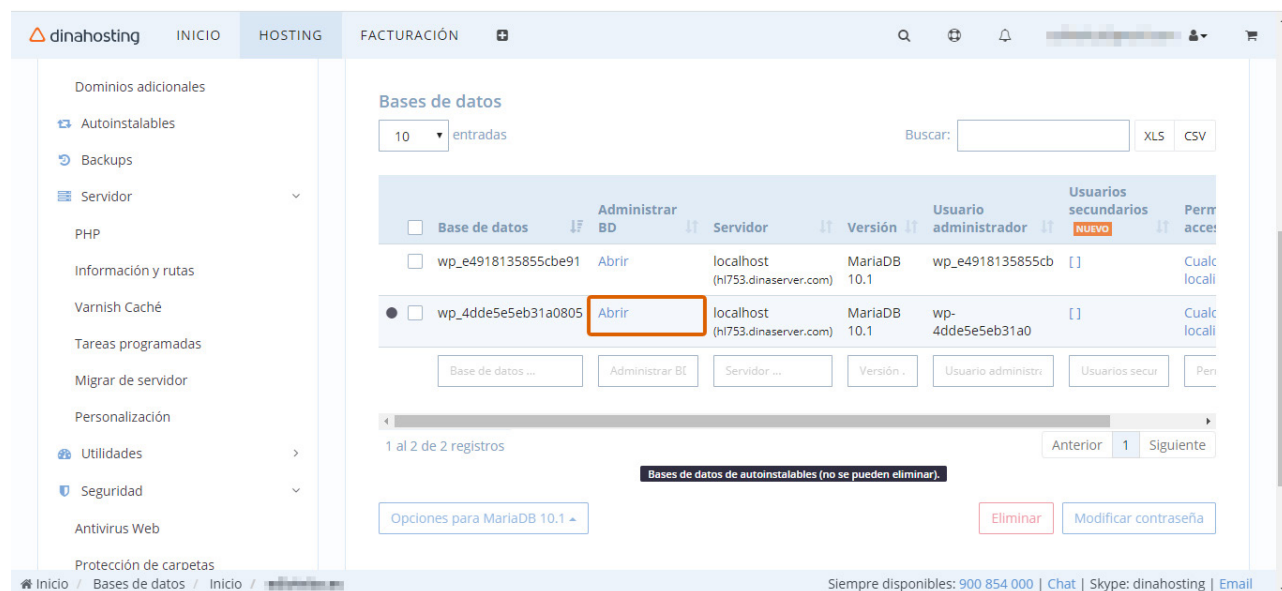
Esta opción requiere unos conocimientos un poco más avanzados, por lo que si te sientes inseguro o tienes miedo a cargarte algo, mejor vuelve a revisar la primera opción.

A continuación realizaré los pasos a seguir en nuestro panel de control. Si no somos tu compañía de hosting, seguramente tendrás unas secciones similares dónde llegar al mismo resultado. Pasos para cambiar tu contraseña en la base de datos:

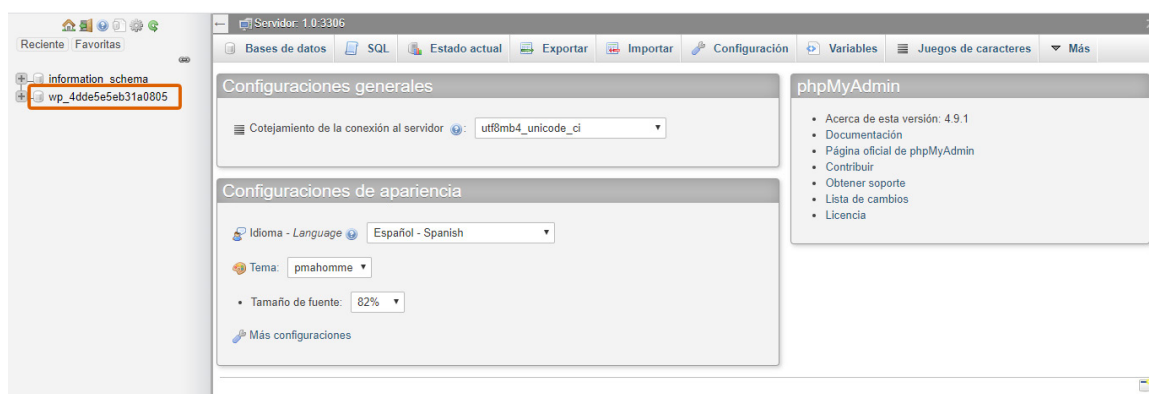
1. Accede a tu [Panel de Control](#) y luego al hosting donde tengas tu WordPress. Ahí ve a Bases de datos.



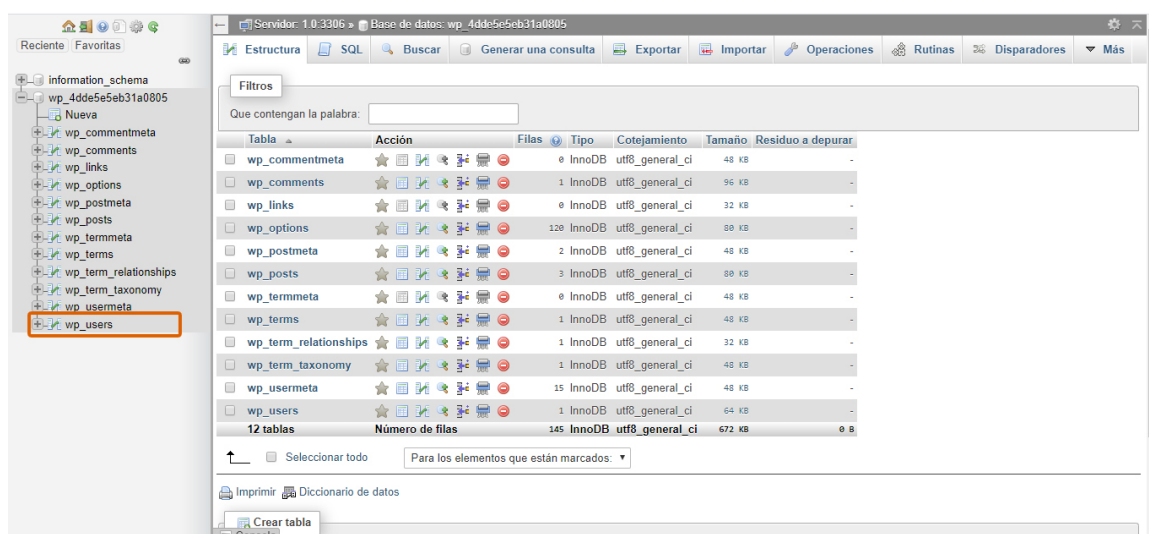
2. Elige la base de datos de tu WordPress y haz clic en Abrir.



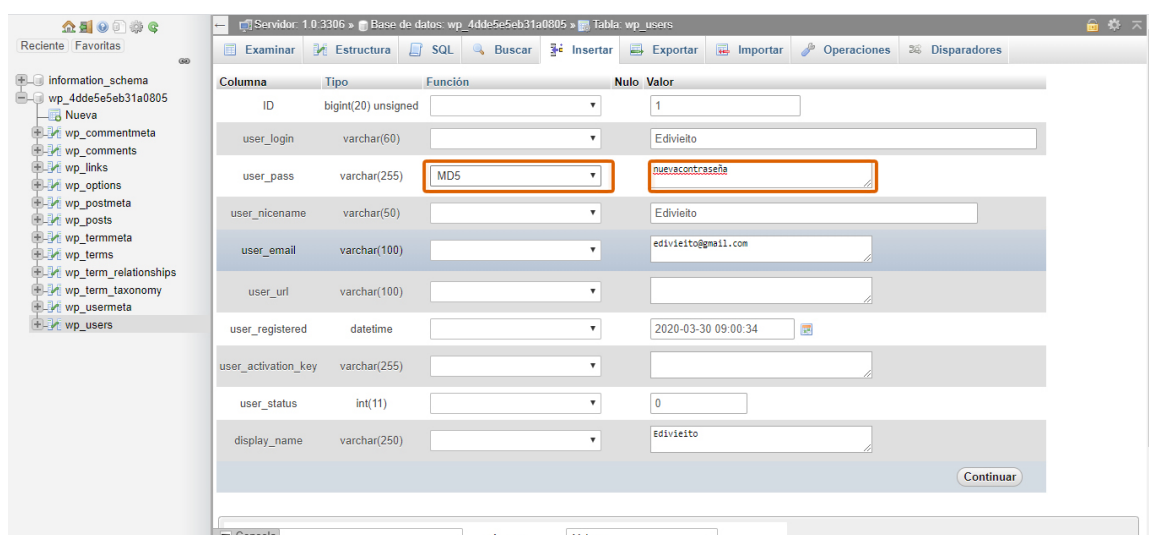
3. Te habrá redireccionado al phpMyAdmin. Este es un panel en el que gestionar y modificar las bases de datos que tengas. Busca la base de datos relacionada con tu WordPress y haz clic para desplegar el resto de apartados.



4. Busca el apartado wp_users, que contiene las contraseñas de todos los usuarios de tu sitio.



5. Como solo tengo un usuario, únicamente cambio mi usuario y mi contraseña. En la columna Función elige MD5 para que la encripte, ya que WordPress no permite guardar contraseñas en texto plano.



6. Ahora solamente tienes que pulsar Confirmar, volver a tu panel de acceso (wp-admin) y acceder con las nuevas credenciales.

Si aún no tienes una web en WordPress, recuerda que en dinahosting contamos con un [autoinstalable vitaminado de serie](#) para que te ahorres tiempo en las configuraciones iniciales.



3.4 6 PLUGINS DE SEGURIDAD EN WORDPRESS

Ya te hemos hablado de los [primeros pasos de seguridad](#) que debes implementar en tu WordPress, y también te hemos dicho lo que puedes hacer para disminuir el riesgo a hackeos sin utilizar ningún plugin. En el post de hoy te recomendaremos **los mejores y más completos plugins de seguridad** para dejar tu WordPress lo más blindado posible.

Recuerda que para que tu web esté protegida uno de los pilares básicos es contar con un [hosting seguro](#).

La seguridad en WordPress se basa en proteger archivos y prevenir ataques de los posibles intrusos. Existen en el repositorio de plugins varias opciones que te ayudaran a realizar estas acciones. Existen dos formas de afrontar la seguridad de WordPress mediante plugins.

1. Instalando plugins ligeros para acciones concretas
2. Instalando plugins generalistas mas pesados que abarquen todas estas acciones

Plugins para acciones concretas

Esta primera acción te permite tener **mejor controlado el flujo de errores**, ya que en caso de fallo, no dependerás de un único plugin, sino que diversificarás y en caso de errores con algún plugin concreto, el resto de protecciones seguirán activas. Ya conoces el dicho, es mejor no poner todos los huevos en la misma cesta.

Limitar los accesos ([Limit Login Attempts](#))

La mayor parte de los accesos al escritorio de WordPress se hacen mediante ataques de fuerza bruta, por lo que es una buena idea, instalar algún plugin que nos limite la cantidad de veces que podemos acceder a una web de forma fallida. Uno de los más populares y que incluimos en la instalación de nuestro [WordPress Optimizado](#) es [Limit login Attempts](#).

Este plugin permite restringir la cantidad de veces que intentas acceder a una web, de forma que si excedes ese máximo te obliga a esperar un período hasta que lo vuelvas a poder intentar.

Ocultar la meta-información ([Meta generator & info remover](#))

La detección de un bug de seguridad en el core de WordPress es pública. Por lo que si un hacker conoce tu versión de WordPress y tiene algún bug de seguridad catalogado, le estás facilitando la forma de hackear tu WordPress. La información sobre tu versión de WordPress está incluida en formato de atributo de meta-información. Este plugin elimina estas meta – descripciones haciéndole el trabajo un poco más complicado a los hackers.

Bloquear IPs ([IQ block Country](#))

Si tu mercado está en un país concreto, puedes bloquear el acceso de IPs de determinados países. Es muy habitual que los ataques vengan de IPs chinas o rusas, por lo que si no tienes mercado en éstos u otros países puedes bloquear el acceso con este plugin.

Plugins generalistas

Esta opción consiste en instalar **plugins más completos que abarquen todas las posibles fallas de seguridad** desde un mismo plugin. Como ventaja destacar que tu seguridad dependerá de un único plugin, lo que en palabras de mantenimiento y actualización, significará que no tendrás que estar pendiente de varios plugins.



All in one WP Security & Firewall

Es uno de los plugins de seguridad gratuitos más completos. Además basa su análisis en puntuaciones, lo que lo hace muy visual y divertido de usar. Cuanto mejor sea tu seguridad, mayor será la puntuación obtenida en cada categoría.

Una de las desventajas de este tipo de plugins es que hay que configurar muchísimos parámetros, por lo que cada vez que los instalas hay que cambiarlos uno a uno. Este plugin posee opciones de exportar e importar settings, de manera que si vas a utilizar este plugin en varias páginas que hayas creado, puedes duplicar las opciones escogidas en un par de clics.

Te permite modificar los archivos .htaccess y wp-config de manera muy segura. Te permite hacer un backup mientras los modificas, por si metes la pata en algún momento poder recuperar los archivos originales.

Tiene opciones para introducir usuarios en una lista negra y bloquearlos en tu web. Además añade un CAPCHA a tu formulario de login para evitar en la medida de lo posible los ataques de fuerza bruta.

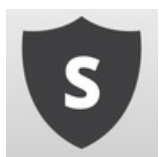
¡Ah! ¡Y está traducido prácticamente todo a castellano!



WordFence

Es un plugin muy popular y completo. Incorpora un sistema de firewall para securizar aún más tu sitio. Además también analiza si alguno de tus links apunta a una página etiquetada como maliciosa por Google, de manera que también te beneficia a nivel SEO.

Escanea exhaustivamente tu sitio en busca de malware o código malicioso. Inspecciona los temas, plugins y core del propio WordPress, indicándote en cada momento si encuentra algo que le pueda resultar sospechoso. Este escáner es un poco lento, por lo que no desesperes mientras lo realiza.



Sucuri

Es también uno de los plugins más utilizados. Te ayuda a fortalecer muchos de los puntos débiles de WordPress a través de un plugin. Quizás de los comentados sea el menos completo, sin embargo merecía revisión por sus descargas y longevidad.

Estos son los principales plugins de seguridad en WordPress, pero lo más importante en la seguridad es el sentido común y la precaución. Si aun así tu web ha sido infectada, recuerda que contamos con un servicio de [Asesoría Técnica](#), que **incluye servicio de desinfección y reportes de seguridad gratis**.

3.5

PLUGINS DE PROTECCIÓN DE DATOS EN TU TIENDA EN WOOCOMMERCE

Cuando nos ponemos a crear una tienda en WooCommerce nos concentramos en la creación de productos, en el proceso de envíos, en los métodos de pago... pero solemos dejar de lado toda la parte legal de nuestra tienda. En este capítulo te haremos un breve repaso de **lo mínimo que necesitas para cumplir el Reglamento General de Protección de datos (RGPD)** en tu WooCommerce, y te presentaremos algunos plugins que pueden facilitarte esta labor.

En una tienda online manejas mucha información confidencial de tus clientes, y alguna de ella sensible, como pueden ser sus datos bancarios. Desde la entrada en vigor de la nueva normativa en 2018 es obligatorio indicar cómo tratas y almacenas esta información.

Textos legales imprescindibles en cualquier tienda online

Existen una serie de aspectos sobre los que deberías dar información siempre. Si estamos hablando de una tienda online tienes que contar, como mínimo, con las siguientes páginas o textos legales:

Aviso legal

Es un texto genérico en el que se informa al usuario sobre tu web y sobre el tratamiento de la información. Proporciona datos fiscales, dice qué permisos tienes y das sobre tu contenido, etc.

En dinahosting te ofrecemos, completamente gratis, un [aviso legal tipo](#). Únicamente tendrás que cubrir un sencillo formulario para personalizarlo.

Condiciones generales de contratación

Este apartado te será muy útil si tu negocio consiste en ofrecer servicios. En estos casos siempre existe una relación entre cliente y proveedor, por lo que es necesario especificar los términos de contratación.

Política de Cookies

Las cookies son muy útiles para que cuando tus usuarios accedan a tu página esta recuerde su contraseña, idioma en el que se le tiene que mostrar la web, etc. Sin embargo, también pueden ser muy conflictivas. Algunas webs estudian el comportamiento de compra de sus visitantes para luego ofrecerle esta información a terceros.

Es por ello que, si tu web emplea cookies, debes informar al usuario de qué tipo son y qué haces después de guardarlas.

Protección de Datos

Durante el proceso de compra recopilas información sobre tus usuarios para realizar la facturación y gestionar los pedidos. De nuevo, es imprescindible informar de lo que haces con sus datos. Dónde los almacenas, cuáles guardas y si los compartes con terceros.

¿Tienes SSL en tu web? Activar un [Certificado SSL](#) es uno de los básicos para proteger las comunicaciones de tus usuarios y que tu web se marque como segura en navegadores.

Plugins de protección de datos en WooCommerce

Existen en el mercado multitud de plugins para ayudarte con la protección de datos de tu tienda online. Muchos son de por sí una solución de lo más completa que integra todo lo necesario para cumplir con el RGPD.

Recuerda que cada caso concreto tiene unas necesidades específicas y ningún plugin garantiza un cumplimiento al 100 %. Si necesitas asesoramiento personalizado ponemos a tu disposición un servicio de [Asesoría Legal](#) especializada en Internet.

¡Vamos con los plugins!

WP GDR Compliance

Es una solución gratuita que te permite adaptar tu sitio al RGPD. Además está pensado para ser completamente **compatible con WooCommerce, Contact Form 7 y los comentarios propios de WordPress**.

Protección de datos RGPD

Con este plugin podrás generar los textos legales cumplimentando un formulario, para después insertar los shortcodes en las páginas que necesites. Por ahora solo garantizan la **compatibilidad con el tema de WooCommerce StoreFront**. Si necesitas corroborar la compatibilidad con otro tema, puedes ponerte en contacto directamente con sus desarrolladores.

Ultimate GDPR Compliance Toolkit for WordPress

Por último, te recomendamos uno de pago. Este plugin ofrece muchas opciones de personalización, entre las que destaca la **encriptación de la información** y notificación en caso de filtración de la misma.

Como ves, mantener al día toda la parte legal de tu web puede ser algo tedioso, sobre todo al principio. Lo bueno es que estos plugins tienen casi todo lo que necesitas: realización de textos, check en formularios, banners de aviso, etc. así que esperamos que te faciliten un poco la tarea. Si lo prefieres, **siempre puedes instalar varios plugins**, cada uno con sus características concretas: uno para las cookies, otro para el consentimiento en el formulario, etc.

Sea cual sea tu elección, no dejes de **usar el sentido común y comprobar que todo encaja con tus necesidades**.

Tip extra: añade un CAPTCHA

Además de estos consejos que te hemos dado, recuerda que la recopilación de los datos de tus usuarios siempre se hace a través de formularios. Por eso, nunca está de más **añadir una capa de seguridad** extra a través de algún método de verificación, para evitar que un bot esté introduciendo información innecesaria dentro de tu base de datos.

Algunos de los plugins recomendados ya introducen un CAPTCHA además del check para aceptar la política de privacidad, pero no todos lo hacen. No pierdas de vista estos otros plugins para añadir un plus de seguridad a tu tienda: [ReCaptcha](#), [Really Simple CAPTCHA](#), [Captcha code](#).

Con estos trucos tu [tienda online en WooCommerce](#) cumplirá con el Reglamento General de Protección de Datos en un abrir y cerrar de ojos.



3.6

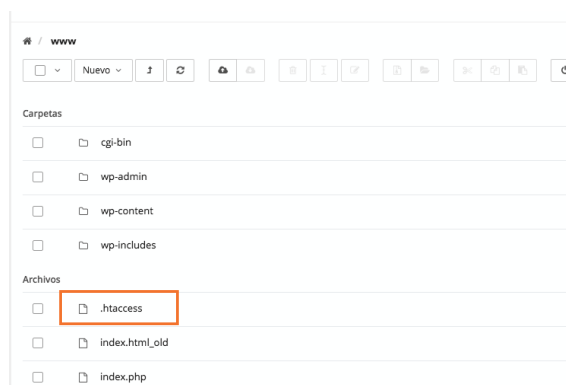
PROTEGER TU WORDPRESS MEDIANTE .HTACCESS: 5 CONSEJOS

El .htaccess es un archivo de configuración que te permite gestionar y manejar configuraciones y accesos al servidor de forma descentralizada, y utilizando instrucciones específicas puedes proteger carpetas, archivos y hasta el propio .htaccess dentro de tu WordPress.

¿Dónde busco el archivo .htaccess?

Este archivo se encuentra en la carpeta de archivos (www) de tu alojamiento web. Inicia sesión por FTP con el cliente que elijas y lo tendrás accesible.

Filezilla es uno de los clientes FTP más populares.
Aquí [te enseñamos cómo usarlo](#).



Vista de la carpeta de archivos (www)

Antes de hacer cualquier cambio...

Este es el aspecto que lucirá por defecto el archivo .htaccess en una instalación limpia de WordPress:

```
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>
# END WordPress
```

Para editarlo puedes **utilizar cualquier editor de texto**, como Notepad++, o mismamente el propio bloc de notas.

Si no puedes guardarlo como .htaccess, hazlo como .txt y una vez subido lo renombas.

Eso sí, antes de comenzar a aplicar cambios, ten en cuenta estos dos puntos:

- Toda configuración que agregues al archivo .htaccess colócala **debajo de la última línea de código “#END WordPress”**, así lo tendrás todo organizado.
- Primero **realiza un backup o copia de seguridad de tu archivo .htaccess** por si te encuentras con algún contratiempo. Basta con que guardes una copia en tu PC para poder volver a la configuración original si lo necesitas.

5 consejos muy fáciles para proteger tu WordPress con .htaccess

Como te decíamos, añadiéndole simplemente unas pocas líneas de código podrás mejorar mucho la seguridad de tu web. ¡Vamos allá!

Restringe el acceso a tu carpeta wp-content

La carpeta wp-content contiene los archivos de temas y plugins de tu instalación. El acceso a esa carpeta no debe ser directo, con excepción de las imágenes, JavaScript y CSS que puedan ser utilizados por el tema que has escogido.

Para corregir eso crea un archivo .htaccess dentro de la carpeta wp-content a través del «Administrador de archivos» de tu Panel de Control, y agrega la siguiente línea:

```
Order deny,allow
deny from all
<files ~ "(.xml|css|jpe?g|png|gif|js)$">
allow from all
</files>
```

Protege el archivo wp-config.php

El archivo wp-config.php de WordPress, localizado en la raíz de la instalación del sistema, es otro elemento importantísimo del CMS. En él se guarda, por ejemplo, la información de la base de datos que estás utilizando (nombre, usuario, contraseña), además de otros datos críticos.

Desactivar el acceso a él también es esencial para mantener tu blog seguro. Añade el siguiente código al .htaccess principal, utilizando la herramienta de edición del Administrador de archivos:

```
<Files wp-config.php>
order allow,deny
deny from all
</Files>
```

Protege el archivo xmlrpc.php

Este archivo permite que una aplicación externa se pueda comunicar con tu WordPress. Es posible anularlo con sólo añadir el siguiente código al .htaccess:

```
<files xmlrpc.php>
order allow,deny
deny from all
</files>
```

Evita el hotlinking

El hotlinking es una mala práctica que se produce cuando un tercero usa imágenes tuyas en sus contenidos, pero en vez de subirlas a su hosting las enlaza desde un URL de tu web. Lo que consigue con eso es ahorrarse recursos de su alojamiento web y consumir los del tuyo.

Añade este código al .htaccess y te protegerás de él:

```
RewriteEngine On
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www.)?dominio-ejemplo.com/.*$ [NC]
RewriteRule (.gif|jpg)$ http://www.dominio-ejemplo.com/hotlinking.png [R,L]
```

Recuerda sustituir “dominio-ejemplo.com” por tu propio dominio y “hotlinking.png” por el nombre del archivo de la imagen de aviso que hayas subido a tu servidor, que será la que se cargue en la web de la persona que haya intentado apropiarse de tus fotos.

No te olvides del propio .htaccess

Protegerlo es muy sencillo. Tan solo tienes que implementar el siguiente código en el archivo .htaccess de la carpeta principal de tu WordPress:

```
<files .htaccess>
order allow,deny
deny from all
</files>
```

Gracias a estos sencillos trucos, y sin tener que usar ningún plugin, podrás proteger muchísimo la seguridad de tu WordPress con .htaccess.



SOLUCIONES AVANZADAS

*Servicios profesionales
para desarrollar
proyectos de alta
exigencia*

*Housing: tus servidores en
buenas manos*



3.7

QUÉ SON WP-ADMIN Y WP-LOGIN.PHP DE WORDPRESS

En WordPress hay dos partes que son imprescindibles tanto para el acceso como para el funcionamiento de las webs creadas con el CMS: nos referimos a wp-admin y wp-login.php. Te contamos qué son y para qué sirven.

Cuando quieres acceder al apartado de administración de tu WordPress es posible que utilices una URL terminada en /wp-admin o por el contrario, utilices otra terminada en /wp-login.php.

Si pruebas a acceder por ambas el resultado seguramente será igual, es por eso que a simple vista puede parecer que sirven para lo mismo, pero no. Te contamos qué son y sus diferencias a continuación.

¿Qué son wp-admin y wp-login.php?

Wp-admin es un directorio o carpeta que viene por defecto en WordPress y alberga diferentes archivos del backend necesarios para el funcionamiento del CMS.

La carpeta wp-admin se genera automáticamente al igual que otras como la de wp-content o la wp-includes, cuando instalas WordPress en tu directorio raíz.

Ni la carpeta wp-admin ni su código son editables. Se trata de una página estática con una serie de instrucciones que no necesitan ni deben ser modificadas por el usuario.

Es por eso que cuando tratas de acceder desde el navegador a /wp-admin (dominioejemplo.com/wp-admin) como tal, en realidad lo que hace WordPress es redirigirte a la página de login y ejecutar el archivo wp-login.php.

El archivo wp-login. php es lo que realmente ves cuando accedes a la carpeta /wp-admin.

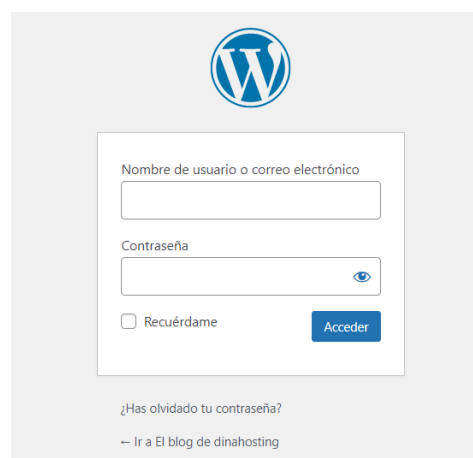
Wp-login.php hace que te salga el formulario habitual para loguearte como usuario editor o administrador y así acceder a los paneles para gestionar la web.

Este archivo es crítico a nivel seguridad porque **es el objetivo de muchos ataques malintencionados**. Es por eso que te recomendamos realizar las siguientes acciones de seguridad para contrarrestar posibles hackeos y mantener tu web y hosting seguros.



Mira el vídeo

¿En qué se diferencian wp-admin y wp-login de WordPress?



Medidas de seguridad para proteger wp-admin y wp-login.php

Cambiar la URL de login

Una de nuestras [recomendaciones básicas para securizar tu WordPress](#) es que modifiques la URL de acceso al panel de gestión por una menos obvia. Es decir que en lugar de entrar al login a través de la URL /wp-admin o /wp-login.php la cambies por otra.

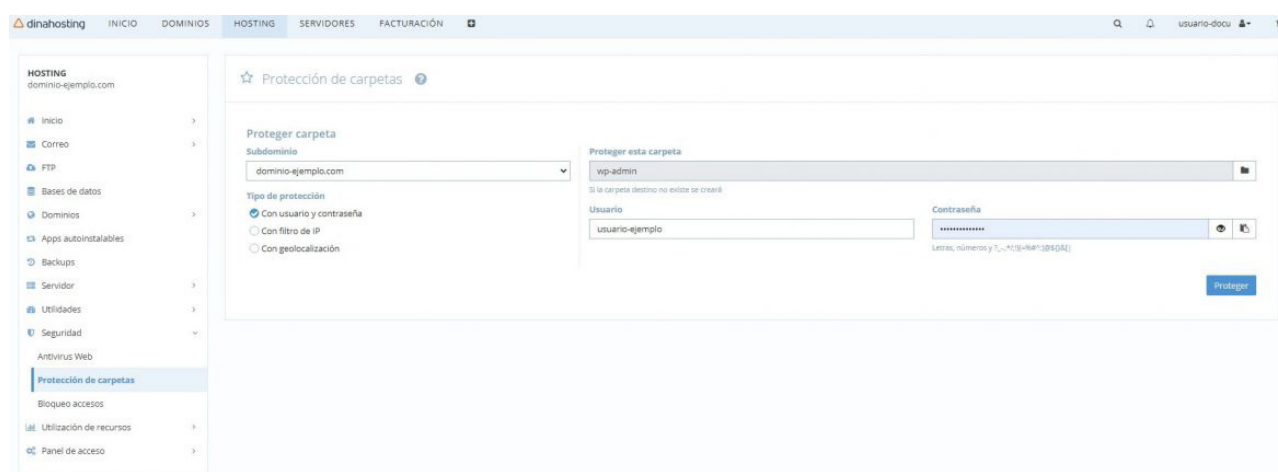
Para ello puedes utilizar el plugin [WP hide login](#) que permite modificar la URL fácilmente y personalizarla al gusto.

Limitar el número de accesos

Por defecto en WordPress el número de accesos a través del login no están limitados. Con los plugins [WP limit login](#) o [Limit Login Attempts](#) también podemos limitar los accesos a un número máximo por usuario o bloquear los intentos masivos a través del login y así evitar ataques.

Restringir el acceso por contraseña, IP o país

Desde el apartado Mi cuenta > Preferencias > Seguridad del Panel de tu hosting puedes restringir los accesos a tu web o a determinadas carpetas como la de wp-admin, para que solo puedan acceder con contraseña o desde una determinada IP o área geográfica.



O si lo prefieres, puedes restringir el acceso al wp-login.php por IP editando el fichero .htaccess con el siguiente código:

```
<Files wp-login.php>
    Order Allow,Deny
    Deny from all
    Allow from ip

</Files>
```

En este post te contamos otras acciones de seguridad para proteger WordPress editando el archivo .htaccess.

Revisar los permisos de usuarios

Échale un ojo a los usuarios y a los permisos que tienen asignados. Si por ejemplo, solamente escriben entradas, no es necesario que tengan permisos de Administrador.

Borra también aquellos usuarios que ya no necesitan acceder a la web. En caso de que vuelvan a necesitar tener acceso es mejor creárselo que dejar la puerta abierta.

Cuanto menos administradores haya, menos probabilidad habrá de que se produzcan accesos o problemas indeseados por una mala gestión de WordPress.

Utilizar contraseñas seguras

Tener una buena contraseña es también una parte muy importante para evitar que accedan a nuestra web a través del login.

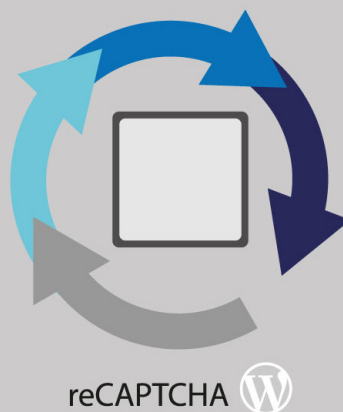
Escribe contraseñas difíciles y lo suficientemente largas para que sean difíciles de descifrar. Combina mayúsculas y minúsculas e incluye números y caracteres raros.

Y no solo tu propia contraseña, **solicita o exige a todos los usuarios de la web que utilicen contraseñas seguras para loguearse.**



HERRAMIENTAS GRATUITAS DE SEGURIDAD PARA TU WEB Y CORREO

Aprovecha todos los recursos que tienes en el Panel de Control y en el Webmail para securizar tu proyecto web y tu servicio de correo.



3.8

CÓMO AÑADIR GOOGLE RECAPTCHA A TU WORDPRESS

Vamos a explicarte cómo añadir [Google reCAPTCHA](#) a tu WordPress en unos sencillos pasos.

Google reCAPTCHA ha demostrado ser una funcionalidad muy útil para combatir las vulnerabilidades en los formularios web, prevenir el [SPAM](#) en los comentarios de una web o evitar ataques por fuerza bruta.

Para poder implementarlo en tu web con WordPress, lo primero que necesitarás son las [claves de Google reCAPTCHA](#) y un plugin que sea compatible con este sistema de verificación.



Mira el vídeo

Cómo añadir Google reCAPTCHA a tu web en WordPress

¿Qué plugin elegir?

Antes de elegir, debes tener en cuenta el tipo de reCAPTCHA vas a implementar (v2 o v3), los formularios donde implementar Google reCAPTCHA y si es compatible con tus otros plugins que muestran formularios en tu web (Contact Form, Woocommerce, MailChimp...). Teniendo estas consideraciones en cuenta podrás elegir la opción que mejor se ajusta a tu sitio.

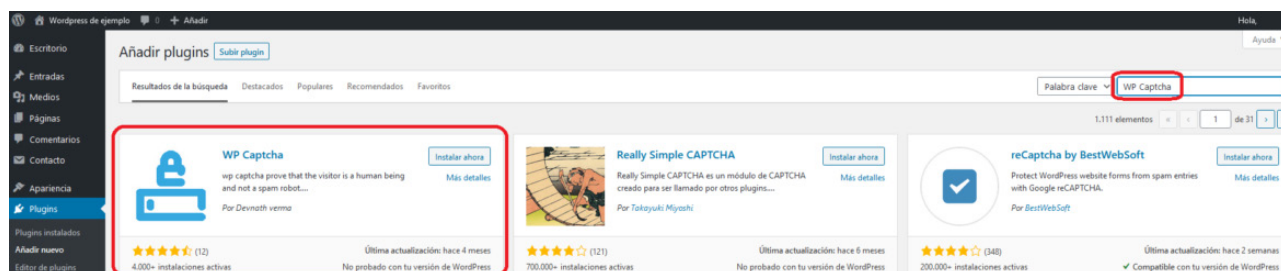
Por ejemplo, si no quieres que tus usuarios tengan que interactuar con el sistema de CAPTCHA para añadir comentarios en tus entradas, puedes optar por la versión v3 de Google reCAPTCHA. Un buen ejemplo de plugin a escoger sería entonces [reCaptcha by BestWebSoft](#), aunque este plugin dispone de una versión de pago, las opciones gratuitas cubren la mayoría de las necesidades.

Por otra parte, si prefieres algo más ligero, compatible con la versión v2 y que permita además otros sistemas de CAPTCHA podrías escoger el plugin [WP Captcha](#). Este plugin es completamente gratuito y es compatible con otros plugins como por ejemplo Woocommerce o MailChimp que otros desarrolladores incluyen como versión de pago.

Añadir Google reCAPTCHA a tu WordPress

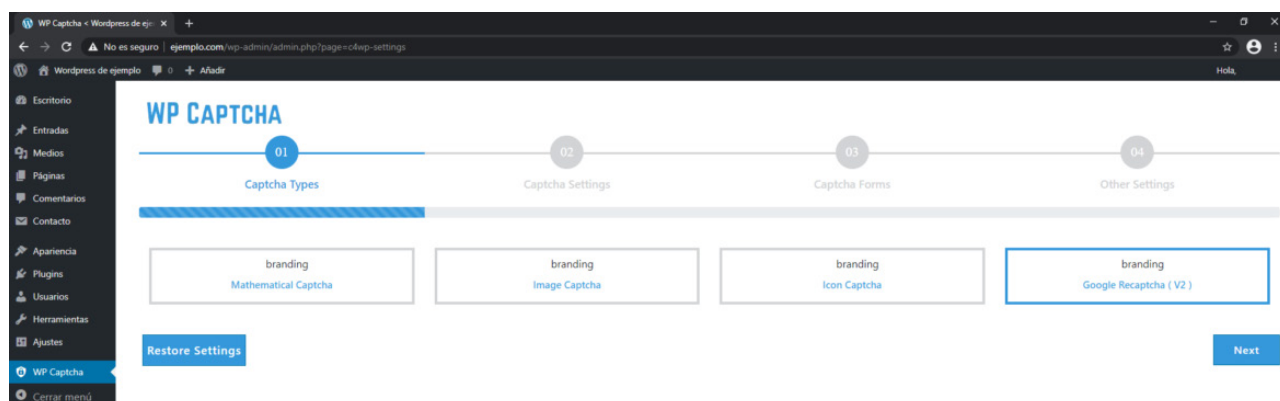
Una vez conseguidas las claves, accede al apartado de administración de tu web en WordPress, en el menú de la izquierda, selecciona Plugins y a continuación pulsa en Añadir nuevo.

Escribe en el buscador de la parte superior derecha "WP Captcha" y en los resultados de la búsqueda pulsa el botón Instalar ahora.

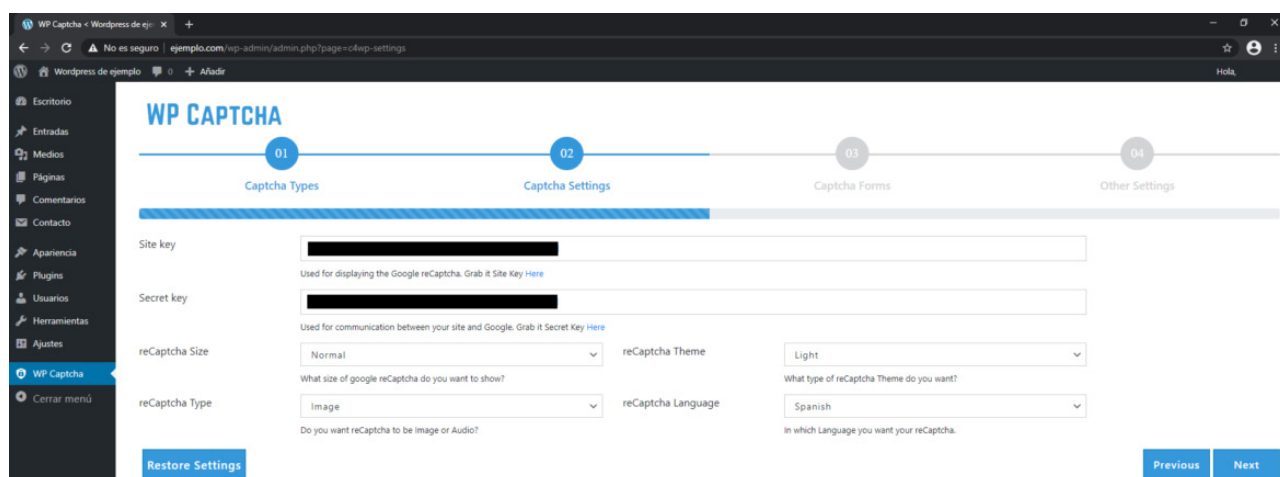


En este ejemplo hemos elegido WP Captcha por sus funcionalidades y compatibilidad con Google reCAPTCHA y otros plugins de WordPress que añaden formularios, sin embargo, puedes instalar el plugin que consideres más acertado para tu sitio.

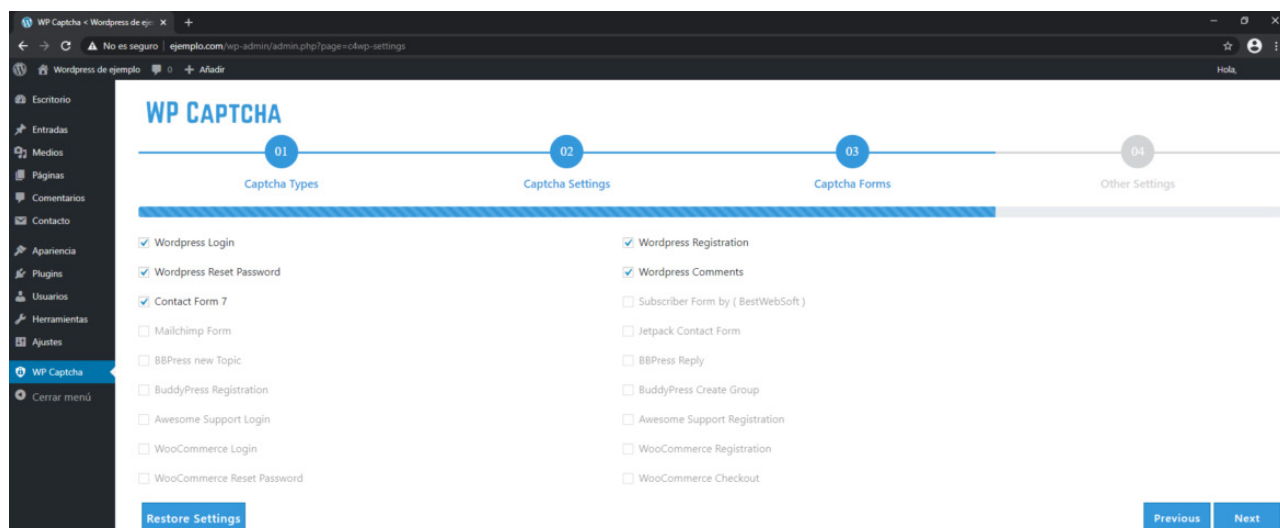
Una vez instalado y activado el plugin, verás una nueva sección en la parte izquierda del menú de WordPress llamada WP Captcha. En este apartado selecciona la opción Google reCAPTCHA (V2) y pulsa Next para continuar.



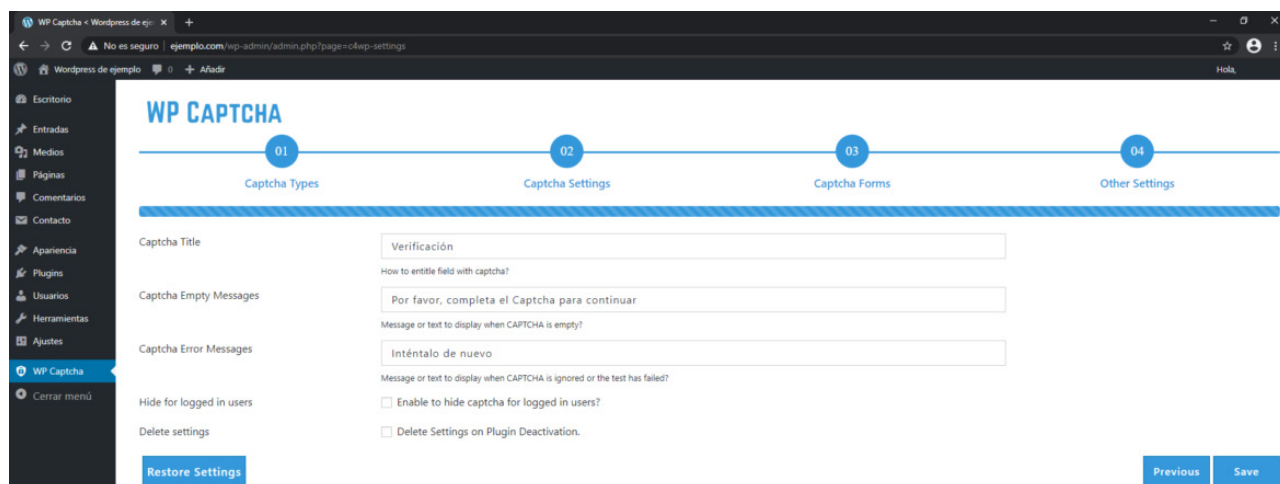
A continuación, introduce las claves que has obtenido desde Google reCAPTCHA y configura el resto de opciones a tu gusto. Para continuar, pulsa Next.



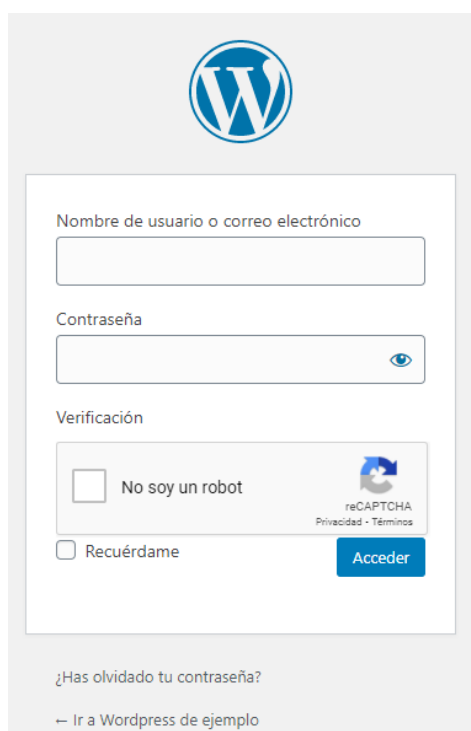
En este nuevo apartado indica las secciones de tu web donde quieres activar Google reCAPTCHA y haz clic en Next para continuar.



Por último configura los mensajes de notificación y pulsa Save para terminar.



Ahora cuando intentes identificarte en tu web o completar un formulario verás la casilla de verificación de Google reCAPTCHA.



GUÍA DE CIBERSEGURIDAD

4. Errores HTTP

[4.1. Soluciona los errores HTTP de tu web con estos tips](#)

[4.2. Error 403 "Forbidden": qué es y cómo solucionarlo en tu web](#)

[4.3. HTTP error 404: ¿qué es? ¿Cómo lo soluciono?](#)

[4.4. HTTP error 500. Qué es y cómo solucionarlo en tu web](#)

[4.5. Qué es un error 502 y cómo solucionarlo](#)

[4.6. ¿Qué es el error 503? Causas y soluciones](#)

[4.7. Cómo arreglar el error 504 Gateway Timeout](#)





Error 404 - Page not found

Don't worry. Return to the previous page...

4.1 SOLUCIONA LOS ERRORES HTTP DE TU WEB CON ESTOS TIPS

¿Qué es lo primero que piensas cuando te saltan errores HTTP como un 404? ¿Qué ha pasado en mi web? **Los códigos de estado o errores HTTP nos dicen cómo ha ido la carga de una página en Internet.** Por eso, si no quieres que las personas usuarias de tu web tengan una experiencia de navegación negativa, es importante que los tengas controlados.

Lo normal es que estos códigos permanezcan invisibles, lo que significaría que todo funciona bien. Si aparecen es porque el servidor no ha sido capaz de procesar la petición que le llegó desde el navegador, y ahí es cuando tienes que entrar tú.

Para que actúes rápido y bien, mira esta guía con los de errores HTTP más importantes y cómo solucionarlos.

Tipos de código de estado

Los errores HTTP **están formados por tres dígitos.** El primero de ellos te indica ante qué categoría de código te encuentras dentro de las cinco posibles. Por ejemplo, el 404 forma parte del tipo de respuesta 4XX (un 4 y los dos números que sean). Empezamos por explicarte en qué consiste cada uno de los grupos:

- **Códigos de estado 1XX:** generan respuestas informativas. La solicitud todavía se estaría procesando.
- **Códigos de estado 2XX:** te dicen que las peticiones son correctas, o lo que es lo mismo, ¡que no tienes que hacer nada! La persona usuaria de tu web está llegando correctamente a la página que quiere.
- **Códigos de estado 3XX:** indican redirección de una página a otra. La persona usuaria de tu web saltará a otra URL automáticamente.
- **Códigos de estado 4XX:** denotan error de solicitud. La petición no puede completarse porque su sintaxis no es correcta.
- **Códigos de estado 5XX:** en este caso estamos ante un error del servidor. Puede que algún servicio esté caído o que por algún tipo de error interno el servidor no pueda procesar la solicitud.

Los errores HTTP más comunes

Ya ves que algunos de los códigos de estado son más relevantes que otros. Los que integran las tres primeras categorías ni siquiera significan que tu web contenga errores, así que vamos a centrarnos en la 4XX y en la 5XX. ¡Y no te preocupes! Media hora a la semana será suficiente para detectar y eliminar estos problemas.

403

Puede que te suene más la palabra "Forbidden". ¿Qué significa? Que los datos a los que quiere acceder la persona usuaria están protegidos. Por eso, le llega un aviso en formato HTML de que su petición es denegada por el servidor.

Solución: primero, revisa que todos los archivos de tu hosting tengan permiso de lectura. Por otro lado, si tienes protección por contraseña en el Panel de Control verifica que estás poniendo la contraseña correcta. También puede darse el caso de que el servidor esté aplicando alguna restricción por seguridad. Revisa el archivo error.log de tu hosting y comprueba que no haya errores.

Aquí te explicamos al detalle [qué es el error 403 y cómo solucionarlo](#).

404

Nada es perfecto. **Es muy probable que tu web contenga algún error 404 y no por eso tienes que crucificarte.** El **"Not Found"** se produce cuando el servidor no encuentra la página solicitada. Puede que la persona haya tecleado mal la URL, que sus contenidos hayan sido trasladados a una dirección nueva de la que el servidor no tenga constancia, o que por lo que sea el enlace esté roto.

Solución: primero (y muy importante), revisa que no hayas escrito mal la URL. Si la dirección está bien, piensa. ¿Ya no contiene información? Pues la eliminas. ¿Te has olvidado de redireccionarla? Hazlo entonces. ¿Es culpa del enlace, que está roto? Si te interesa, linkalo nuevamente al sitio de destino. Si no, bórralo.

Aquí tienes más información sobre [el error 404 y cómo solucionarlo en tu web](#).

500

"Internal Server Error". ¡Vaya! Se ha producido un **error inesperado en el software de tu servidor**. A parte de la notificación de error 500 que llegará a la persona usuaria de tu web, el servidor generará información internamente para detectar qué es lo que falló.

Solución: posiblemente se trate de algún error en la configuración de .htaccess o de algún componente de tu página, por lo que podrás encontrar la causa del problema en el error.log. Si no, llámanos. Como empresa proveedora de tu hosting te diremos de dónde viene el error y te lo solucionaremos ipso facto.

Y si quieres saber más sobre [el error 500, tienes todos los detalles aquí](#).

502

El error 502 o el llamado **Bad Gateway Error** (puerta de enlace incorrecta), se produce porque hay un error causado por un elemento ajeno a tu ordenador o navegador, al igual que todos los códigos de estado HTTP que empiezan por el número 5. Este error te indica que un servidor que estaba actuando como puerta de enlace o proxy ha recibido una respuesta no válida de un servidor entrante.

Solución: primeramente comprueba si tu web se ha caído o solo eres tú el que no puede entrar a la web. Recarga la página o entra desde un navegador diferente. Si el problema no se ha solucionado, borra la caché y las cookies del navegador. Como tercera solución, desactiva la temporalmente la CDN. Otras veces un error 502 puede venir provocado por los plugins o temas que has instalado en tu WordPress o por cambios y actualizaciones recientes en tu web que puedes comprobar en el log de errores.

Si quieres puedes ampliar aquí la información sobre el [error 502 y cómo solucionarlo](#).

503

Este error se produce cuando en el momento de **la petición del servidor este está sobrecargado o se están realizando tareas de mantenimiento**. Por lo tanto, el error es temporal y el servidor estará disponible de nuevo cuando se solucione el problema.

Solución: espera un rato y aprovecha para estirar las piernas. Si ves que el error se alarga y tus solicitudes se siguen rechazando, puede que tengas el servidor limitado a un número determinado de visitas y que en ese momento no pueda recibir más. En cualquier caso, y ante la duda, en dinahosting te atenderemos las 24 horas del día.

O también puedes ampliar aquí la información sobre el [error 503, sus causas y soluciones](#).

504

Este tipo de error indica que un **servidor no ha recibido la respuesta que esperaba** de otro servidor al intentar acceder a un sitio web o completar otra solicitud.

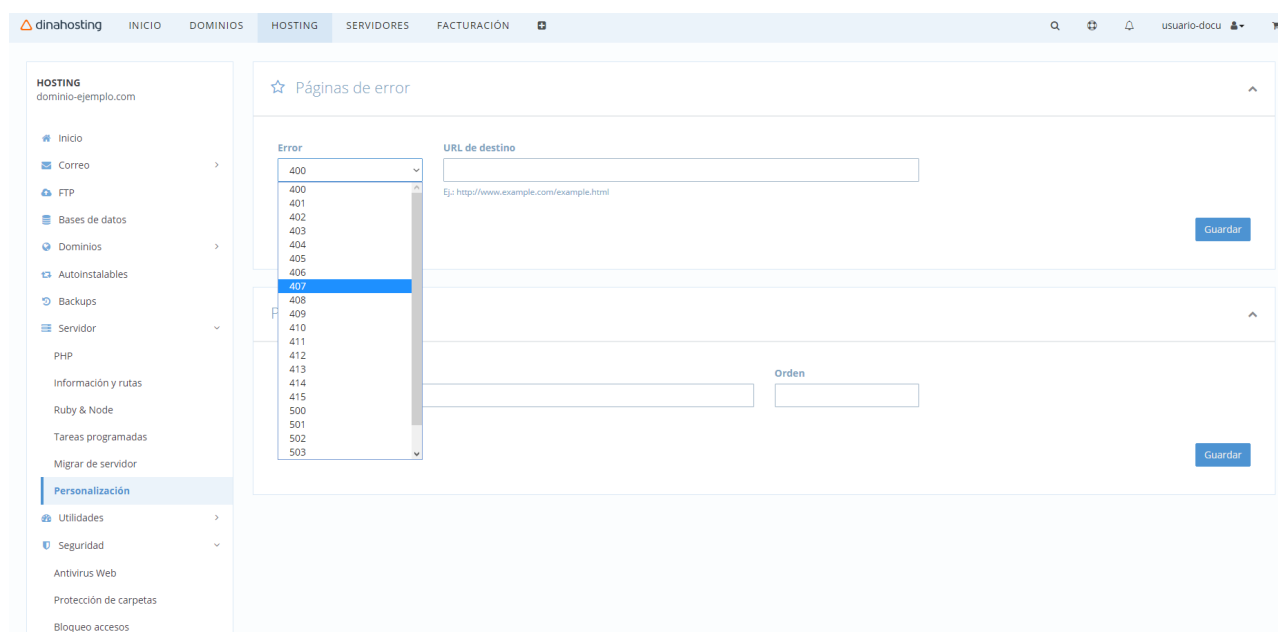
Solución: prueba a hacer F5 y recargar la página. Asegúrate además que no haya problemas con tu red local. Como en otros errores, otra solución es borrar la caché y las cookies, o iniciar una sesión en modo incógnito. Si eres el administrador de la web y has hecho cambios recientes en tu web, comprueba el informe de errores. También puedes desactivar de forma temporal tu CDN y espera a que se propaguen las zonas. Otras razones pueden deberse a la instalación reciente de plugins o temas en tu WordPress. Si el error persiste, [contacta con el Soporte](#) de tu hosting.

¿Prefieres seguir intentándolo por tu cuenta? En esta guía tienes más información sobre el [error 504](#).

Míralo por el lado bueno

Las páginas de error son una oportunidad fantástica para demostrarle a la persona usuaria de tu web que piensas en ella en todo momento. **Tira de creatividad para diseñar ese espacio:** dale un toque de humor, incluye un juego, un GIF... ¡incluso puedes añadir un botón de suscripción! Hazlo cómo quieras, pero hazlo. Es la única manera de sacarle hierro al asunto y mantener el engagement.

En el [Panel de dinahosting](#) tienes una utilidad para [personalizar tu página de error muy fácilmente](#), en Hosting > Servidor > Personalización. Para hacerlo, tienes que crear y guardar en la carpeta principal (donde está el archivo index.html o página inicial) un archivo llamado ".htaccess" con el siguiente contenido: ErrorDocument 404 /error.html. Finalmente, te queda crear un archivo llamado error.html con el diseño e información que tú quieras.



Así, cada vez que una persona usuaria de tu web se encuentre con un 404 Apache (servidor web que se encarga de entregarte cada web), mostrará el archivo error.html que has creado.



403

ERROR!
ACCESS DENIED

4.2 ERROR 403 "FORBIDDEN": QUÉ ES Y CÓMO SOLUCIONARLO EN TU WEB

Si has llegado hasta aquí seguramente sea porque estás accediendo a tu página web y te ha salido en el navegador el mensaje **Error 403 Forbidden**. You don't have permission to access to this server. Efectivamente, este **es uno de los errores más habituales que pueden darse en tu página web**.

En este post te daremos algunas pautas para solucionar o al menos para que puedas conocer la fuente del error 403, pero antes de nada queremos recordarte que si eres cliente de dinahosting nuestro equipo de [Soporte Técnico](#) estará encantado de echarte un cable con lo que necesites.

¿Qué es el error 403?

El error 403 es el que **se produce cuando intentas acceder a una URL o carpeta a la que está bloqueado el acceso**. Es por eso que cuando estás navegando por la red y te aparece este error suele ser debido a que la web que visitas está aplicando algún permiso o filtro que restringe tu acceso de manera intencionada o no.

El error 403 pertenece al grupo de errores HTTP de **código de estado 4XX**. Estos errores se dan cuando la petición que estás intentando realizar no puede completarse porque su sintaxis no es correcta o como es el caso, hay un error en la solicitud (debido a un bloque o a la razón que sea). De ahí que sean llamados también como **errores de solicitud**.

Al contrario que en el caso de códigos de error 5XX que se deben al servidor, los códigos tipo 4XX suelen estar en la parte del usuario.

Este error suele aparecer en pantalla de una de las siguientes formas:

- *Error 403 Forbidden. You don't have permission to access to this server*
- *HTTP Error 403 – Forbidden*
- *403 forbidden request forbidden by administrative rules*
- *403 Forbidden*
- *Access Denied You don't have permission to access*

Igual te da más pistas la palabra Forbidden que el número 403. Ese Forbidden o Prohibido indica que los datos a los que quieres acceder están protegidos. Por eso te llega un aviso en formato HTML de que la petición está siendo denegada por el servidor.

¿A qué es debido el error 403? Posibles causas y soluciones

Actualizar el navegador o contactar

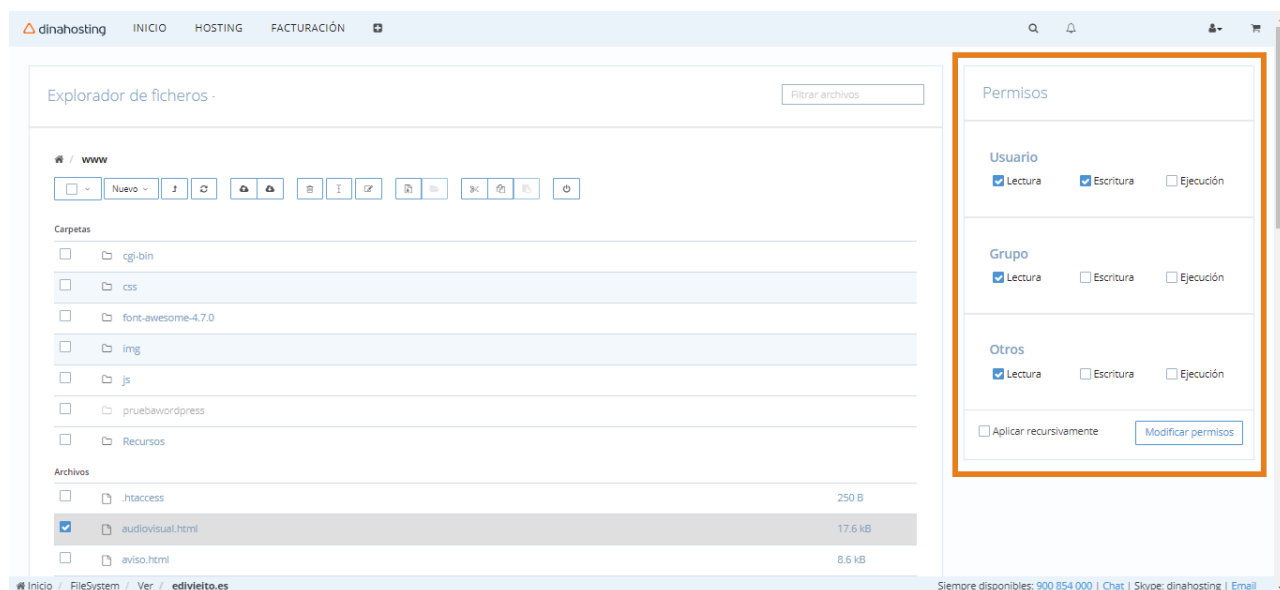
Como te decíamos antes, si estás navegando por la red y te encuentras con este error **es posible que el webmaster de la página haya puesto un bloqueo para que no puedas acceder**. En este caso poco puedes hacer: prueba

bien a refrescar la página para comprobar si el bloqueo es momentáneo o bien, puedes ponerte en contacto con administradores para solicitar que te lo quiten.

Si en cambio el error aparece en tu página y eres administrador puedes probar a con estas otras acciones:

Permisos mal configurados

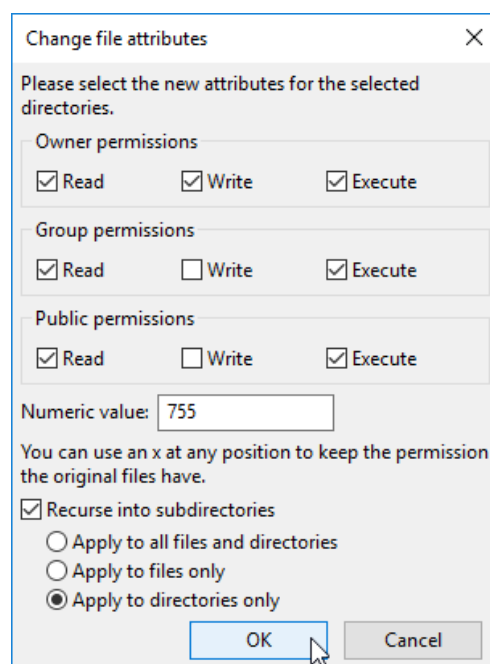
Como hemos comentado suele ser un problema de permisos. Primero, revisa que todos los archivos de tu hosting tengan permiso de lectura. ¿Cómo puedes comprobarlo? Sencillo. Entra a tu [Panel de Control](#) y luego a Hosting > FTP > Explorador de archivos.



Comprueba en el bloque de la derecha que los diferentes archivos que entran en juego en tu página tienen chequeada la opción de lectura. En caso de no ser así, actívala y vuelve a intentar acceder a tu página. Si la causa era esa debería haberse resuelto el error.

Con WordPress puedes revisar y modificar los permisos que tienes asignados a las carpetas accediendo a tu sitio desde un FTP de la siguiente forma:

1. Accede a las carpetas de tu web desde un cliente FTP como puede ser FileZilla.
2. Dirígete al directorio raíz de tu web.
3. Selecciona la carpeta principal que incluya los archivos visibles y con el botón derecho pulsa en Atributos. Generalmente esta carpeta recibe el nombre de public_html.
4. Se abrirá una ventana con los permisos. Ahí puedes revisar si están correctos y aplicar los cambios que consideres a filas y/o directorios. Para las filas deberás aplicar un valor numérico 644 y para los directorios el 755 si quieres que sean visibles y no se produzca el error 403.



Accesos restringidos

Si ya has comprobado que los permisos de los archivos de tu web están correctos, otra posible causa del error puede ser el **acceso restringido**. Si tienes **protección por contraseña** en tu web, verifica que estás introduciendo la contraseña correcta.

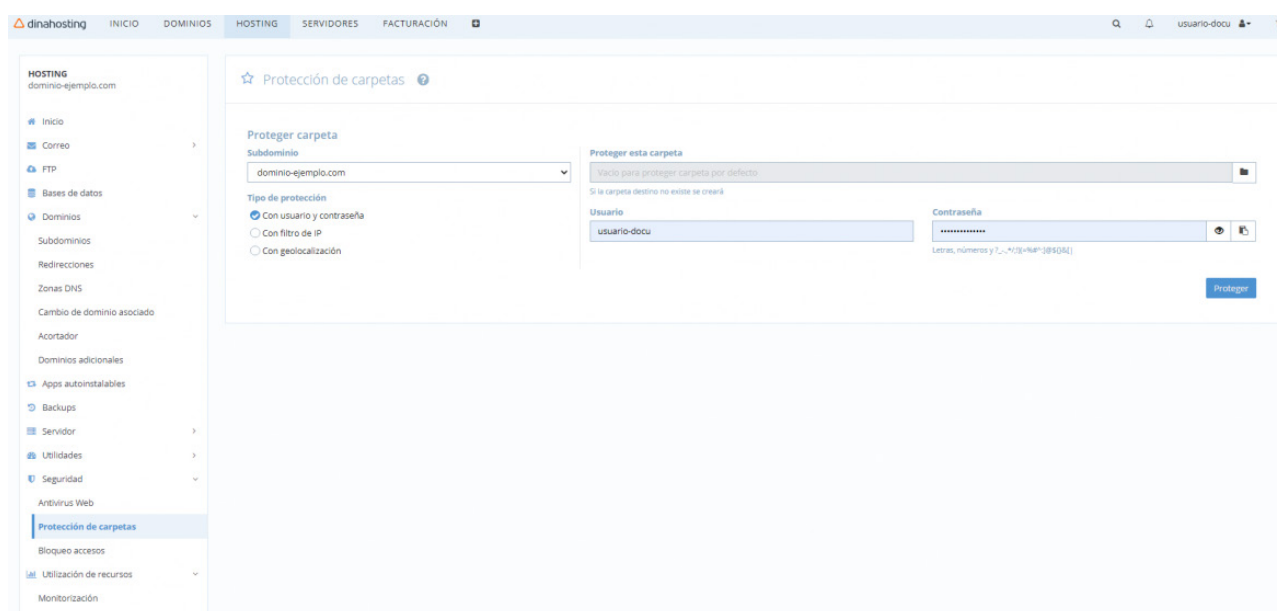
También puede darse el caso de que el servidor esté aplicando alguna **restricción por seguridad**.

Para revisar esta configuración en dinahosting tienes que acceder al apartado Seguridad del [Panel](#) de tu hosting.

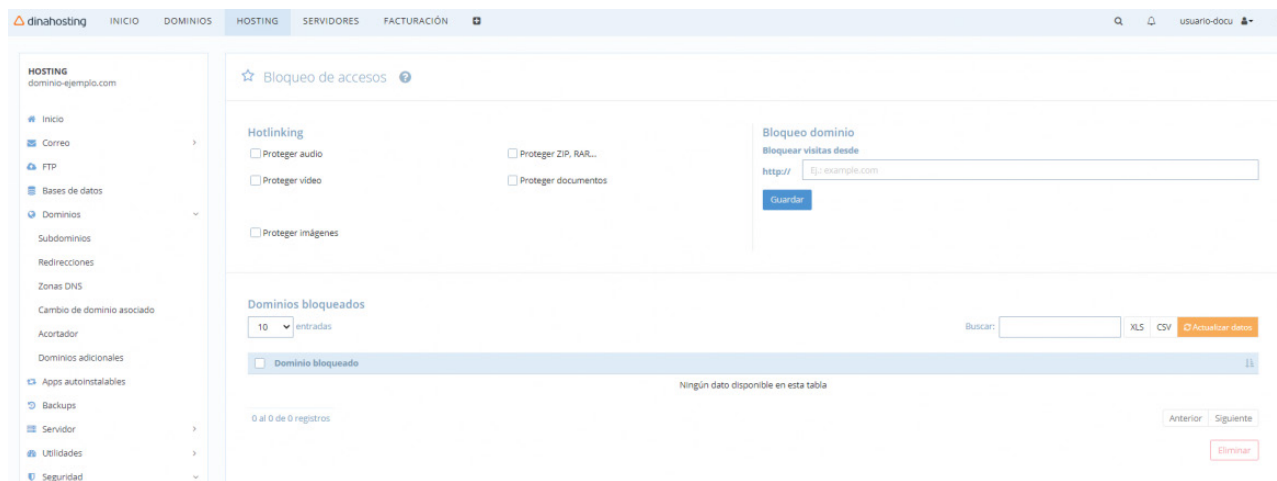
Dentro de las pestañas **Protección de carpetas** puedes establecer diferentes reglas y filtros para proteger y controlar los visitantes de las diferentes carpetas de tu web:

- Con usuario y contraseña
- Con filtro de IP
- Con geolocalización

Cuando proteges una carpeta con un filtro de seguridad también estás limitando el acceso a ella desde la propia web.



Otra restricción que también podría afectar al acceso de algunos usuarios y provocar el Error 403 es la que puedes establecer desde el apartado Seguridad > **Bloqueo de Accesos**.

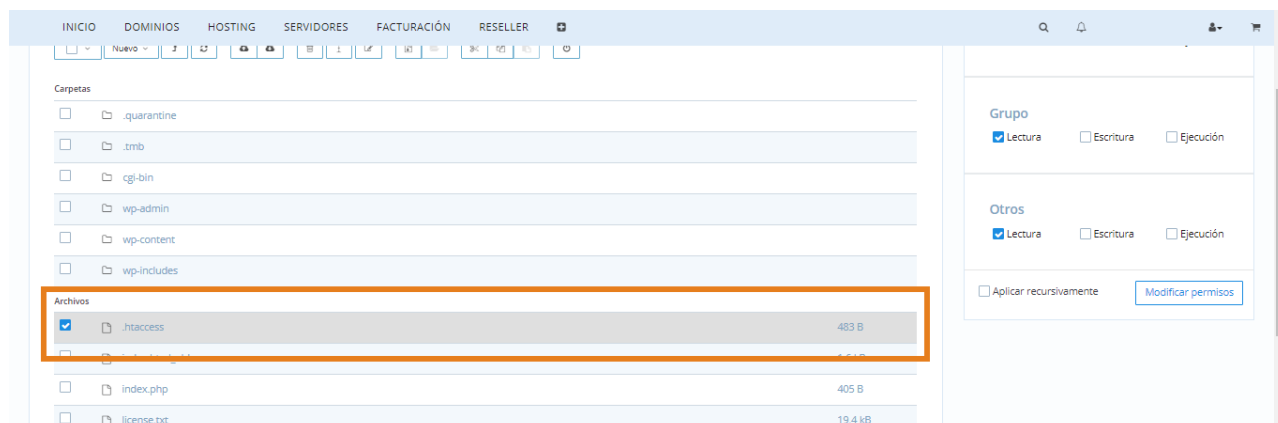


Desde este apartado es posible bloquear determinados dominios para que no puedan acceder a tu página, o también, imposibilitar que determinadas personas enlacen en su web el contenido de la tuya, estableciendo el bloqueo de diferentes formatos tipo: imágenes, vídeo, audio, documentos, etc.

Archivo .htaccess

También es muy común que el error se dé por algún **conflicto con el archivo .htaccess**, sobre todo si estás trabajando con un CMS. Veamos cómo detectarlo y solucionarlo.

Entra en tu Panel de Control y busca en el explorador de archivos dentro de tu carpeta www tu archivo .htaccess. Descárgate una copia de seguridad y borra el archivo de tu página web.



Vuelve a entrar al URL de tu web para comprobar que ya no sale el error 403. Si es así, era que derivaba de una mala configuración del .htaccess.

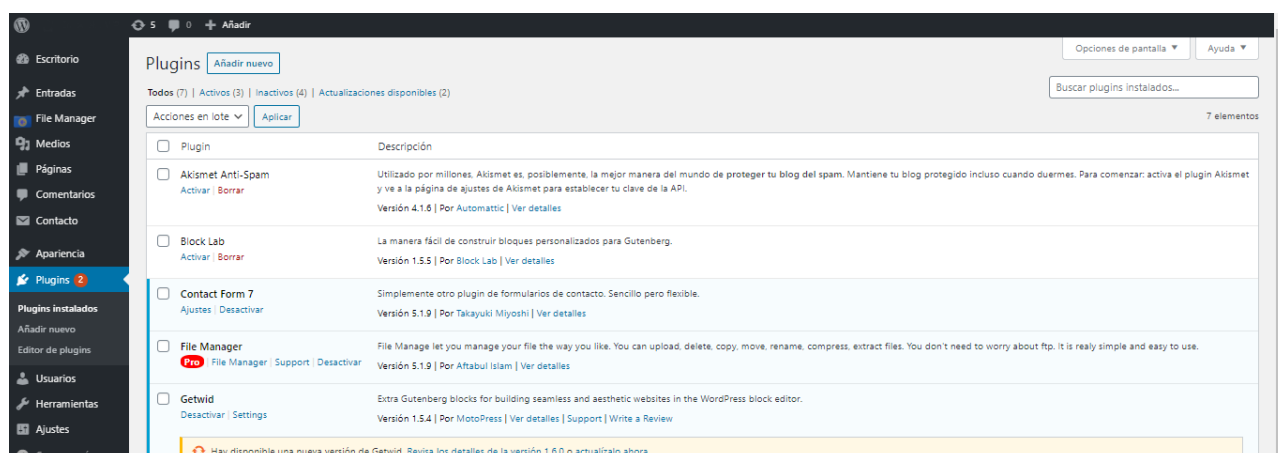
Si tu página va sobre WordPress y lo que quieres es volver a **generar un nuevo archivo .htaccess** los pasos a seguir son muy sencillos:

- Entra en la interfaz de administración de tu WordPress
- Ve a Ajustes > Enlaces permanentes
- Pulsa el botón Guardar cambios sin hacer ninguna modificación

Así ya habrás generado un nuevo archivo .htaccess para tu página web.

Plugins

Si tu página funciona sobre WordPress o algún otro CMS comprueba que el error no derive de ninguno de los plugins instalados en el mismo. En muchas ocasiones las actualizaciones de los plugins dan problemas de seguridad.



La forma más sencilla de detectar incidencias con los plugins es desactivarlos todos e ir activándolos uno a uno comprobando que no sale el error. En el momento en que vuelva a aparecer el 403 ya habrás detectado el plugin que te genera el conflicto.

Si se trata de uno de seguridad, deberás revisar en su configuración si se está bloqueando o restringiendo alguna IP o URL que no debería. Y si no encuentras solución siempre cabe la posibilidad de desinstalarlo y probar uno nuevo.

Desactivar la CDN

Si el error 403 se produce en las URLs de los archivos que forman tu página (imágenes, hojas de estilo, JavaScript...) es posible que el error esté relacionado con la CDN. Aquí te contamos [qué son las CDN y para que se utilizan](#).

Es por eso que si utilizas CDN como CloudFlare o similar, para asegurarte de que el error no proviene de ahí deberás probar a desactivarla momentáneamente y a acceder a tu página de nuevo para ver si continúa saliendo el 403.

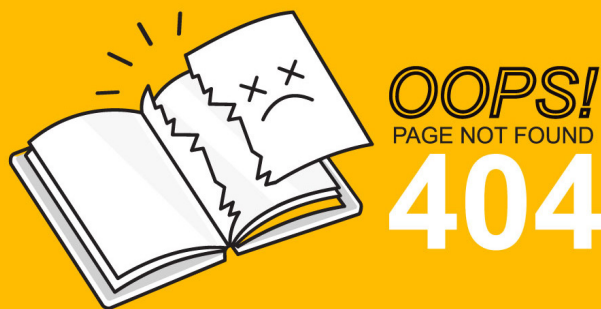
En caso de ser la causa del error te recomendamos cambiar las DNS asociadas o contactar con el servicio CDN que tengas activo.

Si después de todas estas comprobaciones todavía no has resuelto el error, recuerda que **nuestro departamento de Soporte** estará encantado de echarte una mano las 24 horas del día. ¡Llámanos gratis o escríbenos por chat o email!



SERVICIO DE ASESORÍA TÉCNICA

*Contrata nuestros servicios de seguridad
Mantenemos tu hosting libre de malware*



4.3

HTTP ERROR 404: ¿QUÉ ES? ¿CÓMO LO SOLUCIONO?

El error 404 o “not found” es sin duda uno de los errores HTTP más habituales que puedes encontrarte en tu web. Se produce cuando un usuario hace clic en algún link de tu página, pero el servidor no consigue encontrarla para mostrársela.



Si quieres saber más
Mira el vídeo

Cómo solucionar un error 404
en el acceso a tu WordPress

Puede que ese contenido lo hayas trasladado a otro apartado de tu web y te hayas olvidado de redireccionarlo, o que el enlace esté roto porque lleva a una página que ya no es válida. El caso es que en ese momento lo más probable es que ese usuario abandone tu web con un mal sabor de boca.

Además, los errores 404 no solo afectan negativamente a la experiencia de navegación de los usuarios de tu web, sino también a su posicionamiento SEO. En el momento en el que la araña de Google rastree tu web y detecte que haya códigos 404 te penalizará.

Para evitarlo, veamos al detalle en qué consiste el error 404 y cómo puedes solucionarlo.

¿Cuándo se produce el error 404?

Como te hemos adelantado al principio, el error 404 surge **cuando el servidor no consigue entregar la petición realizada por el navegador web**.

Puede que la persona haya tecleado mal la URL. Aunque caiga de cajón, es algo habitual. En este caso no estaría en tu mano solucionar el error, pero sí podrías aprovechar para enseñarle una página personalizada con contenidos que te interesen para mantener su atención y que continúe navegando por otras secciones de tu web. Un poco más abajo te hablaremos de cómo crear una página de error 404 atractiva.

Si la URL no está mal escrita, puede que el error 404 surja porque **te has olvidado de hacer alguna redirección de contenido**, es decir, de redirigir el tráfico que llegue a una determinada página de tu web a otra distinta a la que hayas llevado ese contenido. Desde tu Panel de Control de dinahosting puedes hacer todos los [tipos de redirecciones](#) que necesites.

¿Será que **el enlace ya no existe**? También puede ser. Imagínate que en algún post de blog antiguo incluyen un link a un producto tuyo que ya has dejado de desarrollar. En ese caso, la página arrojaría un error 404.

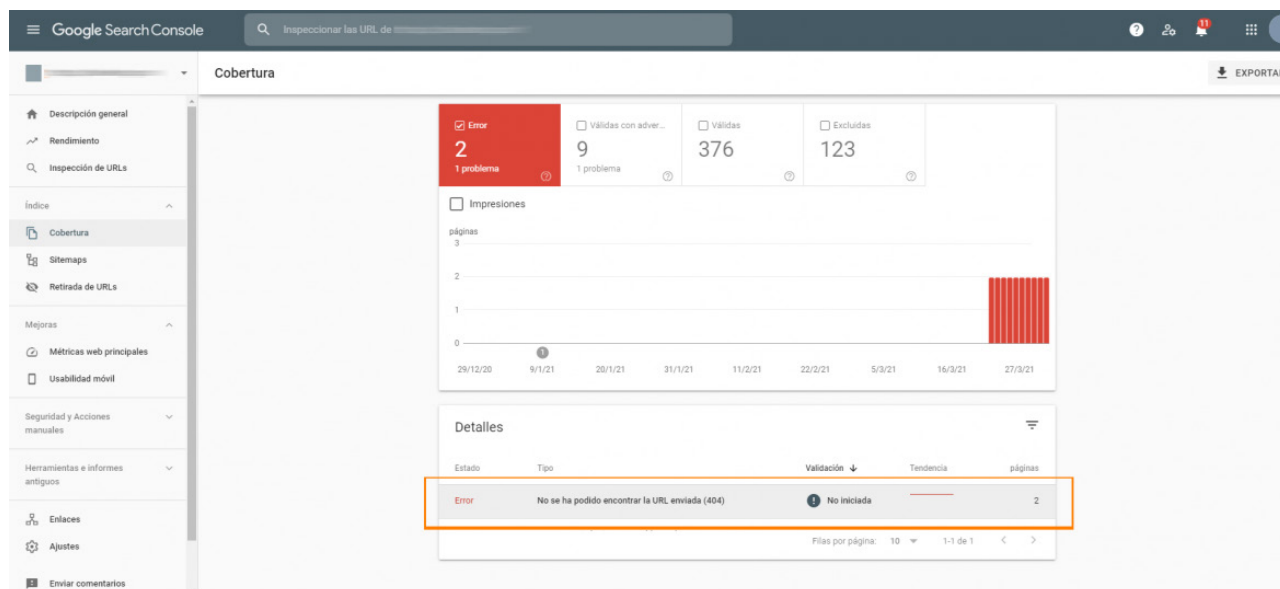
¿Cómo puedo saber si tengo algún error 404 en mi web?

Es muy probable que en el algún momento tengas algún error 404 en tu web y no lo sepas. Por eso, es conveniente que cada cierto tiempo hagas un trabajo de revisión que te permita mantener tu web optimizada.

¿Cómo tener localizadas las páginas con errores? **Ayudándote de [Google Search Console](#)**.

Google Search Console es una herramienta gratuita desarrollada por el propio Google, mediante la que puedes revisar que el contenido que indexa es el que a ti de verdad te interesa.

En el apartado Cobertura de Search Console tienes acceso a todas las URL que ha rastreado y la explicación de por qué están o no indexadas. En caso de que el motivo de que una página no esté indexada sea porque tiene algún tipo de error HTTP, te aparecerá especificado para que puedas corregirlo.



Error 404 en Search Console

Otras **herramientas gratuitas con las que puedes detectar errores** en tus URL son las siguientes:

- [Dead link checker](#)
- [W3C Link checker](#)
- [Broken Link Checker](#)
- [Dr. Link Check](#)

En cualquiera de ellas solo tienes que introducir tu dominio y **te devuelven el estado de todas sus URL avisándote de si hay algún error**.

Si utilizas WordPress para tu web, también puedes probar a analizar tus páginas con alguno de estos **plugins gratuitos**:

- [Broken Link Checker](#)
- [Link Checker](#)
- [Link Whisper Free](#)

Una vez que hayas analizado tus URL y localizado el error 404, ahora toca el siguiente paso, corregirlo.

Cómo solucionar un error 404

Según el tipo de error 404 que hayas detectado deberás aplicar las siguientes soluciones:

Enlace hacia página externa que no existe

Si el error es debido a que tienes un enlace en tu página que apunta a una URL externa que no existe, **comprueba si ha cambiado esta URL para actualizarla o directamente elimina el enlace de tu web**.

Enlace que no existe en tu propia página

Si por ejemplo, tienes un producto que ya no vendes es posible que la URL se haya quedado linkada por algún lado o los usuarios sigan accediendo a ella aunque ya no la tengas publicada.

En estos casos lo habitual es hacer una redirección 301 hacia una página similar o hacia el index. Esta solución es recomendable si la URL tenía bastante tráfico y quieres que esos usuarios permanezcan en tu web.

Si por el contrario lo que quieres es que esa URL no aparezca por ningún lado la solución será aplicar un **error 410 o Redirect Gone**. Este código le indica a los rastreadores que la página ya no existe de forma indefinida.

Enlace hacia URL que ha cambiado

Si has modificado una URL deberás corregir todos tus enlaces hacia la nueva dirección o, al igual que en el caso anterior, realizar una redirección 301.

Soluciones al error 404

Redirecciones 301

Las redirecciones 301 son un tipo de comando que indica de forma permanente que una página se ha cambiado por otra. Su principal ventaja es que con este tipo de redirección se mantiene casi intacto el posicionamiento anterior al cambio de URL.

Puedes aplicar redirecciones 301 de diferentes formas:

301 a través del htaccess

Para ello debes modificar el archivo .htaccess de tu web incluyendo el siguiente código con la nueva URL:

```
redirectMatch 301 ^(.*)$ http://nuevaURL.com$1
```

En este post te damos más detalles sobre [cómo hacer una redirección 301 desde htaccess](#).

301 desde tu Panel de Control

En dinahosting puedes aplicar también redirecciones 301 a toda tu web o a un subdominio de forma sencilla desde tu Panel.

Crear redirección

Quiero... ☒ Una redirección web ☐ Acortar una URL

Para... ☐ Un solo subdominio ☒ Toda la web

Tipo de redirección:

Redirigir a:

* Las redirecciones de correo deben realizarse desde el Panel del Hosting.

Listado de redirecciones

10 entradas

Tipo	Subtipo	Origen	Destino
ACORTADOR	n/a	http://dominio-ejemplo.com/s/1gb/2h (0 clics)	https://dominio-ejemplo.com/carpetas/catalogo/2020/catalogo/7634g.pdf
ACORTADOR	n/a	http://dominio-ejemplo.com/s/1gb/2h (0 clics)	https://dominio-ejemplo.com/carpetas/catalogo/2020/catalogo/7634g.pdf

1 al 2 de 2 registros

Accedes a Dominio > Redirecciones, selecciona si URL 301 e introduces la nueva dirección a la que quieres redirigir. Aquí te contamos más sobre [cómo redireccionar un dominio desde tu Panel](#).

301 mediante plugins de WordPress

Si tienes tu web montada en WordPress otra opción además de las anteriores es hacer la redirección 301 mediante un plugin. Estos son algunos de los más utilizados para esta función:

- [Redirection](#)
- [Simple 301 Redirects](#)
- [404 to 301](#)

Todos son gratuitos y muy sencillos de utilizar :)

Error 410 o Redirect Gone

Como ya te contamos más arriba, este código tiene como función indicar a las arañas o rastreadores que una página ya no existe.

Utilízalo solo cuándo estés seguro de que no vas a volver a esa URL y que esta no se está linkando desde ningún otro sitio.

Suele ser habitual su uso cuando has creado una página por error o la URL está totalmente obsoleta

410 desde .htaccess

Para aplicar este tipo de error debes editar el archivo .htaccess incluyendo el siguiente código y la URL que quieras marcar:

```
Redirect Gone /URL
```

410 desde un plugin de WordPress

Al igual que en las redirecciones 301, también puedes activar el error 410 para una determinada URL utilizando alguno de estos plugins:

[Redirection](#) (este plugin sirve para diferentes tipos de redirecciones)

[410 for WordPress](#)

[Ultimate 410 Gone Status Code](#)

Desindexar una URL antigua

¿Has realizado todos estos pasos pero tu URL obsoleta sigue apareciendo en los resultados de Google? **Comprueba en la Search Console el estado de indexación de esa página** desde la herramienta Inspección de URLs. Si tu URL antigua todavía aparece indexada puedes solicitar que la eliminen desde la herramienta Retirada de URLs.

Ten en cuenta que las arañas de Google tardan un tiempo en reindexar las páginas y que si ya has redireccionado correctamente tu web con un 301 el cambio debería reflejarse en los resultados a corto/medio plazo.

Te recomendamos que utilices esta herramienta solo si tienes urgencia en retirar el contenido indexado, bien porque sea erróneo o por cualquier otro motivo.

Cómo personalizar la página de error 404

Ninguna web es perfecta. Aunque apliquemos todas estas buenas prácticas, tener algún error 404 puntualmente es de lo más habitual. Por eso, antes de dar por terminado el diseño y desarrollo de tu página web **es importantísimo que hayas creado y personalizado la página a la que llegarán tus usuarios en caso de que el error 404 se produzca.**

Si tu web funciona sobre WordPress es probable que el tema que estás utilizando incluya ya un diseño de este tipo, pero si se trata de un desarrollo a medida tendrás que acordarte de implementarlo.

Anteriormente te hemos dado algunos trucos para [construir una página de error 404 perfecta](#). Si hacemos un repaso rápido, lo mínimo que tienes que incluir para evitar que el usuario abandone definitivamente tu sitio web es:

- **Tu imagen de marca** (colores, tipografía, etc.), para que sienta que sigue dentro de tu web, a pesar de que el contenido que buscaba no se ha mostrado.
- **Links en los que pueda clicar para visitar otras partes de tu web.** Puedes redirigirlo al Inicio/Home de la web, o cualquier otra sección que te interese potenciar.

Luego es cuestión de dejar volar la imaginación: incluir algún descuento, gamificar la página, jugar con el humor...

Te recordamos que en tu Panel de Control de dinahosting te lo ponemos fácil a la hora de habilitar tu página de error 404.

Accede al Hosting que te interese, y en el menú de la izquierda haz clic en Servidor > Personalización. Tan solo tendrías que seleccionar entre las opciones del desplegable el tipo de error que quieras (en este caso, el 404), e introducir la URL personalizada a la que quieres redireccionar a tu usuario en caso de que se produzca. Aquí te explicamos al detalle [cómo sacarle todo el partido a esta sección](#).



EL MEJOR SOPORTE 24/7

Esríbenos por email, chat o llámanos gratis al 900 854 000

Simpre disponibles 24x7x365

Hablamos tu idioma

ERROR

500

HTTP Version not supported



4.4 HTTP ERROR 500. QUÉ ES Y CÓMO SOLUCIONARLO EN TU WEB

El HTTP Error 500 es uno de los códigos de estado HTTP más habituales y nos indica que alguna petición a nuestro servidor ha generado errores.

Si en tu web ha aparecido un error 500, ¡no te preocupes! Es un muy común y a continuación te vamos a explicar como puedes solucionarlo en tu página:

¿Qué es el error 500?

El error 500 es un código de estado que indica que se ha producido un fallo en el servidor de la web. Es uno de los errores HTTP más habituales por eso es frecuente que te lo encuentres navegando por la red.

Puede aparecerte en pantalla de diversas formas, algunas de las más comunes son:

- HTTP 500 – Internal Server Error
- 500 Internal Server Error
- Temporary Error (500)
- 500 Error
- 500. That's an error.

Como todos los códigos de estado HTTP 5XX indica un error en el servidor, pero en este caso la causa no está clara. Es por eso que deberás probar diferentes métodos para saber a qué es debido y cómo solucionarlo.

¿Por qué se produce el Error 500?

El error 500 puede producirse por fallas en el proxy, servidor o página web. Debido a este fallo tu web no estará disponible para tus clientes y visitantes y de producirse de forma recurrente podrías ver afectado tu posicionamiento SEO en Google. Por ello es esencial que detectes las causas que pueden provocar el HTTP Error 500, entre las que se encuentran:

- El servidor no es compatible con alguna característica a la hora de responder a la solicitud del navegador.
- Se ha consumido el tiempo de espera sin obtener respuesta.
- alguna de las configuraciones del servidor web son erróneas como por ejemplo archivos .htaccess o archivos de reescritura de Nginx entre otros.
- Has consumido el límite de la memoria PHP de tu web.
- Se están realizando tareas de mantenimiento o actualizaciones en tu servidor.
- Puede que haya carpetas de tu Hosting, WordPress o PrestaShop que estén dañadas.
- La configuración de permisos de las carpetas de tu alojamiento está generando errores.
- No se ha realizado correctamente la actualización que has hecho de un tema o plantilla.
- Has instalado algún plugin que está generando fallos.
- El servidor se encuentra saturado por un elevado consumo.

Cómo detectar el error 500

Mediante el archivo error_log

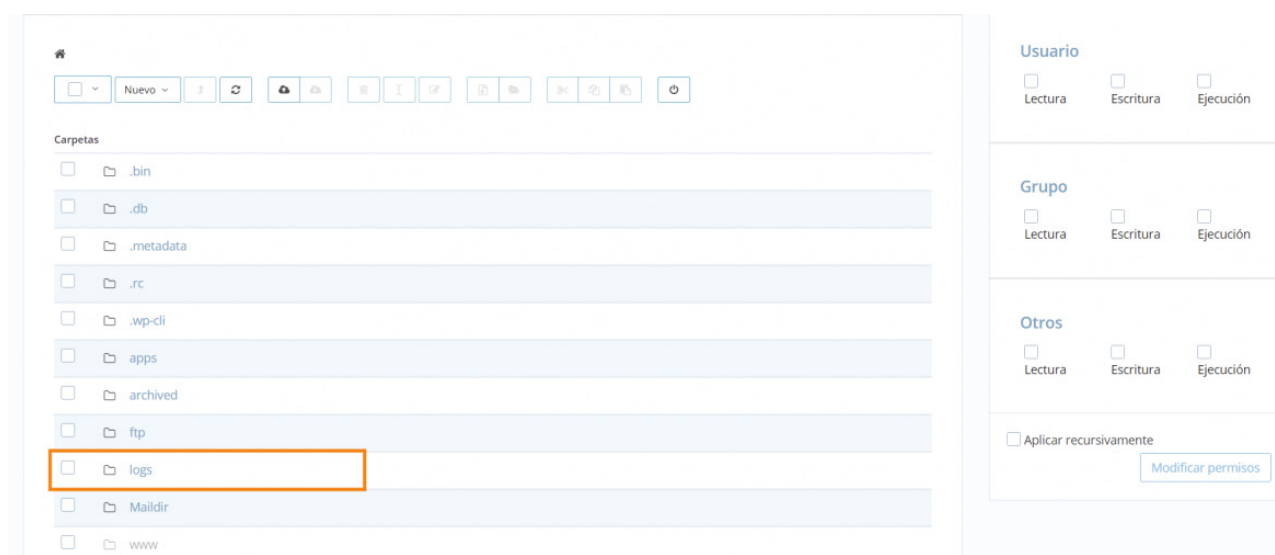
En tu hosting o en tu CMS normalmente puedes registrar los errores en un archivo llamado `php_errorlog`, `error_log` o similar.

En el caso de que hayan producido, en este achivo figurará un listado de errores con la fecha y el código de error. Lo que es muy útil para detectar el error 500 u otros tipos.

Habitualmente puedes localizar este archivo de error en la carpeta de logs.

Desde el Panel lo puedes encontrar con el Explorador de ficheros en Hosting > FTP, accediendo a la carpeta logs y descargándotelo. Para consultarlo puedes abrirlo con un el Bloc de notas u cualquier otro programa compatible.

Dentro de tu hosting también puedes localizar en la misma ruta Hosting > FTP > Explorador de ficheros la carpeta logs. Accediendo a ella puedes comprobar los errores que se han producido en tu web.



Panel dinahosting carpeta logs http error 500

Otra opción para acceder al registro de errores de tu servidor es creando un fichero `phpinfo.php` que incorpore este código:

```
<?php
phpinfo();
?>
```

Ahora debes subir este archivo a la carpeta raíz o `public_html` de tu hosting. Después accede a él escribiendo esta ruta en el navegador `www.tudireccionweb.tudominio/phpinfo.php` y dentro del contenido verás el texto `error_log`.

Mediante un plugin de WordPress

Como sabes en WordPress existen plugins para todo. Y por supuesto para detectar los errores PHP.

Uno de los más conocidos es [Error Log Monitor](#). Este plugin activa una ventana en el Escritorio o Dashboard de tu WordPress donde puedes consultar directamente los errores.

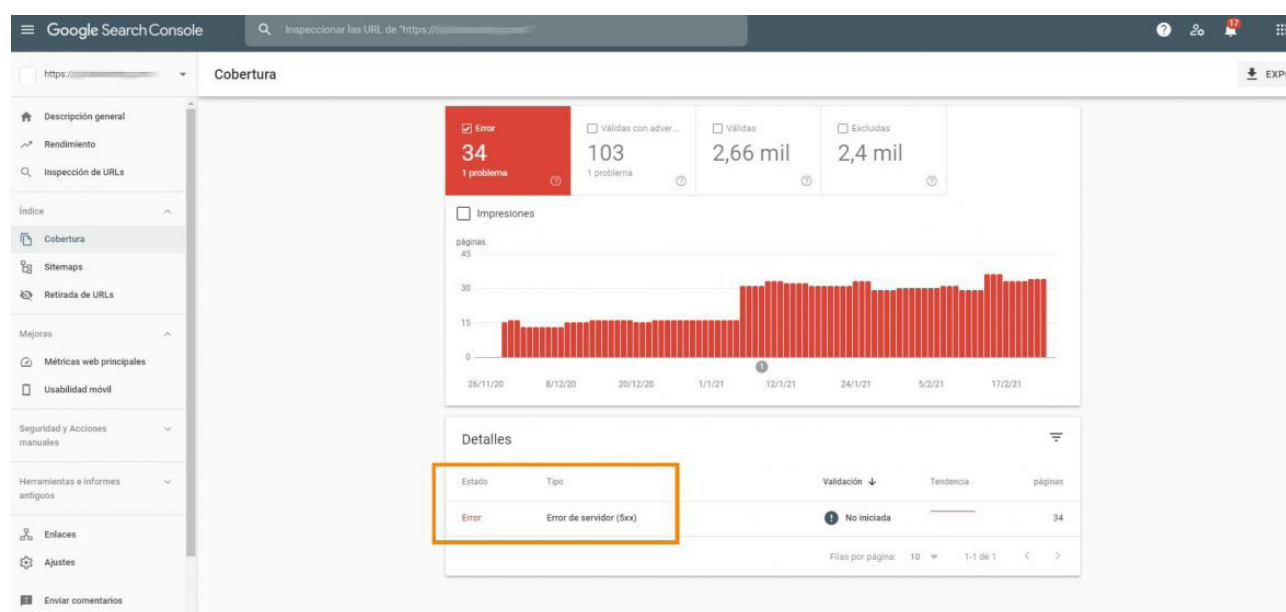
Otro plugin que puedes utilizar en WordPress para detectar el error 500 es el [Plugin Detective](#). Su uso es muy intuitivo,

ya que a través de su asistente te va realizando preguntas hasta dar con la causa del error. Muy recomendable para usuarios con conocimientos básicos.

Por último, [Fatal Error Notify](#) es un plugin que te permite configurar notificaciones por correo para avisarte cada vez que se produzca un error en tu web. Su principal ventaja es que puedes configurar qué tipo de avisos o errores quieres recibir y así enterarte al momento y actuar lo antes posible para corregirlo.

Mediante Google Search Console

[Google Search Console](#) dispone de una herramienta llamada Cobertura donde puedes analizar los errores que suceden en tu página y las URL afectadas.



Accediendo a Índice > Cobertura para abrir la gráfica con el informe de errores. En la tabla, clicando sobre el aviso de error te aparecerá un listado con los enlaces que han fallado y las fechas en las que se produjo el error.

¿Quieres saber más sobre Google Search Console? Échale un ojo a [este post](#).

Cómo solucionar un HTTP Error 500 externo

Si estamos accediendo a una web que no es nuestra, para solventar el error 500 te recomendamos que primeramente pruebes a **recargar la página** y esperar un tiempo hasta que se solucione.

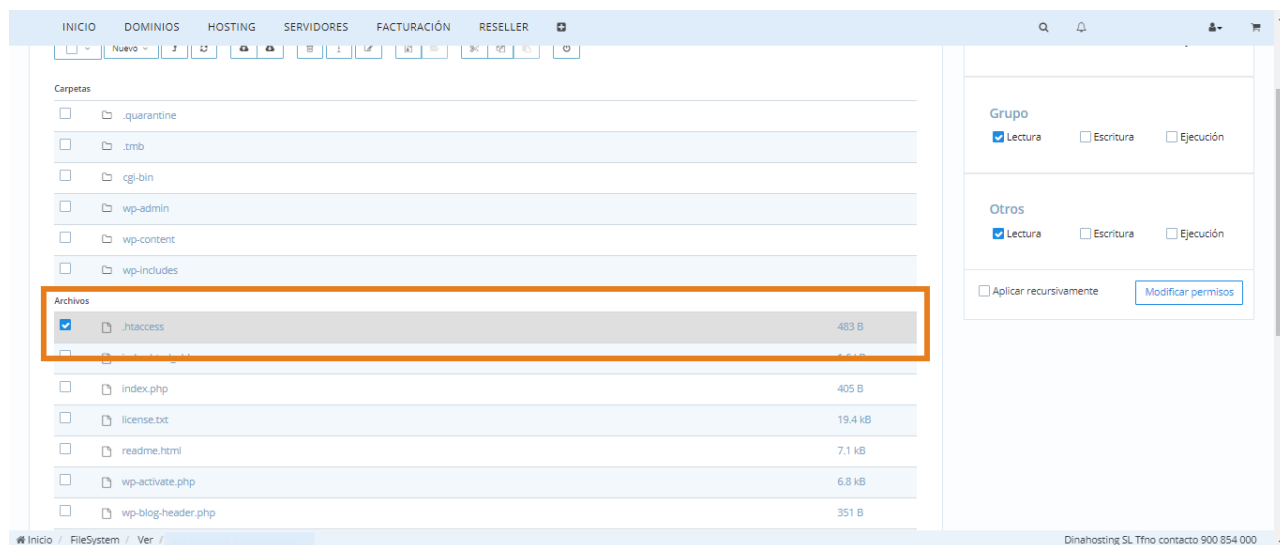
Si sigue persistiendo **borra la caché del navegador** porque puede que te esté mostrando un HTTP 500 – Internal Server Error que lleva tiempo almacenado en tu navegador. También puede deberse a las **cookies** que tienes guardadas. Bórralas y recarga nuevamente.

Cómo solucionar un HTTP Error 500 en nuestra web

Antes de proceder a realizar estas comprobaciones o cualquier tipo de modificación en tu web para corregir el error 500 te recomendamos que realices una copia de seguridad de tu sitio o de los archivos que vayas a modificar. ¡Más vale prevenir!

Error en el archivo .htaccess

Una de las causas más comunes puede deberse a que **el error está en el archivo .htaccess**. En nuestro [Panel](#) solo tienes que entrar en Hosting > FTP > Explorador de ficheros. Selecciona la cuenta que te interesa, abre el explorador de ficheros y accede a la carpeta www para revisarlo.



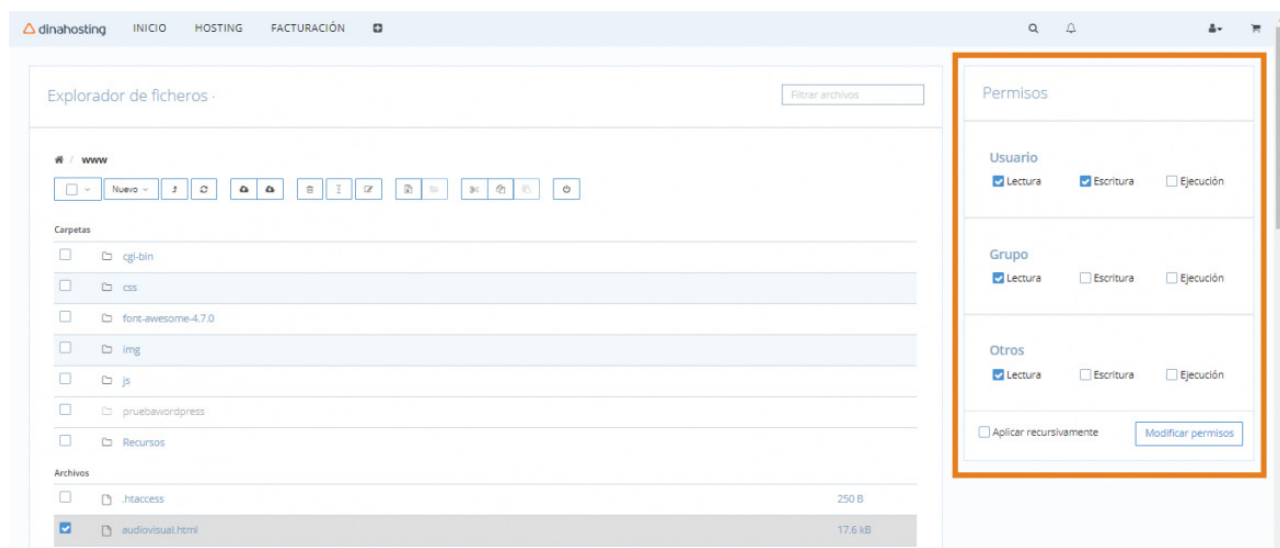
Te recomendamos hacer una copia de seguridad antes de manipular el archivo .htaccess. En este post tienes más información del [archivo .htaccess en tu WordPress](#).

Un fallo de permisos

En muchas ocasiones un error 500 viene provocado por no disponer de los **permisos suficientes para acceder a la carpeta o archivos**, por lo que el servidor bloquea el acceso.

Desde el [Panel](#) de dinahosting accede a Hosting > FTP > Explorador de ficheros y comprueba que todos los ficheros de tu hosting tengan permisos de lectura. Puedes seleccionar la opción Aplicar recursivamente para no ir uno a uno modificando los permisos.

Vuelve a recargar la página, y si ya funciona este era el problema.

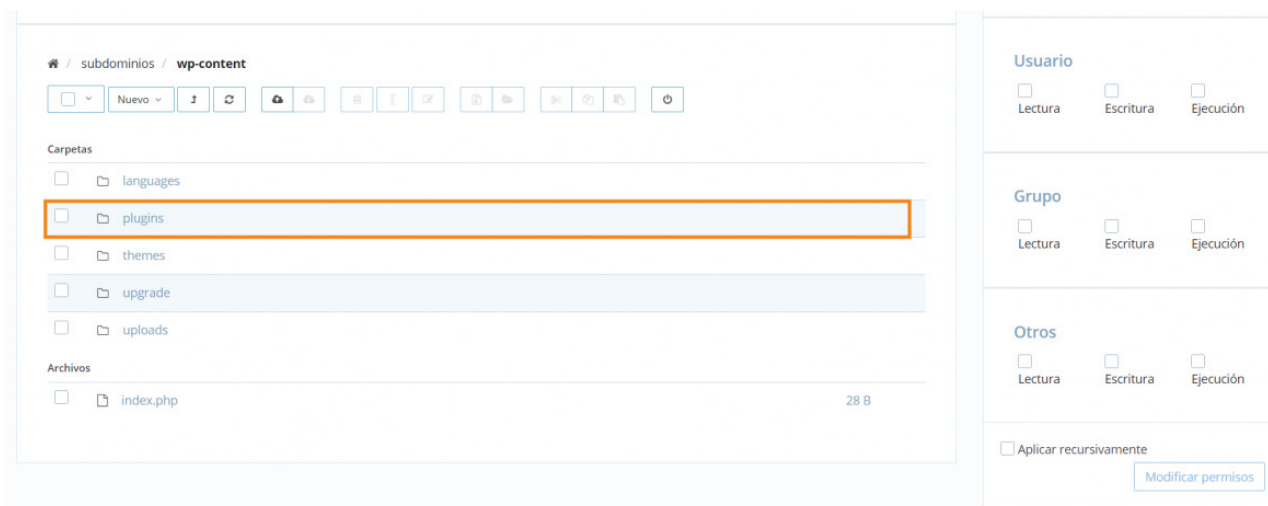


Permisos de lectura dentro de tu Panel de Control de dinahosting

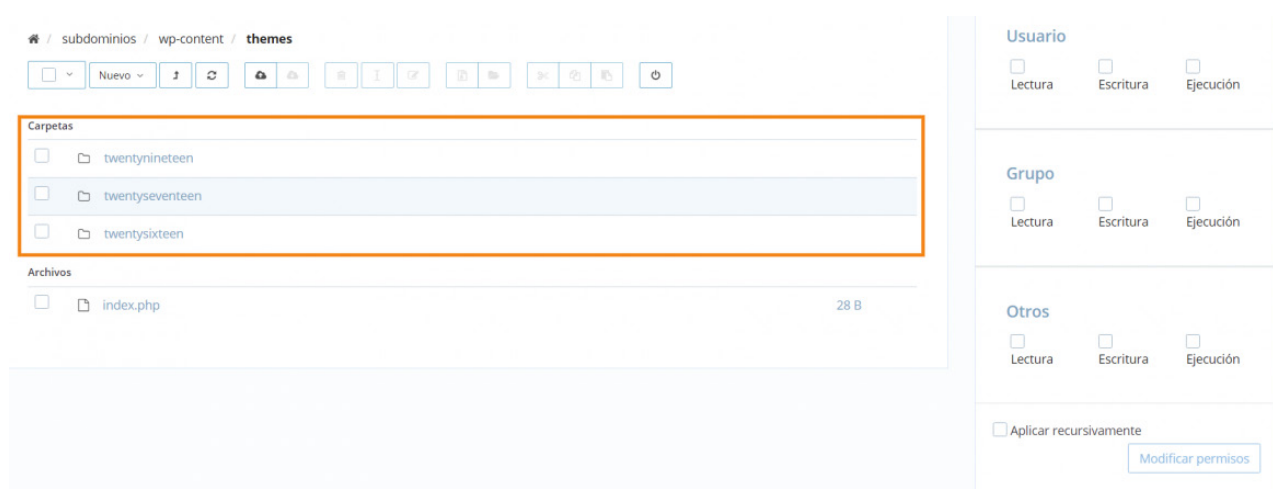
Plugins y temas instalados en nuestro WordPress

Si has experimentado errores mientras instalabas un **plugin**, lo mejor que puedes hacer es desinstalarlo de tu hosting.

Si no sabes cuál es plugin que está haciendo que tengas un HTTP Error 500 en tu web accede desde tu Panel a Hosting > FTP > Explorador de ficheros y localiza la carpeta de plugins disponible en wp-content. Puedes desactivar uno de cada vez para comprobar así que la web ya no da errores.



Si el error lo produce el tema de tu WordPress, sigue los mismos pasos y accede a la carpeta Themes de tu Hosting. Cada carpeta que tengas ahí es un tema que tienes instalado.



Alguna carpeta en nuestro WordPress está dañada

Puede que alguna carpeta esté dañada. Para solventar este error **descarga la última versión de tu WordPress** en un ZIP. Entra en Hosting > FTP > Explorador de ficheros y sustituye las carpetas wp-admin y wp-includes por las nuevas. Guarda y comprueba de nuevo que el error 500 está solucionado.

Has superado el límite de memoria del servidor

Puede que hayas superado el límite de memoria del servidor y este devuelva un HTTP Error 500. Puedes aumentar este límite añadiendo este código a tu archivo wp-config, entrando en Hosting > FTP > Explorador de ficheros.

Por ejemplo:

```
define('WP_MEMORY_LIMIT', '256MB')
```

INICIO	DOMINIOS	HOSTING	SERVIDORES	FACTURACIÓN	RESELLER	+
☐		readme.html				7.3 kB
☐		wp-activate.php				6.8 kB
☐		wp-blog-header.php				369 B
☐		wp-comments-post.php				2.2 kB
☐		wp-config-sample.php				2.8 kB
☐		wp-config.php				3 kB
☐		wp-cron.php				3.8 kB
☐		wp-links-opml.php				2.4 kB
☐		wp-load.php				3.2 kB

Recuerda que antes de editar cualquiera de las carpetas, haz una copia de seguridad descargando previamente el contenido para evitar sorpresas.

De esta forma puedes aumentar los límites de memoria de tu WordPress, pero ten en cuenta que para **que funcione correctamente el límite de memoria PHP establecido por el servidor debe ser superior**.

En dinahosting te damos la opción de aumentar los límites de memoria PHP durante 1 hora. De esta forma puedes editarlos y comprobar si el error viene de ahí.

Puedes modificarlos desde el panel de tu hosting en Servidor > PHP.

Si el problema persiste y necesitas más memoria por tiempo ilimitado, entonces será necesario que te pases a un [plan de hosting superior](#) para solucionarlo.

502 Bad Gateway

4.5

QUÉ ES UN ERROR 502 Y CÓMO SOLUCIONARLO

El error 502 es uno de los más habituales que te puedes encontrar navegando por la red, por lo que lo más probable es que en algún momento también afecte a tu página.

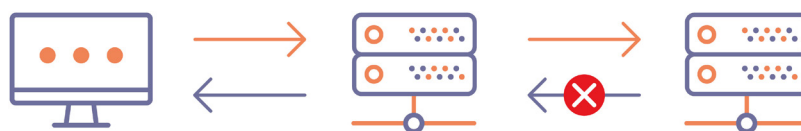
¡Que no cunda el pánico! En este post te explicamos por qué se produce y cómo puedes solucionarlo.

¿Qué es el error 502?

Lo primero que tienes que saber es que el error 502 puede mostrarse en tu navegador de diferentes maneras según el tipo de servidor: "Error 502", "502 Bad Gateway" o "502 Server Error: the server encountered a temporary error and could not complete your request" son algunas de las más comunes.

Como ya te adelantamos antes, **los códigos de estado que empiezan por 5 indican un error del servidor**. Esto significa que puede que algún servicio esté caído o que por algún tipo de fallo interno el servidor no pueda procesar la solicitud.

En concreto el error 502 indica que el **servidor de origen no se está comunicando con el servidor de enlace** (gateway) debido a que ha recibido una respuesta no válida, o a que directamente no ha recibido ninguna respuesta.



Algunas de las **causas más comunes** por las que puede producirse este error son:

- El servidor está fuera de servicio o caído por una sobrecarga
- Un firewall está bloqueando la solicitud
- Error en el código de la web
- Diferentes protocolos o configuración
- Demasiado tiempo de espera entre peticiones
- Problemas con la CDN
- Problemas con el navegador: tienes el error guardado en caché

Cómo solucionar el error 502

Te resumimos las causas más comunes por las que se produce el error 502 y las formas mediante las que puedes corregirlo si está en tu mano.

Las peticiones al servidor pasan por múltiples puertas de enlace, y por este motivo suele ser complicado, que no imposible, encontrar el punto exacto donde se produce el error.

Lo fundamental es ir haciendo pruebas y descartando opciones.

1. Actualiza tu página

Seguro que te suena lo de “¿Has probado a apagar y volver a encender?”. Pues en este caso lo mismo. Es habitual que el error 502 sea temporal, por lo que antes de realizar cualquier otra acción, **espera unos minutos y refresca la página pulsando Ctrl+F5**.

Si el error persiste, **borra la caché y vuelve a actualizar**, o prueba a acceder a tu web en modo incógnito. Así te aseguras de que no haya guardada una versión con el error en el caché almacenado en el navegador.

Es importante borrar la caché de tu navegador de vez en cuando para optimizar su funcionamiento y evitar errores web. En este contenido anterior te contamos [Cómo y por qué borrar la caché en Chrome, Firefox y Safari](#).

2. Prueba en un navegador diferente o en otro dispositivo

Segundo paso. Prueba a entrar desde cualquier otro dispositivo que tengas a mano: otro ordenador, un teléfono móvil, una tablet... Si puedes, inténtalo desde una IP diferente, así puedes descartar que el error está en tu equipo.

Otra opción saber si tu web está caída (para ti o para todo el mundo) es que la analices con alguna herramienta online, como pueden ser [Is It Down Right Now?](#) o [Down for everyone or just for me](#).

Lo mismo con el navegador, prueba a acceder desde Chrome, Mozilla Firefox, Safari...o cualquier otro explorador diferente del que utilices habitualmente.

Si el error no se reproduce en otros navegadores te recomendamos actualizar o reinstalar el navegador que falla para evitar así que vuelva a salirte un 502.

Si por el contrario, el error persiste en diferentes dispositivos y navegadores entonces prueba con las siguientes soluciones.

3. Comprueba los registros de errores

Si el error 502 aparece justo después de una modificación o actualización importante en la página, es muy posible que su origen esté ahí. Para asegurarte, puedes comprobar los registros en el archivo error.log de tu hosting.

En dinahosting puedes acceder a él mediante SSH, una herramienta que tienes disponible en el apartado Hosting > Utilidades > SSH de tu [Panel de Control](#). Verás que en la carpeta de logs de tu hosting cuentas con un fichero de accesos y otro de errores. En este caso tú tienes que seleccionar el segundo.

4. Limpia las DNS

Otra posible causa del error 502 es que el dominio puede no estar resolviendo correctamente la IP. Sobre todo si acabas de migrar tu página, pueden producirse errores en los valores de las DNS, lo que conllevaría de nuevo un error 502.

Para comprobar si es este el problema puedes **renovar la caché de tus DNS locales, lo que se conoce como “flush”**. Se realiza introduciendo la siguiente línea desde la consola del sistema:

- En Windows: `ipconfig /flushdns`
- En MacOS: `dscacheutil -flushcache`
- Y en Linux ejecutar el comando: `/etc/init.d/nscd restart`

¿Lo tienes? Comprueba ahora si el error continúa.

5. Desactiva plugins o temas

Si utilizas WordPress o algún otro CMS que utilice plugins, es posible que el error 502 sea debido a que alguno de ellos tenga algún conflicto que lo provoque.

Para descartar que sea esta la razón **prueba a desactivarlos uno por uno a la vez que vas refrescando la página**. Si la página vuelve a funcionar una vez hayas desactivado un plugin o tema, has encontrado al causante del error.

Para corregirlo deberás comprobar si el plugin está actualizado, si no es así activa su última versión y refresca la página para ver si se soluciona el error.

Es habitual también que algunos plugins dejen de funcionar pasado un tiempo, bien porque han quedado obsoletos o bien porque han dejado de desarrollarlos. En este caso la mejor opción será que lo desinstales y pruebes con otros plugins del repositorio.

6. Desactiva la CDN temporalmente

Una CDN (Content Delivery Network) o Red de Distribución de Contenido mejora mucho la velocidad de carga de las webs, pues ayuda a distribuir su contenido a lo largo del territorio reduciendo la latencia. Sin embargo, también puede provocar errores 502 debido a los firewalls de red que utiliza.

Si tienes alguna CDN activada, prueba a desactivarla momentáneamente para comprobar si el fallo viene de ahí.

¿Quieres saber más sobre las CDN? En este post te hacemos un repaso rápido sobre [qué son y cómo funcionan las CDN](#).

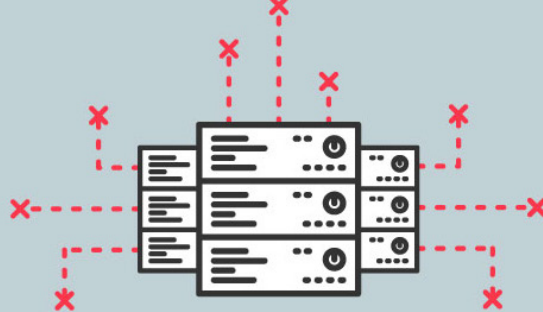
7. Contacta con Atención al Cliente

Si ninguno de los métodos anteriores funciona o si simplemente no tienes tiempo para hacer estas pruebas, lo mejor es que contactes con la proveedora que se encarga de gestionar el hosting en el que está alojada tu página.

En dinahosting contamos con un [equipo de Soporte Técnico disponible las 24 horas](#) del día, todos los días del año. Te atendemos a través del teléfono gratuito 900 854 000, del email o del chat. ¡Y por supuesto en tu idioma!

Como ves los errores 502 en muchos casos son sencillos de solucionar. Y **no es habitual que una web sufra habitualmente este tipo de errores**, si es tu caso igual deberías plantearte cambiar de proveedora.

Si quieres que el error 502 ocurra lo menos posible en tu página, lo mejor es que la alojes en un [hosting de confianza](#) que tenga una buena atención al cliente. ¡Llámanos o escríbenos y te asesoramos!



HTTP Error 503

4.6

¿QUÉ ES EL ERROR 503? CAUSAS Y SOLUCIONES

El error 503 indica que el servidor no puede atender momentáneamente las peticiones que le están llegando. Te detallamos qué es el error 503 junto con sus causas y posibles soluciones.

Aunque es menos frecuente que otros errores HTTP, es posible que te hayas encontrado más de una vez con un error 503.

En muchos casos basta con esperar y se arreglan solos, pero para los casos en que el problema persiste, te explicamos más detalladamente en qué consisten y las causas para que te sea más sencillo solucionarlos.

Código de estado 5XX

Los códigos de estado nos ayudan a entender mejor los diferentes fallos HTTP que pueden producirse en una web: 303, 403, 500...

El primer dígito de estos errores se corresponde con el código de estado y este **nos indica el tipo de error que se ha producido**. En el caso de los errores 503 su código de estado es el 5XX.

El código HTTP 5XX nos indica que el error proviene del servidor. Es decir, que por alguna razón las peticiones con el servidor no se están procesando.

¿Qué es el error 503 Service Unavailable?

El error 503 suele ir acompañado del texto Servicio No Disponible (Service Unavailable) y es una señal de que **el servidor está sobrecargado o por algún otro motivo no puede atender en el momento las peticiones** que se le están haciendo.

El **error 503 no es un problema**, es más bien un aviso. Por regla general se soluciona pasado un tiempo.

Si este error se repite de manera recurrente en tu web entonces es posible que tengas que realizar algún cambio en tu hosting o ponerte en contacto con tu proveedora.

Principales causas y soluciones

1. El servidor está en mantenimiento

Uno de las principales causas por las que se puede producir es debido a **tareas de mantenimiento**: actualizaciones del sistema, realización de backups, cambios en la configuración...

Algunas de estas acciones consumen bastantes recursos en el servidor, por lo que es posible que no puedas acceder a tu web momentáneamente.

Solución: espera unos minutos y vuelve a cargar la página. Por lo general, el error 503 se solventa pasados unos minutos. Si ves que el error se alarga y tus solicitudes se siguen rechazando entonces consulta con tu proveedora de hosting.

Ten en cuenta que si las tareas de mantenimiento son realizadas por tu proveedora o por un tercero, lo normal es que se hagan en horarios de poco tráfico y que te avisen por si hay posibles cortes. De ahí que sea tan importante contar con un proveedor de hosting de confianza ;)

2. Demasiadas visitas en tu web

También puede darse el error 503 si se produce un **gran número de visitas a la vez y tu hosting no está preparado**.

Es frecuente por ejemplo, si tu negocio ha crecido y recibes mucho más tráfico del esperado o si has realizado alguna campaña de marketing que ha resultado muy bien.

Solución: debes **pasarte a un plan de hosting mayor o contratar un aumento temporal**.

En dinahosting puedes cambiarte de plan de hosting en cualquier momento o con el [Cloud Hosting](#), aumentar los recursos puntualmente durante un período concreto.

3. Problemas con el archivo .htaccess

Si acabas de editar el archivo .htaccess y después aparece el error 503 es posible que haya algún problema con las modificaciones que hayas hecho.

Es habitual sobre todo cuando realizas una redirección, estableces páginas predeterminadas o cambias algún apartado que afecte a la configuración del servidor.

Solución: revisa que los [cambios introducidos en .htaccess](#) son correctos o restaura el archivo original para asegurarte de que no viene de ahí el error.

4. Plugins o temas que dan conflicto

Los plugins y temas de WordPress puedes también provocar en ocasiones este error. Piensa que al final son software desarrollado por terceros y no siempre están preparados para todas las casuísticas que puede haber en una web. Para evitar errores o conflictos utiliza mejor aquellos que tengan buenas valoraciones y descárgalos del repositorio oficial.

Solución: desactiva los plugins uno por uno hasta dar con el que produce el error. Si el plugin está actualizado y no ves manera de compatibilizarlo con tu web, entonces mejor desinstálalo y si lo necesitas, busca alguna alternativa.

5. Problemas con las DNS

Otra posible causa que puede provocar un error 503 es un problema con las DNS. Generalmente lo puedes identificar porque el mensaje que aparece es "Error 503: Service Unavailable – DNS Failure"

Solución: reinicia tu ordenador y el router. Si sigue apareciendo el mensaje de error entonces la opción es [establecer un nuevo servidor para tus DNS](#).

6. Otras causas

En algunas ocasiones no es posible conocer el origen del problema que produce el error 503 y por lo tanto, corregirlo uno mismo. Es por eso que es de vital importancia contar con un servicio de Soporte eficaz que te dé una solución rápida para volver a activar tu web.

Solución: contacta con tu proveedora de hosting para saber el motivo y que lo corrijan lo antes posible. ¿Sabías que en dinahosting estamos disponibles 24/7 para ayudarte?



504

Gateway Time-Out

4.7

CÓMO ARREGLAR EL ERROR 504 GATEWAY TIMEOUT

¿Aparece un Error 504 Gateway Time Out cuándo intentas acceder a tu web? ¡No te preocupes! A continuación vemos por qué sucede y cómo puedes arreglar el error 504.

El error 504 es uno de los errores HTTP más frecuentes que te puedes encontrar navegando. El primer dígito de su código, el 5, indica que se trata de un problema con un servidor.

¿Qué es el error 504?

El error 504 indica que **tu servidor no ha recibido la respuesta que esperaba de otro servidor intermedio** al intentar acceder a un sitio web o completar otra solicitud.

Generalmente se debe a un exceso de tiempo de espera por la respuesta de uno de los servidores proxy o Gateway que conectan la red. De ahí el mensaje "Gateway timeout" que a veces acompaña al 504.

¿Qué es un servidor proxy o Gateway?

Los servidores proxy o Gateway son máquinas que funcionan de puente entre tu petición y el servidor final.

Es decir, cuándo tecleas una URL en el navegador, envías una petición al servidor final donde está alojada esa web, pero en muchos casos la petición pasa antes por unos servidores intermedios. Estos serían los servidores proxy o gateway.

Estas son algunas de las funciones más habituales que realizan:

- **Firewall:** actúan como filtro para controlar accesos o contenidos no deseados.
- **Balanceadores de carga:** ajustan el tráfico recibido reenviando peticiones a los servidores menos ocupados.
- **Caché:** almacenan de manera temporal parte de los datos para que sea más rápido acceder a ellos.
- **Otras opciones de seguridad:** funcionan también como una primera capa ante posibles ataques.

Cómo arreglar el error 504

1. Recarga tu web y reinicia la red

En muchos casos el error 504 es temporal. Por este motivo y antes de realizar cualquier otra acción, prueba a **hacer F5** y recargar la página. Asegúrate además que no haya problemas con tu red local.

Otra solución es **borrar la caché y las cookies**, iniciar una sesión en modo incógnito, o probar desde un dispositivo o red diferente.

De esta forma descartas que el error esté en tu equipo o conexión.

2. Comprueba que el servidor funciona correctamente

Si has descartado que el error está en tu equipo, ahora toca ver si falla o no el servidor en el que está alojada tu web.

Una de las maneras más sencillas es realizar un ping a la web. Para hacerlo abre pulsando Windows+R y escribe cmd. En la ventana que se abre escribe el ping y el dominio de tu web.

```
ping tudominio.com
```

Esto te devolverá un mensaje confirmándote si está accesible o no el servidor. Durante el ping se envían 4 paquetes, si los tres son devueltos entonces todo está estará correcto.

Si falla tocará seguir descartando otras posibles causas.

3. Desinstala o desactiva plugins o temas

Si eres administrador y has hecho cambios recientes en tu web como la **instalación de nuevos plugins o temas en tu WordPress** y justo después se ha producido el error, es posible que esta sea la causa.

Para corregirlo será necesario revertir los cambios que hayas hecho. Prueba a desactivar el plugin o tema, revisa también que está actualizado a su última versión y si no ves manera de que sea compatible con tu web, desinstálalo y busca alguna otra alternativa en el repositorio.

4. Desactiva la CDN

Si estás utilizando un servicio de CDN (Content Delivery Network) como pueden ser CloudFlare, Transparent, etc. es posible que haya algún conflicto que produzca el error.

Para descartarlo **prueba a desactivar de forma temporal tu CDN** y espera a [que se propaguen las zonas DNS](#) de nuevo. Si la causa está en la CDN con esta acción debería corregirse y si no, también puedes contactar con el soporte de la plataforma.

5. Revisar la configuración del servidor proxy

Puede pasar que el servidor proxy esté mal configurado y que esté bloqueando innecesariamente peticiones que no debería.

Si eres webmaster o controlas de sistemas puedes echarle un ojo al archivo nginx.conf para revisarlo y comprobar que todo está correcto con la configuración. Y si no es tu caso, entonces mejor pasa al siguiente punto.

6. Contacta con tu proveedora de hosting

Contactar con tu proveedora de hosting puede ser la vía más rápida para solucionar arreglar un error 504, 503, 500, o cualquier otro relacionado con el servidor donde se aloja tu página.

Es por este motivo que siempre te recomendamos alojar tu web en una proveedora de confianza que responda al instante antes posibles errores.

En dinahosting contamos con su [servicio de Soporte Técnico especializado](#) **disponible para ti las 24 horas del día, 365 días al año**. ¡Contáctanos si necesitas ayuda o asesoramiento! Estaremos encantados de atenderte.

GUÍA DE CIBERSEGURIDAD

5. Certificados SSL

[5.1. ¿Tu web no tiene HTTPS? Google dice que no es segura](#)

[5.2. Por qué debes instalar ya un certificado SSL en tu web](#)

[5.3. Certificados SSL Let's Encrypt: seguridad para tu web gratis](#)

[5.4. Nuevos certificados SSL Globalsign](#)





5.1 ¿TU WEB NO TIENE HTTPS? GOOGLE DICE QUE NO ES SEGURA

Desde el 1 de julio de 2018, Google empezó a marcar como no seguras las páginas web que no usen el protocolo https, la versión segura del http.

Hasta el momento, las webs sin https estaban siendo penalizadas solo en los resultados de búsqueda. Sin embargo, la medida se volvió más restrictiva desde entonces. Fíjate, así se mostrará tu web en el navegador sin la capa de seguridad que demanda Google:

¿Qué es https y en qué se diferencia de http?

Por https entendemos el **protocolo de transferencia de datos** entre cliente y servidor. Cuando quieres acceder a una web a través del navegador, ese protocolo es el que intermedia en el intercambio de información entre tu PC y el servidor donde está almacenada la información.

El protocolo https no es ni mucho menos reciente. Hace ya 20 años que se convirtió en el estándar.

Se diferencia de su predecesor, http, en que https **incorpora una capa de seguridad adicional mediante el cifrado SSL/TLS** (Secure Sockets Layer/Transmission Layer Security).

SSL consiste en un protocolo de seguridad que tiene doble función: por un lado, verifica la identidad del sitio web al que estás accediendo para confirmar su propiedad, y por otro, cifra las comunicaciones que se produzcan dentro de la página para que la información que introduzcas en ella como usuario (por ejemplo, tus datos bancarios) viaje de forma confidencial. **TLS no es más que una versión actual y más segura del protocolo SSL.**

Ten claro que aunque el término más popular cuando hablamos de certificados de seguridad sigue siendo SSL por ser el predecesor, en dinahosting usamos el protocolo TLS en todos nuestros servidores.

Si quieres seguir profundizando en las diferencias entre http y https, aquí te las explicamos al detalle.

Diferencias entre HTTPS y HTTP

HTTPS:

- Los URL empiezan por "https://"
- El protocolo seguro utiliza el puerto 443 por omisión
- Canal cifrado entre servidor y cliente (bidireccional)
- Texto cifrado
- Canal seguro
- Indica que la página a la que accedes es la original

HTTP:

- Los URL empiezan por "http://"
- Utiliza el puerto 80 para las comunicaciones
- Interpretación directa del flujo de datos
- Uso de texto plano
- Canal inseguro
- No tienes forma de saber que la página es la original

Podemos decir que al navegar por **páginas HTTP** toda la información que se intercambia entre nuestro dispositivo y el servidor de ese sitio puede ser interceptada al **no cifrar el contenido**. Todo lo que se envía queda expuesto a posibles ataques como man-in-the-middle o eavesdropping, por lo que el sitio web no es seguro.

Por este motivo **te recomendamos siempre que instales un certificado para aportar un extra de seguridad a tu web**. No nos engañemos, un certificado no es infalible, pero protegerá mucho más tus comunicaciones que de no tenerlo.

El caso es que, como te anticipábamos al inicio, no fue hasta el año 2018 cuando Google dijo que consideraría inseguras las webs que usaran http en vez de https, por lo que muchos usuarios propietarios de webs y tiendas online no dieron el salto a https en ese momento.

Una web con http (y, por lo tanto, sin cifrado) no solo tendrá un peor posicionamiento SEO, sino que perderá toda la confianza de sus potenciales visitantes, por lo que si aún no lo has hecho, el momento es ahora. El protocolo https deriva del uso de un certificado SSL, por eso es importante que te hagas con el tuyo cuanto antes.

Los beneficios de un certificado SSL

- **Comunicaciones cifradas y seguras**
- **Mejor posicionamiento SEO**
- **Mejor imagen de cara a tus visitas**
- **Acredita tu identidad**
- **Reconocimiento por parte de los navegadores**

Te contamos más sobre estos beneficios [en el siguiente capítulo](#).



Cómo solucionar el aviso de sitio no seguro

Sigue estos cuatro pasos para hacer de tu web insegura con HTTP un lugar de confianza para tus clientes:

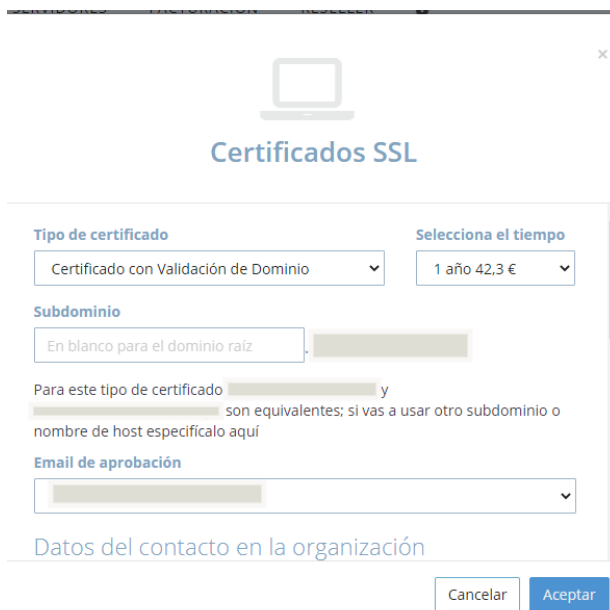
1. Elige un certificado SSL

Acude a nuestra sección de [Certificados SSL](#) y **escoge el tipo de certificado más apropiado para tu web**. Si guardas información altamente sensible, como contraseñas o número de cuenta o tarjeta de tu cliente, **te recomendamos un certificado de pago**, ya que te dará una mayor cobertura y garantías que Let's Encrypt. Como ves, su precio es bastante económico.

Si acabas de dar de alta tu hosting, puedes comprobar en tu [Panel](#), en la sección de Hosting, que **ya tienes preinstalado completamente gratis un Let's Encrypt**, que protegerá tu web personal o tu sitio informativo.



Si quieres cambiar de certificado, solo tienes que pulsar en Eliminar y pasar a otro modelo. Puedes hacerlo desde tu Panel de Control de forma muy fácil. Haz clic en Contratar y selecciona en la ventana modal el certificado que más te interese.



Panel dinahosting contratar certificado SSL

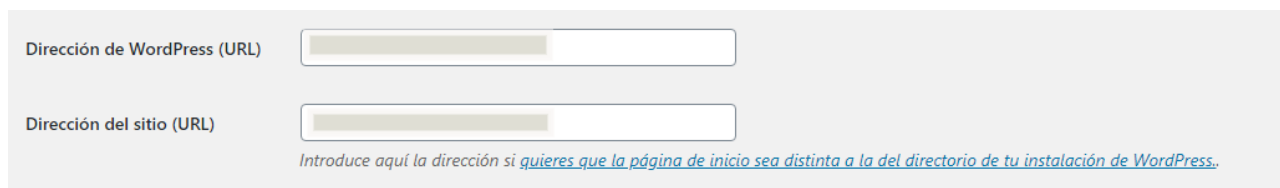
2. Configura tu certificado SSL

La configuración de tu certificado de pago puedes hacerla o bien dentro de la [sección de certificados](#) o en el Panel como te hemos explicado. En la web simplemente escoge la modalidad que necesites y cubre los datos de alta.

Ten en cuenta que el alta del certificado no se hace de forma automática. Debes esperar entre 1 y 2 días a que la entidad GlobalSign pueda verificar toda la información que estás aportando de tu dominio u organización.

3. Cambia el URL de tu web en WordPress

Si estás usando WordPress, entra en el panel de administración. Accede a Ajustes > Generales y cambia HTTP por HTTPS.

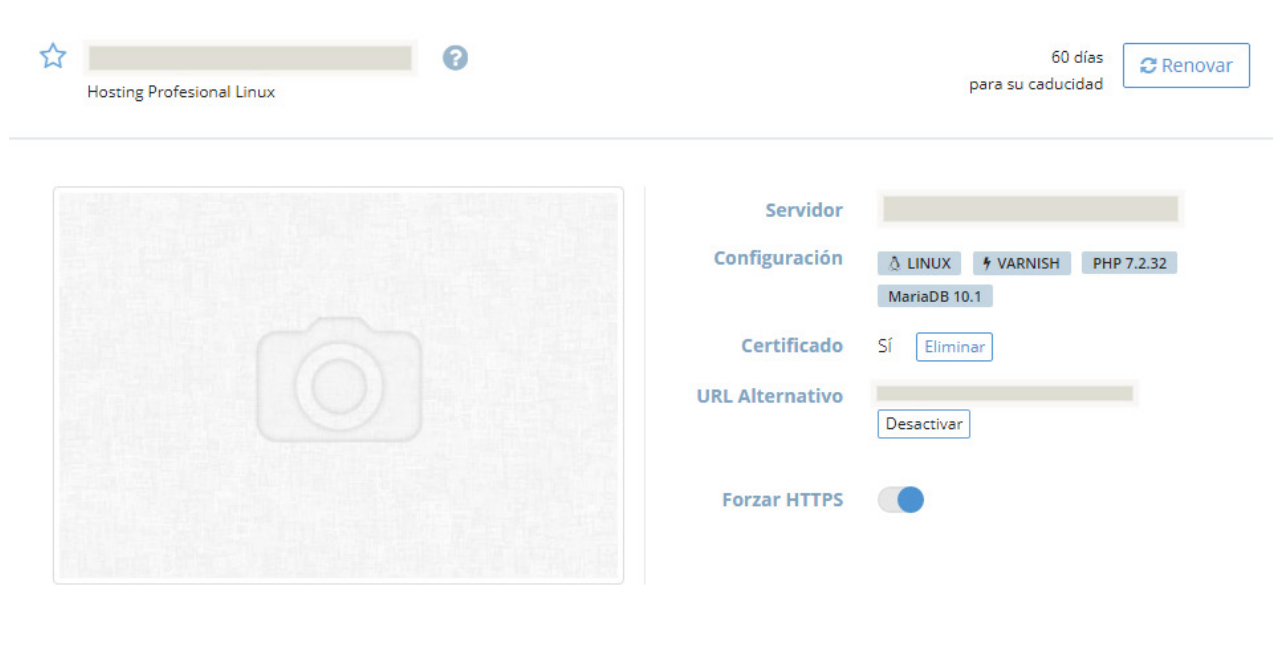


Y te preguntará, por qué hay dos campos diferentes para configurar el URL de WordPress. En **Dirección de WordPress** se indica dónde se encuentran los archivos principales de tu sitio, y en **Dirección del sitio** dónde se ubica el sitio web para los visitantes.

4. Hacer una redirección 301

En este punto tu web ya es visible con HTTPS, pero puede que usuarios hayan guardado tu vieja dirección con HTTP o tu web esté referenciada en post u otros contenidos. **En esta situación debes hacer una redirección de tipo 301** a tu nueva dirección. Este tipo de redirección es de carácter permanente y le indica a los motores de búsqueda que tu sitio web se ha mudado a una nueva dirección de forma permanente.

En dinahosting es muy sencillo. Entra en tu Panel, sección Hosting. Justo en la pantalla inicial tienes un interruptor de Forzar HTTPS. Actívalo y listo.



Ya ves que pasar de HTTP a HTTPS para evitar que tu web sea insegura ha sido muy sencillo. Pero si te has quedado con dudas o quieres comentarnos algo, aquí estamos para ayudarte. Siempre disponibles.



UN DOMINIO PARA CADA PROYECTO

Más de 400 extensiones para elegir
Panel de control exclusivo
Correo profesional incluido
Gestión total de DNS

5.1. ¿Tu web no tiene HTTPS? Google dice que no es segura | 125



5.2

POR QUÉ DEBES INSTALAR YA UN CERTIFICADO SSL EN TU WEB

¿Tu web aún no tiene certificado SSL? Si quieres proporcionar y transmitir seguridad en tu página, la certificación SSL es imprescindible.

Antes este tipo de certificados estaban especialmente recomendados para sitios que manejaran datos personales o bancarios. Pero eso ya es pasado, **ahora el certificado SSL se recomienda para TODAS las webs.**



Si quieres saber más
Mira el vídeo
Instalar un Certificado SSL
en tu web

¿Qué es SSL, TLS y HTTPS?

Seguramente has visto muchas veces los términos SSL, TLS y HTTPS ¿pero sabes bien qué significan y en qué se diferencian? Te lo contamos a continuación.

SSL (Secure Socket Layer) es un protocolo de seguridad que autentifica la identidad de un sitio web y cifra las comunicaciones para que la información entre dispositivos viaje de forma segura y confidencial.

TLS (Transport Layer Security) es un protocolo muy similar al SSL, que también encripta los datos que se comunican entre dispositivos, pero más actualizado y seguro.

El protocolo TLS proporciona un mayor nivel de seguridad, evitando el espionaje o la manipulación de los datos que se transfieren de manera más eficaz, es por eso que sustituye al protocolo SSL.

El uso de SSL ahora mismo incluso se desaconseja. Si tu servidor está bien configurado los protocolos anteriores a TLS 1.2, deben estar deshabilitados.

¿Quieres conocer que protocolos están activos en el servidor de un determinado dominio? Puedes utilizar [esta herramienta](#) de nuestro proveedor de certificados GlobalSign.

HTTPS (HyperText Transfer Protocol Secure) es la versión segura de HTTP y es el protocolo más popular para la transferencia de datos en internet.

Es el más reconocido por los usuarios porque se puede ver si se está utilizando o no directamente desde los navegadores.

Este protocolo solo lo puedes utilizar en tu página si dispones de un Certificado SSL/TLS que lo verifica.

¿Qué son los certificados SSL/TLS?

Los certificados SSL/TLS o Certificados SSL son certificados digitales que se instalan en el servidor y que por un lado verifican la identidad del sitio y por otro, acreditan que se están utilizando correctamente los protocolos SSL y/o TLS.

Para activar el HTTPS y que tu página se marque como segura, es imprescindible disponer de un certificado SSL/TLS.

Estos certificados son otorgados por entidades acreditadoras como pueden ser GlobalSign o Let's Encrypt.

Cabe destacar que protocolo no es lo mismo que certificado. El protocolo que cumple una web va determinado por la configuración del servidor, y el certificado simplemente acredita que se están utilizando.

Hay que tener en cuenta también que la nomenclatura "Certificado SSL" no quiere decir que certifique el uso de protocolos SSL únicamente. **Los Certificados SSL acreditan tanto protocolos SSL como TLS.**

Se siguen llamando así por ser el término más popular, pero cada vez empezarás a verlos más a menudo como Certificados TLS o SSL/TLS.

Tipos de Certificados SSL

Los certificados SSL se clasifican en diferentes tipos según la cantidad de dominios y/o subdominios y según el grado de validación.

Según la cantidad de dominios:

- **Dominio único:** el certificado asegura un único nombre de dominio.
- **Wildcard:** cubre un dominio y todos sus subdominios.
- **Multidominio:** permite asegurar varios nombres de dominio.

Y según el grado de validación:

- **Validación de dominios:** asegura un único dominio con un cifrado básico y verifica la información del titular del mismo. Es el más habitual y es el recomendado si gestionas un blog o una web personal sin subdominios.
- **Validación de organización:** asegura el dominio con un cifrado básico y verifica la información del titular y de la organización. Indicado para páginas de empresas de tamaño medio y ecommerce.
- **Validación extendida (EV):** asegura el dominio con un nivel mayor de cifrado y se hace una investigación en profundidad de la empresa y del sitio web. Recomendado para empresas de mayor tamaño. Habitualmente los distinguirás por que aparece el nombre de la empresa al lado del símbolo de candado o una "barrita verde" que muestra el navegador junto a la URL.

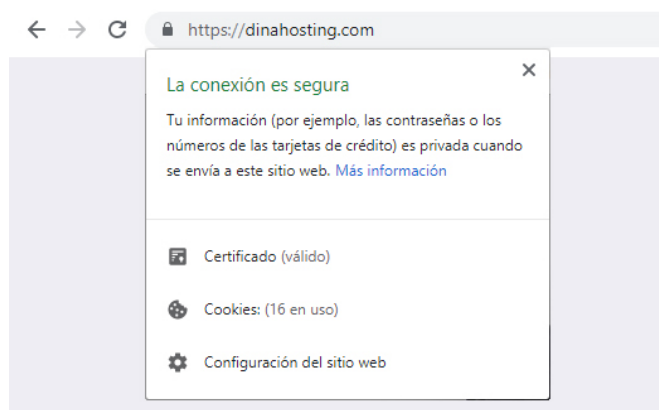
Te contamos todas las ventajas de tener tu web certificada y los inconvenientes que te ocasionará el no tener esta certificación.

Ventajas de tener tu web CON certificado SSL

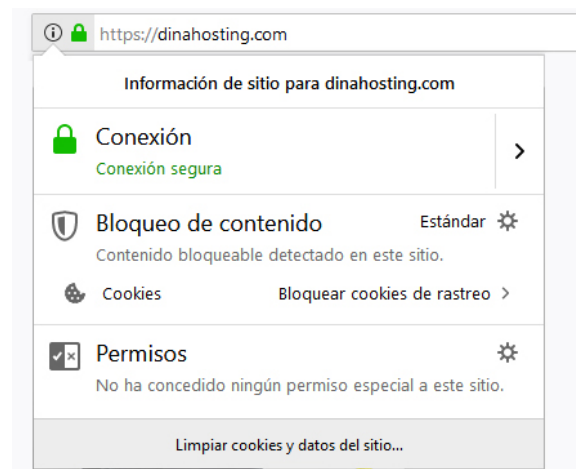
- **Mayor seguridad:** la información que circula por tu página estará cifrada y protegida. Esto evita que terceros puedan obtener los datos personales o bancarios de tu web o ecommerce durante la comunicación con el visitante.
- **Mejor posicionamiento:** Google favorece a las páginas con SSL. Entre los requisitos del algoritmo del buscador está el de la seguridad. Cuanto más seguro sea tu sitio, te será mucho más fácil escalar posiciones.
- **Acredita tu identidad:** cuando entras en una página con esta certificación es una garantía de que esa web es efectivamente quien dice en su dominio. Evita posibles suplantaciones online.
- **Mayor confianza para los usuarios que visitan tu página.** No solo basta con tener seguridad, el usuario tiene que percibirla. En los navegadores aparecerá destacado que posees un certificado.

Si tienes un certificado SSL, verás así tu página en los diferentes navegadores:

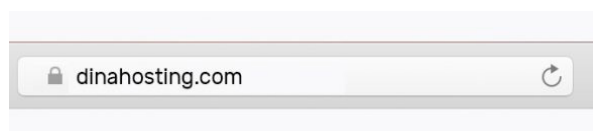
Chrome:



Firefox:

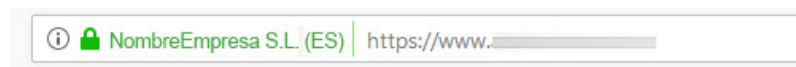


Safari:

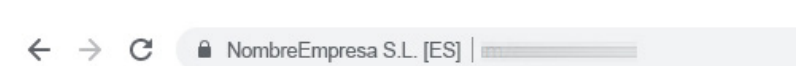


Si tienes el certificado SSL tipo EV en la barra del navegador aparecerá el nombre de tu empresa de la siguiente forma:

Firefox:



Chrome:



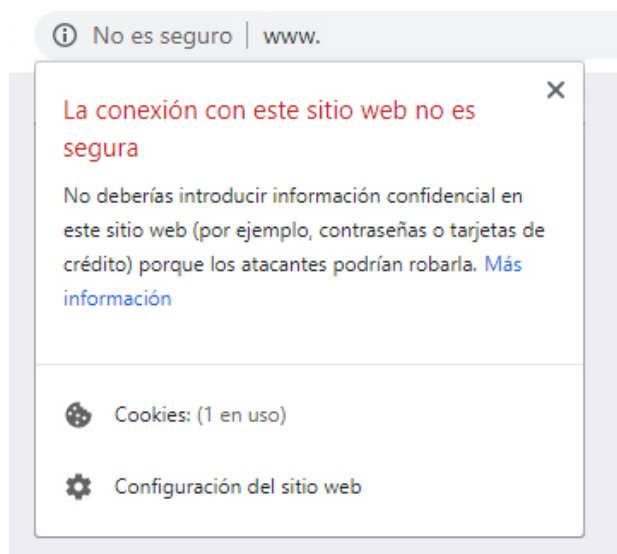
Safari:



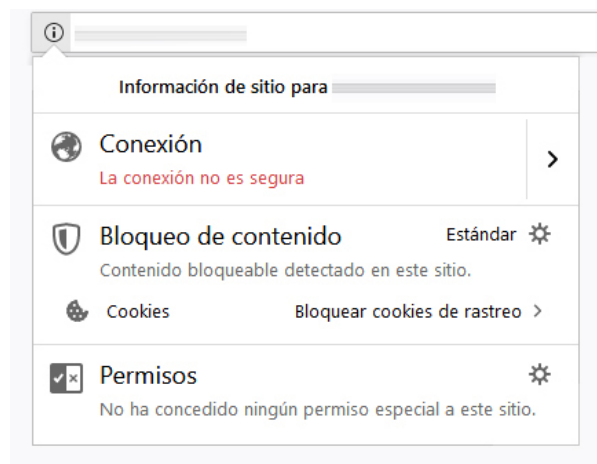
Inconvenientes de tener tu web SIN certificado SSL

- **Inseguridad:** tu web no está cifrando sus comunicaciones. Cualquiera podría obtener fácilmente tus datos y los de tus clientes y esto es especialmente crítico si manejas datos personales o si tienes una tienda online donde solicitas datos bancarios.
- **Mal posicionamiento en buscadores:** Google penaliza las páginas inseguras y no las muestra en sus primeros resultados. Además, tampoco podrás realizar campañas en Google Ads si no tienes un certificado SSL.
- **Desconfianza:** tu sitio irá acompañado del texto "No seguro" o iconos desalentadores para tus visitantes. Sin certificado tu web se mostrará de la siguiente manera en los principales navegadores:

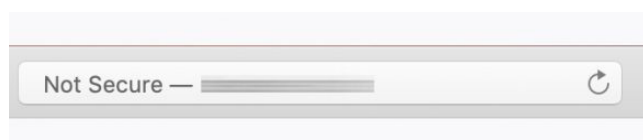
Chrome:



Firefox:



Safari:



VENTAJAS DE TENER CERTIFICADO SSL EN TU WEB

- 1 PROPORCIONA MAYOR SEGURIDAD**
La información que circula por tu página estará cifrada y protegida.



- 2 MÁS PRIVACIDAD PARA TUS USUARIOS**
Dificulta que terceros puedan obtener los datos personales o bancarios de tu web durante la comunicación con el visitante.

- 3 MEJORA EL POSICIONAMIENTO**

Google favorece a las páginas con SSL. Cuanto más seguro sea tu sitio, más fácil es escalar posiciones en los buscadores.



WWW.

- 4 ACREDITA TU IDENTIDAD**
Una página con esta certificación es una garantía de que esa web es efectivamente quien dice en su dominio.

- 5 GENERA CONFIANZA**

Los sitios seguros se destacan en los buscadores como tal para que el usuario lo perciba. Mayor confianza, más probabilidad de conversión.



Si lo prefieres
Mira el vídeo online



5.3

CERTIFICADOS SSL LET'S ENCRYPT: SEGURIDAD PARA TU WEB GRATIS

Cifra tu web y transmite confianza a tus usuarios con los certificados SSL Let's Encrypt gratuitos. ¡Consigue el tuyo con tu alta de hosting!

A día de hoy es imprescindible tener una web con unos niveles mínimos de seguridad para proteger los datos de los usuarios, es por eso que en dinahosting disponemos de [diferentes opciones de certificación SSL](#), entre ellas la opción gratuita Let's Encrypt.

¿Qué es Let's Encrypt?

Let's Encrypt es una Entidad Certificadora que emite certificados SSL para cualquier dominio web de forma completamente gratuita. Esta entidad surgió a partir de Software Libre con el objetivo de facilitar que la red sea un lugar más seguro.

Estos certificados SSL habilitan el [protocolo HTTPS](#) en tu web, un cifrado que aporta un grado de seguridad mayor y hace que los principales exploradores lo marquen como página segura.

La certificación Let's Encrypt es de tipo Validación de dominio, es decir, que valida un único dominio con un cifrado básico.

¿Cómo funciona?

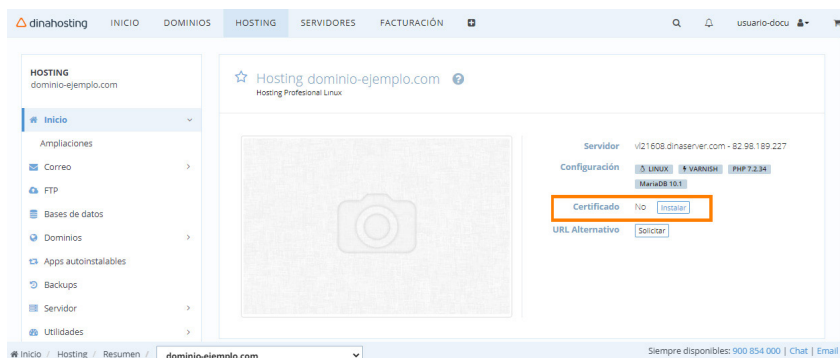
Let's Encrypt valida el dominio identificando al administrador del servidor en el que está alojado mediante el [protocolo ACME](#) (Automatic Certificate Management Environment).

Tras esta validación el administrador estaría autorizado para solicitar el certificado y activarlo en su página.

¿Cómo lo activo en dinahosting?

Let's Encrypt viene preinstalado con tu nueva alta de hosting.

Si eres cliente y todavía no tienes activa ninguna certificación SSL, activar el certificado Let's Encrypt en tu web es súper sencillo. Desde el Panel de tu hosting solo tienes que pulsar Certificado > Instalar y elegir Let's Encrypt o el que prefieras.



Ten en cuenta que la activación del certificado solo es posible si tu dominio tiene los DNS de dinahosting.

Para una mayor garantía de seguridad en dinahosting también ponemos a tu disposición diferentes modalidades de [Certificados SSL GlobalSign](#), entidad acreditadora de prestigio internacional.



5.4

NUEVOS CERTIFICADOS SSL GLOBALSIGN

Los certificados SSL son un requisito casi imprescindible para dar un plus de seguridad y confianza al usuario de tu web. ¿Ya tienes el tuyo?

Los [Certificados SSL de GlobalSign](#) ofrecen una **gran fortaleza de cifrado y seguridad** y el proceso de validación y alta es más rápido que el de otros proveedores.

En dinahosting te ofrecemos **5 certificados GlobalSign SSL adaptados a cada una de tus necesidades** ¡echa un ojo!

Validación de Dominio

La opción más económica y rápida de tramitar. [Asegura un único dominio con un cifrado básico](#) y verifica la información del titular del mismo. Es ideal para blogs personales o webs de tipo portfolio. En 1 – 2 días ¡lo tienes activo!

Validación de Dominio Wildcard

Ofrecen [protección para subdominios ilimitados](#), y van **perfectos para proyectos personales con muchos subdominios**. El certificado verifica la información del titular y cubre un dominio con todos sus subdominios. Su activación se lleva a cabo también en 1 – 2 días.

Para activar tu certificado de Validación de Dominio o WildCard solo tienes que:

1. Acceder al email que has recibido en tu cuenta de correo de aprobación y valida el dominio en el enlace.
2. El certificado se emitirá y se instalará en tu hosting en 24 horas.

Validación de Organización

Perfecto si gestionas un ecommerce o una web de tamaño medio. Además de verificar el titular del dominio, [certifica la información sobre tu empresa](#). Su activación se produce en 1 – 10 días hábiles.

Validación de Organización Wildcard

[Este tipo de certificado](#) verifica la información del titular y de la empresa está pensado para webs corporativas que necesitan encriptar varios subdominios. Se activa en 1 – 10 días hábiles.

El proceso de activación para las Validaciones tipo Organización es muy sencillo:

1. Accede al email que has recibido en tu cuenta de correo de aprobación y selecciona la opción de validación que te interese.
1. Sigue las instrucciones indicadas en el correo.
1. Recibirás una llamada de la entidad certificadora para verificar tu número de contacto.
1. El certificado se emitirá y se instalará en tu hosting en 24 horas.

Validación Extendida

Recomendado para empresas de mayor tamaño y webs de comercio electrónico que manejan información sensible. [Asegura tu dominio](#) con un nivel mayor de cifrado y se realiza una investigación en profundidad de la empresa y del sitio web. Se activa en 1 – 10 días hábiles.

Para la Validación Extendida el proceso de activación es el siguiente:

1. Accede al email que has recibido en tu cuenta de correo de aprobación, firma la documentación adjunta y envíasela a la entidad certificadora respondiendo a ese mismo email.
2. Recibirás una llamada para verificar que la persona solicitante forma parte de la organización.
3. El certificado se emitirá y se instalará en tu hosting en 24 horas.

Ya ves que disponemos de un certificado adaptado a cada web.



AÑADE UN **CERTIFICADO SSL** A TU WEB

Comunicaciones cifradas y seguras

Mejora tu posicionamiento SEO

GUÍA DE CIBERSEGURIDAD

6. Protección de datos

[6.1. Checklist RGPD: ¿tu web cumple esta normativa?](#)

[6.2. Protección de datos en tu tienda online: cómo cumplir con la normativa](#)

[6.3. ¡Que no te sancionen! Pon tu web al día con la Ley de Cookies](#)

[6.4. ¿Qué textos legales necesita tu web o ecommerce?](#)

[6.5. 4 Criterios legales en la elección de tu hosting](#)



6.1

CHECKLIST RGPD: ¿TU WEB CUMPLE ESTA NORMATIVA?

A nivel web gestionar la protección de datos no siempre es sencillo. Te explicamos los puntos básicos sobre cómo proceder para cumplir con el RGPD en tu web.

¿Qué es el RGPD?

El **RGPD** o Reglamento General de Protección de Datos **es la normativa europea que regula los derechos de las personas acerca de sus datos de carácter personal y del tratamiento que se hace de los mismos.**

Este reglamento es aplicable en el caso de que tengas una web y almacenes o utilices cualquier tipo de información acerca de los usuarios o clientes que la visitan.

Por ejemplo, si guardas datos de visitas, emails de contacto o diferentes preferencias de idioma, será necesario que tu web cumpla con esta normativa.

Cada página web es diferente por lo que existen múltiples maneras tanto de almacenar datos, como de aplicación de la norma. Para facilitarte los primeros pasos, toma nota de esta checklist sobre cómo cumplir con el RGPD.

Checklist: protección de datos en tu web

1. Revisa qué tipo de datos estás utilizando

Es decir, analiza qué tipo de datos vas a guardar o utilizar de tus usuarios o visitantes web.

A veces, aunque no nos conste nuestra web guarda ciertos datos. Los más habituales suelen ser los que se obtienen a través de formularios, comentarios, herramientas de analítica, plataformas de pago, redes sociales y de los propios navegadores.

De estos últimos es de donde se obtienen las famosas cookies. Las cookies pueden recoger información de carácter personal, y en estos casos también se deberá cumplir con el RGPD en su tratamiento. Échale un ojo a este post para [saber más sobre las cookies](#).

2. Medidas de seguridad que debes aplicar

En función de los datos que recojas de tu página, tendrás que añadir más o menos medidas de seguridad.

Si tienes un ecommerce y recoges datos bancarios por ejemplo, tus medidas deben ser mayores que las de un portfolio personal donde no hay ninguna transacción.

Como premisas fundamentales e independientes del nivel de seguridad que apliques, **debes garantizar la confidencialidad e integridad de los datos**. Además, deben de estar disponibles para su modificación o cancelación en cualquier momento.

El [certificado SSL](#) es una medida esencial y sencilla de aplicar para encriptar la información que circula por la página y garantizar su confidencialidad. Por eso **te recomendamos que lo instales cuanto antes en tu web**.

3. Informar del tratamiento y solicitar el consentimiento

Antes de recoger cualquier tipo de dato del usuario debes informarlo previamente sobre qué información vas a almacenar y con qué fin.

También debes señalar quién o qué entidad es responsable de los datos y su contacto y los derechos que usuario tiene sobre esta información. Debes dar la opción de poder modificarlos o eliminarlos.

Es importante **recoger el consentimiento explícito del usuario para el uso de sus datos** siempre que no exista otra base legítima para su tratamiento. Naturalmente no es posible utilizar este tipo de información si no nos han autorizado.

Seguro que estás cansado de navegar y ver mensajes para aceptar el uso de las cookies, o el típico check para expresar tu conformidad sobre la política de protección de datos al cubrir un formulario. Ambas son las formas más habituales para conseguir el consentimiento del usuario acerca de sus datos.

4. Identifica todos los responsables del tratamiento

Como ya te comentábamos en el anterior punto, el responsable de los datos puede ser una tercera persona o entidad.

Es decir, debes de revisar bien quién va a tratar los datos y también dónde van a tratarse. Si tu web está alojada en una proveedora de hosting, esta debe cumplir con el RGPD también para que las autoridades competentes puedan considerar que el almacenamiento de los datos cumple con la normativa.

Si tus datos están alojados en dinahosting no tienes de que preocuparte, ya que **nuestra infraestructura cumple con la normativa europea en protección de datos**.

Ojo, porque si tu proveedora está en el extranjero es posible que aplique políticas diferentes para la protección de datos a las requeridas por el RGPD.

5. Políticas de privacidad y textos legales

Por último, tu web debe recoger todos los detalles respecto al uso de datos en los siguientes textos legales:

- **Política de privacidad:** obligatoria si tratas datos de usuario. Debe ser totalmente transparente y detallar todo lo referente al uso y almacenamiento de los datos.
- **Política de cookies:** obligatoria si utilizas cookies no exceptuadas del deber de obtener el consentimiento informado por su instalación. En ella debes informar de las cookies utilizadas y de su finalidad.

- **Aviso legal:** obligatorio para cualquier página de la que se obtenga un beneficio económico directa o indirectamente. Debe incluir los datos de la empresa y aquellas otras funciones que se consideren esenciales para el uso de la web (por ej. propiedad intelectual de los contenidos).
- **Condiciones de contratación:** solo para ecommerces. Se trata de los términos concretos de venta de productos o prestación de servicios, es decir, el contrato entre la empresa y el consumidor o usuario.

En dinahosting te lo ponemos fácil y te ofrecemos un [Aviso legal tipo](#) totalmente gratis para que añadas a tu web.

No es necesario que estos textos legales vayan en secciones independientes, puedes incluirlos todos en una misma página siempre que se muestren bien diferenciados.



CHECKLIST RGPD

¿Tu web cumple esta normativa?

1

REVISAR QUÉ TIPO DE DATOS ESTÁS UTILIZANDO EN TU WEB

Los más habituales suelen ser los que se obtienen a través de formularios, comentarios, herramientas de analítica, plataformas de pago, RRSS y de los propios navegadores.



2

MEDIDAS DE SEGURIDAD QUE DEBES APLICAR

Si tienes un ecommerce y recoges datos bancarios, tus medidas deben ser mayores que las de un portfolio personal donde no hay transacciones.

3

INFORMAR DEL TRATAMIENTO Y SOLICITAR EL CONSENTIMIENTO

Antes de guardar cualquier tipo de dato del usuario debes informarlo sobre qué información vas a almacenar y con qué fin, y recoger su consentimiento explícito para el uso de sus datos.



4

IDENTIFICAR TODOS LOS RESPONSABLES DEL TRATAMIENTO

Debes de revisar bien quién y dónde van a tratarse los datos. Si es una tercera persona o entidad quién guarda los datos (como por ej. tu proveedora de hosting) debes asegurarte de que cumple con el RGPD y dejarlo claro en tus textos legales.



5

TEXTOS LEGALES

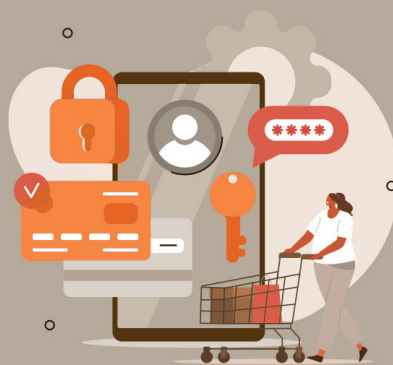
Tu web debe recoger todos los detalles respecto al uso de datos en los siguientes textos legales: política de privacidad y cookies, aviso legal y condiciones de contratación.



Si lo prefieres
Mira el vídeo online

LOPD

Tienda online



6.2 PROTECCIÓN DE DATOS EN TU TIENDA ONLINE: CÓMO CUMPLIR CON LA NORMATIVA

La protección de datos es un pilar imprescindible para cualquier tienda online. Si estás en la fase inicial de desarrollo de tu proyecto, seguro que te preocupan mucho cuestiones como que tu tienda sea estéticamente bonita, que el proceso de compra sea intuitivo, que la web cargue rápido y no sufra una caída, etc. Evidentemente, todos estos aspectos son clave, pero **no servirán de nada si los clientes no se sienten seguros cuando van a comprar**, además de las posibles sanciones que podrías recibir por el incumplimiento de las normativas relacionadas con la protección de datos.

¿Qué leyes afectan a la materia?

Si hablamos de protección de datos y vas a montar tu tienda online en España, hay dos normativas que tienes que conocer.

La más popular, el [RGPD](#), es el Reglamento General de Protección de Datos y tiene efectos a nivel europeo. Los Estados miembros de la UE deben ajustarse a este reglamento. En España tenemos además la [LOPDGDD](#), la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.

A mayores, otras dos normativas amparan a los consumidores. Son la [LSSI](#), o Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico, y la [Ley General de Defensa de los Consumidores y Usuarios](#).

Principios de aplicación

De lo que se trata cuando tienes un negocio en Internet es de que las personas que te van a ceder sus datos tengan claro qué información vas a recoger y qué vas a hacer con ella. Por lo tanto, los textos legales que incluyas en tu web -de los que hablaremos un poco más abajo-, tienen que dejar bien claros estos puntos:

- **Los datos que vas a recoger**

Ya sea en la plataforma de pago de tu tienda, en los formularios de contacto, en las herramientas de analítica que utilices... Lo primero es identificar qué datos personales vas a pedirle a tus clientes.

- **El tratamiento que vas a hacer de esos datos**

Una vez sabidos, lo que toca es informar al usuario de qué datos vas a guardar y para qué. Además, tienes que identificar al responsable de ese tratamiento, sea una persona o una entidad, y decirle a los usuarios qué derechos tienen sobre ellos.

Ya sabes que como mínimo es imprescindible que el cliente pueda modificarlos, o eliminarlos si no le interesa que los sigas almacenando.

- **El consentimiento**

El último paso. Una vez informado del tratamiento, es cuando le pides al usuario consentimiento para él. ¿Te suena el

mensaje de uso de cookies que aparece al principio de la navegación en cualquier web? Pues es un ejemplo claro de solicitud del consentimiento.

Las leyes de protección de datos son tajantes en este sentido. No puedes recoger y almacenar datos personales de tus usuarios si no te han autorizado previamente a hacerlo.

Y ojo, este consentimiento **tiene que ser explícito**. No basta con que digas algo así como “Al registrarte en esta web aceptas que almacenemos tus datos personales para realizar tus gestiones como cliente”. Intentar que el consentimiento sea implícito puede conllevar una sanción. Asegúrate de que la pregunta sea directa y de que el usuario tenga que **marcar una casilla o ejecutar alguna acción** para que el proceso de consentimiento se haga con transparencia, garantizando que ha leído las condiciones y sabe lo que acepta.

Importante también: no confundir cuestiones relacionadas con la gestión del servicio, con envío de promociones o newsletters. Si quieres enviar a tus clientes algún tipo de oferta por correo, también es imprescindible que le pidas consentimiento expreso, no sirve con una autorización genérica. Por supuesto, tampoco puedes ceder sus datos a terceros sin pedir permiso antes.

¿Qué textos legales tiene que incluir una tienda online?

Los textos legales son una serie de documentos que tienes que elaborar al poner en marcha tu tienda online y que han de estar accesibles para consulta en todo momento.

Si necesitas ayuda con la preparación de los textos legales, no dudes en recurrir a nuestro [servicio de Asesoría Legal](#). Sabemos que resolver tus asuntos jurídicos es un esfuerzo extra, por eso estamos aquí para asesorarte y proporcionarte documentos legales adaptados a tu página.

Aviso Legal

Su función es **recoger los datos empresariales del titular de la web**. ¿Qué tienes que incluir en un aviso legal?

- Denominación social de la web y datos de contacto: dirección física, dirección de correo electrónico y teléfono.
- Número de inscripción en el Registro Mercantil (en caso de ser una sociedad inscrita en el mismo).
- CIF o NIF del titular de la web.
- En el caso de que la actividad esté sujeta a un régimen de autorización previa, los datos referentes a esa autorización y el órgano encargado de su supervisión.
- Si ejerces una profesión regulada, indica los datos del Colegio Profesional al que perteneces y número de colegiado, título académico oficial o profesional, lugar donde se expidió y las normas profesionales aplicables.
- Información sobre el precio de los productos, indicando si se incluyen o no los impuestos aplicables y los gastos de envío.
- Los códigos de conducta a los que se esté adherido y la forma de consultarlos electrónicamente.

En dinahosting te ofrecemos un [aviso legal tipo gratis](#), que puedes usar de base para desarrollar el de tu web.

Política de privacidad

En ella se informa a los usuarios de qué **datos se han obtenido de ellos y el tratamiento que se va a realizar de los mismos**. Debe incluir:

- Identificación del responsable del tratamiento o sus representantes.
- Finalidad para la que se recogen los datos.
- Plazos durante los que vas a mantener la información en las bases de datos.

- Si se va a ceder o no la información a terceros.
- Vías del usuario para ejercer los derechos de Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad y Oposición.

Política de Cookies

Si en tu página web recoges cookies, tienes que informar de ellos a los usuarios en la política de cookies.

Añade una explicación detallada de para qué vas a utilizar las cookies en tu web, ya sean cookies de seguimiento, que almacenen información sobre el comportamiento de los usuarios dentro de tu web, o las cookies de terceros usadas con fines analíticos o publicitarios. Por eso también tienes que indicar quién instala las cookies en el equipo del usuario, si es la propia tienda online o un tercero (por ejemplo, las cookies de Google Analytics). Además, tienes que especificar si la cookie se guarda de forma temporal o permanente.

Condiciones generales de venta o contratación

Son el conjunto de **normas que tienes que definir previamente, y que el comprador acepta** cada vez que está realizando una compra. Tienen un carácter general, por lo que son iguales para todos los compradores. ¿Qué deben incluir?

- Características de los productos o servicios que se comercializan.
- Identidad del vendedor.
- El precio total, que debe incluir impuestos u otras tasas y los gastos de envío si los hay. Además, en caso de ofertas o descuentos, debe constar el precio original y el descuento.
- Las condiciones y proceso de pago: métodos de pago aceptados, métodos de envío, plazos de entrega...
- El proceso de compra, indicándose los pasos a seguir para completar la compra.
- Idiomas en los que se puede realizar una contratación.
- Las soluciones que tiene el comprador para devolver o reclamar un producto.
- Cómo ponerse en contacto con el servicio de posventa.

Cuestiones básicas de ciberseguridad

Te dejamos unas cuantas recomendaciones básicas de seguridad que fomentarán la protección de datos personales dentro de tu tienda online.

Lo primero es incluir un [certificado SSL](#) de seguridad en tu web, para proteger los datos de tus clientes y que viajen de forma cifrada por tu web. Así, si cualquiera con malas intenciones intenta hacerse con los datos de las tarjetas de crédito, por ejemplo, el cifrado le impedirá acceder a esa información.

También muy importante [establecer contraseñas seguras](#) en el acceso a tus gestores de contenidos, como WordPress o PrestaShop. Las contraseñas son la primera barrera ante un intento de robo de datos.

Por supuesto, mantén actualizado el software de los dispositivos con los que trabajes en tu tienda online, incluidas las aplicaciones antimalware que tengas instaladas.

Y por último, es básico realizar copias de seguridad periódica (backups) para restaurar tu web, bases de datos o correo a un estado anterior. En dinahosting disfrutas de una copia de seguridad diaria de los últimos 30 días que puedes [recuperar fácilmente desde el Panel de Control](#).

Ya sabes que en caso de incumplimiento de la protección de datos personales, la tienda online puede enfrentarse a **sanciones muy comprometidas**, además de lo que supondría desde el punto de vista de la pérdida de confianza de tus clientes. Aquí tienes unos cuantos ejemplos de las [últimas resoluciones de la Agencia Española de Protección de Datos](#) en relación con procedimientos sancionadores.



6.3

¡QUE NO TE SANCIONEN! PON TU WEB AL DÍA CON LA LEY DE COOKIES

Las interpretaciones subjetivas o erróneas de la vigente Ley de Cookies ya han empezado a desencadenar las primeras sanciones. Te contamos los puntos clave a seguir para que esto no te suceda ¡toma nota!

Las cookies son datos que almacena el navegador sobre los sitios que visitas.

Cuando vuelves a un sitio que ya hayas visitado y permaneces logueado, o se muestran los resultados según tus preferencias anteriores, o se mantiene el idioma, todo eso es gracias a las cookies.

¿En qué consiste la Ley de Cookies?

A lo que comúnmente llamamos “Ley de Cookies” es al apartado de la Ley de Servicios de la Sociedad de la Información (LSSI) donde se declara que **el usuario debe dar su consentimiento explícito para la implementación de cualquier tipo de cookie no necesaria en su equipo.**

Esto implica que cualquier cookie que no sea estrictamente necesaria y que quieras que funcione en tu web o blog debe ser detallada al usuario y este debe dar su consentimiento a cada una de ellas.

Disponer de unas adecuadas Política de Cookies y de Privacidad es una de las [20 comprobaciones que debes hacer antes de publicar tu web.](#)

¿Qué cookies son estrictamente necesarias y cuáles no?

Son **cookies necesarias o técnicas** aquellas que intervienen en el funcionamiento de la página, como pueden ser las de idioma, datos de sesión, carrito de la compra, etc.

Son consideradas **cookies no necesarias** aquellas que no influyen en el funcionamiento de la web. Las más habituales son las de analítica, redes sociales y publicidad.

Estas cookies suelen utilizarse para segmentar los datos de los usuarios y obtener información de sus preferencias para darle resultados adaptados. Pueden ser cookies propias de la web que estás visitando o de terceros: Analytics, AdWords, Google Maps, Facebook...

¿Qué debo hacer para cumplir con la Ley de Cookies?

- **Avisar al usuario de las cookies que utilizas y solicitar su consentimiento:** ya sea con un banner, faldón o popup, debes mostrar al usuario de forma clara todas las cookies que utilizas en tu página para que pueda dar su consentimiento a cada una de ellas. En ningún caso se podrán instalar cookies en su equipo sin su consentimiento explícito.

Puedes ver aquí la [sentencia](#) que se ha emitido a este respecto donde se sanciona el habitual marcado por defecto, o [esta otra](#) donde se sanciona a una conocida empresa por la aceptación tácita de las cookies al seguir navegando.

- **Configuración y permisos de cookies editables:** el visitante de tu web debe de tener la opción de retirar su consentimiento o editar la configuración de sus cookies en todo momento.
- **Apartado de Política de Cookies en tu página:** debes tener un apartado o documento en tu web donde se detalle la Política de Cookies que aplicas en tu sitio. Ahí deben aparecer detalladas con los datos de quién las gestiona, el plazo de tiempo que están activadas y su finalidad.

Hace unos meses la AEPD también actualizaba su guía de uso, considerando que la opción de Seguir navegando no constituye en ninguna circunstancia una forma válida de prestar el consentimiento. Puedes verla [aquí](#).

Si todavía tienes dudas sobre la aplicación de esta ley y quieres quedarte tranquilo, en dinahosting disponemos de un [Servicio Jurídico de Política de Cookies](#) en el que te ayudaremos a confeccionar los textos legales que necesitas.

Si ya dispones de este servicio, te recomendamos que actualices tu web teniendo en cuenta estas últimas novedades en la ley.

VEN A DINAHOSTING

Migramos tu web gratis
Tus webs más rápidas y seguras: NVMe y SSL
Disfruta del mejor Soporte 24/7



6.4 ¿QUÉ TEXTOS LEGALES NECESITA TU WEB O ECOMMERCE?

Si estás pensando en montar una web o ecommerce, o justo acabas de construir tu sitio, **necesitarás incorporar una serie de textos legales para cumplir así con la normativa vigente.**

Dentro de nuestra checklist a la hora de montar una web están los textos, las imágenes, vídeos, formularios y no solemos preocuparnos del Aviso legal, Política de Privacidad o Política de Cookies hasta el final.

En este post te detallaremos qué textos legales son imprescindibles para tu web, blog o comercio electrónico. ¡Empezamos!

¿Por qué necesitas incluir textos legales en tu web?

La finalidad de los textos legales es **informar a tus visitantes de cómo se van a usar sus datos, de las normas de tu página web o si utilizas cookies** de seguimiento. Si te paras a pensar, esto no dista mucho del mundo offline. Por ejemplo, cuando vas a una cafetería dispones de información sobre las tarjetas aceptadas, su horario de apertura y cierre, si tienen terraza... En la consulta de un fisioterapeuta podrás ver sus titulaciones y certificaciones académicas, las empresas de seguro médico con las que trabajan, etc.

Los textos legales son obligatorios si realizas una actividad comercial en tu web, si recoges datos a través de un formulario o si monetizas tu blog con publicidad. ¿Y qué se entiende por venta online? Una compra online es la acción voluntaria de adquirir un bien o contratar un servicio por medio de internet. Y aquí entra todo tipo de productos, desde ropa, calzado u ordenadores, hasta la comercialización de cursos online, guías de contenido o servicios de asesoría o mentoría.

De forma regular la AEPD (Agencia Española de Protección de Datos) impone sanciones a diferentes páginas y ecommerce por no cumplir con las políticas europeas. **Las sanciones más habituales son debidas principalmente a la no aplicación o a la aplicación incorrecta de las medidas exigidas por el RGPD en la gestión y almacenado de datos.** No disponer de un certificado SSL en tu ecommerce o no llevar a cabo las acciones que detallas en tu Política de Privacidad son algunos ejemplos de infracciones que han acabado en sanción.

Puedes ver aquí las últimas [resoluciones de los procedimientos sancionadores](#) llevados a cabo por la Agencia.

Incorporar textos legales a tu web o ecommerce, además de ser imprescindible para no enfrentarte a sanciones y cumplir así con la normativa vigente, es importantísimo a la hora de transmitir credibilidad y dar confianza a tus clientes. Más confianza significa un incremento de las posibilidades de que tu cliente complete la transacción.

Leyes y normativas vigentes

Por lo tanto, si vendes algún producto o servicio, o si recoges información de tus visitantes, debes acogerte a esta normativa:

- [Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico](#) (conocida como LSSICE ó LSSI). Regula las reglas que deben regir la contratación online y las comunicaciones comerciales por correo electrónico, o la instalación de cookies, entre otros aspectos.
- El [Reglamento \(UE\) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas](#) y la [Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales](#). Se ocupan de indicar cómo se debe efectuar el tratamiento de datos personales en territorio europeo y español, respectivamente.
- [Ley 7/1996 de Ordenación del Comercio Minorista](#).
- [Real Decreto Legislativo 1/2007, de 16 de noviembre](#), por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
- [Reglamento \(UE\) 2018/302 del Parlamento Europeo y del Consejo de 28 de febrero de 2018](#). Este reglamento indica que los clientes tendrán libre acceso al comercio electrónico, independientemente del país del que proceda.

Tipos de textos legales para tu web o ecommerce

Una vez te hayas leído las leyes y reglamentos vigentes, toca definir los textos legales que necesitarás en función de tu actividad. Estos son los documentos legales:

Aviso legal

Incluye la información general de tu web para que tus visitantes conozcan quién está detrás de ella. Debes incorporar tus datos de contacto y las titulaciones o certificaciones de que dispongas para realizar tu actividad profesional, asimismo es habitual incluir las condiciones de acceso y uso del sitio web y el régimen de propiedad intelectual sobre los contenidos publicados.

En dinahosting te ofrecemos un [aviso legal tipo gratuito](#) para que incorpores a tu web, seas particular/autónomo o una empresa/organización.

Política de privacidad

Este documento se indican [los datos que recoges, cuáles se guardarán y qué uso harás de ellos](#): finalidades, destinatarios, derechos y todo lo que afecte al tratamiento de datos. Además, los usuarios deben estar informados sobre cómo acceder, modificar o cancelar dichos datos.

Política de cookies

Se trata de un aviso imprescindible para informar al usuario del uso en tu web de cookies, como las que analizan tus hábitos de navegación o tu interacción con redes sociales.

Si quieres ampliar la información sobre la Ley de Cookies, [échale un ojo al anterior capítulo](#).

Condiciones de contratación

Si vendes productos o servicios a través de tu web, esta será la información más importante que debes incluir. Tendrás que crear un documento, donde explicar las características del proceso de compra: datos del vendedor, precios, disponibilidad, devoluciones, garantías, forma de pago o formas de envío, entre otras cuestiones.

Si deseas ver cómo son las condiciones de contratación, [echa un vistazo a las nuestras](#).

SUSCRÍBETE A NUESTRO BOLETÍN

Guías de iniciación a WordPress y recursos básicos de Marketing gratis con tu alta.

Nombre o nombre completo

Email

☐ Acepto la política de privacidad

SUSCRÍBETE

Ejemplo formulario de suscripción con política de privacidad

¿Y necesito incluir todos los textos legales?

Dependiendo de la web que tengas, necesitarás unos u otros. ¡Respondemos a modo FAQ tus dudas!

1. Tengo una tienda online

Necesitarás incorporar el aviso legal, política de privacidad, política de cookies y condiciones de contratación.

2. Tengo un formulario de suscripción y envío newsletters

Tendrás que añadir la política de privacidad como mínimo. Puede que necesites la política de cookies dependiendo del uso que hagas en tu web.

3. Soy freelance y vendo servicios de consultoría en mi web

En este caso, tendrás que incorporar el aviso legal, política de privacidad y las condiciones de contratación.

4. Solo anuncio mis servicios, pero la contratación no es vía web

Si este es tu caso, solo tendrás que añadir el aviso legal y la política de privacidad si dispones de un formulario. En este formulario deberás incluir un link a la política de privacidad.

5. Tengo un blog y tengo instalado Google Analytics

Si recoges información analítica de las visitas de tu web e instalas cookies en tus navegadores, entonces incorpora la política de cookies.

6. En mi web solo tengo un formulario de contacto

Si es tu caso, incorpora únicamente la política de privacidad mediante un check en el que el usuario indica de forma explícita que está conforme con el documento.

7. Tengo un blog personal sin formulario de contacto

En blogs personales en donde no hay finalidad económica no es necesario incorporar ningún texto legal.

8. Mi blog tiene un plugin que genera cookies

En esta situación sí tendrás que incorporar la política de cookies

9. Tengo un blog que recibe comentarios

Incluye la política de privacidad que deberán aceptar tus lectores mediante un check.

10. Estoy monetizando mi blog con publicidad

Tendrás que incorporar todos los textos legales que hemos visto, aviso legal, política de privacidad, política de cookies y condiciones de contratación.

Si necesitas alguno de los textos legales para tu web o ecommerce, echa un vistazo a nuestra sección de [Tu web legal](#). Podrás hacerte con los textos a incluir en la política de privacidad para tu blog, newsletter, formulario de contacto, foros o webs de comercio electrónico.



Para saber más
Mira el vídeo

Tu web más segura:
Asesoría Técnica y Legal



6.5

4 CRITERIOS LEGALES EN LA ELECCIÓN DE TU HOSTING

Uno de los aspectos en los que menos solemos fijarnos a la hora de elegir alojamiento para nuestro proyecto online suele ser el de la legislación, y sin embargo, es de los más importantes. A continuación te resumimos los principales criterios legales a tener en cuenta antes de decidirte por una u otra proveedora de hosting.

Ubicación geográfica del servidor

¿Tienes claro en qué país se va a almacenar toda la información que guardes en tu hosting? Para eso necesitas estar atento a la ubicación geográfica del servidor y a su dirección IP, pues afectará a la legislación por la que se rijan las webs alojadas en él.

No es lo mismo que el servidor se encuentre en España o en Europa que lo haga, por ejemplo, en Estados Unidos. **El servidor que aloja los datos debe estar ubicado dentro del Espacio Económico Europeo** o en un país autorizado al efecto para que pueda considerarse que cumple con el RGPD (Reglamento General de Protección de Datos).



Para saber más
Mira el vídeo
Ventajas de tener un
hosting con IP española

Nuestras webs están alojadas en servidores ubicados en Madrid que cumplen al 100 % con la legislación del país donde llevamos a cabo nuestra actividad. Si quieres saber más sobre nuestra infraestructura, [echa un vistazo a nuestro Centro de Datos](#).

Que la proveedora esté situada en territorio español no te asegura que sus servidores también lo hagan. Si los servidores se ubican fuera de España, comprueba en qué país o países se encuentran. Dado que podría producirse una transferencia internacional de datos a territorios con normativas aplicables diferentes del RGPD, podría ser necesaria una intervención de las autoridades competentes. Para que esto no suceda es necesario que las autoridades comunitarias los califiquen como “seguros” (con una protección equiparable a la proporcionada por nuestra normativa sobre protección de datos).

Condiciones legales de prestación del servicio

La proveedora de alojamiento debe comprometerse escrupulosamente a que no hará un uso de tus datos o de los de tus clientes más allá de lo que consta en las Condiciones de Contratación del servicio que preste. Especial mención a los ecommerce o a las webs que recojan un gran volumen de datos de sus usuarios, debiendo asegurar en todo momento su privacidad.

Si quieres, puedes revisar aquí todas [nuestras condiciones legales](#).

Atención al cliente

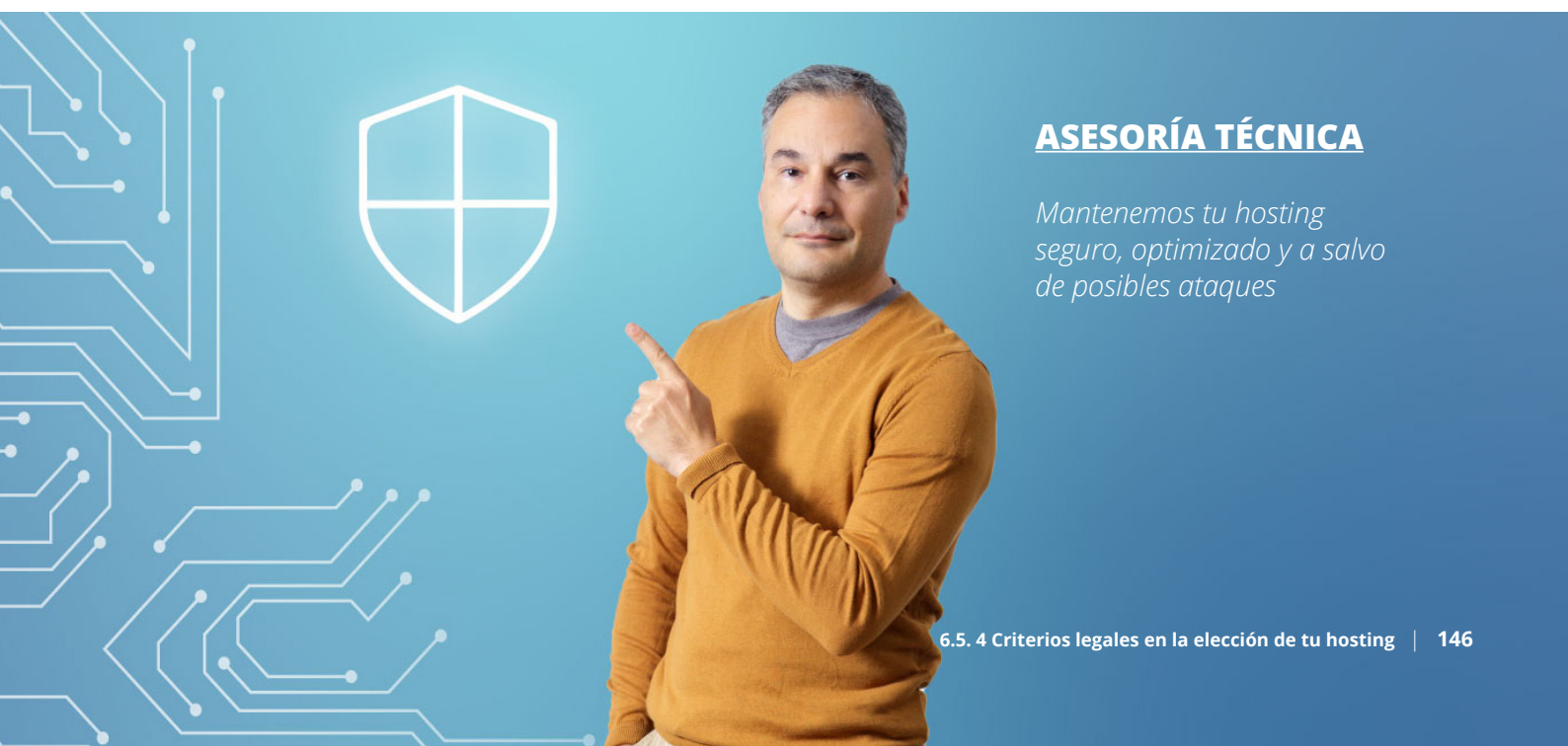
En cuestiones legales, lo tendrás más fácil en todos los sentidos al tratar con una empresa local. Pide referencias sobre el servicio postventa y de soporte técnico que te pueda brindar tu proveedora teniendo en cuenta factores como la disponibilidad horaria, los métodos de contacto que proporciona o el idioma de atención.

Llegado el momento agradecerás que hablen en tu idioma, que te ofrezcan un trato cercano o que no haya diferencia horaria con tu país.

Asesoría legal especializada en Internet

Desarrolla tu negocio con tranquilidad en el mundo online. La [Asesoría legal](#) es un servicio que en dinahosting ofrecemos desde hace años y que puede ser un muy buen complemento a tu presencia en Internet.

Si quieres despreocuparte de [todos los textos legales que requiere tu web o ecommerce](#) (Aviso Legal, Política de Cookies, Condiciones Generales de Contratación, etc.) o si necesitas asesoramiento sobre algún asunto jurídico vinculado con Internet, llámanos y te asesoramos.



ASESORÍA TÉCNICA

Mantenemos tu hosting seguro, optimizado y a salvo de posibles ataques

GUÍA DE CIBERSEGURIDAD

7. Amenazas online

[7.1. Protege tu pyme: las 10 amenazas online más frecuentes](#)

[7.2. ¿Qué es el email phishing?](#)

[7.3. ¿Qué hacer si has recibido un correo phishing?](#)

[7.4. Phishing con fraude en bitcoins](#)

[7.5. Cuidado donde compras: ojo al phishing en ecommerce](#)

[7.6. Ransomware: qué es y cómo combatirlo](#)

[7.7. ¿Qué es el SPAM? ¿Cómo defendernos de él?](#)





7.1 PROTEGE TU PYME: LAS 10 AMENAZAS ONLINE MÁS FRECUENTES

Las amenazas online han ido en aumento y pueden suponer un riesgo para tu negocio. Te contamos las 10 ciberamenazas más frecuentes para que estés al tanto y protejas tu pyme.

Tristemente, junto con el crecimiento de Internet y el auge de las nuevas tecnologías también **ha ido en aumento la ciberdelincuencia**.

El ingenio de los hackers no tiene límite y los ataques y amenazas online han evolucionado de múltiples formas para tratar de robar información, dinero, datos personales... o simplemente causar daños o perjuicios sin otro fin.

Sobre todo en los negocios, los ataques informáticos pueden ser especialmente perjudiciales y conllevar consecuencias graves a nivel económico, legal o de imagen de marca. O en los casos más extremos, incluso provocar el cierre.

Es por eso que nunca está de más tomar las precauciones y medidas que sean necesarias tanto a nivel usuario como empresarial para minimizar riesgos y evitar en la medida de lo posible estas amenazas.

Si quieres mantener tu negocio protegido te recomendamos que pongas en práctica estos [consejos de ciberseguridad para pymes](#).

Las 10 ciberamenazas más habituales

A la vez que suman capas de seguridad es conveniente estar informado y actualizado sobre las amenazas online para saber como afrontarlas y actuar sobre ellas. Estas son las 10 más frecuentes:

1. SPAM

El SPAM o correo basura es una de las plagas que más afectan y saturan la red. Cada día, en todas las bandejas de entrada se reciben miles de mensajes de SPAM.

Este tipo de correos basura no solo son molestos, también pueden ser peligrosos, ya que muchos de ellos son utilizados para transmitir malware, engañar a los usuarios o llevar a cabo diferentes tipos de ataques.

Además de los riesgos de seguridad, el SPAM ocupa bastante espacio en los servidores y consume ancho de banda, recursos y sobre todo, tiempo. ¿Quién no ha perdido el tiempo leyendo o identificando correos falsos?

Para evitar el SPAM es importante que actives filtros y reglas en tu correo para que lo bloqueen y borren.

Contar con un [correo electrónico profesional](#) te será de mucha utilidad para mantener tu bandeja de entrada y la de tus empleados protegida.

Si quieres saber más échale un ojo al capítulo [¿Qué es el SPAM? ¿Cómo defendernos de él?](#)

2. Phishing

El phishing se trata de una **estafa o técnica de suplantación de identidad** mediante la cual el ciberdelincuente intenta hacerse pasar por una marca o persona para engañar al usuario y que este realice una determinada acción o facilite datos sensibles.

Suelen utilizar el **correo electrónico, mensajes de texto o webs espejo con apariencia muy similar a la de la marca que están suplantando**, por lo que en determinadas ocasiones son muy difíciles de detectar.

Generalmente, utilizan un tono de urgencia para requerir credenciales de acceso o aprovechan campañas promocionales para que realices una compra sin pensarlo mucho.

Es clave fijarse en las direcciones de correo y en las URL que utilizan, porque aunque puedan parecer las correctas si revisas el enlace al que linkan por regla general este es diferente del habitual.

Revisar bien los correos, comprobar que vas a realizar una compra en el sitio oficial y no en uno parecido, o confirmar con la empresa si es correcta la información que se solicita puede salvarnos de caer en la estafa.

Si quieres saber más sobre phishing [échale un ojo al siguiente capítulo](#).

3. Ransomware

El Ransomware es un **programa de malicioso (malware) que infecta el equipo y muestra un mensaje exigiendo dinero** al usuario para restablecer el sistema.

Como te adelantábamos en el apartado de SPAM, este malware suele llegar como adjunto en emails sospechosos o también puede descargarse por error en páginas fraudulentas.

La mejor manera de afrontar el Ransomware es utilizar un buen antivirus y evitar descargar archivos o abrir correos dudosos. Con estas precauciones no debería afectarte ni a ti ni a tu empresa.

Si aun así, te aparece un mensaje de Ransomware es vital que no accedas al chantaje, ya que pagar no te garantiza que tu equipo quede liberado ni que se termine la estafa. Lo habitual es que exijan más dinero o que el malware permanezca en tu dispositivo.

Desconectar y desenchufar el equipo también puede salvarnos de que la infección siga propagándose.

Si quieres saber más sobre esta amenaza revisa el contenido [Ransomware qué es y como combatirlo](#)

4. Spyware

El spyware es otro tipo de software malicioso que **se esconde en los equipos para recopilar y robar información del usuario**. De ahí su nombre spy (espía)+ware (software).

Al igual que en el caso del Ransomware, el archivo infeccioso suele enviarse por correo u ocultarse en descargas aparentemente legítimas.

Las acciones que realiza el spyware en nuestro equipo pueden ser diversas, pero algunas de las más habituales son:

- Copiar datos de tarjetas o credenciales de pago
- Recopilar información o datos personales
- Grabar sonido y vídeo accediendo a las cámaras de los dispositivos

El spyware se ejecuta en los equipos en segundo plano, por lo que es difícil detectarlo a simple vista. Sospecha si tu equipo se ralentiza por causas desconocidas o si aparecen mensajes emergentes o utilidades (barras de herramientas, por ejemplo) raras en tu navegador.

La mejor manera de detectar y eliminar este tipo de amenazas es de nuevo, ser precavido con nuestras acciones online y utilizar un antivirus potente.

5. Ataques DDoS

Los ataques DDoS o de Denegación de Servicios Distribuido son aquellos que **actúan sobre redes o servidores webs sobrecargándolos** con un aumento de tráfico simulado para que se colapsen y no puedan responder correctamente.

Generalmente, el aumento de tráfico se produce desde dispositivos y equipos controlados por los atacantes mediante malware. Estos equipos reciben el nombre de bots y pueden ser controlados de forma remota para que envíen solicitudes a una determinada red o servidor.

Al tratarse de dispositivos comunes, los bots son muy difíciles de diferenciar de equipos lícitos, por eso estos ataques son especialmente efectivos.

Los ataques DDoS pueden causar que se sature el servicio de una determinada red, servidor o servicio, provocando que vaya lento o directamente se corte.

Un ejemplo de este tipo de ataque ha sido el que recientemente ha afectado a Andorra Telecom y que dejó sin servicio a varios conocidos streamers allí afincados. De la noticia se hicieron eco diferentes medios como [La Vanguardia](#) o [Xataka](#), entre otros.

6. Virus troyanos

Los troyanos son **virus que se disfrazan de programas aparentemente legítimos**. De ahí, que su nombre provenga de la leyenda del caballo de Troya.

Estos virus por norma general, lo que hacen es dejar un acceso o “puerta trasera” para que el hacker pueda acceder al dispositivo o equipo de manera remota y sin el consentimiento del propietario.

El objetivo de los troyanos suele ser robar información o tomar el control del equipo hackeado para realizar todo tipo de acciones.

Mantén tu software y hardware actualizado así como tu antivirus siempre en activo para afrontar este tipo de amenaza online.

7. Inyección SQL

El lenguaje SQL es uno de los más utilizados en la [creación de bases de datos](#). Los ataques de inyección de SQL consisten en **introducir un código malicioso en las consultas que hace una web cuando llama a su base de datos**.

Esto puede permitirle al atacante modificar las instrucciones que se dan a la base de datos, obtener la información que almacenan o borrarlas, entre otras acciones que afectan a la integridad de los datos.

La inyección de código suele realizarse a través de los campos de formularios desde donde se generan las bases de datos, **aprovechando vulnerabilidades que puede haber en el código de las páginas web.**

Es por eso, que la mejor manera de prevenirlos es comprobar y analizar el código para que no haya errores ni queden puertas abiertas por donde introducir el código invasor.

8. Adware

El adware consiste en un **programa que muestra anuncios publicitarios (ads) en tu ordenador para recopilar información sin tu consentimiento.** Esto último es lo que diferencia de los anuncios legales.

Si en tu PC te salen mensajes tipo ¡¡Enhorabuena has sido el ganador de un iphone!! O se te abren muchos mensajes emergentes con anuncios dispares. Posiblemente, estés infectado con un adware. Este tipo de **anuncios engañosos e invasivos** son los clásicos ejemplos de adware.

El objetivo del adware es que el hacker o atacante obtenga beneficios, bien vendiendo tus datos o bien por los clics y descargas que reciba desde el anuncio.

La manera más habitual de infectarse es realizando descargas online de sitios dudosos o mediante troyanos. Al igual que en el caso de estos, mantén tus programas actualizados para que se parcheen posibles vulnerabilidades y utiliza un antivirus o firewall para detectarlos y borrarlos de tu equipo.

9. Ciberextorsión

La ciberextorsión puede presentarse de muy diversas formas. Grosso modo la ciberextorsión se trata de aprovecharse de los usuarios o víctimas a través de la **intimidación a través de medios digitales.**

Las más habituales suelen ser aquellas en las que se obtiene de manera engañosa (o no) información confidencial del usuario para usarla en su contra. Por ejemplo, si envías online una foto de un desnudo y alguien te amenaza con compartirla sin tu consentimiento, es un caso claro de ciberextorsión. El Ransomware por ejemplo, también sería un tipo de ciberextorsión.

En esta técnica o amenaza online entra muy en juego la ingeniería social. En muchos casos el atacante, sea un hacker o una persona malintencionada, puede utilizar los puntos débiles o conocimientos que tenga de la víctima para convencerla de que le ceda información confidencial (credenciales, datos bancarios, fotografías, información comprometida...).

El contacto puede realizarse a través de cualquier medio online: correo, web, red social, mensajería... Y suele afectar mayormente a usuarios confiados, menores o con conocimientos de internet básicos.

Tras la obtención de la información suelen seguirse amenazas e intimidaciones para que se facilite más información o se realicen transacciones de dinero o cualquier otro requerimiento con fines lucrativos o de perjuicio para el usuario.

Ante esta amenaza la única manera de defensa es estar atento, informar a las personas con desconocimiento sobre estas prácticas y en general, ser precavido a la hora de compartir cualquier información por la red.

10. Cryptojacking

El cryptojacking es una amenaza que ha surgido recientemente junto con el auge de las criptomonedas.

Se trata de una **infiltración en equipos y dispositivos con el objetivo de utilizarlos para minar criptomonedas sin el consentimiento del usuario.**

Para obtener los nuevos activos digitales o criptomonedas es necesario realizar una serie de operaciones a través de una red de equipos informáticos descentralizados del que cualquiera puede formar parte. Esto se conoce como minería y es para lo que se utilizan los equipos infectados por cryptojacking.

Cuanto más equipos “mineros” tenga el atacante mayor será su beneficio en criptomonedas. El atractivo económico que despiertan estas divisas junto con el desconocimiento de su funcionamiento hacen que estas estafas sean bastante prolíficas últimamente.

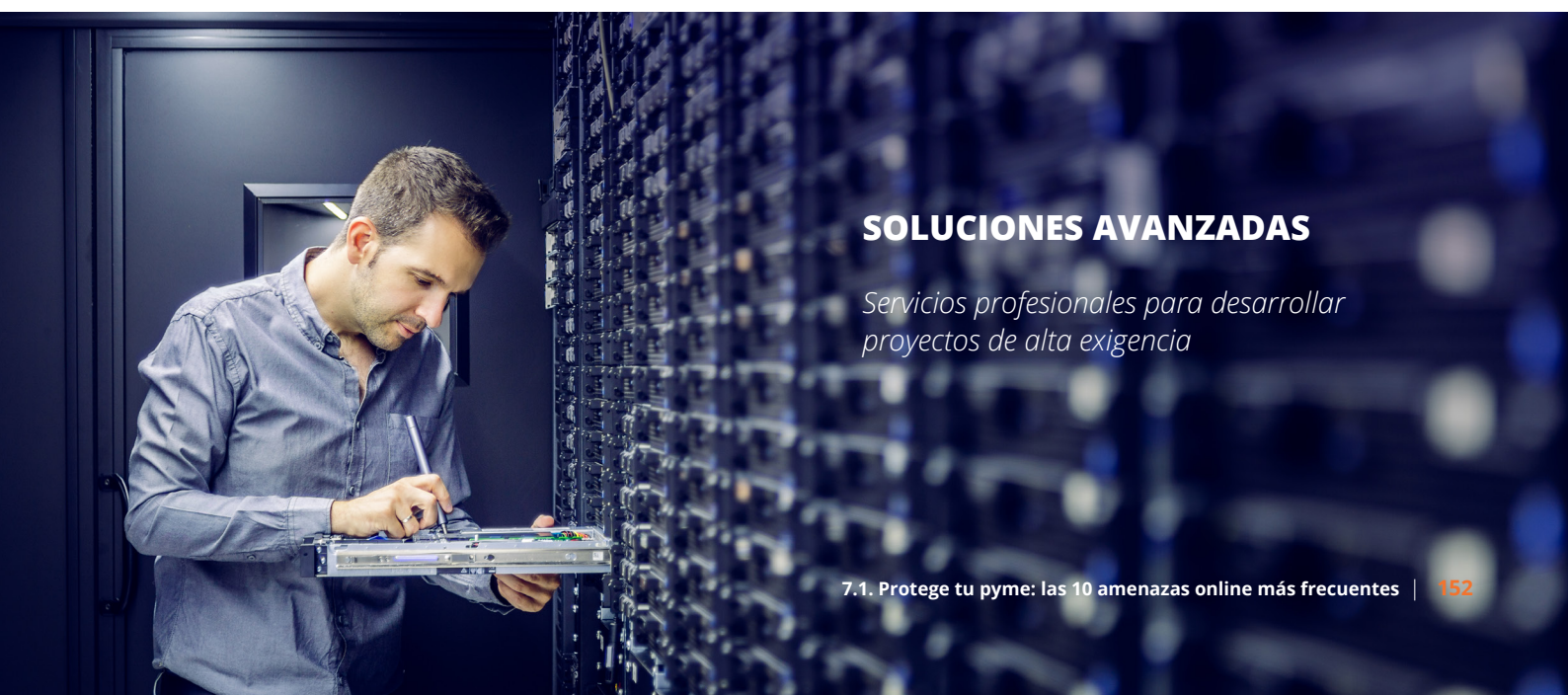
El malware también puede introducirse en los equipos a través de descargas o correos sospechosos. Por lo que las acciones defensivas son las mismas que en los casos anteriores.

Cada vez más, esta práctica se realiza también por todo tipo de programas y apps legalmente solicitando el consentimiento a los usuarios. De hecho, hace poco llamó la atención [el caso de un conocido antivirus](#), que además de luchar contra virus y troyanos también mina de paso unas criptomonedas.

Para terminar nuestro repaso a las 10 amenazas online más habituales te recordamos que **todas ellas son delito, y como tales son denunciables.**

Si sufres algún ataque de estas u otras amenazas digitales cuentas con el derecho de denunciarlas y emprender acciones legales contra los autores.

Esperamos que nuestra información te sirva para estar prevenido y que tu negocio no se vea afectado por ninguna de estas estafas o ataques :)



SOLUCIONES AVANZADAS

Servicios profesionales para desarrollar proyectos de alta exigencia



7.2 ¿QUÉ ES EL EMAIL PHISHING?

Es posible que alguna vez hayas recibido un correo electrónico en nombre de dinahosting u otras marcas que fuera falso, es decir, un **intento de suplantación por phishing**. Ayudándonos de un ejemplo, te explicamos pormenorizadamente qué es el email phishing y cómo puedes prevenirte de estos ataques que persiguen hacerse con tus datos personales.



Para saber más
Mira el vídeo
¿Qué es el email phishing?

Intento de suplantación

Varios de nuestros clientes nos han notificado que han recibido emails como el siguiente:



Este es un ejemplo claro de correo falso (phishing) que intenta suplantar nuestra identidad corporativa. Como ves, se trata de un supuesto email de dinahosting a un cliente para informarle de que su cuenta ha sido suspendida. ¿Con qué nos encontramos si clicamos en el enlace?

El contenido lleva típicamente a una página de login (para robar datos de usuario y contraseña) y después de pago (web con una estética clonada que intenta suplantar a la fuente suplantada y misma pasarela de pago). Cuando estás a punto de pagar para renovar el dominio, el precio del producto se multiplica por 10, o incluso por 100, por lo que si en ese momento no estás alerta y pulsas en pagar, los ciberdelincuentes acaban de vaciarte la cartera.

¿De dónde obtienen los ciberdelincuentes tus datos?

¿Cómo se han apropiado de las direcciones de email? ¿Cómo las han relacionado con el nombre de dominio? Para explicar cómo es posible que se obtengan estos datos, tenemos que hablarte del **WHOIS de dominio**.

Cuando se registra un dominio, los datos de registro pasan a formar parte de una base de datos llamada WHOIS. En ella se almacena información relativa al dominio: quién es el titular, la fecha de registro y caducidad, los servidores de DNS asociados, etc.

Hasta hace unos meses, esta base de datos debía ser (por normativa para todas las empresas registradoras de dominios) **completamente pública** y cualquiera podía acceder a la información de sus diferentes contactos: propietario (o titular), administrativo, de facturación y técnico. El WHOIS recopilaba el nombre, dirección y teléfono de cualquier propietario de un dominio sin que esta persona diese consentimiento explícito. Algunos registradores, como dinahosting, ofrecían precisamente por este motivo un [servicio adicional de privacidad WHOIS](#).

¿Cómo afecta el nuevo RGPD al WHOIS?

Con la entrada en vigor del nuevo Reglamento General de Protección de datos (RGPD), y salvo autorización previa, [los datos que establezcas para tu dominio son siempre privados](#), a excepción de los servidores DNS, registrador, fechas y estado del dominio, que todavía son de acceso público.

Terceras personas se aprovecharon de que todos estos datos aún no eran privados para guardar miles y miles de direcciones y darles después un uso malicioso en forma de fraude vía email. **E incluso después de la puesta en marcha del RGPD, personas malintencionadas seguían utilizando los pocos datos de los que se dispone (nombre de dominio, empresa registradora y poco más) para intentar hacerse pasar por una fuente fiable**, enviando indiscriminadamente correos falsos a cuentas con un patrón típico (por ejemplo: info@dominio.com) donde saben que, por estadística, alguien recibirá el correo.

¿Quién hace los envíos y aloja estas webs falsas?

Normalmente ambas acciones son realizadas por servidores o webs infectados previamente con malware. Por norma general, el titular de los servicios no es consciente de que alberga contenido que puede estar haciendo mailings fraudulentos u hospedando contenidos que intentan robar datos o realizar cobros no autorizados.

La infección de su sistema puede venir ocasionada por múltiples motivos (como cualquier fuente de malware). **Los sistemas normalmente no tienen nada que ver con la entidad a la que se intenta suplantar**. Por ejemplo, en el caso que del que os hemos advertido esta semana, los envíos se hacían desde distintas partes del mundo (sobre todo desde Alemania) y las webs falsas se encontraban (en una gran parte) en servidores italianos. Como sabes, dinahosting no posee sistemas en ninguno de estos dos países.

La actuación en este caso siempre pasa por denunciar la situación (bien la empresa suplantada o bien cualquier otro afectado) para que las entidades infectadas tomen medidas al respecto.

Precauciones que puedes tomar

A la hora de detectar un ataque como este, hay técnicas sencillas a las que puedes recurrir. Aunque la redacción del mensaje se parezca a la que te suele enviar tu remitente habitual, siempre hay detalles que hacen levantar sospechas:

- **El saludo del mensaje.** En email phishing, se recurre a saludos genéricos como “Estimado cliente” o “Apreciado cliente”. Dinahosting, y la mayoría de las empresas, se dirigen a ti siempre por tu nombre.
- **La dirección de correo electrónico.** Fíjate bien en ella y comprueba si el dominio del que procede el email coincide con los datos reales de la empresa. Dinahosting nunca te enviará un correo desde una dirección como root@localhost. Si dudas, revisa bien los detalles o cabeceras del correo, pues una dirección de email se puede enmascarar. Si se da el caso verás información del estilo “Empresa legítima <from:direccion@dedudoso.origen”.
- **Enlaces disfrazados.** Lo normal es que tu proveedora no te pida que ejecutes una acción relacionada con la gestión de tus servicios desde un enlace integrado en el propio mensaje. No es seguro y por lo tanto no es lo habitual. Si antes de pinchar en el enlace (que puede tener un aspecto medianamente confiable) copias y pegas su ruta, podrás ver que el destino no tiene relación alguna con la empresa suplantada.
- **Solicitud de información sensible.** Si en el contenido del correo te solicitan el número de tu tarjeta de crédito, la contraseña de tu cuenta, etc. haz caso omiso. Estás ante un claro intento de phishing.

- **La firma.** La mayoría de las empresas personalizan su firma de correo electrónico con un nombre de contacto, email y teléfono en caso de que el cliente necesite asistencia. En caso de phishing, esta información suele omitirse.
- **Formato corporativo.** Fíjate bien en si el email respeta la apariencia habitual de los correos de la marca: logotipo, tipografía, lenguaje, sin errores ortográficos, etc.
- **Urgencia en el mensaje.** Los emails de phishing están pensados para que actúes al momento. Se aprovechan de esta sensación de urgencia para despistarte y que no te pares a analizar el mensaje. Piensa que una empresa sería siempre te avisará en repetidas ocasiones antes de dar de baja cualquier servicio que tengas y con una antelación prudente.
- **Web de destino.** Aún en el caso de que el correo haya conseguido engañarte, cuando llegues a la página de destino falsa fíjate siempre en ella con detenimiento. Habrá elementos que no concuerden con los de una fuente legítima: normalmente no tienen "https" (certificado digital de seguridad) en la URL, puede que la URL directamente no guarde relación alguna con la de la entidad suplantada, faltarán contenidos y/o enlaces en la web, etc.

¿Qué hicimos en dinahosting?

A nivel técnico, hemos denunciado el caso al administrador de los sistemas de origen. También hemos reportado el caso a todas las fuentes de registro de malware y phishing posibles, y se ha comunicado a otros proveedores de correo para solicitar que lo consideren directamente correo basura y no lo entreguen a sus usuarios.

Si tu cuenta de correo está alojada en dinahosting, no hay de que preocuparse, pues estos emails se etiquetarán automáticamente como SPAM. Si por el contrario tu servicio de correo está en un gestor externo al nuestro, cabe la posibilidad de que el email infectado llegue a tu bandeja de entrada en algún momento. ¡Presta mucha atención para que no te la cuelen!

Y por supuesto, si dudas, consulta con Soporte Técnico antes de aportar tus datos de pago. Ten en cuenta que para cualquier acción de renovación de servicios tienes que pasar por tu [Panel de Control de dinahosting](#), accediendo con tu usuario y contraseña.



CÓMO DETECTAR el EMAIL PHISHING

1

FÍJATE EN LA DIRECCIÓN DEL REMITENTE

Comprueba si el dominio del que procede el email coincide con los datos reales de la empresa.

De: "Empresa legítima" <from: **direccion@dedudoso.origen**>

2

UTILIZA SALUDOS GENÉRICOS

"Estimado cliente", "Apreciado usuario"... La mayoría de empresas personalizamos los correos con tu nombre.

Estimado **cliente**, ❌

Hola **Pablo**, ✅

3

SOLICITA INFORMACIÓN SENSIBLE

Si te solicitan el número de tu tarjeta de crédito, la contraseña de tu cuenta, etc. haz caso omiso.

Introduce **aquí** tus datos bancarios. ❌

<http://enlacedeposible>
estafa.fake/nolosigas ❌

4

ENLACES DISFRAZADOS

Antes de clicar revisa la ruta de los enlaces. Sospecha si el destino no tiene relación alguna con la empresa suplantada.

5

FORMATO CORPORATIVO

Fíjate bien en si el email respeta la apariencia habitual de los correos de la marca: logotipo, tipografía, firma, lenguaje...



6

URGENCIA EN EL MENSAJE

El phishing está pensado para que actúes al momento. Aprovecha la sensación de urgencia para despistarte y que no te pares a analizar el mensaje.

Necesitamos que nos remitas esta información **lo antes posible**. ❌

7

WEB DE DESTINO

Si llegas a la página de destino falsa fíjate siempre en ella con detenimiento. Habrá elementos que no concuerden con los de una fuente legítima.



Si lo prefieres
**Mira el vídeo
online**



7.3 ¿QUÉ HACER SI HAS RECIBIDO UN CORREO PHISHING?

Si has recibido en los últimos días un correo con phishing intentando suplantar a dinahosting u otra compañía, ¿qué debes hacer?

Para empezar los ataques phishing pueden llegarte a través de un correo electrónico o SMS y es algo bastante común. En sí mismos no son peligrosos si no das tus datos personales o bancarios, pero debes actuar con mucha cautela siempre que recibas uno.

1. Sigue la información que publique tu proveedor

Lo primero que debes hacer es seguir la información que publique tu **proveedor en su blog, web y redes sociales** para mantenerte al tanto en todo momento y resolver tus dudas.

En dinahosting, como respuesta al phishing de las últimas ocasiones, hemos denunciado el caso al administrador de los sistemas de origen. También reportamos el correo a todas las fuentes de registro de malware y phishing posibles, y nos hemos comunicado con los proveedores de correo para solicitar que lo consideren directamente correo basura y no lo entreguen a sus usuarios.

2. Marcar el remitente como SPAM

Después de seguir la información de tu empresa proveedora, **marca la dirección del remitente como SPAM** para no recibir correos de nuevo. Fíjate que el remitente no vaya enmascarado, de lo contrario puede que estés marcando como SPAM direcciones válidas.

En dinahosting, siempre que detectamos un phishing, etiquetamos directamente estos correos como SPAM.

3. Nunca contestes al correo phishing ni cliques en los links

La estrategia de los correos phishing es **buscar interacción**, por lo que siempre te harán preguntas o te informarán de que tu servicio se ha eliminado y que de forma urgente lo renueves.

En definitiva, los ciberdelincuentes juegan con **el tiempo y la urgencia**, para que no nos fijemos en los links adjuntos, en la redacción del correo, o en el saludo, elementos claves para detectar el phishing.

Ten cuidado en descargar los adjuntos y hacer clic en los links, ya que pueden contener malware y poner en riesgo nuestros dispositivos.

4. Borra el mensaje

Borra el mensaje para evitar despistes futuros.

5. Colabora

La colaboración de todos es clave para frenar el phishing. La OSI pone a disposición de todos los ciudadanos un buzón donde puedes reportar todos los casos de phishing que detectes.

He dado mis datos en un correo phishing, ¿qué pasos debo seguir?

- **Comunícate con tu entidad bancaria** para que puedan asesorarte en este fraude y eliminar los cargos que hagan en tu cuenta. Siempre es muy recomendable que actives alertas antifraude en tu cuenta como prevención.
- **Cambia las contraseñas** del servicio que fue hackeado y de tu cuenta de correo.
- **Interpón una denuncia** ante la Policía o Guardia Civil en sus oficinas de delitos telemáticos.



TU **HOSTING** DE ALTO RENDIMIENTO

Más espacio gratis

Garantía de reembolso: 30 días

Pruébalo gratis y paga al publicar tu web



7.4 PHISHING CON FRAUDE EN BITCOINS

En los últimos días hemos detectado que hay activa una campaña de phishing que extorsiona a los usuarios para que entreguen un rescate en forma de bitcoins a cambio de no difundir contenido comprometido suyo. ¿Te suena el tema?

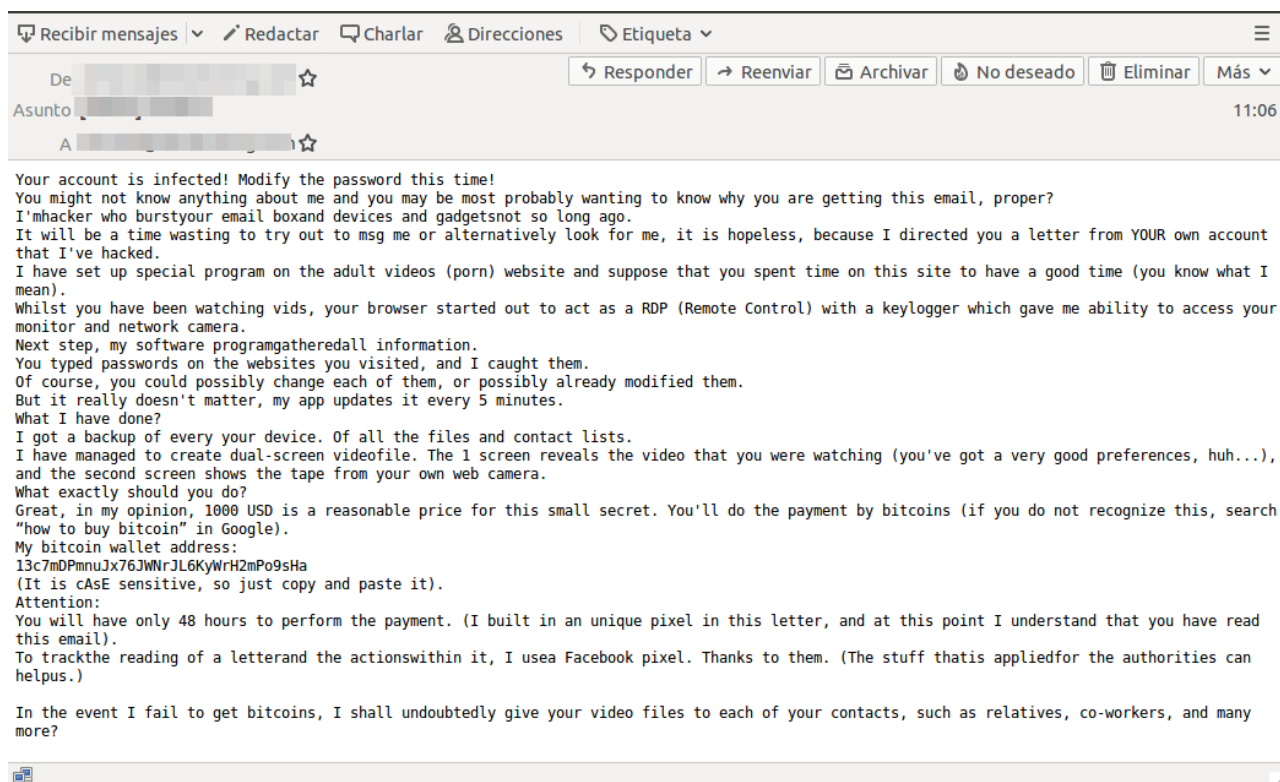
El phishing es una técnica de captación ilícita de datos personales (principalmente relacionados con claves para el acceso a servicios bancarios y financieros) a través de correos electrónicos o páginas web que imitan/copian la imagen o apariencia de una empresa o entidad.

En el caso que nos ocupa, **la campaña de email phishing se apoya en el chantaje económico**. El crecimiento del mercado de las criptomonedas y la dificultad que conlleva rastrear su origen ha llevado a los ciberdelincuentes a **optar por la moneda digital a la hora de cometer infracciones como esta**.

¿En qué consiste la estafa?

La víctima recibe un correo electrónico indicando que un delincuente informático accedió a sus dispositivos y a su cuenta de correo. Gracias a este acceso, el atacante podría haber instalado en el equipo de la víctima un software que le permitiría grabar vídeos de su Webcam. Más concretamente, mientras visitaba supuestamente webs de contenido adulto.

La estafa consiste en que si el atacante no recibe 1000\$ en bitcoins en menos de 48 horas, hará públicas las grabaciones y las enviará a todos los contactos de la víctima. Este es un **ejemplo de un email** de este tipo:



Desde luego, se trata de un engaño

En ningún momento los ciberdelincuentes tienen acceso a la cuenta de correo ni a los dispositivos del usuario. Sin embargo, abundan por la Red correos de phishing como este, que incluso incluyen la contraseña de la cuenta de correo del usuario, lo que hace todavía más creíble el fraude. La contraseña la obtienen de recopilatorios de bases de datos que hay en Internet, tanto públicamente como en la red profunda (Deep Web).

Si has sido víctima de algo así, te recomendamos cambiar lo antes posible la contraseña de tu cuenta y de cualquier otro servicio en el que estés utilizando la misma clave. Puedes [comprobar aquí si tu cuenta de correo está en alguna de estas bases de datos](#).

Y esto no es lo único. A la hora de detectar ataques de email phishing, hay otras técnicas más sencillas a las que puedes recurrir, [revisa el capítulo anterior para conocerlas](#). **Lo importante siempre es mantener la calma y no dejarse llevar por la incertidumbre del momento.**

SIEMPRE DISPONIBLES

Te atendemos las 24 horas del día, todos los días de la semana, durante todo el año, vía teléfono, email o chat.





7.5 CUIDADO DONDE COMPRAS: OJO AL PHISHING EN ECOMMERCE

Evita estafas y protege tu tienda: te contamos cómo detectar el phishing en ecommerce y cómo estar prevenido para que no te suceda en tu tienda online.

Cuanto más en auge están las compras o acciones online, más proliferan las estafas para tratar de engañar a los usuarios y robarles su dinero o datos. Es por eso que es muy importante estar informados y saber cómo detectar estas técnicas ilícitas para que no nos afecten, tanto como usuario como si gestionas una web o ecommerce.

El phishing es una de las estafas online más frecuentes. Se trata de una acción malintencionada que trata de robar información o dinero de los usuarios mediante la suplantación de identidad a través del correo, de mensajes, de una web o, como el caso que nos ocupa, a través de una tienda online.

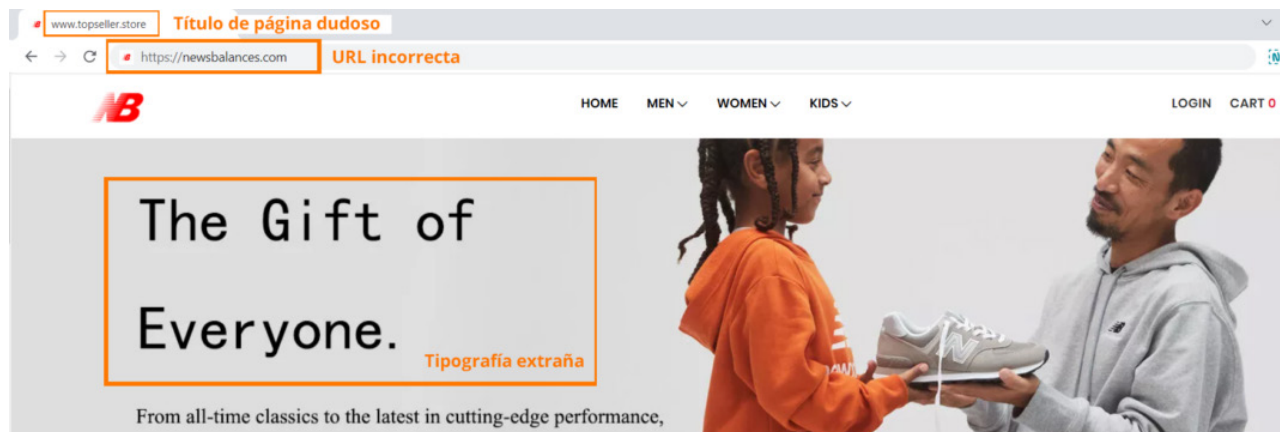
¿En qué consiste el phishing en ecommerce?

El phishing en ecommerce consiste en utilizar una web falsa y aparentemente igual a una tienda online real para que los usuarios la confundan con la original y realicen compras a través de ella.

Los estafadores **se aprovechan de la confianza de los usuarios en una determinada marca o persona para hacerse pasar por ellos** y solicitar transacciones ilícitas por unos supuestos productos o servicios que ni siquiera existen. Para llevar a cabo estos ataques realizan páginas web con diseños muy similares o iguales a otras tiendas online reales, las llamadas **webs espejo**. Utilizan también URL con dominios parecidos al original y replican el estilo de colores, textos, botones, fotos... o directamente los copian.

Suelen captar a los usuarios por correo, mensaje o incluso con anuncios en redes sociales. Es frecuente también que se aprovechen de las campañas de fechas señaladas para crear urgencia en los usuarios y que compren fijándose menos. **Su objetivo es que realices una compra para quedarse con tu dinero y posiblemente aprovecharse de tus datos.**

Aquí vemos un **ejemplo de phishing en ecommerce** sobre la conocida marca de zapatillas New Balance:



Aparentemente, parece la página correcta, pero si te fijas en los detalles se aprecian elementos sospechosos. La URL por ejemplo es newsbalances.com (la URL correcta sería newbalance.com). En el título que aparece en las pestañas muestra una página sospechosa topsellers.stores. También se ve que la tipografía del banner es rara y no cuadra con la imagen corporativa habitual de la marca.

Al continuar navegando por la página surgen también otras alertas, pero como ves, son pequeños matices o detalles, fáciles de pasar por alto. Por eso hay que estar atentos.

Cabe mencionar que los ecommerce copiado o webs afectadas no tienen culpa de este hecho, y directamente tampoco pueden hacer nada para evitarlo. En cambio, esto sí puede **repercutirles negativamente afectándoles a su imagen de marca**, ya que es frecuente que los usuarios responsabilicen al ecommerce original de haber sido engañados.

¿Cómo detectar una web de phishing?

Para evitar caer en una tienda online falsa puedes seguir estas precauciones:

Fíjate en la URL y en el diseño

Como te adelantábamos antes, este tipo de webs espejo cuenta con una URL similar a la del ecommerce original.

Por ejemplo, si zara.com es la URL original, una de phishing podría ser zaara.com, zara.online, zarah.es.... Es frecuente que cambien dígitos o el TLD (parte final del dominio) por uno que suene real.

Revisa en internet, buscadores y redes sociales **cuál es la URL correcta del ecommerce antes de realizar una compra**.

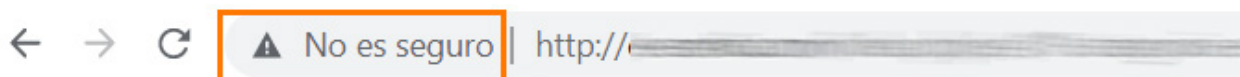
Revisa el diseño. Aunque cada vez los hackers del phishing son más cuidadosos, es posible que pasen por alto detalles. Si hay incoherencias estéticas, cambios de tipografía, falta el favicon, carece de etiquetas de título y descripciones, etc. Si algo te canta, mejor verifica varias veces que estás comprando en el sitio correcto.

Compra solo en sitios seguros

Comprueba que el sitio en el que vayas a comprar cuente con todos los textos legales. Cualquier ecommerce debe contar con un Aviso Legal, una Política de Privacidad y Cookies, y con las Condiciones de contratación bien visibles en su web.

Si te cuesta encontrar estos apartados en su web o no existen, sospecha del sitio.

También **es frecuente que las páginas de phishing no cuenten con certificado SSL** que proteja la información de los usuarios y la marque como segura. Fíjate en la barra del navegador, debe aparecer un candado cerrado o nada. Si sale un aviso de que el sitio no es seguro, desconfía y realiza las siguientes comprobaciones.



Pero ten en cuenta que esto es solo un detalle, los hackers van evolucionando y son cada vez más las páginas de phishing que también aparecen marcadas como seguras. Y también al contrario, algunos ecommerce reales y lícitos, todavía no tienen certificado SSL y aparecen marcados como inseguros. Para que esto no te pase asegúrate de tener un [Certificado SSL en tu tienda online](#).

Por otro lado, existen páginas web donde nos alertan de diferentes ataques de phishing. Está bien revisarlas si nos surgen dudas con una web. Algunas de las más populares son: [INCIBE](#), [OSI](#) o [fakeinet](#).

Contrasta los datos

Es habitual que en las páginas de phishing tampoco se muestre **información sobre la empresa o datos de contacto**. O en caso de contar con ellos pueden ser falsos o incluso estar copiados de la página original.

Por eso, si cuenta con unos datos de dirección en su web que indiquen donde se ubica físicamente la sede de la tienda online, comprueba por otras vías si efectivamente existen. Puedes buscarlo en Google Maps o en cualquier otro buscador. Generalmente, los datos de dirección figuran en su Contacto o en su Aviso Legal.

En el Aviso Legal también puedes revisar el NIF de la empresa y comprobar si existe en el Registro Mercantil de la ciudad o si aparece en algún otro directorio público de sociedades.

Probar al llamar por teléfono o contactar por la vía que indiquen también es una buena forma de verificar que el sitio es lícito.

Evita métodos de pago dudosos

Paga solo a través de **plataformas que ofrezcan garantías**. Si cuando llegas al carrito de compra te faltan elementos o te parece que la información que piden no es necesaria, o si la pasarela de pago te resulta extraña, mejor no continúes con el pago.

Hace un tiempo se cambió la normativa para que los pagos a tienda fuesen más seguros (PSD2). Ahora lo normal es que se solicite la doble autenticación para la mayoría de las transacciones online.

También desde las entidades bancarias se han incrementado las medidas de seguridad: facilitando apps propias, verificando pagos o incluso, impidiendo directamente operaciones desde sitios dudosos.

Revisa comentarios y valoraciones la página

Si dudas sobre una determinada web en la que quieres comprar, prueba a buscar valoraciones sobre ella. Si se trata de una estafa que lleva tiempo funcionando es posible que haya comentarios en sus redes sociales alertando de esto.

Los usuarios engañados o estafados suelen también dejar su valoración negativa bien clara en redes, en Google My Business o donde sea.

Las páginas que tienen desactivadas las valoraciones y comentarios o no tienen apenas interacción en las redes son las más sospechosas. ¡Cuidado con ellas!

¿Qué hacer si han suplantado mi ecommerce?

Si has sufrido un ataque de phishing en tu ecommerce, puedes realizar estas acciones:

Denuncia la web estafadora

Si has detectado un caso de phishing sobre tu ecommerce o sobre cualquier otro, **lo primero es denunciarlo**. Para ello la Oficina de Seguridad del Internauta facilita en [esta web](#) un correo para reportarlo.

Avisa a tus usuarios

Para **que ninguno de tus clientes se vea afectado por la estafa**, mejor avísalos en cuanto detectes el caso. Esto también te ahorrará que descarguen sobre tu marca el fiasco del engaño.

Protege tu marca

Para estar prevenido, revisa tu marca en buscadores y analiza de vez en cuando si existen URLs sospechosas similares a tu tienda online que se puedan utilizar en tu contra.

[Registrar aquellos dominios más habituales](#) para que no lo utilicen sitios fraudulentos, es una buena manera de dificultar las técnicas de phishing.

También, como señalábamos antes, añadir un plus de seguridad con un [Certificado SSL](#) nunca está de más.

Por último, ten en cuenta que **comprar online es generalmente seguro si lo haces desde sitios de confianza y aplicas el sentido común en tus compras.**

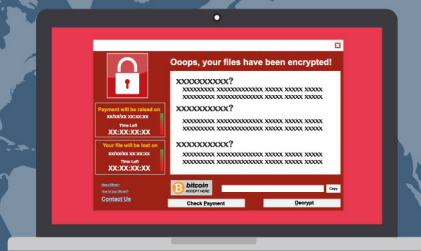
Esperamos que estos consejos te ayuden a evitar los ataques de phishing en ecommerce y a mantener tu tienda protegida.

CREA TU **TIENDA ONLINE** EN POCOS MINUTOS

Planes WordPress
con WooCommerce o
PrestaShop en 1 clic

Garantía de reembolso:
30 días





7.6

RANSOMWARE: QUÉ ES Y CÓMO COMBATIRLO

Todo lo que necesitas saber sobre el Ransomware: qué es, cómo protegerte de él y cómo combatirlo en caso de infección. ¡Vamos allá!

¿Qué es el Ransomware?

Del inglés, *ransom* (rescate) y *ware* (producto o mercancía). El Ransomware es un **programa de software malicioso que infecta tu equipo**, mostrándote mensajes donde se **exige el pago de dinero** para restablecer el funcionamiento normal del sistema.

La forma más habitual de contraer la infección es abriendo un archivo que nos envían como adjunto por email, en formato PDF o como documento de texto.

Normalmente estos emails están enmascarados bajo remitentes conocidos, pero **la redacción del mensaje puede hacer que sospeches de que no se trata del verdadero remitente habitual**: saludos genéricos, fallos gramaticales, solicitud de información sensible sobre el propio email...



Ejemplo de ataque de Ransomware @BBCNews

Este es solo un ejemplo de ataque de Ransomware. Échale un ojo y verás que sigue un patrón muy determinado:

- Juega con el miedo, insistiendo en que puedes perder toda la información si no sigues sus instrucciones.
- Crea sensación de urgencia incluyendo el tiempo que te queda para pagar el rescate.
- Indica claramente la cantidad de dinero que quieren que les ingreses, generalmente en bitcoins.

El popular “virus de la Policía”

Otro de los ejemplos más populares lo tenemos en el conocido como “virus de la Policía”. Se produce cuando en tu equipo se muestra repentinamente un mensaje procedente supuestamente del Cuerpo de Policía, en el que **se te alerta de que has estado accediendo a webs vinculadas con alguna actividad ilegal** (generalmente pornografía, webs de apuestas no reguladas, etc.).



Ejemplo de ataque del “virus de la Policía” @policia.es

Con tu equipo ya bloqueado, te solicitan el pago de un rescate para recuperarlo, y de nuevo, se repite el mismo patrón:

- Se incluye el logotipo de la Policía, así como la dirección IP del equipo, para hacer más creíble el mensaje.
- Se indica la cantidad a abonar en concepto de rescate.

Aunque es evidente que la Policía nunca exigiría un pago de dinero mediante este tipo de canales no oficiales, hay muchos usuarios que se dejan llevar por el miedo y terminan sucumbiendo a la estafa.

¿Cómo puedo protegerme del Ransomware?

Cuando a tu correo electrónico, teléfono móvil, cualquier red social... Llegue un mensaje en el que se te coaccione u obligue a actuar para evitar consecuencias negativas sobre tus dispositivos o tus ficheros privados, desconfía automáticamente de que estás siendo víctima de Ransomware.

Sin lugar a dudas estamos ante una de las amenazas que más se está produciendo en los últimos tiempos, y no solo afecta a particulares sino también a grandes empresas. **Lo básico, y por lo que siempre deberías empezar para**

protegerte, es por mantener tus dispositivos tecnológicos libres de virus. Ten en cuenta que el Ransomware puede llegar a colarse en tu ordenador sin que tú te enteres, capturando todo tipos de datos personales en un segundo plano.

Además, siendo el email su principal vía de entrada, es importante que tomes algunas precauciones. Estos son **algunos trucos que puedes usar como usuario para no caer en la trampa:**

- No abras mensajes de usuarios desconocidos ni mucho menos sus archivos adjuntos. Por supuesto, tampoco instales nada.
- Desconfía de los enlaces que te envían, especialmente si se presentan como enlaces acortados.
- No te olvides de actualizar el sistema operativo, el navegador y el antimalware que utilices.
- Utiliza contraseñas seguras y la [autenticación en dos pasos](#) en los logins de todos los servicios que puedas, empezando por el email.

¿Qué hacemos en dinahosting para ayudarte?

Como te hemos dicho, el email es una de las vías de entrada más comunes para los ciberdelincuentes. Por eso, en dinahosting trabajamos continuamente en nuestro sistema de detección de virus del correo electrónico para que los emails enviados a través de nuestros hostings no propaguen este tipo de virus.

Filtros de SPAM

Nuestros servidores cuentan con filtros de SPAM que revisamos de forma continua para evitar que los emails con Ransomware lleguen a tu bandeja de entrada. Además, desde el apartado Hosting > Correo > Reglas y filtros de tu [Panel de Control](#) puedes añadir reglas personalizadas para que se marquen como SPAM los correos que tú consideres oportunos.

Registro SPF

Cuando das de alta un hosting o dominio en dinahosting, [creamos por defecto un registro SPF](#). Su función es comprobar que el servidor desde el que te envían un correo es ciertamente el que indica el dominio.

Escaneo de correos

Tenemos un sistema dedicado a escanear todos los correos entrantes y salientes con reglas para filtrar determinados ficheros que puedan incluir amenazas.

Firewall DNS

Contamos con [Firewall DNS en nuestros servidores](#). Con esta protección evitamos servir al usuario dominios que en el pasado hayan alojado virus, páginas de phishing y otro malware. O lo que es lo mismo, bloqueamos determinadas direcciones IP por estar en listados de IP maliciosas.

Además, desde el apartado de Hosting > Seguridad > Antivirus web de tu [Panel de Control](#) puedes escanear directorios de tu web para ver si hay algún fichero infectado. Al terminar la revisión te proporcionamos un informe gratuito con el resultado del chequeo y, **en caso de que se detecte algún tipo de archivo malicioso, tienes la posibilidad de solicitarnos una desinfección bajo presupuesto.** En dinahosting contamos con un departamento especializado en combatir todo tipo de malware.

¿Qué hago si soy víctima de Ransomware?

Los ciberdelincuentes se lucran con este tipo de prácticas, por eso es importante no contribuir a su negocio haciendo cualquier tipo de pago. Además:

- Si pagas una vez, lo más probable es que sigas siendo objeto de estos ataques en el futuro.
- En cuanto hagas el primer depósito pueden solicitarte una segunda cifra todavía mayor.
- Se trata de una estafa. El hecho de pagar no te garantiza que vayas a recuperar tu equipo.

Ante todo hay que mantener la calma y no dejarse llevar por la incertidumbre del momento:

- ¿Tienes dudas acerca de la veracidad del mensaje? No lo abras.
- Si ya lo has hecho y tu equipo está infectado, apágalo inmediatamente.
- Si el equipo tarda en apagarse, desconecta el cable de corriente.

Tenemos que tratar de aislar rápidamente el equipo antes de que la infección continúe propagándose.

Si dispones de [copias de seguridad de tu web, correo y bases de datos como las que te proporcionamos en dinahosting](#), podrás acceder a una versión prácticamente igual de los servicios que se hayan visto afectados. Tan solo tienes que restaurar las copias en tu equipo, una vez esté formateado y securizado.



HOSTING EN PRUEBAS

Con [nuestro hosting en pruebas](#) podrás testear todas las funcionalidades de tu plan de alojamiento totalmente gratis.

No pagarás nada hasta que la web sea pública.



7.7 ¿QUÉ ES EL SPAM? ¿CÓMO DEFENDERNOS DE ÉL?

El SPAM afecta a toda la comunidad de usuarios de Internet, tanto a individuos como a empresas. ¡Veamos cómo funciona y como protegernos!

¿Qué es el SPAM?

Solemos denominar SPAM a los mensajes de correo electrónico no solicitados que recibimos, también llamados correo no deseado o correo basura.

Son mensajes que buscan producir beneficios para su emisor, resultando en la mayoría de casos molestos para sus múltiples receptores, ya que suelen consistir en la **difusión de publicidad engañosa**.

¿A quién afecta el SPAM?

En mayor o menor medida, el SPAM afecta a toda la comunidad de usuarios de Internet, tanto a individuos como a empresas.

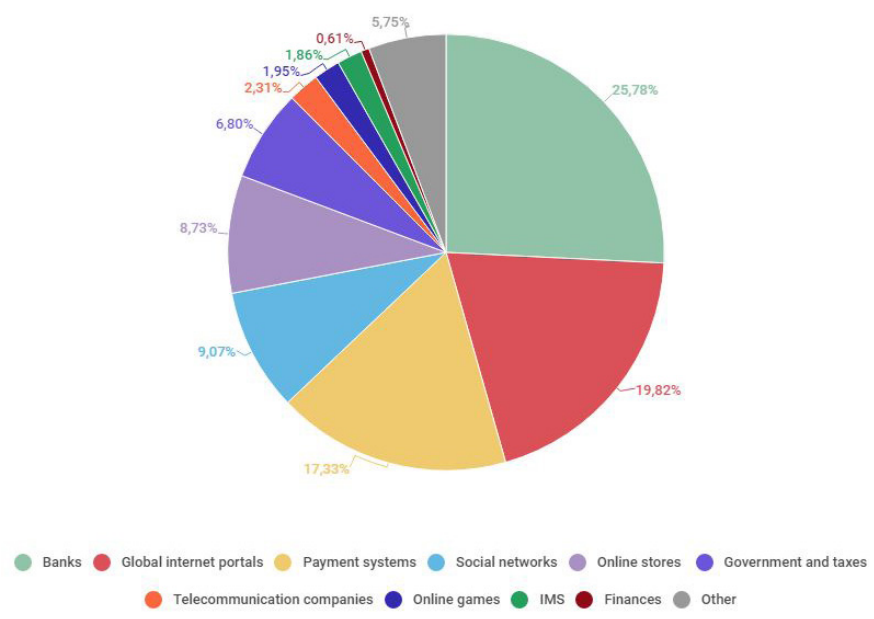
Según diferentes analistas y empresas, el correo basura ya supera actualmente el 85% del correo electrónico generado (fuente [talosintelligence.com](https://www.talosintelligence.com)), lo que supone, cada vez más, un problema importante para Internet.

¿Cómo nos perjudica el SPAM?

Los daños que ocasiona el SPAM pueden presentarse a distintos niveles:

- Pérdida de tiempo para usuarios y empresas, que tienen que invertir tiempo en su eliminación.
- Pérdidas económicas por daños en los sistemas o robo de información financiera.
- Genera tráfico, ancho de banda y espacio superfluo, dejando menos recursos disponibles para actividades productivas.
- Obliga a destinar a los proveedores de servicios recursos de hardware y software para su transmisión, análisis y filtrado, cada vez con mayor intensidad.
- Daños de reputación, por hackeo de la cuenta de correo o página web.
- Irritación y descontento. Como usuarios es habitual sentirnos molestos al tener que identificar y eliminar frecuentemente correos no deseados. En el proceso podríamos además perder correos importantes por error.
- Falsos positivos. Perjudican a correos lícitos que no se entregan correctamente al destinatario por ser catalogados de forma errónea como SPAM.
- El contenido de los correos basura puede ser muy distinto, aunque suelen estar relacionados con sistemas de pago, bancos, productos farmacéuticos, juegos online, etc.

Como referencia, [Kaspersky](#) nos facilita estos datos sobre las categorías de SPAM que se movieron en la red en el primer trimestre de 2019:



Gráfica sobre el Spam - Fuente Kaspersky

¿Por qué a mí?

Existen múltiples formas mediante las que un spammer consigue tu dirección de email. En la mayor parte de casos se obtienen rastreando la web y extrayendo todas las direcciones de correo que aparecen publicadas.

Otra de las fórmulas más habituales consiste en acceder a listas de discusión o foros en los que figura como referencia una dirección de email.

También surge de empresas que venden datos de contacto a terceras personas, un aspecto que se suele consentir al aceptar condiciones de uso que casi nadie se para a leer. Este fenómeno es frecuente en suscripciones a boletines, listas de distribución o cualquier otro tipo de servicio que requiera un correo de contacto.

En caso de tener un dominio registrado, es posible figurar en bases de datos públicas a nivel internacional, que muchos spammers utilizan para enviar correo basura a direcciones aleatorias que se puedan construir a partir de este dominio.

¿Qué hace dinahosting para ayudarme?

Todo el correo que llega a los servidores de dinahosting es filtrado para evitar la proliferación de virus y SPAM:

- En relación con los virus, la eficacia de nuestros sistemas se aproxima al 100 %, eliminando automáticamente las posibles amenazas.
- En el caso del SPAM, los filtros instalados suelen identificar a la mayoría de mensajes no deseados, marcándolos con la etiqueta [SPAM] para facilitar su reconocimiento y posterior borrado.

¿Por qué no se impide que me lleguen estos mensajes?

Cada vez resulta más difícil distinguir un correo electrónico convencional de un mensaje considerado como SPAM. Es más, dependiendo del perfil de cada usuario, un mensaje puede ser considerado o no SPAM. Por ejemplo, la publicidad de una revista deportiva puede ser útil a ciertos usuarios y ser considerada SPAM por otros.

Los filtros de dinahosting analizan las cabeceras, cuerpos de texto y características de cada mensaje para detectar si recibes correo malintencionado, aunque existe la posibilidad de que, por su formato, un mensaje que quieras recibir pueda ser marcado como SPAM (por ejemplo, un mensaje con “Hola como estás???” como asunto). Por ello, preferimos que seas tú mismo quien decida qué mensajes borrar y qué mensajes confirmar. Aun así, si estás seguro de que el filtro identifica correctamente todos los mensajes considerados SPAM, indica en el apartado Filtros y Reglas de tu [Panel de Control de hosting](#) que quieres borrar automáticamente este tipo de mensajes.

Como el SPAM es enviado por terceras personas que imitan los mensajes convencionales y examinan los filtros para detectar formas de superarlos, la batalla contra el SPAM evoluciona continuamente, resultando **prácticamente imposible asegurar una eficacia total contra este tipo de amenaza**.

¿Cómo puedo protegerme?

- **Nunca publiques en una web una dirección de correo** que quieras que sea segura. Tampoco firmes comentarios en foros o listas de discusión con este correo. También debes tener cuidado con las suscripciones a boletines o fuentes informativas que en ocasiones venden los datos de contacto a terceros. Resultan especialmente peligrosas las suscripciones a páginas web que proporcionen contenidos para adultos, ya que muchas de ellas han sido creadas específicamente para captar receptores de correo malintencionado.
- **Utiliza varias cuentas de correo**, una segura para tus contactos habituales o la recepción de correo importante y otra/s para su difusión pública o usos diversos. Cuando hagas pública la dirección puedes optar por escribirla en texto en una imagen. De esta forma evitarás su localización automática. Con un plan de [Hosting Profesional dispones de cuentas ilimitadas](#), que puedes aprovechar plenamente para alternar diferentes direcciones de email.
- **Nunca respondas a un correo identificado como SPAM** ni accedas a las solicitudes de baja de suscripción sin asegurarte de que el origen es confiable. Muchas veces se usan para confirmar que una dirección de correo está activa.
- Otro elemento de riesgo está en las **imágenes anexas en correos no deseados, que debes evitar abrir**. Suelen contener códigos de programación que confirman al emisor de SPAM que el mensaje ha sido recibido en tu cuenta. La mayoría de programas de gestión de correo bloquean por defecto la descarga de imágenes de los mensajes, en caso contrario puedes señalar esta opción como predeterminada en las preferencias.
- **Ignora o elimina los mensajes de phishing o cadenas de correo con información poco fiable**, este tipo de correos no solo sirven para robar tu información, también se utilizan para comprobar si es una cuenta que se está empleando.

¿Qué puedo hacer ahora?

Si recibes mensajes de SPAM en una cuenta de correo, ten por seguro que sus emisores seguirán enviando mensajes no deseados a esta dirección.

En caso de que necesites mantener esta cuenta, deberás limpiarla con cierta frecuencia para evitar la acumulación de este tipo de mensajes.

También te recomendamos la opción de crear reglas a través de un programa de gestión de correo (como Outlook o Thunderbird), señalando rasgos distintivos de los correos no deseados que recibas con más frecuencia para su eliminación automática.

También puedes personalizar los filtros y reglas que actúan en el servidor al recibir los mensajes, como explicaremos más adelante.

¿Cómo se propaga?

Estos mensajes suelen enviarse de forma masiva y automatizada a miles de usuarios, sin tener en cuenta la identidad de los receptores. Hacen esto tras recopilar las direcciones de correo mediante robots de búsqueda, compra de datos o técnicas ilícitas. Entre estas técnicas está el uso de determinados virus para la obtención de contactos (por ejemplo, a través de la agenda que utilizamos en nuestro programa de gestión de correo).

Los virus también pueden hacer que los usuarios enviemos miles de correos electrónicos sin saberlo, ya que los emisores de SPAM usan también este método para garantizar su anonimato. Además los spammers pueden ocupar servidores para utilizarlos como propagadores de correo no deseado, falsificar las cabeceras y los correos remitentes, cambiar continuamente de direcciones, etc., lo que complica la correcta identificación de los autores de estas prácticas ilícitas.

¿Cómo definir filtros y reglas en el servidor para eliminar SPAM antes de que llegue a mi correo?

Desde tu [Panel de Control de dinahosting](#), dentro de la sección Correo > Reglas y filtros puedes personalizar la configuración a tu gusto, para minimizar la recepción de SPAM en tu bandeja.



Si lo prefieres
Mira el vídeo

Cómo configurar reglas y filtros de correo

¿Mis correos llegan como SPAM, cómo puedo evitarlo?

Existen una gran cantidad de técnicas para que tus comunicaciones no sean etiquetadas como SPAM, como puede ser revisar la reputación de nuestra IP o evitar que nuestro correo tenga la estructura de un correo de SPAM. [En nuestro blog](#) que explicamos en detalle cómo puedes evitar este problema.

¡Esperamos que hayas resuelto tus dudas sobre el SPAM!

VEN A DINAHOSTING

*¿Tus webs en otra empresa?
Nos encargamos gratis de toda la migración*



Guía de Ciberseguridad

PARA MANTENER TU WEB Y TU PYME SEGURAS

MAY. 2022



 **dinahosting**

LLAMADA GRATIS

900 854 000

dinahosting.com

