CAPTCHA - reCAPTCHA

Proteja su tienda de mensajes de spam y cuentas de usuario de spam

El producto de PrestaHero

Contenido

I. BIENVENIDO 3

II. INTRODUCCIÓN 3

III. INSTALACIÓN 4

IV. CONFIGURACIÓN 4

1. Posición 5

2. Los tipos de CAPTCHA 10

3. Lista negra de IP y lista negra de correo electrónico 16

4. Consejos 17

V. GRACIAS 22

I. BIENVENIDO

Gracias por comprar nuestro producto. Esperamos guiarle a través de todos los aspectos de la instalación del módulo y la configuración del módulo dentro de este documento. Lo si tiene alguna pregunta que esté fuera del alcance de esta documentación, no dude en contactarnos.

Nota:

Todas las capturas de pantalla de instrucciones se toman de PrestaShop 1.7, pero la instalación y configuración de este módulo en PrestaShop 1.6 es similar.

II. INTRODUCCIÓN

¿Se molesta con los mensajes de spam enviados continuamente desde el formulario de contacto del sitio web? ¿Tener un dolor de cabeza con cuentas de clientes de spam registrados diariamente en su sitio web de dinero?

¡Decir “adiós” a los problemas de spam ahora! **CAPTCHA - reCAPTCHA** resolverá todos los problemas de spam que está tratando con.

** "**CAPTCHA - reCAPTCHA**" es compatible con PrestaShop de la versión 1.5.x a la versión 8.x*

III. INSTALACIÓN

1. Vaya a "**Módulos / Módulos & servicios**", haga clic en "**Cargar un módulo / Seleccionar archivo**".

2. Elegir el archivo de módulo "**ets_advancedcaptcha.zip"** desde el ordenador a continuación, haga clic en **"Abrir"** para instalar.

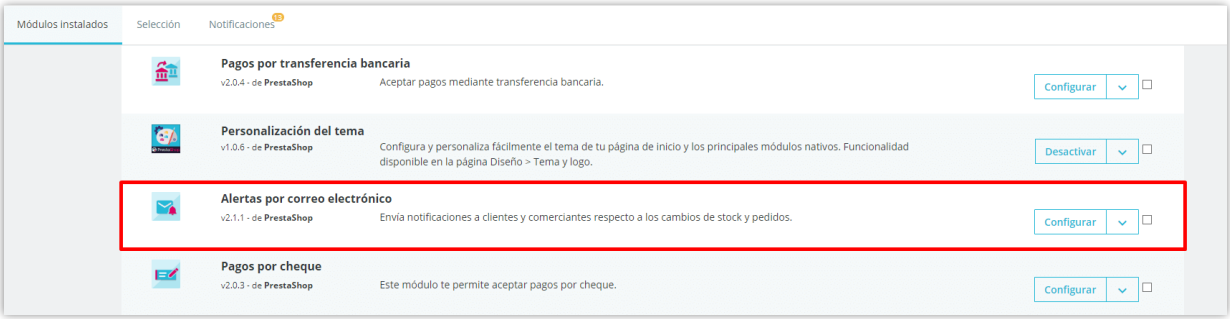
❖ Haga clic en el botón **"Configurar"** del módulo que acaba de instalar para abrir la página de configuración del módulo.

IV. CONFIGURACIÓN

Desde la lista de módulos instalados (que se encuentra en **"Módulo / Módulos & servicios / Módulos instalados")**, busque "**CAPTCHA - reCAPTCHA**" y luego haga clic en el botón **"Configurar"** para abrir Página de configuración.

Nota:

a) Para habilitar el **Formulario de alerta "Fuera de stock"**, debe instalar primero el módulo **"Alertas por correo electrónico"**.

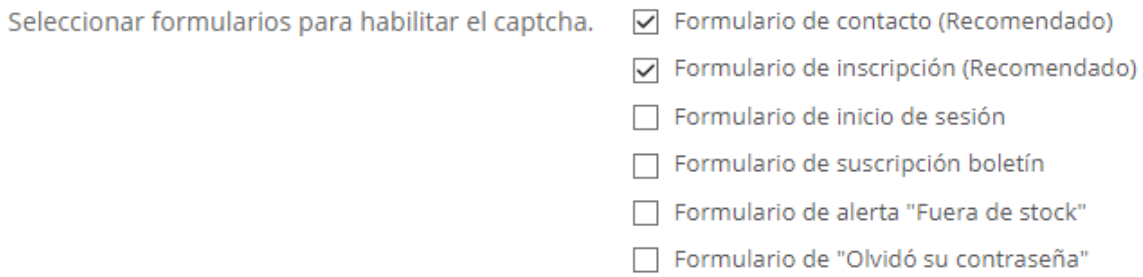


b) Al utilizar el módulo **CAPTCHA - reCAPTCHA** de *PrestaHero* junto con el módulo "**Creative Elements**" desarrollado por *WebshopWorks*, tenga en cuenta que la funcionalidad CAPTCHA - reCAPTCHA no será compatible con los formularios creados por el módulo "**Creative Elements**".

Si necesita mostrar CAPTCHA/reCAPTCHA en los formularios generados por "**Creative Elements**", póngase en contacto con el desarrollador *WebshopWorks* para obtener más ayuda.

1. Posición

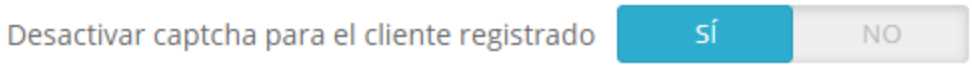
Puede seleccionar el formulario donde se mostrará el cuadro de captcha. **CAPTCHA - reCAPTCHA** admite la caja de captcha de pantalla en 6 diferentes tipos de forma:



Nota

CAPTCHA - reCAPTCHA *no es compatible con la función de captcha para "Formulario de suscripción de boletín" en PrestaShop 1.5.x*

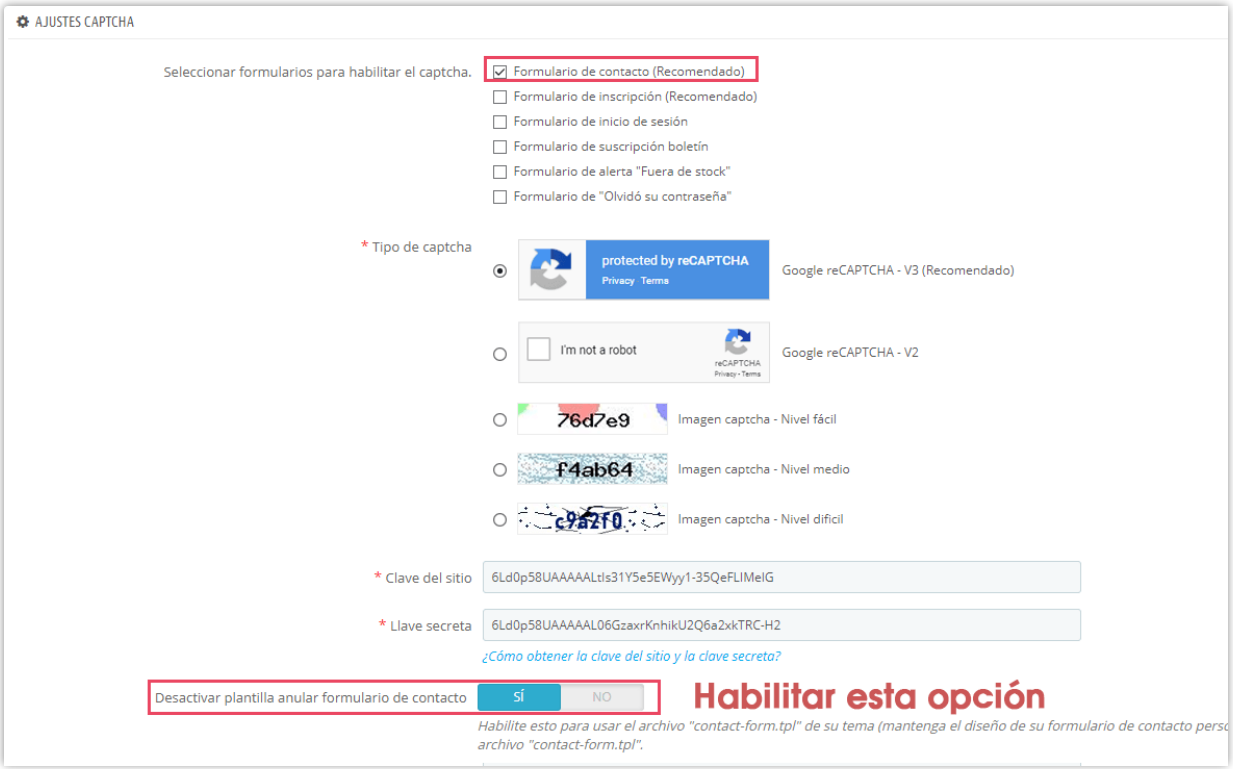
Para el propietario de la tienda que están utilizando **PrestaShop 1.7.x**, después de elegir posiciones para mostrar captcha caja, hay una opción para activar/inhabilitar captcha cuando el cliente iniciado sesión.



Con los propietarios de tiendas que utilizan **PrestaShop 1.5 y 1.6**, para ciertas ubicaciones verá más opciones para configurar. Si está utilizando un tema personalizado u otro módulo personalizado, puede tener algunos problemas al instalar **CAPTCHA - reCAPTCHA** en su sitio Web. Para evitar estos problemas, por favor siga nuestra siguiente guía:

- **Formulario de contacto**

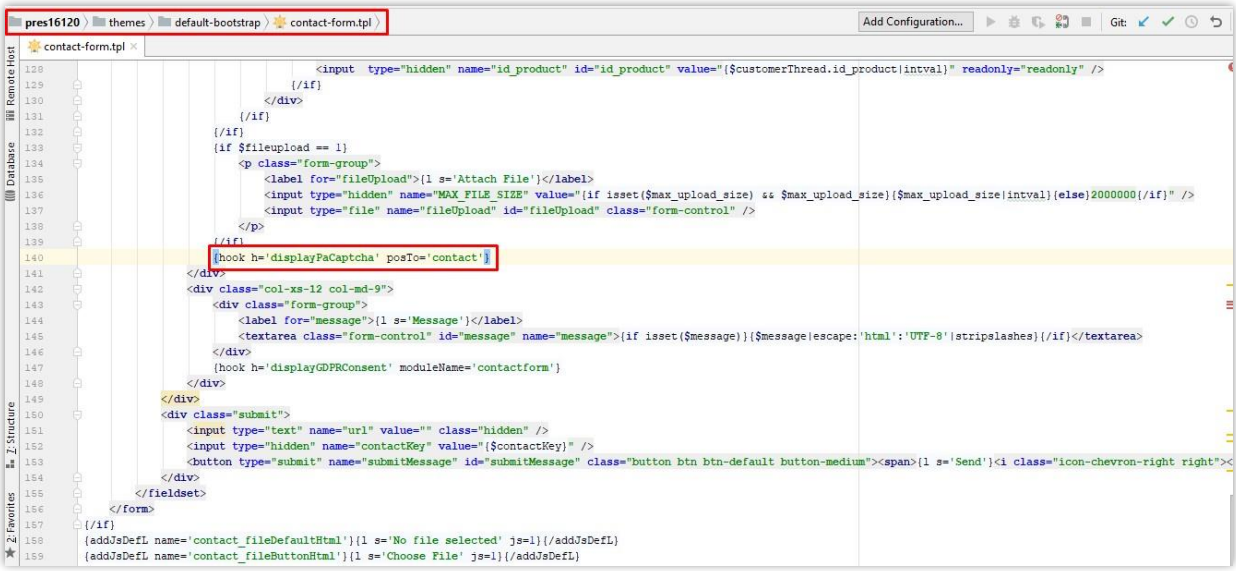
Habilite esta opción: **"Desactivar plantilla anular formulario de contacto"**



Copie este código: *{hook h='displayPaCaptcha' posTo='contact'}*

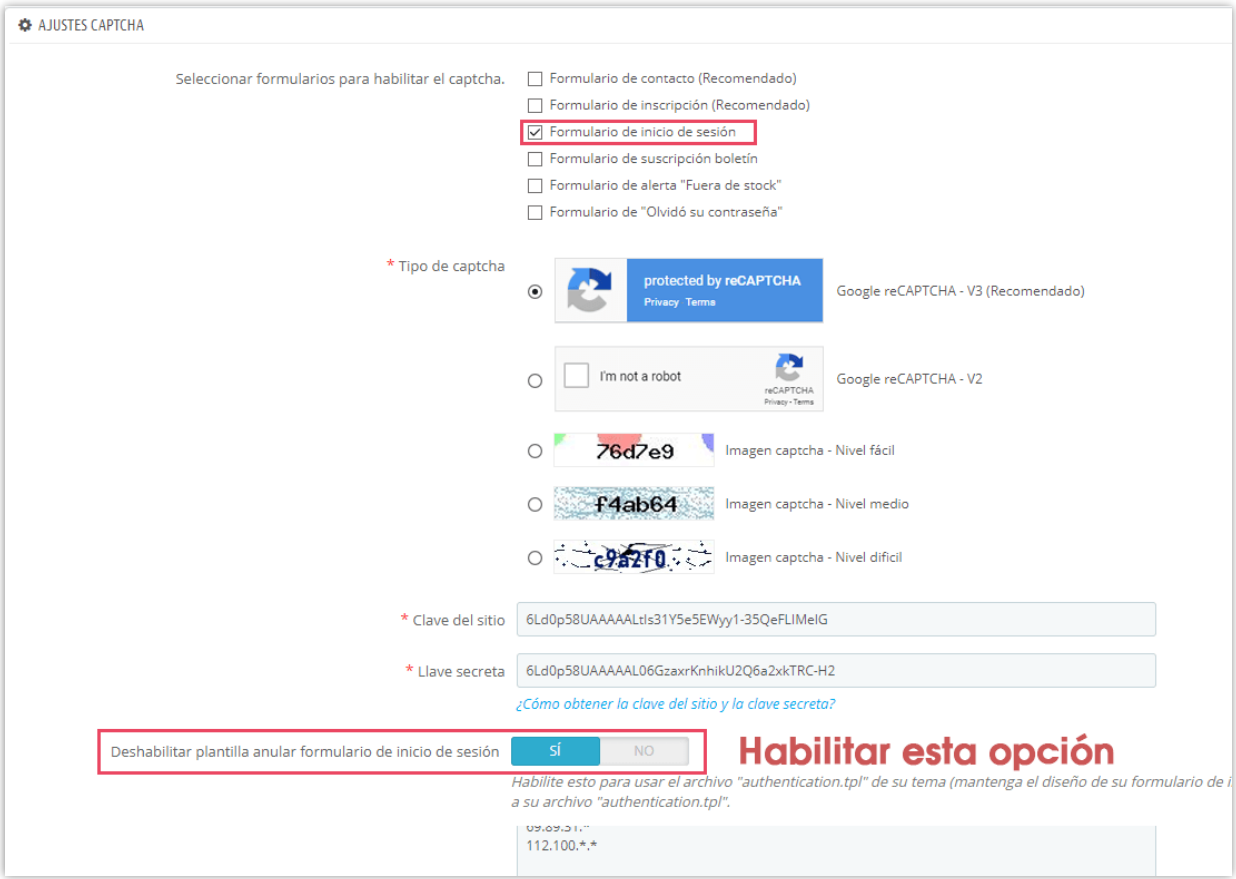
Abra este archivo: *root/TU-SITIO/themes/TU-TEMA/contact-form.tpl*

Pegue el código que copió antes en **contact-form.tpl** justo debajo del **campo de carga de archivos** y luego guarde los cambios.



❖ Formulario de inicio de sesión

Habilite esta opción: **"Deshabilitar plantilla anular formulario de inicio de sesión"**



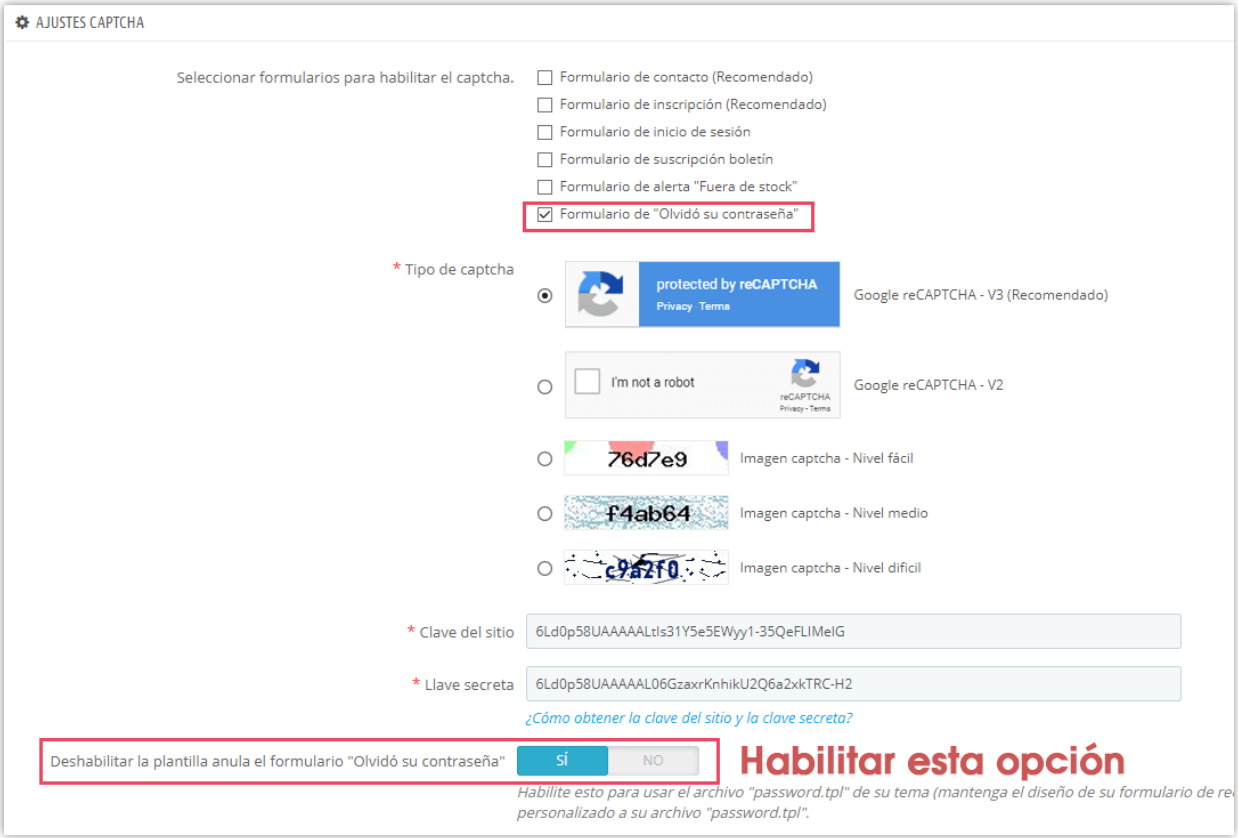
Copie este código: *{hook h='displayPaCaptcha' posTo='login'}*

Abra este archivo: *root/TU-SITIO/themes/TU-TEMA/authentication.tpl*

Pegue el código que copió antes en la **authentication.tpl** justo debajo del **campo de carga de archivos** y luego guarde los cambios.

- **Formulario de "Olvidó su contraseña"**

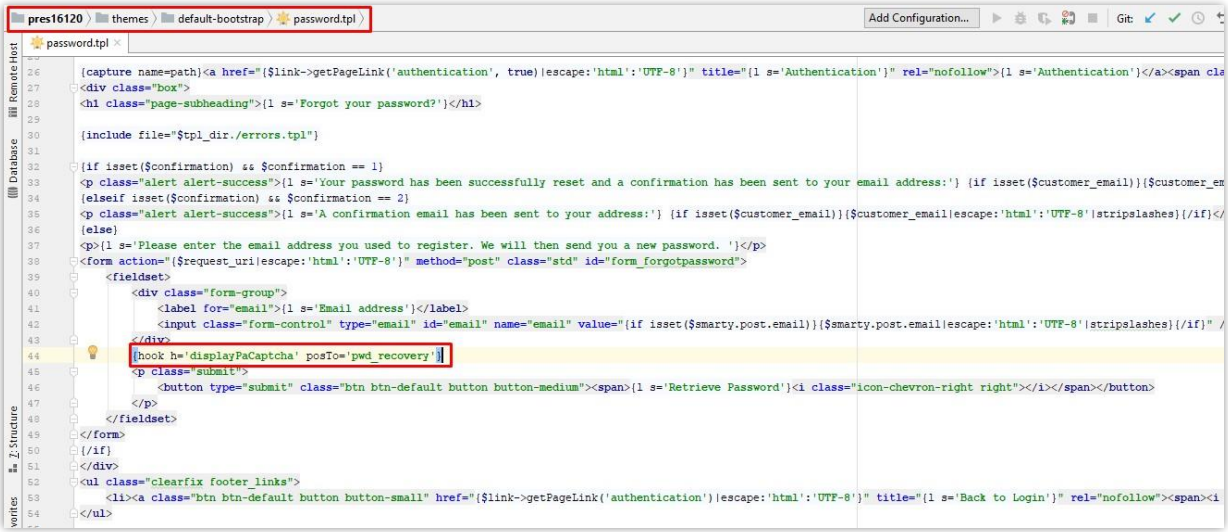
Habilite esta opción: **Deshabilitar la plantilla anula el formulario "Olvidó su contraseña"**



Copie este código: *{hook h='displayPaCaptcha' posTo='pwd_recovery'}*

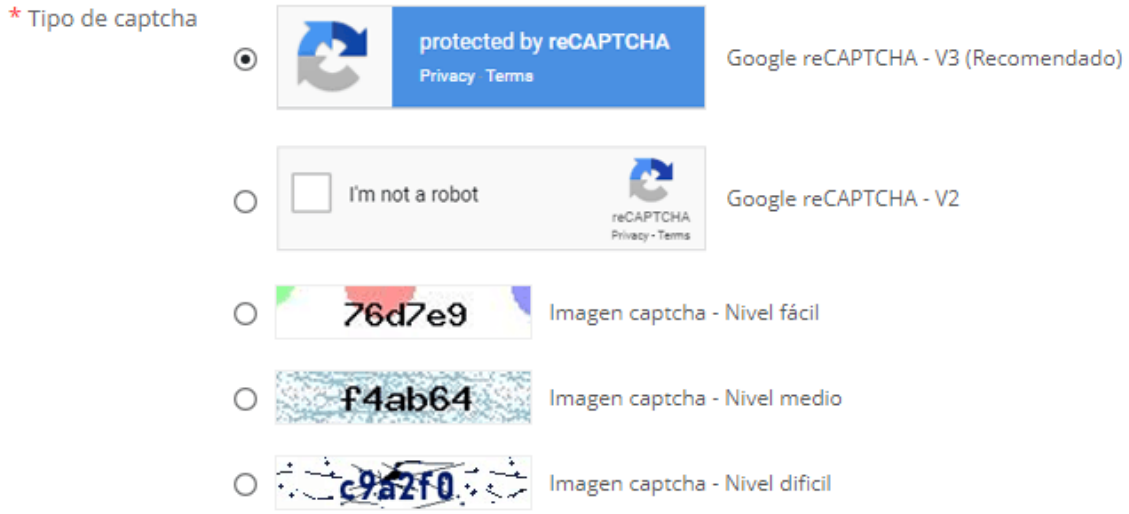
Abra este archivo: *root/TU-SITIO/themes/TU-TEMA/password.tpl*

Pegue el código que copió antes en la **password.tpl** justo debajo del **campo de carga de archivos** y luego guarde los cambios.



2. Los tipos de CAPTCHA

CAPTCHA - reCAPTCHA ofrece 5 tipos de captcha para que seleccione el más adecuado con su tema actual.



Para usar Google reCAPTCHA, debes ingresar la **Clave del sitio y la Clave secreta** (para la clave clásica de reCAPTCHA) o el **ID de reCAPTCHA** (para el nuevo proyecto de reCAPTCHA creado en Google Cloud Console).

Google ha anunciado que **todas las claves clásicas de reCAPTCHA deben migrarse a Google Cloud Console antes de finales de 2025**. Anteriormente, las claves de reCAPTCHA se gestionaban por separado en la **Consola de administración de Google reCAPTCHA**, donde los usuarios podían crearlas de forma gratuita sin necesidad de vincular una tarjeta de crédito. Sin embargo, ahora **Google ha trasladado todos los servicios de reCAPTCHA a Google Cloud Console para una gestión centralizada**.

❓ **¿Qué significa esto para ti?**

- Si **ya tienes claves clásicas de reCAPTCHA**, puedes seguir usándolas **hasta finales de 2025**, pero debes migrarlas a un **proyecto de Google Cloud**.
- Si **estás configurando reCAPTCHA por primera vez**, debes **generar nuevas claves en Google Cloud Console**, en lugar de usar la antigua consola de administración de Google reCAPTCHA.

🔷 **¿Qué debes hacer?**

👉 **Si estás usando claves clásicas de reCAPTCHA:**
Para seguir utilizando tus claves actuales, debes migrarlas a Google Cloud Console. Sigue esta guía: Cómo migrar reCAPTCHA Classic a Google Cloud

👉 **Si necesitas nuevas claves de reCAPTCHA:**
Debes crear nuevas claves, dependiendo de dónde quieras gestionarlas:

- **En la antigua Consola de administración de Google reCAPTCHA (hasta que se desactive por completo):** Crear una clave de reCAPTCHA en la Consola de administración de Google reCAPTCHA
- **En Google Cloud Console (recomendado para compatibilidad futura):** Cómo crear claves de reCAPTCHA en Google Cloud

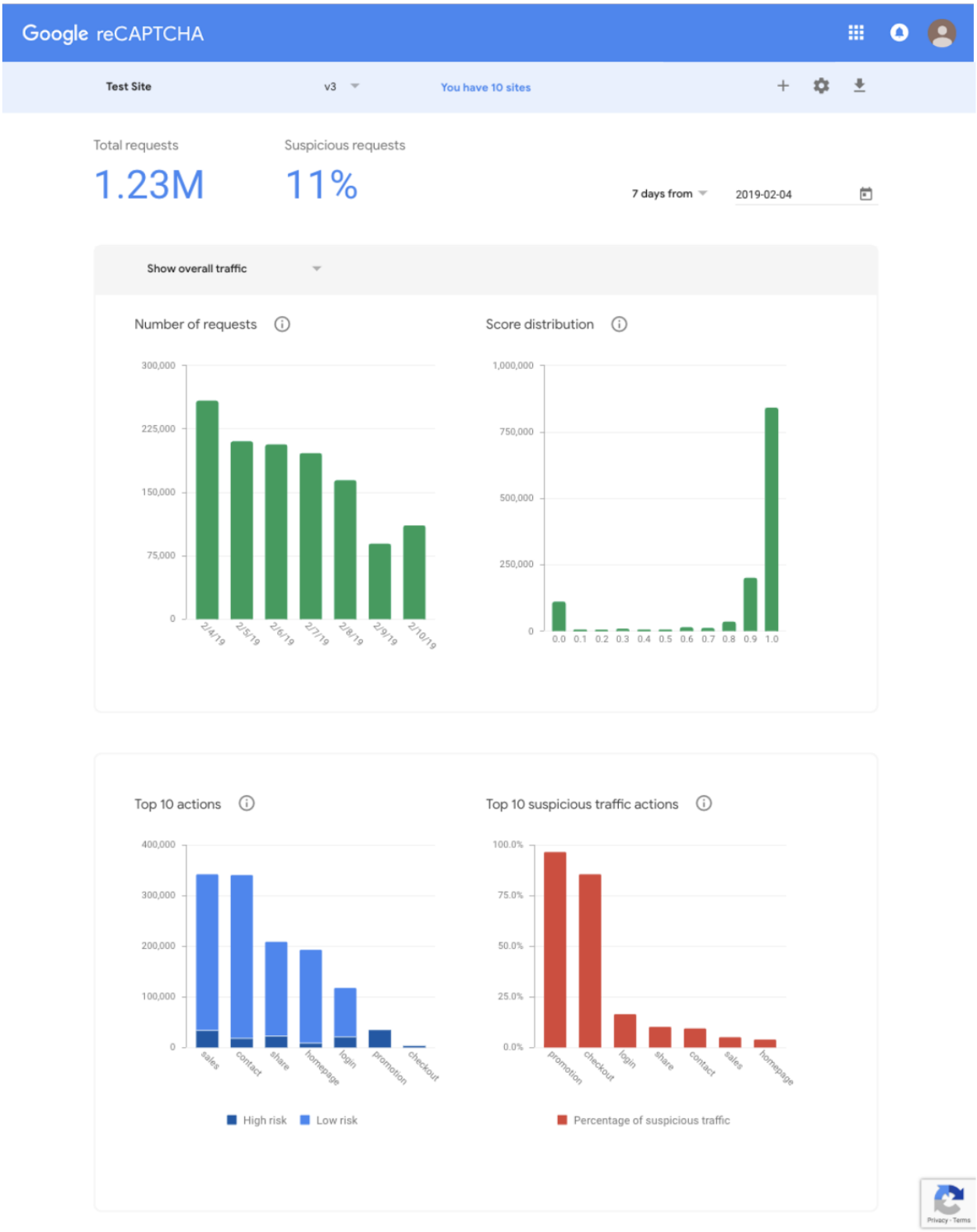
Una vez que tengas tus nuevas claves, actualízalas en la configuración del módulo **CAPTCHA - reCAPTCHA** en tu back office de PrestaShop.

Acerca de Google reCAPTCHA v3

Google reCAPTCHA v3 es una herramienta poderosa y no intrusiva para la prevención de spam que opera en segundo plano, analizando las interacciones de los usuarios con su sitio web sin requerir desafíos explícitos (por ejemplo, hacer clic en casillas de verificación o resolver rompecabezas). En lugar de eso, reCAPTCHA v3 asigna una **puntuación** a cada interacción del usuario, que varía de **0.0 a 1.0**:

- **Puntuación cercana a 1.0**: Indica una alta probabilidad de que la interacción sea de un usuario humano genuino.
- **Puntuación cercana a 0.0**: Sugiere una alta probabilidad de actividad de bots o automatizada.
- **Puntuaciones intermedias (por ejemplo, 0.3 a 0.7)**: Indican diferentes niveles de confianza, requiriendo una evaluación adicional o verificación suplementaria.

Esta puntuación le permite definir cómo su sitio web de PrestaShop maneja diferentes tipos de tráfico, como permitir que los usuarios legítimos continúen, requerir verificación adicional para interacciones sospechosas o bloquear directamente posibles bots.



Configuración del Umbral de Puntuación

- El **Umbral de Puntuación** determina la puntuación mínima requerida para considerar una interacción como legítima. Las interacciones con puntuaciones por debajo de este umbral pueden ser bloqueadas o requerir verificación adicional (dependiendo de la configuración de su módulo).
- El umbral puede establecerse en un valor entre 0.0 y 1.0.

Configuraciones Recomendadas para el Umbral de Puntuación

Elegir un umbral de puntuación adecuado es crucial para equilibrar la prevención de spam con una experiencia de usuario fluida. El umbral óptimo depende de las necesidades de su sitio web, los formularios que está protegiendo y el nivel de actividad de spam que experimenta. A continuación, se presentan recomendaciones generales:

Recomendación predeterminada: 0.5	Un umbral de 0.5 es un buen punto de partida para la mayoría de los sitios web de PrestaShop. Bloquea eficazmente las interacciones con alta probabilidad de ser bots (puntuaciones por debajo de 0.5) mientras permite que la mayoría de los usuarios legítimos continúen sin verificación adicional.	**Adecuado para**: Sitios web de propósito general, formularios de contacto y formularios de inicio de sesión con actividad de spam moderada.
Configuración permisiva: 0.3	Utilice un umbral más bajo (por ejemplo, 0.3) si desea minimizar las interrupciones para los usuarios, especialmente en	**Adecuado para**: Tiendas de comercio electrónico de alto tráfico que priorizan la experiencia del usuario

	formularios críticos para conversiones (por ejemplo, formularios de registro o de pago). Esta configuración puede permitir el paso de algunos bots de bajo riesgo, pero reduce la probabilidad de bloquear a usuarios legítimos.	sobre un filtrado estricto de spam.
Configuración estricta: 0.7	Se recomienda un umbral más alto (por ejemplo, 0.7) para formularios altamente atacados por spam, como formularios de suscripción a boletines o de recuperación de contraseñas. Esta configuración ofrece una protección más fuerte, pero puede marcar a algunos usuarios legítimos para verificación adicional, lo que podría afectar la experiencia del usuario.	**Adecuado para**: Sitios web que experimentan un alto nivel de spam o ataques de bots.

Personalización Basada en Análisis

- Después de establecer un umbral inicial, monitoree los análisis de su sitio web (por ejemplo, envíos de spam, interacciones bloqueadas o quejas de usuarios) para ajustar la puntuación.

- Si nota que pasa demasiado spam, aumente el umbral (por ejemplo, de 0.5 a 0.6). Si los usuarios legítimos reportan problemas (por ejemplo, ser bloqueados o solicitados para verificación adicional), reduzca ligeramente el umbral (por ejemplo, de 0.5 a 0.4).
- Utilice la Consola de Administración de Google reCAPTCHA para revisar las distribuciones de puntuaciones de su sitio y ajustar en consecuencia.

3. Lista negra de IP y lista negra de correo electrónico

❖ Lista negra de IP

Con **CAPTCHA - reCAPTCHA**, puede introducir direcciones IP de los los spammers y prohibirlos de enviar su formulario.

Nota:

Las direcciones IPv4 generalmente se representan en notación de punto-decimal, que consta de cuatro números decimales, cada uno de los cuales oscila entre 0 y 255, separados por puntos, cada parte representa un grupo de 8 bits (un octeto) de la dirección.

Lista negra de IP (direcciones IP a bloquear)

```
69.89.31.226
69.89.31.*
112.100.*.*
```

Ingrese el patrón de IP o IP exacto usando "", cada patrón de IP / IP en una línea. Por ejemplo: 69.89.31.226, 69.89.31.*, *.226, etc.*

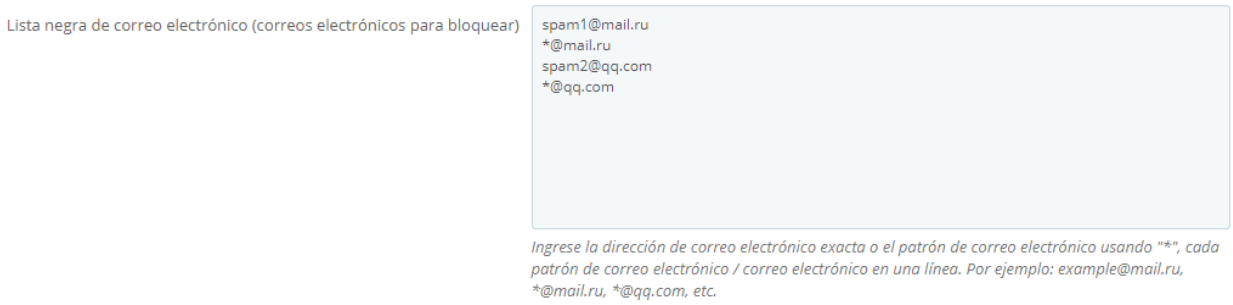
Usted puede ingresar la dirección IP exacta (por ejemplo: 69.89.31.226) o un patrón IP usando el carácter "*", cada patrón IP/IP en una línea.

Nota

El patrón IP es una forma de representar un rango de direcciones IP. Puede reemplazar uno o varios octetos de dirección IP con el carácter "". Por ejemplo, si ingresa este patrón IP: 69.89.31.*, **CAPTCHA - reCAPTCHA** prohibirá todas las direcciones IP de 69.89.31.0 a 69.89.31.255*

❖ Lista negra de correo electrónico

Similar a prohibir direcciones IP, también puede prohibir direcciones de correo electrónico que a menudo envían correos electrónicos no deseados a su bandeja de entrada. **CAPTCHA - reCAPTCHA** también admite la prohibición de direcciones de correo electrónico de dominio de correo electrónico como mail.ru, qq.com, etc.



Puede introducir la dirección de correo electrónico exacta o el patrón de correo electrónico utilizando el carácter "*", cada patrón de correo electrónico o correo electrónico en una línea.

Por ejemplo, si ingresa el patrón de correo electrónico *@mail.ru , **CAPTCHA - reCAPTCHA** prohibirá todos los correos electrónicos que se envíen de los usuarios que tengan "@mail.ru" en sus direcciones de correo electrónico.

4. Consejos

Este módulo debe funcionar perfectamente en la mayoría de los sitios web de PrestaShop sin ninguna modificación de código, sin embargo, si su sitio web se instala con un tema personalizado o módulos personalizados, puede (raramente) tener algunos problemas al instalar el módulo en su sitio Web.

Los siguientes consejos le guiarán cómo solucionar rápidamente los problemas modificando algún código para que pueda solucionar los problemas usted mismo, pero le recomendamos que se contacte con nosotros. ¡Estamos encantados de apoyarlos y le ayudaremos a resolver los problemas de forma gratuita!

- **Para PrestaShop 1.7. x**

Si ve un error que dice que los métodos **validate** y **getFormat** son reemplazados ya por otro módulo, significa que algunos otros módulos han reemplazado el método que hace que el bloqueo del módulo **CAPTCHA - reCAPTCHA** implemente su código de invalidación. Para resolver el problema, necesita editar manualmente los métodos (en anular de archivos) con el código de anulación de la **CAPTCHA - reCAPTCHA** module.

ERROR: "MÉTODO VALIDATE() YA SE OVERRIDEN"

Paso 1: abra este archivo:

root/TU-SITIO/modules/ets_advancedcaptcha/override/classes/form/CustomerForm.php

Paso 2: copia el código resaltado en la foto de abajo

```
23  if (!class_exists('CustomerFormCore') || version_compare(_PS_VERSION_, '1.7', '<'))
24      exit;
25  class CustomerForm extends CustomerFormCore
26  {
27      public function validate()
28      {
29          if (Tools::isSubmit('submitCreate') && Module::isEnabled('ets_advancedcaptcha') && ($captcha = Module::getInstanceByName('ets_adva
30          {
31              $captchaField = $this->getField('captcha');
32              $errors = array();
33              $captcha->captchaVal($errors);
34              if ($errors)
35              {
36                  $captchaField->addError(implode(',', $errors));
37              }
38          }
39          return parent::validate();
40      }
41  }
```

Paso 3: abra este archivo: *root/TU-SITIO/override/classes/form/CustomerForm.php*

Paso 4: encuentra un método (function) llamado "**validate**", pega el código que copiaste en el paso 2 en el inicio del método y luego guarda tus cambios.

ERROR: "MÉTODO GETFORMAT() SE OVERRIDEN YA"

Paso 1: abra este archivo: *root/TU-SITIO/modules/ets_advancedcaptcha/override/classes/form/CustomerFormatter.php*

Paso 2: copia el código resaltado en la foto de abajo

```
22
23  if (!class_exists('CustomerFormatterCore') || version_compare(_PS_VERSION_, '1.7', '<'))
24      exit;
25  class CustomerFormatter extends CustomerFormatterCore
26  {
27      public function getFormat()
28      {
29          if (Module::isEnabled('ets_advancedcaptcha') && ($captcha = Module::getInstanceByName('ets_advancedcaptcha')) && $ca
30          {
31              $formats = parent::getFormat();
32              $formats['captcha'] = (new FormField)
33                  ->setName('captcha')
34                  ->setType('hidden')
35                  ->setRequired(true)
36                  ->setValue(1);
37              return $formats;
38          }
39          return parent::getFormat();
40      }
41  }
```

Paso 3: abra este archivo:

root/TU-SITIO/override/classes/form/CustomerFormatter.php

Paso 4: encontrar un método (función) llamado "**getFormat**", pegue el código que copió en el paso 2 en el inicio del método y luego guarde los cambios.

ERROR: "MÉTODO SUBMIT() YA ESTÁ OVERRIDEN"

Paso 1: abra este archivo:

root/TU-SITIO/modules/ets_advancedcaptcha/override/classes/form/CustomerLoginForm.php

Paso 2: copia el código resaltado en la foto de abajo

```
22
23  if (!class_exists('CustomerLoginFormCore') || version_compare(_PS_VERSION_, '1.7', '<'))
24      exit;
25  class CustomerLoginForm extends CustomerLoginFormCore
26  {
27      public function submit()
28      {
29          if (Tools::isSubmit('submitLogin') && Module::isEnabled('ets_advancedcaptcha') && ($captcha = Module::getIns
30          {
31              $captcha->captchaVal($this->errors['']);
32          }
33          return !$this->errors''']? parent::submit() : !$this->hasErrors();
34      }
35  }
```

Paso 3: abra este archivo:

root/TU-SITIO/override/classes/form/CustomerLoginForm.php

Paso 4: encontrar un método (función) llamado "**submit**", pegue el código que copió en el paso 2 en el inicio del método y luego guarde los cambios.

- **Para PrestaShop 1.5 y 1.6**

ERROR: " OVERRIDE CONTROLLER"

Si métodos: *processSubmitAccount, processSubmitLogin, sendRenewPasswordLink, postProcess, initContent* ya se reemplazan, siga estos pasos para solucionar el problema.

Paso 1: abrir 3 archivos: *AuthController.php, ContactController.php, PasswordController.php* que se encuentran en "root/TU-SITIO/modules/ets_advancedcaptcha/override/controllers/front/" carpeta

Paso 2: copiar métodos (funciones) que están definidos en los archivos.

Paso 3: Abra estos archivos de reemplazo respectivos (*AuthController.php, ContactController.php, PasswordController.php*) en la carpeta de reemplazo de su sitio web en "root/TU-SITIO/override/controllers/front/"

Paso 4: encuentre y reemplace los métodos definidos en esos archivos por los métodos que copió en el paso 2 y luego guarde los cambios.

**** Nota:*** *Si reemplaza todos los métodos que otros módulos anulan, es posible que los otros módulos ya no funcionen correctamente (pero el módulo* ***CAPTCHA - reCAPTCHA*** *seguramente funcionará).*

Por lo tanto, si tiene conocimientos de programación, debe comprobar los métodos anulados existentes y solo insertar los códigos necesarios que se definen en la anulación de archivos del módulo **CAPTCHA - reCAPTCHA**.

Le recomendamos ponerse en contacto con nosotros para una solución rápida y gratuita del problema (ya que requiere trabajo de codificación), we estamos encantados de apoyarlo.

V. GRACIAS

Gracias de nuevo por comprar nuestro producto y pasar por esta documentación. Esperamos que este documento sea útil y eficiente en la configuración completa de este módulo. Si tiene alguna pregunta para la que la respuesta no está disponible en este documento, por favor no dude en ponerse en contacto con nosotros.