

RECOMENDACIONES DE SEGURIDAD PARA LOS SITIOS WEB



Política de Seguridad Sitios JOOMLA

Preparado para:



por:

Johanna Quintero

RECOMENDACIONES DE SEGURIDAD PARA LOS SITIOS WEB



Tabla de Contenido

1.	Objetivo	3
2.	Descripción del Problema	3
3.	Recomendaciones SE	3

RECOMENDACIONES DE SEGURIDAD PARA LOS SITIOS WEB



1. **Objetivo**

Este documento tiene la finalidad de realizar recomendaciones básicas para disminuir estas vulnerabilidades que se pueden generar sobre el Hosting Compartido Web de la Secretarías.

2. **Descripción del Problema**

El Hosting en que se alojan los sitios de la Secretarías es compartido y sobre el cual se asigna el espacio y herramientas para tal fin. Debido a que el desarrollo, gestión y administración de cada sitio es competencia de cada Secretaria, Se presentan vulnerabilidades de seguridad sobre los CMS implementados en los sitios, ya sean de herramientas que se encuentran en el mercado o desarrollos propios de las Secretarías, permitiendo latencias sobre las cuales podemos recibir ataques de HACKERS

3. **Recomendaciones SE**

Para evitar vulnerabilidades de seguridad que se pueden presentar sobre los sitio Web (Joomla) y luego de los análisis de seguridad realizados en el aplicativo Web, se hace necesario que se apliquen las siguientes recomendaciones con el fin de evitar el hackeo del sitio Web de la Secretaria de Educación y así minimizar las vulnerabilidades que este pueda contener, así:

1. Se recomienda mantener su sitio Joomla actualizado con la última versión liberada, ya que esta corrige vulnerabilidades que no se habían tenido en cuenta en versiones anteriores. Actualmente la ultima versión de Joomla es la 1.5.14 (<http://www.joomla.org/download.html>)
2. Es importante tener en cuenta las recomendaciones realizadas por los desarrolladores de Joomla, con el fin de evitar ataques de SQL INJECTION (<http://developer.joomla.org/security/articles-tutorials/258-preventing-sql-injections.html>)
3. Es importante tener en cuenta las recomendaciones realizadas por los desarrolladores de Joomla, con el fin de evitar ataques por reinicio remoto de la contraseña de administración del sitio por parte de usuarios no autorizados. (<http://developer.joomla.org/security/news/241-20080801-core-password-remind-functionality.html>)
4. Cambiar el usuario Administrador para que no corresponda al default **admin**
5. Cambiar el nombre estándar de la página index.php bajo el directorio **administrator** para dificultar mas las actividades de los hackers
6. Es importante modificar la contraseña de administración periódicamente
7. Usar contraseñas fuertes

RECOMENDACIONES DE SEGURIDAD PARA LOS SITIOS WEB



- Longitud mayor a 8 caracteres
 - Utilizar combinación de
 - letras mayúsculas y minúsculas
 - números
 - caracteres especiales
 - Fáciles de recordar
 - Difíciles de adivinar
8. Realizar un backup periódico del Sitio Web (Aplicación y Base de Datos).

Johanna Quintero Caldas
Global Crossing