**Lista de verificación de la seguridad del ANDA y el servidor web**

* Está deshabilitado ver el contenido de las carpetas a través del navegador web.
* La base de datos del ANDA está configurada con una cuenta de usuario de la base de datos específica para el ANDA y está limitada con los permisos necesarios de la base de datos para solamente ejecutar el ANDA. Por ejemplo: no utilizar el usuario **ROOT (en MySQL)** o la cuenta **SA (en MS-SQL)**.
* La contraseña de la base de datos tiene un mínimo de 12 caracteres de largo, además, contiene mayúsculas, números y puntos o algún carácter especial, y no es una palabra encontrada en un diccionario.
* La contraseña de la cuenta de usuario administrador del ANDA tiene un mínimo de 12 caracteres de largo, además, contiene mayúsculas, números y puntos o algún carácter especial, y no es una palabra encontrada en un diccionario.
* El administrador del ANDA comprende la importancia de utilizar contraseñas complejas para las cuentas de usuario administrador y la importancia de limitar el número de personas que tienen una cuenta administrador en el ANDA.
* La carpeta “datafiles” del ANDA ha sido ubicada fuera de la carpeta raíz del servidor web.
* La carpeta “cache” del ANDA ha sido ubicada fuera de la carpeta raíz del servidor web.
* La carpeta “logs” del ANDA ha sido ubicada fuera de la carpeta raíz del servidor web.
* La carpeta “datafiles” del ANDA sólo tiene permisos de LECTURA y ESCRITURA, NO de Ejecución.
* La carpeta “cache” del ANDA sólo tiene permisos de LECTURA y ESCRITURA, NO de Ejecución.
* La carpeta “logs” del ANDA sólo tiene permisos de LECTURA y ESCRITURA, NO de Ejecución.
* Todas las cuentas de usuario administrador del ANDA creadas temporalmente para la instalación y configuración o que ya no son utilizadas por el/los administrador/es actual/es del ANDA, han sido eliminadas del ANDA.
* Si se ha otorgado acceso a través de CPanel solicitar al administrador que cambie la contraseña una vez finalizada la instalación/configuración del ANDA.
* Todas las aplicaciones, como phpMyAdmin instaladas para facilitar la instalación y configuración del ANDA han sido desinstaladas luego de ser utilizadas.
* Todos los archivos tales como aquellos que contienen la función phpinfo() u otros “scripts” (que dan información sobre el entorno) ubicados en el servidor para probar el ambiente han sido removidos, por ejemplo: archivos info.php o phpinfo.php
* La URL de administración del sitio ha sido personalizada y no es la URL “admin” por defecto.
* El ANDA ha sido instalado en una carpeta diferente a ANDA o NADA, es decir, se ha establecido una URL personalizada.
* Se conoce el procedimiento sobre cómo respaldar los archivos del ANDA.
* Se conoce el procedimiento sobre cómo respaldar la base de datos del ANDA.
* Conoce los contactos de soporte técnico de la OCDE y el Banco Mundial ([info@ihsn.org](mailto:info@ihsn.org)).
* Conoce los beneficios de la seguridad agregada con la instalación de un certificado SSL para un control de acceso (login) seguro y se ha evaluado la posibilidad de adquirir uno.
* Si un certificado SSL está disponible en el servidor, entonces se ha habilitado el login HTTPS en la configuración del ANDA.
* Se han tenido en cuenta las buenas prácticas sobre seguridad en general listadas a continuación.

**Buenas prácticas generales, recursos y guías**

La seguridad del servidor web y la aplicación es importante puesto que cualquier violación a la seguridad puede ocasionar no sólo pérdida o alteración en la información publicada, sino también podría provocar un daño importante en la imagen y reputación de la organización.

* No instalar aplicaciones que no son necesarias
* Remover todos los archivos y “scripts” (pore j. phpinfo) utilizados para el desarrollo, pruebas o instalaciones.
* Deshabilitar los servicios que no son necesarios para el servidor web (por ej. ftp, LDAP, email server).
* Limitar el número de usuarios que tienen acceso al servidor.
* Limitar los roles de usuarios en el servidor a las funciones que cada uno debe cumplir (por ej. limitar el número de usuarios que pueden iniciar y parar los servicios o modificar directorios o permisos de scripts).
* Limitar los permisos en carpetas para la ejecución de scripts o el acceso web a un único directorio.
* Limitar la carga de archivos a directorios que no están habilitados para lectura por el servidor web (en el caso del ANDA esto podría aplicar a la carpeta “datafiles”).
* Forzar que la contraseña expire.
* Forzar al usuario a utilizar contraseñas complejas.
* Remover usuarios que ya no trabajan en la organización.
* Asegurarse de que siempre los programas/Sistema Operativo y las aplicaciones tienen las últimas actualizaciones (patches) sobre seguridad (por ej. PHP, si es posible debería tener instalada siempre la última versión disponible desde php.net)
* Habilitar registro de acividades (logging) en el servidor y las aplicaciones.
* El monitoreo de los firewalls funciona apropiadamente.
* Mantener actualizado el software Antivirus.
* Mantener un respaldo total de los programas/aplicaciones del servidor y sitios web en un lugar seguro (no en el servidor web).
* Deshabilitar la opción para ver el contenido de directorios.

Si el sitio web está en un servidor externo (hosting externo) de un Proveedor de Servicios de Internet (ISP) entonces de algunas de las actualizaciones las aplicaciones (patching), registro de actividades y eventos (loggin) y seguridad del firewall se ocupará el proveedor, pero otras recaen bajo su responsabilidad.

**Deshabilitar ver el contenido de directorios en Apache**

**Deshabilitar ver el contenido de directorios usando .htaccess:**

* Abrir el archivo .**htacces**
* Buscar **Options Indexes**
* Si **Options Indexes** existe, cambiarlo a **Options -Indexes** o sino agregar **Options -Indexes** en una nueva línea.
* Ahora ver el contenido de directorios debería estar dehabilitado.

**Deshabilitar ver el contenido de directorios usando httpd.conf:**

* Abrir el archivo httpd.conf, generalmente está ubicado en /usr/local/apache/conf ó /etc/httpd.conf
* Ir a la configuración de Virtual Host y buscar “**Options Indexes**”
* Cambiar Indexes a -Indexes si la Option Indexes existe ó sino agregar la línea **Options -Indexes**
* Reiniciar el servidor apache.
* Ahora ver el contenido de directorios debería estar dehabilitado.

**Deshabilitar ver el contenido de directorios en ambientes de alojamiento de sitios web (web hosting) CPanel Share:**

* Acceder (Login) a CPanel.
* Hacer clic en **Index Manager**.
* Hacer clic en el nombre del directorio en el cual desea deshabilitar ver el contenido en el navegador web.
* Seleccionar **No Index** y hacer clic en Guardar.

**Deshabilitar ver el contenido de directorios en Microsoft IIS 6, 7+**

Los métodos utilizados para esto pueden variar dependiendo de la versión del IIS que se esté usando. Ver las siguientes páginas que pueden ser de utilidad:

http://technet.microsoft.com/en-us/library/cc731109(v=ws.10).aspx

http://www.iis.net/ConfigReference/system.webServer/directoryBrowse

http://technet.microsoft.com/en-us/library/cc732820.aspx

**Crear cuentas de usuario y bases de datos en MySQL**

*Secuencia de comandos de ejemplo para configurar un usuario de la* ***base de datos*** *para el* ***ANDA*** *– el objetivo es evitar usar* ***ROOT*** *para la configuración del ANDA.*

**Desde la línea de comando escribir lo siguiente:**

***mysql -u root -p***

* Ingresar la contraseña del usuario Root configurada cuando se instaló MySQL.
* Ahora crear la base de datos para el ANDA – en este ejemplo la base de datos se llama *anda*.

***mysql> CREATE DATABASE anda;***

* Crear un usuario que pueda acceder a la nueva base de datos *anda* y otorgar al usuario solo los permisos necesarios para ejecutar el ANDA.

***mysql> GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER, CREATE TEMPORARY TABLES,LOCK TABLES ON anda.\* TO 'anda'@'localhost' IDENTIFIED BY 'sucontraseña';***

* *'****sucontraseña****'* puede ser lo que usted elija. ***anda*** es el nombre de la base de datos a la que el usuario obtendrá acceso. ***localhost*** es la ubicación (servidor o PC) que obtendrá acceso a la base de datos. Nota: recuerde esta contraseña pues la necesitará para configurar el instalador del ANDA! Salga de la consola de MySQL escribiendo exit.

***mysql> exit***

**Crear cuentas de usuario y bases de datos en MS-SQL**

**User and database security**

* Nunca utilizar la cuenta SA para ejecutar o configurar el ANDA
* Más información: http://msdn.microsoft.com/en-us/library/ms174173.aspx

**Notas y advertencias sobre phpMyAdmin**

Si se decide instalar phpMyAdmin y dejarlo en el servidor (NO RECOMENDADO) entonces siga esta guía de seguridad:

***http://wiki.phpmyadmin.net/pma/Security***

Nuevamente: si es realmente necesario instalar *phpMyAdmin* tener en cuenta la necesidad de mantener seguridad extra de la contraseña, usar control de acceso *SSL login* y nunca acceder con la cuenta *root* desde otro lugar excepto el propio servidor. Acceder a la base de datos del ANDA vía *phpMyadmin* puede comprometer la seguridad del ANDA y otros sitios.