|  |  |  |  |
| --- | --- | --- | --- |
| Dibujo_LOGO | **Tipo de Macroproceso:** | **Código:**  BP-SEC-I-303 | **Fecha elaboración:**  03/10/2017 |
| **Macroproceso :**  Administración TI y SI | **División:**  Todas | **Fecha de Actualización:** |
| **Proceso:** | **Versión:**  1.0 | **Fecha de aprobación del Responsable:** |
| **Subproceso:** | **Custodio del documento**  Riesgo Operativo | **Paginas:**  13 |

**CHECKLIST – INTERNET INFORMATION SERVER 8.5 V1.0**

|  |  |  |
| --- | --- | --- |
| **Elaborado por:** | **Revisado por:** | **Aprobado por:** |
| Efraín Chamba  Ingeniero de Seguridad – TCS  Andrés Tubón  Ingeniero de Seguridad - TCS | Rafael Pintag  Jefe de Equipo – Infraestructura TCS  Ana Caiza  Jefe de Equipo – Ingeniería de Seguridad TCS | Robert Soto  Jefe de Equipo – Seguridad Informática BP |

**CONTENIDO**

[1. OBJETIVO 3](#_Toc512418342)

[2. ALCANCE 3](#_Toc512418343)

[3. DOCUMENTACIÓN RELACIONADA 3](#_Toc512418344)

[4. ÍTEMS DE REVISIÓN 4](#_Toc512418345)

[4.1. Planificación e Instalación 4](#_Toc512418346)

[4.1.1. Paquetes de Instalación 4](#_Toc512418347)

[4.1.2. Certificados digitales 4](#_Toc512418348)

[4.1.3. Directorios predeterminados 4](#_Toc512418349)

[4.1.4. Configuración del sitio de publicación 5](#_Toc512418350)

[4.1.5. Puertos predeterminados 5](#_Toc512418351)

[4.1.6. Divulgación de información del servidor web 6](#_Toc512418352)

[4.1.7. Divulgación de puertos 6](#_Toc512418353)

[4.1.8. Banners predeterminados 6](#_Toc512418354)

[4.1.9. Cabeceras de respuesta predeterminadas 6](#_Toc512418355)

[4.1.10. Configuración de cabeceras de respuesta de seguridad 6](#_Toc512418356)

[4.1.11. Directorios Innecesarios 7](#_Toc512418357)

[4.1.12. Métodos HTTP innecesarios 7](#_Toc512418358)

[4.1.13. Configuración de errores 8](#_Toc512418359)

[4.2. Gestión de Logs 9](#_Toc512418360)

[4.2.1. Activación de LOGS 9](#_Toc512418361)

[4.3. Configuraciones Adicionales 10](#_Toc512418362)

[4.3.1. Usuarios predeterminados 10](#_Toc512418363)

[4.3.2. Deshabilitar WebDAV 10](#_Toc512418364)

[4.3.3. Deshabilitar protocolos inseguros 11](#_Toc512418365)

[4.3.4. Deshabilitar cifrados nulos y débiles 11](#_Toc512418366)

## OBJETIVO

Controlar el cumplimiento del esquema de seguridad que debe implementarse en los Servidores Web Internet Information Server de Banco Pichincha, en función de las Normas y Políticas de Seguridad Informática

## ALCANCE

Todos los Servidores de Banco Pichincha que tengan Intenet Information Server implementado.

## DOCUMENTACIÓN RELACIONADA

Banco Pichincha - Estándar de seguridad BP-SEC-I-300 STD Internet Information Server 8.5.

## ÍTEMS DE REVISIÓN

|  |  |  |
| --- | --- | --- |
| Planificación e Instalación | | **Observaciones** |
| Paquetes de Instalación | |  |
|  | Durante la Instalación de IIS se debe escoger únicamente los paquetes necesarios evitando aquellos paquetes que no se van a utilizar o que comprometan la seguridad del sistema. Ir a Inicio 🡪 Server Manager. Validar la instalación únicamente los siguientes paquetes:   |  |  | | --- | --- | | **PAQUETE** | **COMPONENTES** | | **Common HTTP Features** | * Static Content * Default Document * HTTP Errors | | **Application Development** | * ASP.NET * .NET Extensibility * ISAPI Extensions * ISAPI Filters | | **Health and Diagnostics** | * HTTP Logging * Request Monitor | | **Security** | * Request Filtering * IP and Domain Restrictions | | **Performance** | * Static Content Compression | | **\*WAS** | * WAS-Process-Model * WAS-Config-APIs | | **Management Tools** | * IIS Management Console | |  |
| Certificados digitales | | **Observaciones** |
|  | Validar la Configuración del certificado digital emitido por el controlador de dominio.  Para servidores de red interna, se debe utilizar la opción **“Server Certificate”**, seleccionar el certificado digital dar clic en “View …” y verificar las características del servidor web. |  |
| Directorios predeterminados | | **Observaciones** |
|  | Validar la existencia una carpeta llamada **“sitios\pub”** en la partición de datos que se haya creado en el servidor. Esta carpeta será el lugar donde se publicarán las aplicaciones web.   * **D:\sitios\pub\**   Para validar esta configuración utilizar la opción “Basic Settings…”, ubicada en “Default Web Site”.  Verificar el valor d:\sitios\pub en “Physical path:” debe ser “D:\sitios\pub”. |  |
| Configuración del sitio de publicación | | **Observaciones** |
|  | Ingresar al IIS (inetmgr) 🡪 Sitio web de la Aplicación 🡪 Documento Predeterminado 🡪 Validar que existan los siguientes registros y en el orden que se muestra en la siguiente pantalla:    Finalmente, validar la configuración del archivo Default.htm en el sitio principal de la aplicación:  WIN+E 🡪 Ir al Sitio Disco:\sitios\aplicación 🡪 crear el archivo Default.htm con el siguiente contenido:  <meta http-equiv="refresh" content="0; URL=**'https://formiik.com/login.'**" />  En el Campo URL validar el ALIAS creado en el DNS incluido el directorio virtual y el archivo de inicio de la aplicación publicada. |  |
| Puertos predeterminados | | **Observaciones** |
|  | Verificar que no existan configuraciones de puertos por defecto en el servidor web  Se debe utilizar la opción **“Bindings…”**, para realizar la verificación, esta opción se encuentra ubicada en **“Default Web Site”**.  Validar que no existan configuraciones de protocolos inseguros HTTP. Verificar que el protocolo seguro **HTTPS** se encuentre configurado en el puerto **8043**. |  |
| Divulgación de información del servidor web | | **Observaciones** |
|  | Validar la configuración de la eliminación de cabeceras de respuesta.  Se debe utilizar la opción **“URL Rewrite”** que se encuentra ubicada en **“Default Web Site”** y en **“ARR”**, para validar que se encuentren las siguientes entradas  Ocultar la versión de IIS  **Name:** Ocultar Server Response  Eliminación del banner de información sobre sitios:  **Name:** Ocultar XPower Response  Eliminación del banner de información sobre la versión de ASP.NET:  **Name:** Ocultar Asp.Net Response  Eliminación del banner de información sobre la versión del framework MVC:  **Name:** Ocultar Asp.Net Response |  |
| Divulgación de puertos | | **Observaciones** |
|  | Validar la configuración el servidor web, para evitar divulgar el puerto enmascarado.  Se debe utilizar la opción **“URL Rewrite”** que se encuentra ubicada en **“ARR”**. Verificar la siguiente información:  **Name:** Reverse Proxy Rules |  |
| Banners predeterminados | | **Observaciones** |
|  | Validar que se encuentre configurado el servidor web para eliminar la información de la página de inicio de IIS:  Se debe utilizar la opción **“Default Document”**, para realizar la deshabilitación del banner de inicio, ir a la opción se encuentra ubicada en **“Default Web Site”** y **“ARR”** validar que la opción se encuentre en Enable. |  |
| Cabeceras de respuesta predeterminadas | | **Observaciones** |
|  | Validar que no se divulgue la información de X-Powered-By de las cabeceras de respuesta del servidor web:  Se debe utilizar la opción **“HTTP Response Headers”** que se encuentra ubicada en **“Default Web Site”** yen**“ARR”**,verificar que el “X-Powered-By” no se encuentre en este listado de cabeceras de respuesta. |  |
| Configuración de cabeceras de respuesta de seguridad | | **Observaciones** |
|  | Verificar la configuración de las cabeceras de seguridad en la respuesta del servidor web:  Se debe utilizar la opción “**HTTP Response Headers**” para habilitar banners que blindan el servidor contra ataques de Cross Site Scripting XSS, validar los siguientes valores:  **Name:** X-XSS-Protection  **Value:** 1; mode=block  Blindaje de cabeceras para forzar el uso de protocolo seguro:  **Name:** Strict-Transport-Security  **Value:** max-age=31536000; includeSubDomains; preload  Blindaje de cabeceras para evitar ataques de secuestro de clic:  **Name:** X-Frame-Options  **Value:** SAMEORIGIN  Blindaje de cabeceras para evitar contenido malicioso:  **Name:** X-Content-Type-Options  **Value:** nosniff  Blindaje de cabeceras para evitar el almacenamiento de información de páginas web:  **Name:** Cache-Control  **Value:** no-cache; no-store; max-age=0 |  |
| Directorios Innecesarios | | **Observaciones** |
|  | Validar que no existan Directorios Innecesarios:   * **aspnet\_client**   Validar que la carpeta mencionada anteriormente, no exista: **C:\inetpub\wwwroot\aspnet\_client** |  |
| Métodos HTTP innecesarios | | **Observaciones** |
|  | Verificar la configuración segura de métodos HTTP innecesarios:  Clic derecho en Computer 🡪 Manage 🡪 Roles🡪 Web Server(IIS) -> Internet Information Server 🡪 Seleccionar Default Web Site 🡪 IIS 🡪 Request Filtering 🡪 Escoger el TAB HTTP Verbs:      Verificar los siguientes métodos uno a uno: **OPTIONS, TRACE Y DEBUG**, sean configurados con false.  Validar que la configuración del parámetro “**EnableTraceMethod**” se encuentre establecido en 0, dentro de la siguiente llave del registro:  **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters** |  |
| Configuración de errores | | **Observaciones** |
|  | Validar el respaldo de la carpeta de errores personalizados del servidor web a otra carpeta:  **C:\inetpub\custerr\en-US** a la carpeta **“D:\stios\custerr\en-US”**, en el directorio **C:\inetpub\custerr\en-US.**  Luego verificar en la consola de IIS la configuración de los errores de IIS, seleccionar Error Pages:  Verificar que cada uno de los ítems que aparecen se encuentre direccionado a **“D:\stios\custerr\en-US”**, según corresponda.    Dar clic derecho en Computer 🡪 Manage 🡪 Roles🡪 Web Server(IIS) -> Internet Information Server 🡪 Seleccionar Default Web Site 🡪 Management 🡪 Configuration Editor    Posicionarse en el combo Section y escoger la opción **“system.webServer”** luego escoger **httpErrors**    Validar que se encuentre configurado como: **“ApplicationHost.config <location path=’Default Web Site’** luego validar la opción **allowAbsolutePathsWhenDelegated** y validar que se encuentre configurado en **True.** |  |
| Gestión de Logs | |  |
| Activación de LOGS | | **Observaciones** |
|  | Validar la configuración de logs conforme los siguientes pasos:  Clic derecho en Computer 🡪 Manage 🡪 Roles🡪 Web Server(IIS) -> Internet Information Server 🡪 Seleccionar Default Web Site 🡪 IIS 🡪 Logging:    Validar que el campo “Schedule” se encuentra opción Daly:    🡪 Hacer clic en **“Select Fields”**, y verificar los siguientes parámetros:   * Date * Time * Client IP Address * User Name * Server IP Address * Server Port * Method * URI Stem * Protocol Status * User Agent * Referer * Bytes send * Bytes received |  |
| Configuraciones Adicionales | |  |
| Usuarios predeterminados | | **Observaciones** |
|  | Validar que no exista el usuario IUSR\_MACHINE siempre y cuando una Aplicación no lo utilice |  |
| Deshabilitar WebDAV | | **Observaciones** |
|  | Verificar que no se encuentre activo webdav.   * Iniciar el Editor del Registro (Regedt32.exe). * Buscar la siguiente clave del Registro:   HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters   * Validar el siguiente valor al Registro:   Nombre de valor: **DisableWebDAV**  Tipo de datos: **DWORD**  Información del valor: **1** |  |
| Deshabilitar protocolos inseguros | | **Observaciones** |
|  | Verificar que las siguientes configuraciones para deshabilitar protocolos inseguros como SSL, se encuentre configurado en el registro de Windows (regedit):   * Iniciar el Editor del Registro (Regedt32.exe). * Buscar la siguiente clave del Registro:   HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 2.0\Client   * Verificar el siguiente valor al Registro:   Nombre de valor: **Enabled**  Tipo de datos: **DWORD**  Información del valor: **0**   * Iniciar el Editor del Registro (Regedt32.exe). * Buscar la siguiente clave del Registro:   HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 2.0\Server   * Verificar el siguiente valor al Registro:   Nombre de valor: **Enabled**  Tipo de datos: **DWORD**  Información del valor: **0**   * Iniciar el Editor del Registro (Regedt32.exe). * Buscar la siguiente clave del Registro:   HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 3.0\Client   * Verificar el siguiente valor al Registro:   Nombre de valor: **Enabled**  Tipo de datos: **DWORD**  Información del valor: **0**   * Iniciar el Editor del Registro (Regedt32.exe). * Buscar la siguiente clave del Registro:   HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\SSL 3.0\Server   * Verificar el siguiente valor al Registro:   Nombre de valor: **Enabled**  Tipo de datos: **DWORD**  Información del valor: **0**   * Iniciar el Editor del Registro (Regedt32.exe). * Buscar la siguiente clave del Registro:   HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols\TLS 1.0   * Verificar el siguiente valor al Registro:   Nombre de valor: Server  Tipo de datos: DWORD  Información del valor: 0 |  |
| Deshabilitar cifrados nulos y débiles | | **Observaciones** |
|  | Verificar que las siguientes configuraciones para deshabilitar protocolos inseguros como el cifrado nulo, se encuentre configurado en el registro de Windows (regedit):  Iniciar el Editor del Registro (Regedt32.exe).  Buscar la siguiente clave del Registro:  HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL  Validar el siguiente valor al Registro:  Nombre de valor: Enabled  Tipo de datos: DWORD  Información del valor: 0  Buscar la siguiente clave del Registro:  HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56  Validar el siguiente valor al Registro:  Nombre de valor: Enabled  Tipo de datos: DWORD  Información del valor: 0  Buscar la siguiente clave del Registro:  HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128  Validar el siguiente valor al Registro:  Nombre de valor: Enabled  Tipo de datos: DWORD  Información del valor: 0  Buscar la siguiente clave del Registro:  HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128  Validar el siguiente valor al Registro:  Nombre de valor: Enabled  Tipo de datos: DWORD  Información del valor: 0  Buscar la siguiente clave del Registro:  HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128  Validar el siguiente valor al Registro:  Nombre de valor: Enabled  Tipo de datos: DWORD  Información del valor: 0  Buscar la siguiente clave del Registro:  HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128  Validar el siguiente valor al Registro:  Nombre de valor: Enabled  Tipo de datos: DWORD  Información del valor: 0  Buscar la siguiente clave del Registro:  HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128  Validar el siguiente valor al Registro:  Nombre de valor: Enabled  Tipo de datos: DWORD  Información del valor: 0  Añadir \ Modificar las siguientes claves en el registro:  Buscar la siguiente clave del Registro:  HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128  Validar el siguiente valor al Registro:  Nombre de valor: Enabled  Tipo de datos: DWORD  Información del valor: 0 |  |