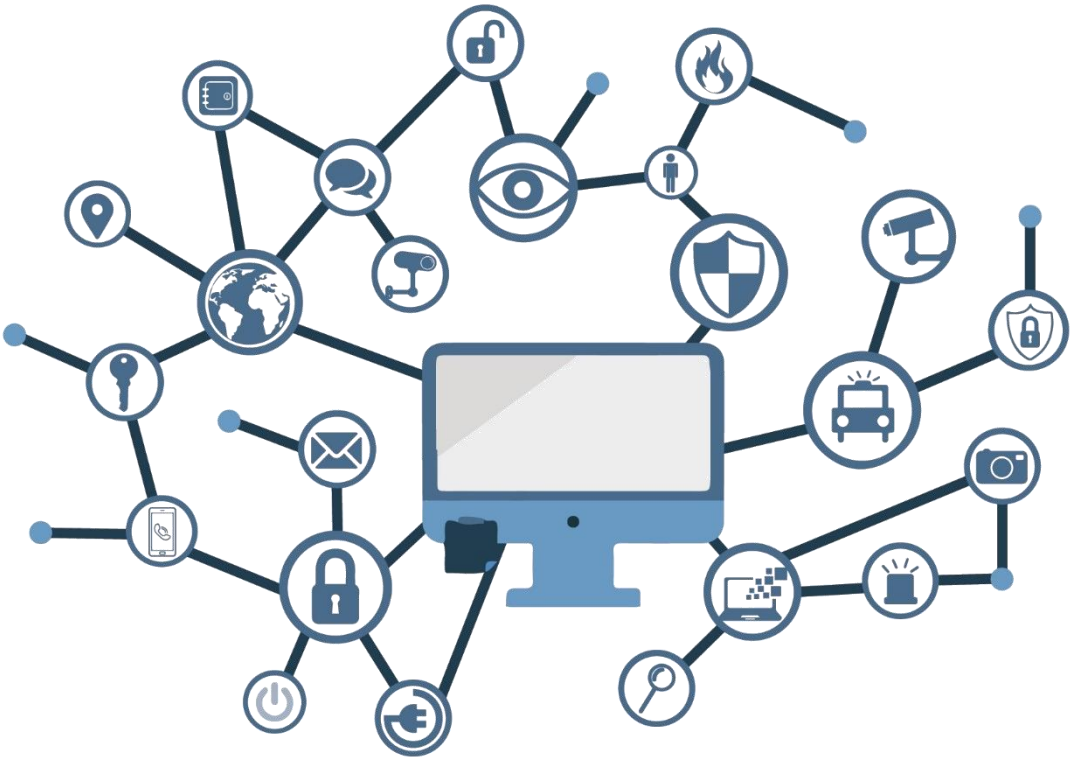
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC-673

GUÍA DE CONFIGURACIÓN SEGURA EN SERVIDORES WEB



ENERO 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.02.14 10:24:37 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-036-5.

Fecha de Edición: enero de 2023
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

ÍNDICE

1. INTRODUCCIÓN

Con motivo de la aparición de nuevas versiones y cambios en el software esencial como los **sistemas operativos**, es altamente importante contar con unas medidas de seguridad y de evaluación constantes que puedan detectar de forma proactiva y previa a su implementación cualquier vulnerabilidad, amenaza o riesgo.

Esto permitirá elaborar un plan de seguridad acorde a los resultados obtenidos y minimizar al máximo posible los vectores de ataque o malas configuraciones sobre los activos, intentando también que estas medidas no afecten a la funcionalidad o usabilidad del sistema y sus objetivos.

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional, siendo de aplicación para la Administración pública en el cumplimiento del Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para los sistemas que manejen información clasificada nacional.

2. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para aplicar un perfilado de seguridad basado en la realización de un análisis de riesgos, en sistemas que implementen servicios web.

La configuración que se aplica a través de la presente guía se ha diseñado para adaptarse a las características específicas de cada entorno, en función de los resultados obtenidos del análisis de riesgos preceptivo. Se trata de la aproximación del MARCO MODERNO DE SEGURIDAD que desde el Centro Criptológico Nacional se persigue para una adaptación adecuada al ecosistema en cuestión, el cual basa sus pilares fundamentales en los siguientes objetivos.

a) Las medidas a adoptar estarán condicionadas por el análisis de riesgos preceptivo de cada escenario, la probabilidad de materialización de la amenaza y la superficie de exposición del sistema.

b) Se tendrán en cuenta los avances tecnológicos y el estado del arte más reciente en ciberseguridad.

c) Será adaptable en la aplicación de medidas evitando una aplicación monolítica y estanca, utilizando la Declaración de Aplicabilidad como elemento fundamental sobre el que vertebrar la seguridad, en base a responsabilidad compartida.

d) La Declaración de Aplicabilidad (conjunto de medidas a implementar) utilizará de base los niveles del Esquema Nacional de Seguridad validados por el análisis de riesgos preceptivo utilizado en base a una categorización ENS MEDIO.

e) Las medidas de seguridad se podrán aplicar a sistemas ya implementados o nuevos sistemas, minimizando el impacto en la producción.

f) Las guías se revisarán y se actualizarán según las nuevas amenazas y mejoras tecnológicas.

Este marco de aplicación basado en un perfilado de seguridad tiene en consideración la diversidad de escenarios que se pueden dar, con sus particularidades, riesgos y amenazas, por lo que será cada organización que implementa las medidas de seguridad la que deba determinar qué medidas serán de aplicación, compensadas o complementadas, en función de sus condiciones específicas, asumiendo una responsabilidad compartida en la puesta en operación del sistema.

Para ayudar a las organizaciones a implementar las medidas de seguridad, se ha considerado la necesidad de crear tres (3) alcances de implementación:

a) Alcance básico.

b) Alcance intermedio.

c) Alcance avanzado.

Para la elaboración de esta guía, se ha hecho un esfuerzo de revisión exhaustiva de las distintas configuraciones de seguridad disponibles para servidores web, alineándolas y clasificándolas en función de los riesgos que cada una de ellas mitigan o abordan individualmente.

De esta forma, se pretende dar mayor coherencia al conjunto de medidas resultantes o perfilado de seguridad, siendo necesario aplicar únicamente aquellas medidas que realmente atienden a un riesgo declarado en función de los niveles de alcance señalados anteriormente.

Se trata de implementar medidas con un criterio claro, conociendo los riesgos, el contexto de la amenaza y la superficie de exposición de cada sistema en particular, y adaptando las medidas de seguridad a aplicar en función de ello.

3. ALCANCE

Para ayudar a las organizaciones a identificar los riesgos de seguridad, y por lo tanto realizar el perfilado correspondiente para cada uno de sus sistemas, se ha incorporado a esta guía un apartado denominado declaración de riesgos donde se identifican y se explican los principales riesgos del producto del que trata la guía.

Esta guía se ha elaborado con el objetivo de proporcionar información específica sobre los riesgos y las medidas de mitigación recomendadas para los escenarios planteados. En particular, se incluirá la configuración para realizar un análisis de medidas de seguridad en un entorno web.

Para garantizar la seguridad de los clientes y servidores, deberán instalarse las actualizaciones recomendadas por el fabricante. Hay que tener presente que determinadas actualizaciones, por su criticidad, pueden ser liberadas en cualquier momento y, por lo tanto, deberá prestarse especial atención a dichas publicaciones.

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que, en ocasiones, se realizan para las distintas actualizaciones de seguridad.

Antes de aplicar esta guía en producción, deberá asegurarse de haberla probado en un entorno aislado y controlado, en el cual se habrán aplicado las pruebas y posteriores cambios en la configuración que se ajusten a los criterios específicos de cada organización.

El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones, sino a servir como línea base de seguridad que deberá ser adaptada a las necesidades propias de cada organización.

Este documento incluye:

a) Descripción de uso de esta guía. Breve explicación acerca de los pasos a seguir para identificar, seleccionar y aplicar las medidas de seguridad recomendadas.

b) Declaración de riesgos. En esta sección se identifican los principales riesgos asociados al producto o tecnología del que trata la guía CCN-STIC. Por ejemplo, un servicio web puede tener riesgos relacionados con el acceso remoto, mientras que un controlador de dominio puede tener riesgos relacionados con los procesos de autenticación. La organización podrá hacer uso de los riesgos identificados en este punto y añadir los que considere necesarios para su escenario en particular.

c) Identificación del valor de riesgo. En esta sección se muestran una serie de tablas o mapas de calor, con tres (3) niveles de superficie de exposición y los valores de riesgo resultantes de la intersección de los niveles de impacto y probabilidad. Se trata de una muestra de cómo alterando alguna de estas variables (superficie de exposición, impacto y probabilidad), los resultados del riesgo de adecúan a cada realidad.

d) Perfilado de seguridad. En este punto se establecen las medidas de seguridad que se deberán aplican al producto o tecnología del que trata la guía. Su clasificación se realiza en tres (3) niveles, cada uno de ellos asociado a un conjunto de niveles de riesgos.

4. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de seguridad, es conveniente explicar el proceso de aplicación de seguridad que describe y los recursos que proporciona. Este proceso constará de los siguientes pasos:

a) **Identificación de riesgos del producto**. Se recomienda realizar un inventario de riesgos que puedan existir por la propia naturaleza del producto o tecnología, como por la funcionalidad prevista por la organización. Para ello, se han identificado una serie de riesgos inherentes al producto o tecnología, los cuales deberán ser completados con los riesgos particulares del sistema que se vaya a implementar.

   Para la identificación inicial de riesgos, se ha empleado la metodología MAGERIT y la herramienta PILAR, sobre un escenario basado en servicios web.

b) **Cuantificación de probabilidad de cada riesgo**. Se deberá cuantificar la probabilidad de ocurrencia de cada riesgo en función de las condiciones particulares que cada organización conoce de sus sistemas.

c) **Cuantificación de impacto de cada riesgo**. Se deberá cuantificar el impacto en las operaciones y en el negocio, en función de las condiciones particulares que cada organización conoce de sus sistemas.

d) **Cuantificación de superficie de exposición del sistema o servicio**. La organización deberá determinar el nivel de superficie de exposición que tendrá el activo (servicio que presta o información que maneja).

e) **Identificación del valor de riesgo haciendo uso de tablas de mapas de calor**. Para cada guía se han desarrollado una serie de tablas de mapas de calor, permitiendo calcular e identificar donde se sitúa cada uno de los riesgos identificados en los primeros pasos. Una vez identificado el nivel de riesgo, en el siguiente paso se procederá a aplicar la medida mitigadora correspondiente a dicho nivel de riesgo.

f) **Identificación de medidas (básico, intermedio o avanzado) según valor de riesgo y guía CCN-STIC**. La lista de medidas de seguridad está agrupada en categorías y ordenada según el nivel de riesgo resultado de los cálculos anteriores. Es importante señalar que cada categoría puede conllevar la necesidad de aplicar una o varias medidas de seguridad, que a su vez se pueden traducir en distintas configuraciones, directivas de seguridad o la instalación de software de protección.

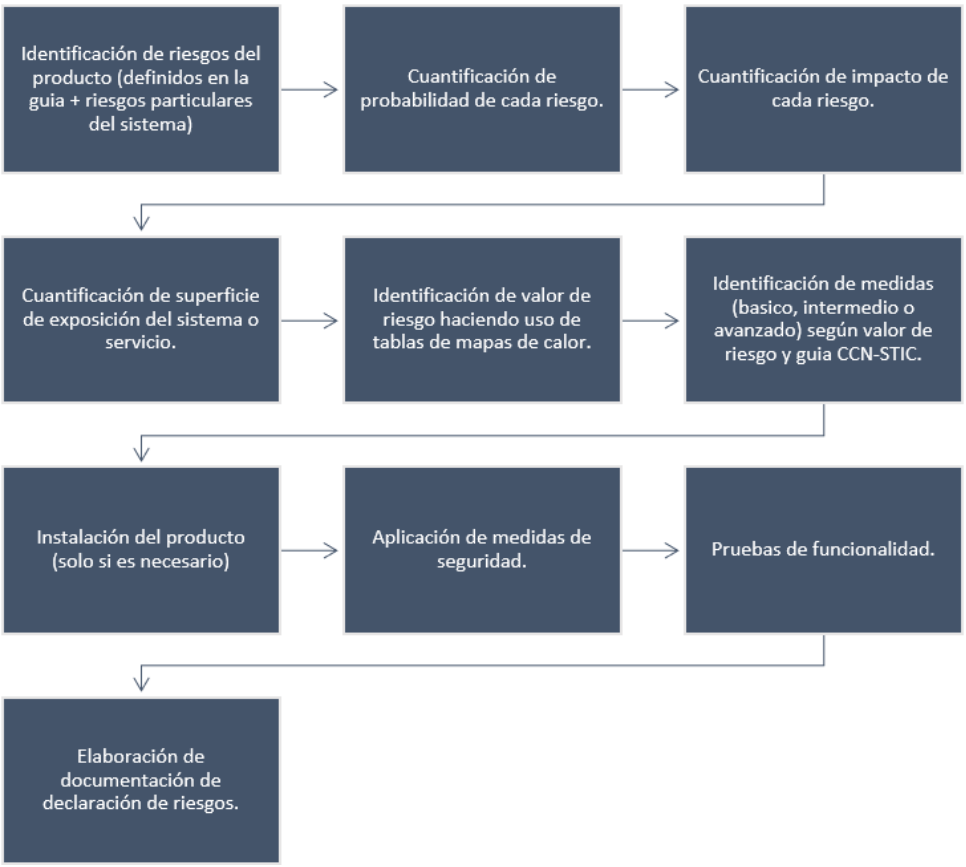
   Cada organización deberá determinar cómo configurar el sistema para el cumplimiento de la medida correspondiente. De esta forma, se ofrece un mayor grado de flexibilidad a la hora de proteger el sistema, necesario sobre todo en sistemas que ya están en funcionamiento o en producción. Es decir, en esta guía de seguridad se identifican qué medidas de seguridad serán necesarias aplicar, pero el cómo aplicarlas se deja a elección de las propias organizaciones.

g) **Instalación del producto (en nuevas instalaciones)**. Una vez conocidos los riegos y las medidas de mitigación de éstos, se procederá con la instalación del sistema operativo, en el caso de nuevas implementaciones. En caso de que el sistema ya se encuentre instalado, se puede saltar este paso.

h) **Aplicación de medidas de seguridad**. En este paso se aplicarán las medidas de seguridad recomendadas según el nivel de riesgo resultante para hacer efectiva la mitigación, reducción o eliminación del riesgo. Es lo que se denomina el perfilado de seguridad. Cada organización puede tener un perfilado distinto y como se ha indicado anteriormente, se deberán aplicar las medidas de seguridad en función de dicho perfilado.

i) **Pruebas de funcionalidad**. Se recomienda diseñar y ejecutar un plan de pruebas de funcionalidad posterior a la aplicación de medidas, dado que alguna de ellas puede haber deshabilitado o bloqueado funcionalidades que requiere la organización. En ese caso se podrán establecer directivas de excepción para revertir los cambios, asumiendo el riesgo que ello conlleva.

j) **Elaboración de documentación de declaración de riesgos**. Se recomienda elaborar un documento de declaración de riesgos donde se establezca claramente cada uno de los riesgos identificados y las medidas de seguridad aplicadas.



5. DECLARACIÓN DE RIESGOS

Se trata del primer paso a realizar para la aplicación de las medidas de seguridad acordes a la realidad y condiciones donde estará operando el sistema.

Con motivo de la aparición de nuevas versiones y cambios en el software de base, como los sistemas operativos, es altamente recomendable contar con unas medidas de seguridad y de evaluación constantes que puedan detectar, de forma proactiva y previa a su aplicación, cualquier vulnerabilidad, amenaza o riesgo.

El análisis de riesgos permitirá elaborar un perfilado para la aplicabilidad de medidas acorde a los resultados obtenidos, minimizando los vectores de ataque, brechas o malas configuraciones de seguridad sobre los activos, e intentando también que estas medidas no afecten a la funcionalidad o usabilidad del sistema y sus objetivos.

Esta guía de seguridad tiene como uno de sus objetivos ayudar a la implementación de las medidas de seguridad, por lo tanto, para la elaboración de la propia guía se ha realizado un análisis de riesgos específico para un entorno de servidor web.

Para la ejecución del presente Análisis de Riesgos, se han definido dos (2) escenarios base, los cuales se consideran esenciales y estándar de uso del sistema.

a) El primer escenario será un sistema aislado en red, quiere decir que estará conectando a elementos de red internos dentro de una organización o entidad, pero no realizará conexiones externas hacia redes no seguras como Internet.
b) El segundo escenario será un sistema conectado a redes no seguras como puede ser Internet, quiere decir que tendría la capacidad de establecer conexiones con elementos de red externos de una organización o entidad.

5.1 RIESGOS ASOCIADOS A SERVIDORES WEB

A continuación, se identifican los resultados de este análisis, los cuales forman parte de la declaración de riesgos y constituye, como ya se ha indicado, el primer paso a realizar en la implementación de esta guía de seguridad. Estos riesgos se deberán tener en consideración cuando la organización diseñe y elabore su propio análisis de riesgos.

Para facilitar la tarea de identificar, cuantificar y valorar cada uno de los riesgos, se ha elaborado la tabla de control que se presenta en la siguiente página, donde se podrá ir registrando en cada caso los niveles de probabilidad e impacto asociados a cada riesgo para un equipo en concreto.

EXP	NOMBRE DEL EQUIPO			
	SISTEMA OPERATIVO		BUILD	
	FUNCION PRINCIPAL		FECHA DE AA.RR.	

NUM	RIESGOS	APLICA (S/N)	PROBABILIDAD [1…5]	IMPACTO [1…5]
1.	[A.3] Manipulación de los registros de actividad.			
2.	[A.4] Manipulación de los ficheros de configuración.			
3.	[A.5] Suplantación de la identidad.			
4.	[A.6] Abuso de privilegios de acceso.			
5.	[A.7] Uso no previsto.			
6.	[A.11] Acceso no autorizado.			
7.	[A.15] Modificación de la información.			
8.	[A.19] Revelación de información.			
9.	[A.24] Denegación de servicio.			
10.	[E.24] Caída del sistema por agotamiento de recursos.			

5.2 CUANTIFICACIÓN DE PROBABILIDAD DE CADA RIESGO

El siguiente paso, será cuantificar la probabilidad de cada uno de los riesgos. Los valores de probabilidad podrán ir desde el valor uno (1) hasta el valor cinco (5), siendo uno (1) muy poco probable y cinco (5) muy probable:

a) **Probabilidad 1**: Es muy poco probable que se materialice el riesgo, ya sea por las condiciones específicas del sistema en la organización o porque existan salvaguardas ya implementadas que hagan que el riesgo prácticamente desaparezca.

b) **Probabilidad 2**: Es poco probable que se materialice el riesgo, aunque se puede materializar.

c) **Probabilidad 3**: Es probable que se materialice el riesgo dadas las condiciones específicas del sistema en la organización. Se deberá atender detalladamente a las medidas de seguridad que hagan que este riesgo se minimice en la medida de lo posible.

d) **Probabilidad 4**: Es bastante probable que se materialice el riesgo, dadas las condiciones específicas del sistema en la organización. Se deberá atender detalladamente a las medidas de seguridad que hagan que este riesgo se minimice en la medida de lo posible.

e) **Probabilidad 5**: Es muy probable que se materialice el riesgo, dadas las condiciones específicas del sistema en la organización o porque no existen salvaguardas que reduzcan la probabilidad de materialización del riesgo. Las medidas de seguridad a aplicar cuando se da este nivel pueden ser más estrictas que en niveles inferiores.

5.3 CUANTIFICACIÓN DE IMPACTO DE CADA RIESGO

Al igual que sucede con la cuantificación de la probabilidad, se deberá cuantificar el grado de impacto en el servicio o negocio en el supuesto de que el riesgo se materialice. Los valores de impacto podrán ir desde el valor uno (1) hasta el valor cinco (5), siendo uno (1) cuando no tiene un impacto conocido o es muy pequeño y cinco (5) cuando el impacto es muy importante:

a) **Impacto 1**: El riesgo, en el caso de que se materialice, no tiene un impacto conocido o es muy pequeño, prácticamente despreciable. Los datos y el servicio no se ven comprometidos y el sistema funciona correctamente. Este nivel de impacto puede requerir la aplicación de medidas de prevención.

b) **Impacto 2**: El riesgo, en el caso de que se materialice, tiene un impacto pequeño. No se han comprometidos los datos ni el servicio, sin embargo, es posible que, si no se corrige, el sistema se vuelva inestable o pueda existir acceso no autorizado a información sensible. Este nivel de impacto puede requerir la aplicación de medidas de prevención.

c) **Impacto 3**: El impacto en el sistema es preocupante. No se han comprometido los datos, sin embargo, el servicio puede continuar de forma limitada y a corto plazo podría haber una degradación de la seguridad del sistema. Si no se aplican las medidas necesarias puede existir acceso no autorizado a información sensible. Este nivel de impacto puede requerir la aplicación de medidas de prevención, pero también medidas de corrección.

d) **Impacto 4**: El impacto en el sistema es importante. Es posible que algunos datos hayan sido comprometidos y los servicios se hayan visto afectados. También es posible que el sistema se haya vuelto inestable o comience a ser vulnerable. Se debe actuar lo antes posible para restablecer el correcto funcionamiento.

e) **Impacto 5**: El impacto en el sistema es muy importante. Afecta directamente a la disponibilidad del servicio, imposibilitando el acceso a la información. El sistema ha sido comprometido, y algunos o todos los datos han sido comprometidos. Un atacante externo puede haber obtenido acceso privilegiado y puede estar controlando el sistema. Se deben aplicar medidas de recuperación de forma inmediata.

5.4 CUANTIFICACIÓN DE SUPERFICIE DE EXPOSICIÓN DEL SISTEMA

Por último, se deberá tener en cuenta el nivel o grado de exposición del sistema a las amenazas y riesgos externos. Este valor actuará como modulador a la hora de calcular el valor final de cada uno de los riesgos.

Por ejemplo, ante un riesgo cuyo impacto y probabilidad son altos o muy altos, si el sistema se encuentra en un nivel de superficie de exposición bajo, es lógico pensar que el valor final del riesgo se vea atenuado en parte por las condiciones de exposición en las que encuentra el sistema. Por el contrario, si un riesgo tiene unos niveles de impacto y probabilidad bajos, ante un nivel de superficie de exposición alto, es lógico pensar que el valor final del riesgo se vea incrementado por este mismo motivo.

Es evidente que pueden existir multitud de escenarios y configuraciones de red, siendo prácticamente imposible reflejar todas ellas en una sola guía de seguridad. Sin embargo, para una mejor comprensión y simplificación de las medidas que se deberán adoptar, se han agrupado en tres (3) niveles las distintas opciones de superficie de exposición:

a) **Nivel de superficie de exposición 1**: Representa aquellos sistemas que no están expuestos a riesgos externos, procedentes de redes interconectadas o redes no confiables como Internet. En este nivel se encuentran los sistemas aislados, sin ningún tipo de comunicación con otras redes.

b) **Nivel de superficie de exposición 2**: Representa aquellos sistemas que tienen algún tipo de conexión de red local o de interconexión con otras redes. Estos sistemas se conectan únicamente con redes confiables. En este nivel se encuentran los sistemas compuestos por más de un equipo conectado a través de una red local (LAN) o varios sistemas que están interconectados entre si a través de otros medios, pero que no son accesibles desde Internet o redes no confiables.

c) **Nivel de superficie de exposición 3**: Representa aquellos sistemas accesibles desde o con conexión directa o indirecta con Internet y otras redes. Dado que Internet se considera una red no confiable, el riesgo de explotación de vulnerabilidades de ejecución remota es mucho mayor que en los niveles inferiores. En este nivel se encuentra la mayoría de los sistemas en producción de las organizaciones.

6. IDENTIFICACIÓN DE LOS VALORES DE RIESGO RESULTANTES

Una vez identificados los distintos riesgos inherentes al sistema y después de calcular los valores de probabilidad, impacto y superficie de exposición de cada uno de ellos, el siguiente paso será determinar el valor final de cada riesgo. Tal y como ya se ha indicado, este valor variará en función de cada una de las tres variables que se han tenido en cuenta.

Para facilitar su cálculo, se han elaborado las siguientes tablas con un diseño de mapas de calor, que varían según la superficie de exposición que tendrá el sistema. Cada una de ellas servirá como referencia para determinar el valor final del riesgo, el cual se podrá anexar a la tabla de riesgos del punto "5.1 RIESGOS ASOCIADOS A ".

SUPERFICIE DE EXPOSICIÓN	1				
PROBABILIDAD	NIVEL DE RIESGO				
5	5	6	7	7	8
4	4	5	6	7	7
3	3	4	5	6	7
2	2	3	4	5	6
1	2	2	3	4	5
IMPACTO	1	2	3	4	5

SUPERFICIE DE EXPOSICIÓN	2				
PROBABILIDAD	NIVEL DE RIESGO				
5	6	7	7	8	9
4	5	6	7	7	8
3	4	5	6	7	7
2	3	4	5	6	7
1	2	3	4	5	6
IMPACTO	1	2	3	4	5

SUPERFICIE DE EXPOSICIÓN	3				
PROBABILIDAD	NIVEL DE RIESGO				
5	7	7	8	9	10
4	6	7	7	8	9
3	5	6	7	7	8
2	4	5	6	7	7
1	3	4	5	6	7
IMPACTO	1	2	3	4	5

7. PERFILADO PARA LA APLICABILIDAD DE MEDIDAS

A continuación, se muestran las categorías o agrupación de medidas de seguridad que deberán ser aplicadas a un Servidor Web, en función de los resultados obtenidos por el análisis de riesgos y la cuantificación de cada uno de éstos.

Para una mejor comprensión, se han agrupado las medidas en tres (3) alcances de implementación, cada uno de ellos asociado a un grupo de niveles de riesgos:

a) Alcance básico.

b) Alcance intermedio.

c) Alcance avanzado.

Una vez obtenido el nivel de riesgo de cada uno de los riesgos identificados, se aplicará la siguiente tabla para determinar las medidas necesarias en cada nivel.

Esta tabla indica que, si se ha obtenido un valor menor o igual a tres (3), se deberán aplicar las categorías de perfilado de seguridad de alcance básico. Si el valor obtenido para un riesgo determinado está entre cuatro (4) y seis (6), se deberán aplicar las categorías de perfilado de seguridad de alcance intermedio. Por último, se el valor obtenido es siete (7) o superior, se deberán aplicar las categorías de perfilado de alcance avanzado.

	ALCANCE		
NIVEL DE RIESGO	(B)ÁSICO	(I)NTERMEDIO	(A)VANZADO
9	SI	SI	SI
8	SI	SI	SI
7	SI	SI	SI
6	SI	SI	
5	SI	SI	
4	SI	SI	
3	SI		
2	SI		
1	SI		

En la siguiente tabla se muestra la asociación entre los riesgos identificados en el primer paso de esta guía y las categorías de perfilado de seguridad que los mitigan, controlan o reducen.

Como se puede observar, pueden existir categorías de perfilado de seguridad que actúen sobre uno o varios riesgos. Por lo tanto, para una mejor identificación, se han codificado cada una de las categorías, asociándolas al primer riesgo que mitigan, obteniendo la siguiente nomenclatura de categorías:

a) A.3: corresponde con el código de riesgo que especifica la herramienta PILAR.

b) SEC-MSEWL1: corresponde con la categoría de seguridad 1 para dicho riesgo referente a sistemas Linux, en caso de sistemas Windows se identificaría como SEC-MSEWW1.
El número se incrementará en uno para cada nueva categoría que se haya identificado.

La siguiente tabla define qué conjunto de medidas de seguridad deben ser aplicadas, en función de los niveles de riesgo obtenidos. Cabe destacar que en función del sistema operativo que utilice para la implementación del sistema, deberá seguir un proceso de bastionado u otro.

7.1 CATEGORÍAS DE SEGURIDAD PARA SISTEMAS WEB BASADOS EN LINUX

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA SERVIDORES WEB LINUX	ALCANCE		
		B	I	A
[A.3] Manipulación de los registros de actividad (log).	[A.3.SEC-MSEWL1] Configurar opciones de auditoría y registro de logs			
[A.4] Manipulación de los ficheros de configuración	[A.4.SEC-MSEWL1] Cambiar directorio raíz de Apache (chroot)			
	[A.4.SEC-MSEWL2] Configurar directivas: Options			
[A.5] Suplantación de la identidad.	[A.5.SEC-MSEWL1] Modificar usuario y grupos del servicio			
	[A.5.SEC-MSEWL2] Configurar módulos de autenticación			
[A.6] Abuso de privilegios de acceso.	[A.6.SEC-MSEWL1] Restringir el acceso a ficheros y directorios fuera del árbol web			
	[A.6.SEC-MSEWL2] Restricción de direcciones IP			
	[A.5.SEC-MSEWL2] Configurar módulos de autenticación			
[A.7] Uso no previsto.	[A.7.SEC-MSEWL1] Eliminación de ficheros y directorios no necesarios			
	[A.7.SEC-MSEWL2] Restringir protocolos y algoritmos			
	[A.7.SEC-MSEWL3] Configurar filtrado de peticiones			
	[A.7.SEC-MSEWL4] Impedir ejecución de aplicaciones externas			
	[A.7.SEC-MSEWL5] Limitar y controlar el uso de aplicaciones PERL			
	[A.7.SEC-MSEWL6] Limitar y controlar el uso de aplicaciones PHP			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA SERVIDORES WEB LINUX	ALCANCE		
		B	I	A
[A.11] Acceso no autorizado.	[A.5.SEC-MSEWL2] Configurar módulos de autenticación			
	[A.11.SEC-MSEWL1] Configurar limites en el sistema para impedir ataques.			
[A.15] Modificación de la información.	[A.15.SEC-MSEWL1] Restringir y controlar páginas de índice			
	[A.15.SEC-MSEWL2] Configurar módulos SSL/TLS			
	[A.7.SEC-MSEWL3] Configurar filtrado de peticiones			
[A.19] Revelación de información.	[A.19.SEC-MSEWL1] Configurar directivas: ServerTokens			
	[A.19.SEC-MSEWL2] Configurar directivas: ServerSignature			
	[A.19.SEC-MSEWL3] Configurar directivas: ErrorDocument			
[A.24] Denegación de servicio.	[A.7.SEC-MSEWL4] Impedir ejecución de aplicaciones externas			
	[A.7.SEC-MSEWL5] Limitar y controlar el uso de aplicaciones PERL			
	[A.7.SEC-MSEWL6] Limitar y controlar el uso de aplicaciones PHP			
	[A.11.SEC-MSEWL1] Configurar limites en el sistema para impedir ataques.			
[E.24] Caída del sistema por agotamiento de recursos.	[E.24.SEC-MSEWL1] Establecer cuotas para el usuario de servicio			
	[A.11.SEC-MSEWL1] Configurar limites en el sistema para impedir ataques.			

7.2 CATEGORÍAS DE SEGURIDAD PARA SISTEMAS WEB BASADOS EN WINDOWS

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA SERVIDORES WEB WINDOWS	ALCANCE		
		B	I	A
[A.3] Manipulación de los registros de actividad (log).	[A.3.SEC-MSEWW1] Configurar permisos de ubicaciones de logs			
	[A.3.SEC-MSEWW2] Configurar opciones de registro			
	[A.3.SEC-MSEWW3] Habilitar registro de eventos IIS			
[A.4] Manipulación de los ficheros de configuración.	[A.4.SEC-MSEWW1] Cambiar rutas por defecto instalación IIS			
[A.5] Suplantación de la identidad.	[A.5.SEC-MSEWW1] Configurar métodos de autenticación y deshabilitar autenticación anónima.			
	[A.5.SEC-MSEWW2] Modificar usuario y grupos del servicio de las aplicaciones			
[A.6] Abuso de privilegios de acceso.	[A.6.SEC-MSEWW1] Restricción de direcciones IP y dominios			
	[A.6.SEC-MSEWW2] Restringir el acceso a ficheros y directorios fuera del árbol web			
[A.7] Uso no previsto.	[A.7.SEC-MSEWW1] Restringir protocolos y algoritmos			
	[A.7.SEC-MSEWW2] Configurar HSTS			
	[A.7.SEC-MSEWW3] Deshabilitar aplicaciones externas y SMTP			
[A.11] Acceso no autorizado.	[A.5.SEC-MSEWW1] Configurar métodos de autenticación y deshabilitar autenticación anónima.			
	[A.11.SEC-MSEWW1] Configurar limites en el sistema para impedir ataques.			
[A.15] Modificación de la información.	[A.15.SEC-MSEWW1] Configurar filtrado de solicitudes			
	[A.15.SEC-MSEWW2] Configurar módulos SSL/TLS			
[A.19] Revelación de información.	[A.19.SEC-MSEWW1] Cambiar páginas de error			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA SERVIDORES WEB WINDOWS	ALCANCE		
		B	I	A
[A.24] Denegación de servicio.	[A.11.SEC-MSEWW1] Configurar limites en el sistema para impedir ataques.			
[E.24] Caída del sistema por agotamiento de recursos.	[A.11.SEC-MSEWW1] Configurar limites en el sistema para impedir ataques.			

ANEXO A. MEDIDAS DE SEGURIDAD APLICABLES

Existen varios aspectos que deberán llevarse a cabo sobre los sistemas independientemente de su nivel de adecuación. Estas recomendaciones generales vienen a cubrir aspectos esenciales en los sistemas que publican servicios web, minimizando la superficie de exposición, aumentando la trazabilidad y reduciendo la información que exponen dichos sistemas.

a) Deberá modificar la ruta donde se almacena el sitio web por defecto, evitando realizar la instalación en el mismo disco donde se almacene el sistema operativo.

b) En caso de ser posible, deberá cambiar y limitar el usuario bajo el que se ejecutan los servicios web del sistema, evitando usuarios privilegiados o usuarios utilizados para otros propósitos, con el fin de minimizar las acciones de un atacante en caso de comprometer el sistema.

c) Se analizará la exposición del sistema y se limitarán los rangos de red que tienen acceso a los servicios web. Si es un sistema interno, que da servicio únicamente dentro de la red corporativa, se establecerán exclusivamente rangos de red internos con posibilidad de acceso.

d) Es de vital importancia que el sistema se encuentre configurado con certificados que protejan la integridad de las comunicaciones y su confidencialidad. Dichos certificados deberán ser emitidos con protocolos seguros y ser renovados periódicamente.

e) Adicionalmente al apartado anterior, si el sistema no cuenta con autenticación en el servicio web, se deberán configurar los módulos de autenticación para evitar que usuarios anónimos accedan a los recursos publicados.

f) Se deshabilitarán protocolos no seguros tales como *SSLv3* o *TLS1.0* en el caso de que el servicio web o los clientes que van a acceder no los necesiten. Es recomendable utilizar protocolos seguros como *TLS1.2* o *TLS1.3*.

g) Se configurarán en el sistema los módulos para el filtrado de peticiones, impidiendo las solicitudes hacia extensiones de archivo no necesarias o verbos *HTTP* que no sean de uso en el servicio web.

h) Se deberá generar una directiva de retención de registros adecuada para la organización, en la que se deberán almacenar las peticiones realizadas al sistema sin sobreescritura durante un tiempo prudencial. La recolección de eventos deberá estar habilitada.

A continuación, se definirán las medidas indicadas en las tablas anteriores, y cuyo fin es la mitigación o reducción del riesgo al cual están asociadas.

Nota: En las descripciones detalladas en los siguientes anexos de medidas de seguridad aplicables para los diferentes sistemas web, se procederá a la descripción de todas las medidas obtenidas tras el análisis de riesgos realizado, independientemente del alcance de implementación de las medidas, ya sean de nivel básico, intermedio, o avanzado.

ANEXO A.1. MEDIDAS DE SEGURIDAD PARA SISTEMAS WEB BASADOS EN LINUX

a) **[A.3.SEC-MSEWL1] Configurar opciones de auditoría y registro de logs**. Se deberá configurar el registro de logs, así como las opciones de auditoría que permitan; la obtención de un registro cronológico de la totalidad de actividades e incidentes que ocurren en el sistema, así como la correcta identificación del usuario que ha ejecutado cada una de las acciones registradas, pudiendo determinar las responsabilidades ante los incidentes provocados como consecuencia de las mismas.

b) **[A.4.SEC-MSEWL1] Cambiar directorio raíz de Apache (chroot)**. Se debe aislar el directorio raíz de Apache en un entorno *chroot*, de este modo las aplicaciones que se ejecuten dentro de dicho entorno no podrán acceder al resto de directorios y así, en el caso de aprovechar un fallo de seguridad en el servidor web, el atacante no podrá acceder al exterior del entorno *chroot*.

c) **[A.4.SEC-MSEWL2] Configurar directivas: Options**. La configuración de la directiva *Options* permitirá establecer las características que estarán disponibles para un directorio en particular, la configuración de esta directiva permitirá bloquear determinadas características, restringiendo así las opciones del atacante.

d) **[A.5.SEC-MSEWL1] Modificar usuario y grupos del servicio**. De manera predeterminada, el servidor web Apache se ejecuta inicialmente con el usuario *root*, el proceso *root* arrancará otros procesos hijos que se ejecutarán con el usuario *www-data* y el grupo *www-data* por lo que se recomienda cambiar dicho usuario y grupo con el fin de evitar las opciones de suplantación de identidad por parte del atacante.

e) **[A.5.SEC-MSEWL2] Configurar módulos de autenticación**. Se deben configurar los módulos de autenticación disponibles, dichos módulos permiten restringir el acceso al servidor únicamente a una serie de usuarios que habrán sido configurados previamente a la concesión de los derechos de acceso.

f) **[A.6.SEC-MSEWL1] Restringir el acceso a ficheros y directorios fuera del árbol web**. Se recomienda restringir el acceso a todos los directorios exceptuando "*DocumentRoot*", que será el directorio donde se alojará el sitio web, dichas restricciones se podrán establecer con el uso de las directivas *Allow* y *Deny*. Esta restricción permitirá evitar los posibles saltos hacia otras rutas del sistema por parte del atacante.

g) **[A.6.SEC-MSEWL2] Restricción de direcciones IP**. En el caso de que el sitio web sea atacado de manera constante, dependiendo de la frecuencia de los ataques, puede ser aconsejable bloquear la dirección IP del atacante, ya que esto puede tener un impacto significativo en el tráfico de red y ancho de banda.

   Por lo tanto, para restringir algunas zonas del sitio web, basándonos en la dirección IP del atacante, como se ha mencionado anteriormente, bastará con realizar la configuración correspondiente del módulo *mod_authz_host* y la directiva *Require,* la cual proporciona una variedad de métodos aplicables para permitir o denegar el acceso a los recursos.

   Adicionalmente, como buena práctica de seguridad, debe minimizarse la superficie de exposición de los sistemas, estableciendo los rangos de red desde los que se accederá al servidor web.

h) **[A.7.SEC-MSEWL1] Eliminación de ficheros y directorios no necesarios**. Se recomienda eliminar tanto ficheros como directorios los cuales no son necesarios, con el fin de reducir la superficie de ataque, así como reducir la ocupación de recursos, aumentando de este modo las capacidades de rendimiento del servicio.

i) **[A.7.SEC-MSEWL2] Restringir protocolos y algoritmos**. Deberá minimizarse el número de protocolos y algoritmos soportados en el sistema, deshabilitando aquellos obsoletos o vulnerables tales como *SSLv2*, *SSLv3*, *TLS1.0* y *TLS1.1*.

j) **[A.7.SEC-MSEWL3] Configurar filtrado de peticiones**. Por defecto, Apache no establece ningún límite para las peticiones, por lo que al configurar una petición desmesurada al servidor web, este podría sufrir un ataque que podría tener como consecuencia una denegación del servicio.

   Dicho comportamiento puede modificarse aplicando un límite para las peticiones en el fichero de configuración de Apache mediante la directiva '*LimitRequestBody*'.

   No obstante, se recomienda limitar los verbos *HTTP* y las extensiones permitidas en el servidor, con el fin de evitar que un atacante utilice verbos *HTTP* con fines maliciosos o realice peticiones hacia tipos de archivo inexistentes en el servidor.

k) **[A.7.SEC-MSEWL4] Impedir ejecución de aplicaciones externas**. Se deberá controlar en el sistema web el uso de aplicaciones externas que puedan poner en riesgo el servidor, ya sean aplicaciones *SMTP* o aplicaciones para cualquier otro uso. Estas aplicaciones externas aumentan la superficie de exposición del sistema y abren posibles brechas de seguridad ante desarrollos sin actualización adecuada o tecnologías obsoletas.

l) **[A.7.SEC-MSEWL5] Limitar y controlar el uso de aplicaciones PERL**. Es posible que el servicio web cuente con aplicaciones o scripts desarrollados en *PERL*. Estas aplicaciones deben controlarse y auditarse correctamente, dado que un error en la programación de las mismas puede poner al descubierto aspectos del sistema o permitir la realización de acciones no autorizadas como es la creación de ficheros o exfiltración de datos.

m) **[A.7.SEC-MSEWL6] Limitar y controlar el uso de aplicaciones PHP**. Esta medida es de vital importancia en los sistemas, cualquier aplicación *PHP* se ejecutará directamente sobre el servidor, cualquier deficiencia en estas aplicaciones pueden acarrear problemas en las bases de datos o incluso permitir la exfiltración de información, como sucedía en la medida previa.

n) **[A.11.SEC-MSEWL1] Configurar limites en el sistema para impedir ataques**. Se recomienda configurar la cantidad de ancho de banda, la cantidad de conexiones concurrentes y el tiempo de espera de conexión para las solicitudes de los clientes del servidor web. Con la aplicación de estas limitaciones se podrá evitar que los posibles atacantes sobrecarguen el sistema pudiendo llegar a provocar una caída del mismo.

   Para ello se podrán configurar el módulo *mod_ratelimit* y las directivas *MaxClients* y *Max--execution-time* entre otras.

o) **[A.15.SEC-MSEWL1] Restringir y controlar páginas de índice**. A través de la directiva *IndexOptions* se podrá especificar el comportamiento de la indexación del directorio, mientras que la directiva *IndexIgnore* permitirá definir el conjunto de nombres de ficheros que no se mostraran en los listados de directorios, de este modo se podrá reducir la información proporcionada a los posibles atacantes.

p) **[A.15.SEC-MSEWL2] Configurar módulos SSL/TLS**. Deberán configurarse los módulos *SSL* del sistema mediante la incorporación de certificados de servidor web. De esta forma se protegerán las conexiones realizadas y se cifrará el tráfico o posibles credenciales.

q) **[A.19.SEC-MSEWL1] Configurar directivas: ServerTokens**. Se debe configurar la directiva *ServerTokens*, la cual configura la cabecera de respuestas *HTTP* del servidor, dicha directiva controla si el campo "*Server*" de las cabeceras de las respuestas que se envían de vuelta incluye una descripción genérica del sistema operativo, así como información sobre los módulos compilados en el servidor.

   Se debe evitar mostrar dicha información con el fin de proporcionar información no deseada que el atacante puede utilizar para penetrar en el sistema.

r) **[A.19.SEC-MSEWL2] Configurar directivas: ServerSignature**. Al igual que en el caso anterior, se debe configurar la directiva *ServerSignature*, la cual añade una línea en la cual se indica la versión del servidor con el fin de evitar proporcionar información no deseada al atacante.

s) **[A.19.SEC-MSEWL3] Configurar directivas: ErrorDocument**. Es recomendable configurar la directiva *ErrorDocument*, la cual ofrece la posibilidad de configurar las respuestas que muestra el servidor Apache cuando se producen algunos errores o problemas.

   La configuración de dicha directiva ayudará a ocultar los mensajes de error predeterminados del sistema que proporcionan al atacante información no deseada.

t) **[E.24.SEC-MSEWL1] Establecer cuotas para el usuario de servicio**. Las cuotas obligan a los usuarios a mantenerse por debajo de su límite de consumo de disco, evitando de este modo la posibilidad de consumir espacio ilimitado en un sistema.

   Es por ello por lo que se debe establecer una cuota para la cuenta del servicio con el fin de evitar una caída del sistema por agotamiento de recursos.

ANEXO A.2. MEDIDAS DE SEGURIDAD PARA SISTEMAS WEB BASADOS EN WINDOWS

a) **[A.3.SEC-MSEWW1] Configurar permisos de ubicaciones de logs**. Se deberá configurar el registro de logs, así como las opciones de auditoría que permitan; la obtención de un registro cronológico de la totalidad de actividades e incidentes que ocurren en el sistema, así como la correcta identificación del usuario que ha ejecutado cada una de las acciones registradas, pudiendo determinar las responsabilidades ante los incidentes provocados como consecuencia de las mismas.

b) **[A.3.SEC-MSEWW2] Configurar opciones de registro**. Los archivos de registro de *IIS* permitirán simplificar la depuración, resolución de problemas y optimización del sitio web, por lo que se recomienda realizar la configuración correspondiente del registro.

c) **[A.3.SEC-MSEWW3] Habilitar registro de eventos IIS**. *IIS* utiliza una arquitectura de registro flexible y eficiente, de tal modo que cuando ocurre un evento registrable, *IIS* llama al módulo de registro seleccionado que grabará el evento en uno de los registros almacenados en la siguiente ruta: *%SystemRoot%\system32\Logfiles\<service_name>*.

d) **[A.4.SEC-MSEWW1] Cambiar rutas por defecto instalación IIS**. Para un mayor aislamiento del sistema, deberá separar la ruta donde se encuentran los ficheros de configuración de *IIS* en un disco diferente del que contiene el sistema operativo, esto permitirá evitar posibles saltos hacia otras rutas y segmentar su sistema.

e) **[A.5.SEC-MSEWW1] Configurar métodos de autenticación y deshabilitar autenticación anónima**. Los métodos de autenticación permitirán limitar el acceso a una lista determinada de usuarios.

   De manera predeterminada los servicios web de *IIS* utilizaran la autenticación anónima, la cual proporciona a los usuarios acceso a las áreas públicas del sitio web sin solicitarles un nombre de usuario ni una contraseña, lo cual se considera una importante brecha de seguridad en el sistema, por lo que se debe deshabilitar dicho tipo de autenticación para cualquier sitio web.

   Existen distintos métodos de autenticación sin tener en cuenta la autenticación anónima mencionada anteriormente que permitirán asegurar los servidores *IIS*, por lo que se deberá planear el método más adecuado para cada caso en particular.

f) **[A.5.SEC-MSEWW2] Modificar usuario y grupos del servicio de las aplicaciones**. Las identidades de los grupos de aplicaciones (*Application pool identities*) son el nombre de las cuentas de servicio con las que se ejecuta el proceso de trabajo de dicho grupo. De manera predeterminada, los grupos de aplicaciones funcionan con ella y es el medio más seguro ya que proporciona un alto nivel de aislamiento.

   Dichas identidades de grupo de aplicaciones no requieren de gestión alguna y no tienen contraseña, lo que facilita su administración y evita problemas de seguridad por falta de mantenimiento.

g) **[A.6.SEC-MSEWW1] Restricción de direcciones IP y dominios**. La restricción de direcciones *IP* y dominios ofrece la opción de permitir o denegar a usuarios, grupos, redes, etc. el acceso al sitio. Se pueden crear tantas entradas como se considere necesario, las cuales se podrán ordenar para obtener el efecto buscado, ya que un acceso será restringido o permitido según la primera línea que le afecte, por lo que el orden de prioridad es importante para un correcto funcionamiento.

   Dichas restricciones de direcciones *IP* y dominios se obtendrán con un módulo instalable individual para el cual, mientras no se cree ninguna entrada, el servidor permitirá todos los accesos.

h) **[A.6.SEC-MSEWW2] Restringir el acceso a ficheros y directorios fuera del árbol web**. Es recomendable denegar el acceso a ciertas carpetas o archivos a los que se puede acceder a través del servidor.

   Esta denegación se podrá realizar de manera grafica desde el administrador de *IIS*, en la sección '*Filtrado de solicitudes*' de la pestaña '*Segmentos ocultos*'. Se podrá realizar, igualmente, modificando directamente el archivo *web.config* donde se indicarán los ficheros y archivos a bloquear mediante la etiqueta <*hiddenSegments*>

i) **[A.7.SEC-MSEWW1] Restringir protocolos y algoritmos**. Deberá minimizarse el número de protocolos y algoritmos soportados en el sistema, deshabilitando aquellos obsoletos o vulnerables tales como *SSLv2*, *SSLv3*, *TLS1.0* y *TLS1.1*. Deberá tener constancia de los protocolos soportados por su sistema y únicamente admitir aquellos estrictamente necesarios para el funcionamiento del sitio web.

j) **[A.7.SEC-MSEWW2] Configurar HSTS**. *HSTS* permitirá a un sitio web declararse como un host seguro e informar a los exploradores de que solo deben ponerse en contacto con él a través de conexiones *HTTPS*.

   Se trata de una mejora de seguridad recomendable que aplicará *HTTPS* y reducirá de manera significativa la capacidad de ataques del tipo "*man in the middle*" para interceptar solicitudes y respuestas entre servidores y clientes.

k) **[A.7.SEC-MSEWW3] Deshabilitar aplicaciones externas y SMTP**. Es importante que no tener configurado un *relay SMTP* en el servidor web, de lo contrario, cualquier atacante podría realizar envíos de correo electrónico a la organización sin control. Adicionalmente, se deberá revisar que no existan aplicaciones web ejecutándose en el sistema con otros fines. Esta configuración reducirá la superficie de exposición y evitará que, ante errores en el código de otras aplicaciones, el sistema pueda quedar vulnerable.

l) **[A.11.SEC-MSEWW1] Configurar limites en el sistema para impedir ataques**. Se recomienda configurar la cantidad de ancho de banda, la cantidad de conexiones concurrentes y el tiempo de espera de conexión para las solicitudes de los clientes del servidor web. Con la aplicación de estas limitaciones se podrá evitar que los posibles atacantes sobrecarguen el sistema pudiendo llegar a provocar una caída del mismo.

   Estos límites se podrán configurar con la etiqueta <*limits*> dentro de <*siteDefaults*>.

m) **[A.15.SEC-MSEWW1] Configurar filtrado de solicitudes**. Los filtros de solicitudes permitirán controlar las conexiones entre el servidor y el cliente, restringiendo el comportamiento de protocolos y contenidos.

Se considerará una buena práctica de seguridad realizar una configuración básica para el servidor en función de los usos que se prevén y luego ajustarla posteriormente en cada uno de los sitios generados según los requisitos necesarios.

El filtrado de solicitudes permitirá crear reglas sobre extensiones de nombre de archivo, reglas, segmentos ocultos, dirección *URL*, verbos *HTTP*, encabezados y cadenas de consulta.

n) **[A.15.SEC-MSEWW2] Configurar módulos SSL/TLS**. El protocolo *SSL* facilitará a la red una comunicación segura para identificar y autenticar el servidor, además de garantizar la protección de la privacidad y la integridad de los datos transmitidos, por tanto, se debe configurar el módulo *SSL* para proporcionar la seguridad mencionada anteriormente.

Para habilitar la verificación de certificados de servidor *SSL* y proporcionar el nivel de seguridad deseado, se debe obtener un certificado de una entidad de certificación de terceros. Dicho certificado estará asociado al servidor web y más específicamente al sitio web al que se va a enlazar *SSL*.

o) **[A.19.SEC-MSEWW1] Cambiar páginas de error**. La emisión de páginas de error detalladas puede ayudar a los administradores a la hora de resolver incidencias, pero también ofrece información a posibles atacantes, por lo que se deberán tomar medidas para que dichos avisos proporcionen la mínima cantidad de información necesaria.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL