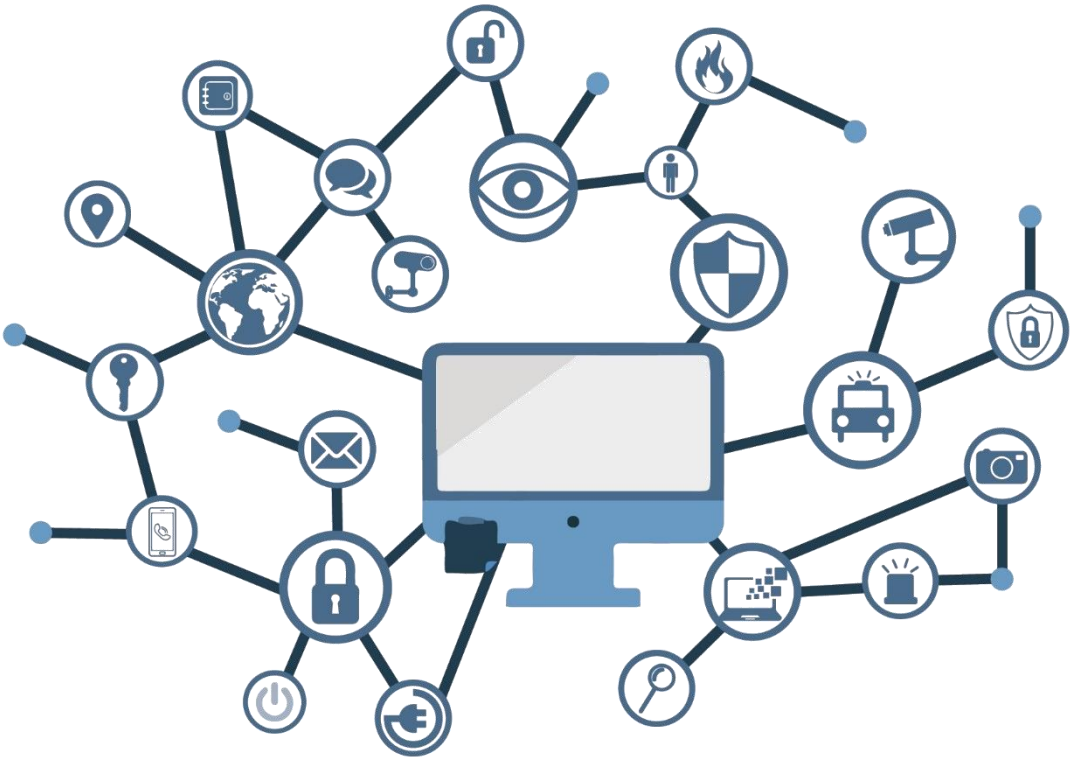
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC-462A22

GUÍA DE APLICACIÓN DE PERFILADO DE SEGURIDAD JOOMLA! 4



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 12:08:45 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-035-X
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

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos Linux (incluidos en la serie CCN-STIC-400), siendo de aplicación en el cumplimiento del Esquema Nacional de Seguridad (ENS) y para los sistemas que manejen información clasificada.

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 Joomla! 4 como gestor de contenidos.

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 estado del arte tecnológico en ciberseguridad.

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 una revisión exhaustiva de las distintas configuraciones de seguridad disponibles en Joomla! 4, 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 aplicar un perfilado de seguridad de un equipo que cuente con Joomla! 4 como gestor de contenidos.

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 Joomla! 4.

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.

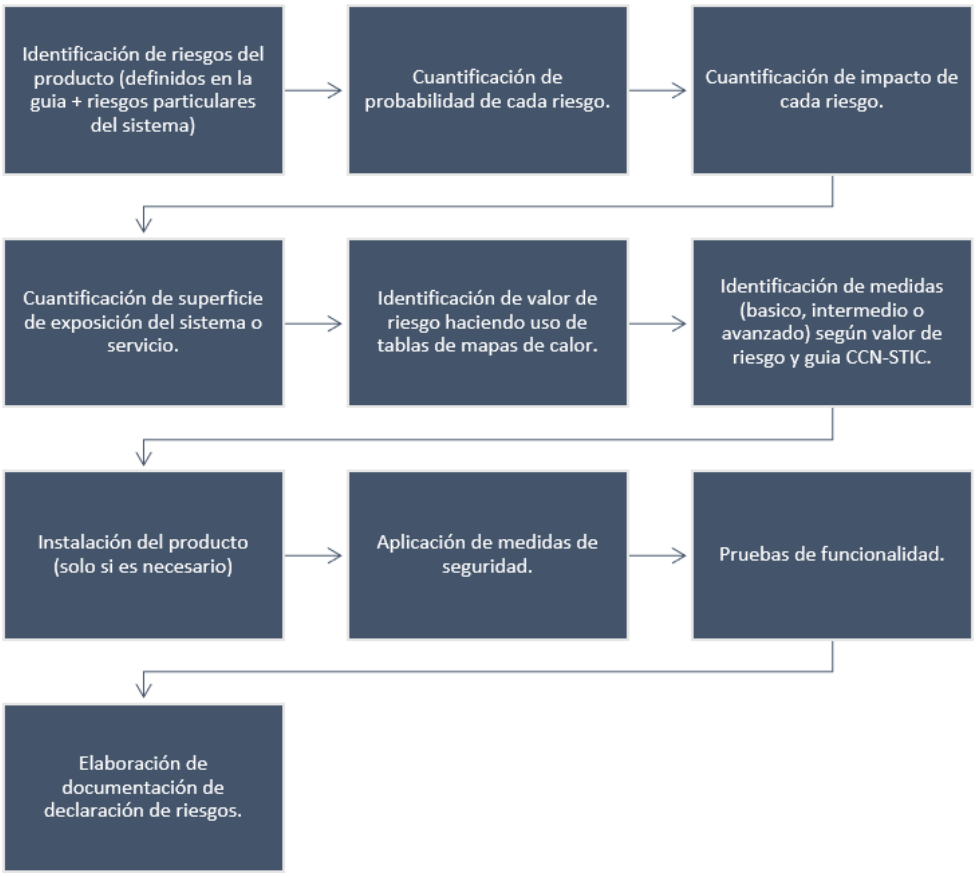
   Cada organización deberá determinar cómo configurar el sistema para el cumplimiento de la medida correspondiente. De esta forma, se ofrece un mayor grado de flexibilidad a la hora de proteger el sistema, necesario sobre todo en sistemas que ya están en funcionamiento o en producción. Es decir, en esta 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 riesgos y las medidas de mitigación de éstos, se procederá con la instalación del sistema operativo, así como los productos necesarios para dar soporte a Joomla! 4 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 sistema basado en Linux con Joomla! 4 instalado.

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 JOOMLA! 4

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.5] Suplantación de la identidad.			
3.	[A.6] Abuso de privilegios de acceso.			
4.	[A.11] Acceso no autorizado.			
5.	[A.13] Repudio (Negación de actuaciones).			
6.	[A.15] Modificación de la información.			
7.	[A.19] Revelación de información.			
8.	[A.24] Denegación de servicio.			
9.	[A.25] Robo de equipos.			
10.	[E.24] Caída del sistema por agotamiento de recursos			
11.	[E.25] Pérdida de equipos.			

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 Joomla! 4, 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 mitigan, controlan o reducen dicho riesgo.

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-JO1: corresponde con la categoría de seguridad 1 para dicho riesgo. 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.

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA JOOMLA! 4	ALCANCE		
		B	I	A
[A.3] Manipulación de los registros de actividad (log).	[A.3.SEC-JO1] Se auditan los inicios de sesión fallidos.			
	[A.3.SEC-JO2] Se auditan las modificaciones sobre los elementos del sitio.			
	[A.3.SEC-JO3] El producto se encuentra siempre actualizado, así como los complementos que se instalen en él			
[A.5] Suplantación de la identidad.	[A.5.SEC-JO1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC-JO2] Se dispone de una política de credenciales robusta.			
	[A.5.SEC-JO3] Se utilizan métodos de doble factor de autenticación.			
	[A.5.SEC-JO4] Se establece un tiempo máximo de sesión inactiva.			
	[A.5.SEC-JO5] Se crean usuarios nominales siendo estos fácilmente distinguibles.			
	[A.5.SEC-JO6] Para los usuarios administradores no se emplearán nomenclaturas comunes como “admin” o “administrador”			
[A.6] Abuso de privilegios de acceso.	[A.6.SEC-JO1] Se delimitan de forma clara los permisos y roles de los usuarios.			
	[A.6.SEC-JO2] Se eliminan los usuarios innecesarios que existan en el producto.			
[A.11] Acceso no autorizado	[A.5.SEC-JO1] Se controlan los permisos de inicio de sesión y suplantación de identidad.			
	[A.5.SEC-JO2] Se dispone de una política de credenciales robusta.			
	[A.5.SEC-JO4] Se establece un tiempo máximo de sesión inactiva.			
	[A.6.SEC-JO1] Se delimitan de forma clara los permisos y roles de usuario.			
	[A.6.SEC-JO2] Se eliminan los usuarios innecesarios que existan en el producto			
	[A.11.SEC-JO1] Se deshabilita el registro automático de los usuarios.			
[A.13] Repudio (Negación de actuaciones)	[A.6.SEC-JO1] Se delimitan de forma clara los permisos y roles de usuario.			
	[A.13.SEC-JO1] Se restringe el acceso físico al servidor salvo personal autorizado a ello.			
[A.15] Modificación de la información.	[A.6.SEC-JO1] Se delimitan de forma clara los permisos y roles de usuario.			
	[A.15.SEC-JO1] Se refuerza la seguridad del protocolo SSH.			
	[A.15.SEC-JO2] Se protegen los ficheros de configuración ante modificaciones.			

RIESGO	CATEGORÍAS DE PERFILADO DE SEGURIDAD PARA JOOMLA! 4	ALCANCE		
		B	I	A
	[A.15.SEC-JO3] Se protege el acceso del panel web de administración añadiendo ACL por IP.			
	[A.15.SEC-JO4] Se realizan copias de seguridad con frecuencia.			
[A.19] Revelación de información.	[A.5.SEC-JO2] Se dispone de una política de credenciales robusta.			
	[A.5.SEC-JO4] Se establece un tiempo máximo de sesión inactiva.			
	[A.6.SEC-JO1] Se delimitan de forma clara los permisos y roles de usuarios.			
	[A.19.SEC-JO1] Durante el inicio de sesión, el producto muestra un texto en cumplimiento con las normas o directivas de la organización.			
	[A.19.SEC-JO2] Se deshabilita la depuración del sistema.			
[A.24] Denegación de servicio	[A.24.SEC-JO1] Se implementan mecanismos anti DoS en el sistema.			
	[A.24.SEC-JO2] Se limita la instalación de extensiones y funcionalidades a los usuarios con rol de administrador			
[A.25] Robo de equipos.	[A.5.SEC-JO4] Se establece un tiempo máximo de sesión inactiva.			
	[A.15.SEC-JO4] Se realizan copias de seguridad con frecuencia.			
[E.24] Caída del sistema por agotamiento de recursos	[A.24.SEC-JO1] Se implementan mecanismos anti DoS en el sistema.			
	[A.24.SEC-JO2] Se limita la instalación de extensiones y funcionalidades a los usuarios con rol de administrador			
[E.25] Pérdida de equipos.	[A.5.SEC-JO4] Se establece un tiempo máximo de sesión inactiva.			
	[A.15.SEC-JO4] Se realizan copias de seguridad con frecuencia.			

ANEXO A. PASO A PASO. CONFIGURACIÓN BASE DE SEGURIDAD SOBRE JOOMLA! 4

En el presente anexo, se incluye una línea base de seguridad para el aseguramiento de los sistemas que cuenten con un Sistema Gestor de Contenidos (En inglés CMS, Content Management System) Joomla! 4, según los aspectos definidos en cada uno de los puntos anteriores de este documento.

Esta configuración se ofrece a modo de referencia o ejemplo de aplicabilidad de medidas en función de unos resultados concretos del análisis de riesgos ejecutado. Es posible que en otros escenarios y con otra superficie de exposición, el perfilado de aplicación de medidas sea diferente.

Es necesario remarcar que la línea base de seguridad establecida dentro del presente anexo corresponde con un **perfilado intermedio**.

Nota: En caso de que el perfilado de seguridad y superficie de exposición obtenidos, en base al análisis realizado, requieran de una **configuración de seguridad avanzada, será necesario implementar medidas adicionales de seguridad**. Por el contrario, en caso de que el resultado de dicho análisis indique que la necesidad de configuración solo deba establecerse según el perfilado básico, será posible evitar ciertas medidas de seguridad de las establecidas en el presente anexo.

Por otro lado, es necesario indicar que las categorías de seguridad presentadas en esta guía no pueden ser aplicadas por medio de configuraciones exactas (mediante scripts), por ello se ha desarrollado un único apartado específico que permita establecer ejemplos de configuración sobre las diferentes categorías, las cuales deberán ser adaptadas por cada organización en caso necesario.

Nota: Las configuraciones, directorios, ficheros y rutas que aparecen en los diferentes apartados, variarán dependiendo del servidor web instalado, así como de las configuraciones de la organización. La configuración presentada en este documento ha sido realizada sobre un servidor web Apache 2.4.

Debe tenerse en consideración que antes de realizar la puesta en producción de los procedimientos descritos en la presente guía, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

A modo de ejemplo, se procede a realizar un perfilado intermedio de seguridad, aplicado al gestor de contenido Joomla! 4.

ANEXO A.1. CERTIFICADOS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.15.SEC-JO1]** Se refuerza la seguridad del protocolo SSH.

Es necesario añadir certificados en el servidor web para cifrar las conexiones que se establecen contra el servidor y evitar así fugas de información en la red.

Para realizar los siguientes pasos, es necesario contar con un certificado junto a la clave privada, previo a la instalación de este.

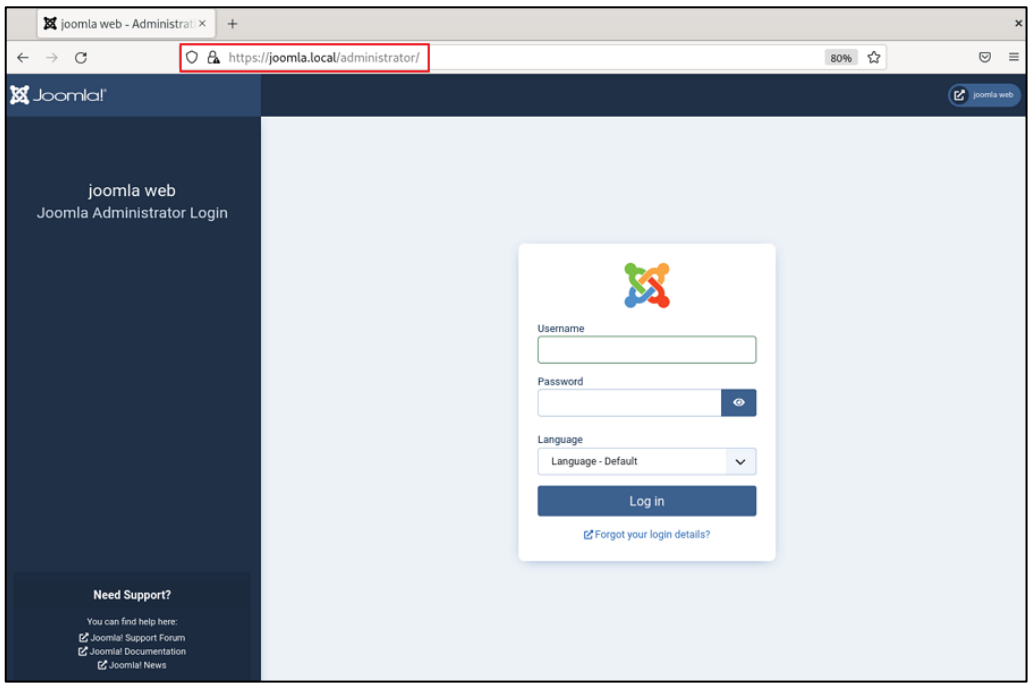
Paso	Descripción
1.	Se debe iniciar sesión en el equipo que cuenta con Joomla! 4 utilizando una cuenta con permisos de administrador.

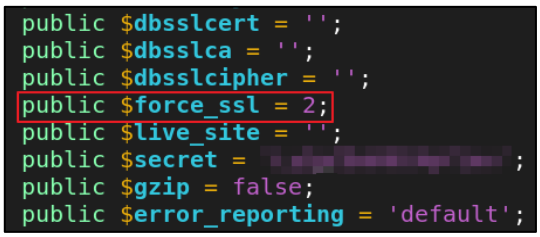
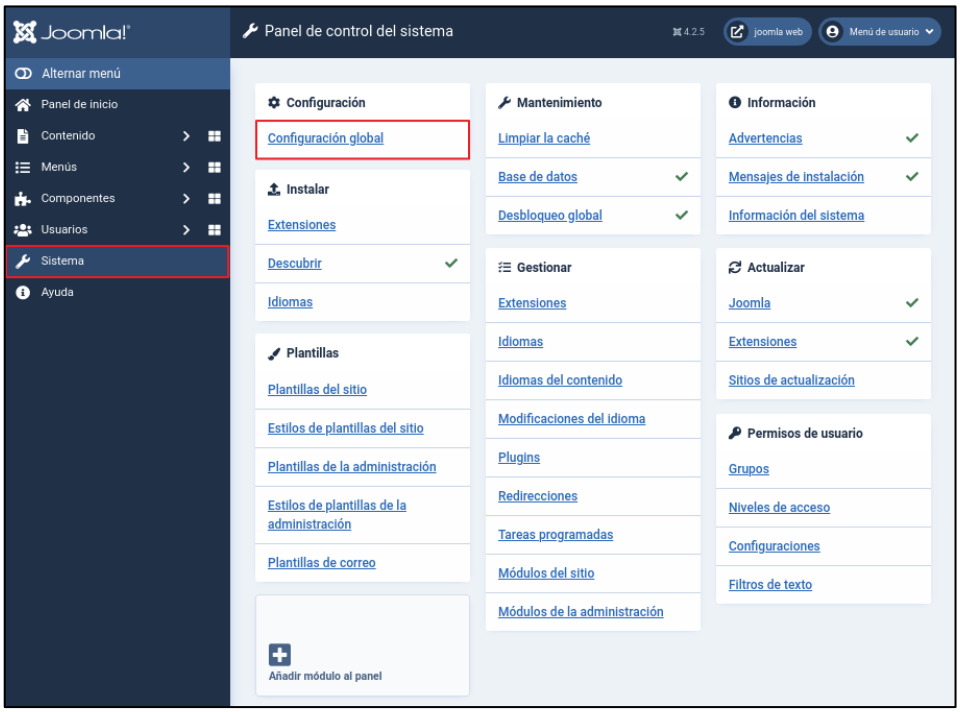
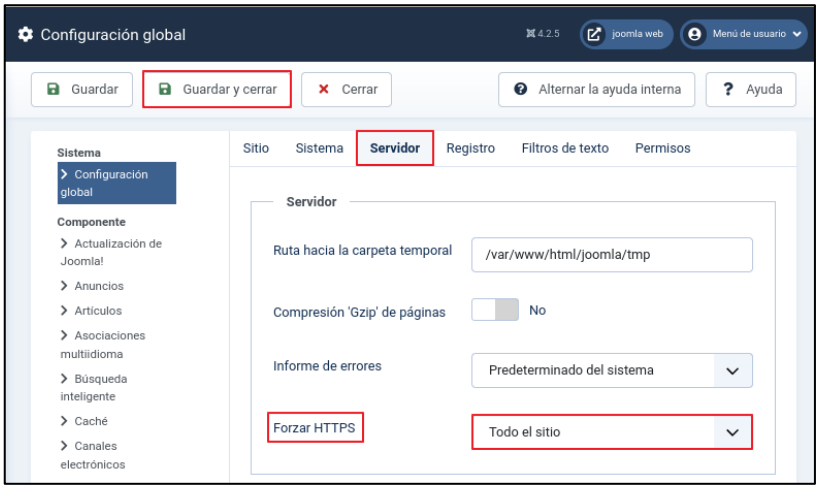
2.	Utilizando un terminal en el equipo, se descarga el módulo **mod_ssl** si no se encontraba previamente habilitado.
	$ sudo yum install mod_ssl
	`[aCdCmN462@joomla conf.d]$ sudo yum install mod_ssl`
	`Última comprobación de caducidad de metadatos hecha hace 0:16:30`
	`Dependencias resueltas.`
	`=========================================================================`
	` Paquete Arquitectura Versión`
	`=========================================================================`
	`Instalando:`
	` mod_ssl x86_64 1:2.4.53-7.0.1.el9`
	`Actualizando:`
	` httpd x86_64 2.4.53-7.0.1.el9`
	` httpd-filesystem noarch 2.4.53-7.0.1.el9`
	` httpd-tools x86_64 2.4.53-7.0.1.el9`
	`Instalando dependencias:`
	` httpd-core x86_64 2.4.53-7.0.1.el9`

3.	Editando el fichero de configuración del módulo ssl, se añadirá la ruta donde se encuentren el certificado y la clave que van a ser utilizados para el servidor. Para esta ocasión se han agregado los certificados en **/etc/httpd/conf.d/ssl.conf**.
	`#  Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)`
	`#  require an ECC certificate which can also be configured in`
	`#  parallel.`
	`SSLCertificateFile /home/aCdCmN462/certificates/joomla.crt`
	
	`#  Server Private Key:`
	`#  If the key is not combined with the certificate, use this`
	`#  directive to point at the key file.  Keep in mind that if`
	`#  you've both a RSA and a DSA private key you can configure`
	`#  both in parallel (to also allow the use of DSA ciphers, etc.)`
	`#  ECC keys, when in use, can also be configured in parallel`
	`SSLCertificateKeyFile /home/aCdCmN462/certificates/joomla.key`

Paso	Descripción

4.	En el fichero de configuración del servidor web, se añadirá el campo correspondiente a los certificados y la ruta hacia los mismos.
	
	`<VirtualHost *:443>`
	`SSLEngine on`
	`SSLCertificateFile /home/aCdCmN462/certificates/joomla.crt`
	`SSLCertificateKeyFile /home/aCdCmN462/certificates/joomla.key`
	`ServerAdmin admin@linuxshelltips.network`
	`DocumentRoot /var/www/html/joomla/`
	`ServerName linuxshelltips.network`
	`ServerAlias www.linuxshelltips.network`
	`ErrorLog /var/log/error.log`
	`CustomLog /var/log/access.log combined`
	`<Directory /var/www/html/joomla/>`
	`Options FollowSymLinks`
	`AllowOverride All`
	`Require all granted`
	`</Directory>`
	`</VirtualHost>`

5.	Debe habilitarse la lectura de los certificados en Selinux con el siguiente comando. **$ sudo setsebool -P httpd_read_user_content 1**
6.	Posteriormente se reiniciará el servidor web. **$ sudo systemctl restart httpd**
7.	Una vez reiniciado el servicio, se accederá la URL del sitio, seguido de **/administrator** para acceder al panel web de administración de Joomla! 4. De manera adicional se verificará que se ha habilitado el servicio con las comunicaciones cifradas. Tras ello, se inicia sesión con un usuario con el rol superadministrador. 

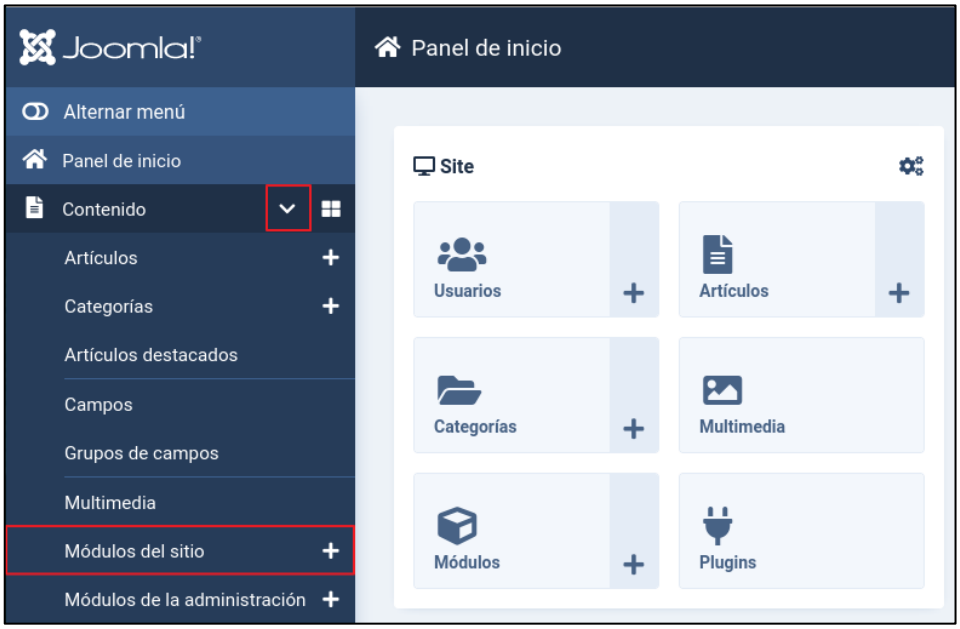
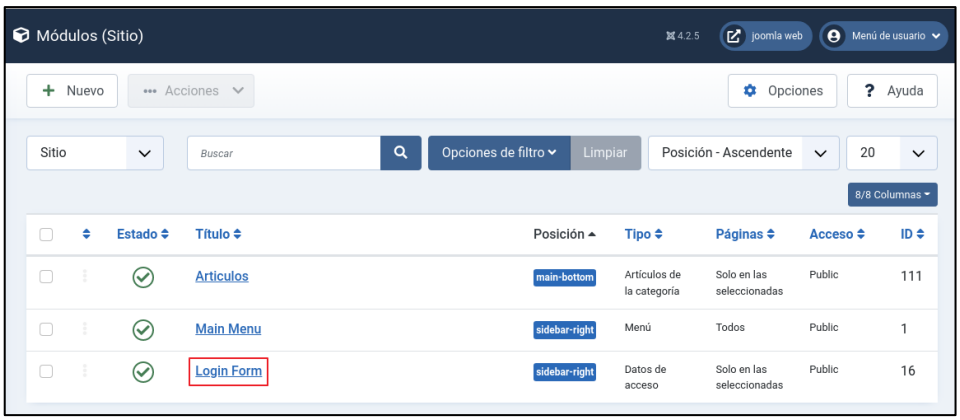
Paso	Descripción
8.	Se deberá editar el fichero **configuration.php** que se encuentra por defecto dentro del directorio donde se han descomprimido los ficheros de Joomla!, a continuación, se modificará la línea con el parámetro **public $force_ssl** y se configura su valor en 2. 
9.	Se accederá al panel web de administración y en el menú de administración a la opción **Sistema**, tras ello, se accederá a **Configuración global**. 
10.	En la parte central de la pantalla, pulsando sobre la pestaña **Servidor** se habilita la opción **Forzar HTTPS**. 

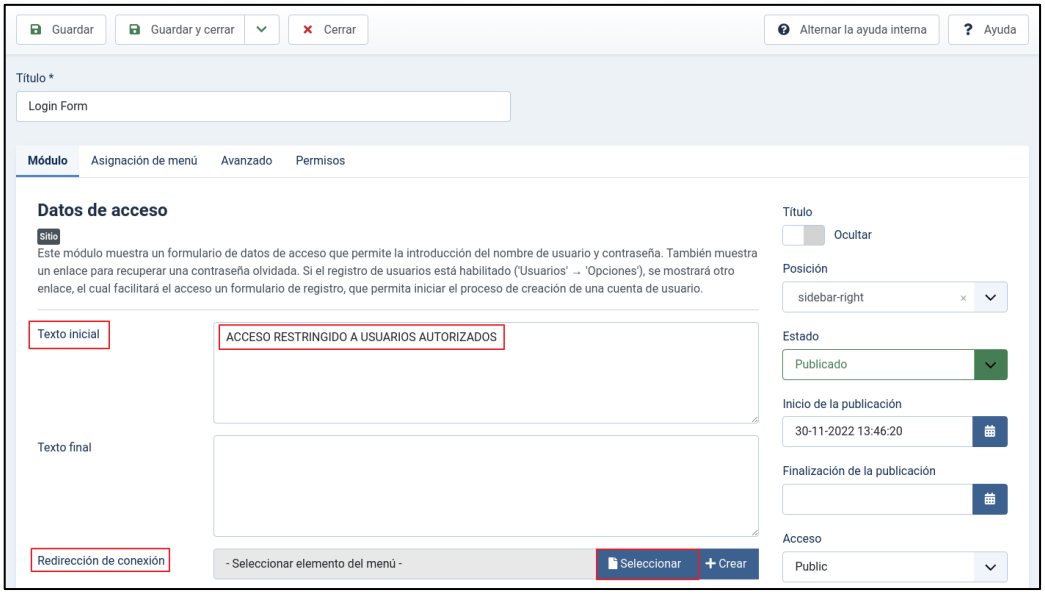
ANEXO A.2. MENSAJE DISUASORIO

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.19.SEC-JO1]** Durante el inicio de sesión, el producto muestra un texto en cumplimiento con las normas o directivas de la organización.

Se configura un mensaje disuasorio ante posibles intrusiones indicando el incumplimiento de la legislación vigente en materia de protección de datos ante accesos no autorizados, así como la configuración requerida por las directivas de la organización.

Paso	Descripción
11.	Abriendo un navegador se accede al panel web de administración, iniciando sesión con un usuario con permisos de superadministrador sobre el sitio.
12.	En el menú de administración, expandiendo el desplegable de la sección **Contenido** mostrará el apartado **Módulos del sitio** en el que se deberá situar. 
13.	A continuación, en el panel central, se procederá a configurar el apartado **Login Form**. 

Paso	Descripción
14.	En el campo **Texto inicial** se deberá configurar el banner deseado para el sitio. Posteriormente, se puede establecer una redirección a la página que se desee tras la autenticación de los usuarios. 
15.	Se accederá ahora como cliente insertando en la URL el nombre de su dominio e ingresará al sitio web y observando la nueva configuración. 

ANEXO A.3. USUARIOS

ANEXO A.3.1. USUARIOS NOMINALES

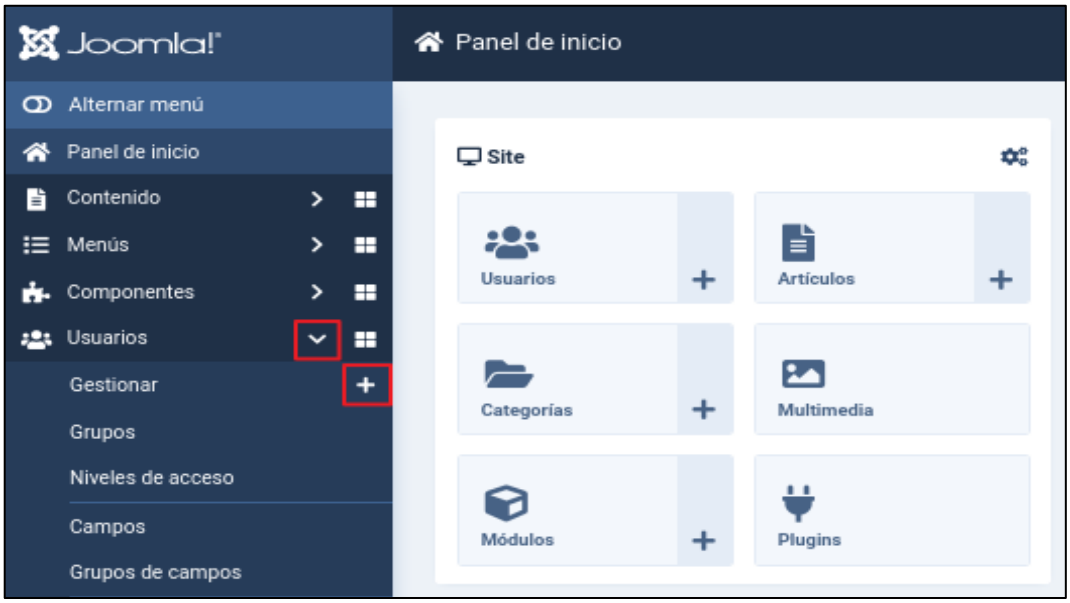
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

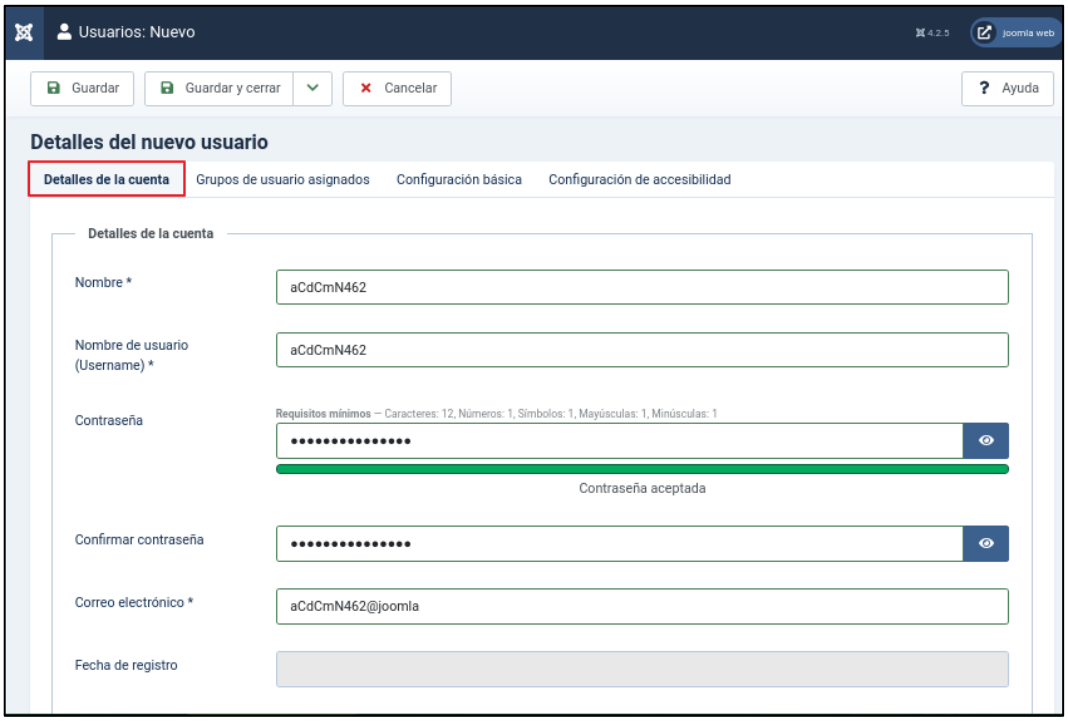
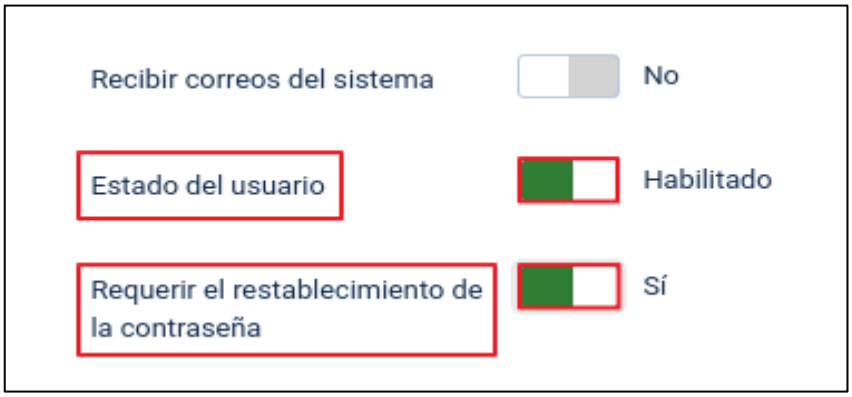
a) **[A.5.SEC-JO1]** Se controlan los permisos de inicio de sesión y la suplantación de identidad.

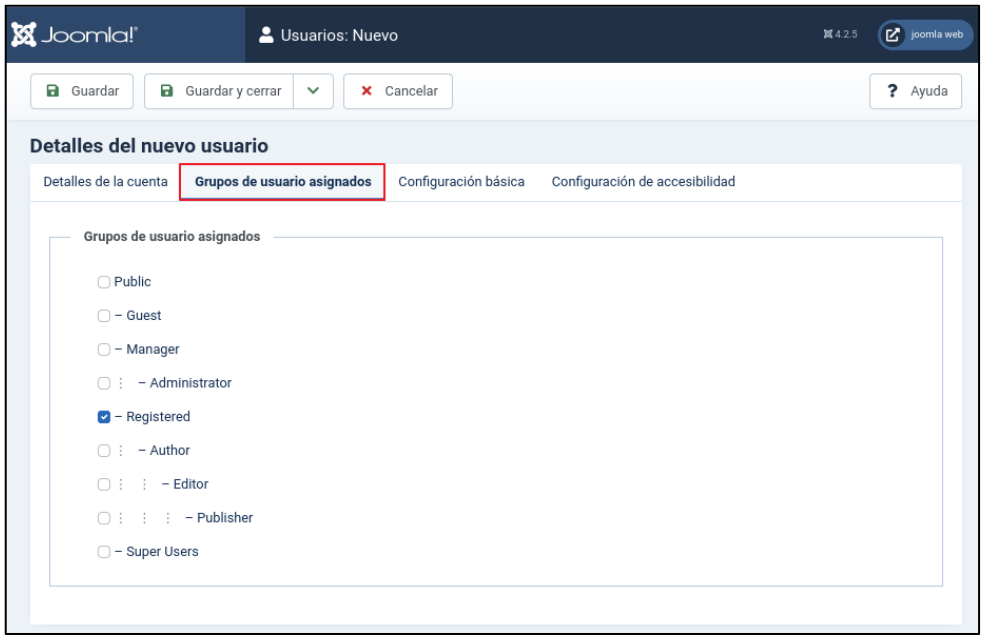
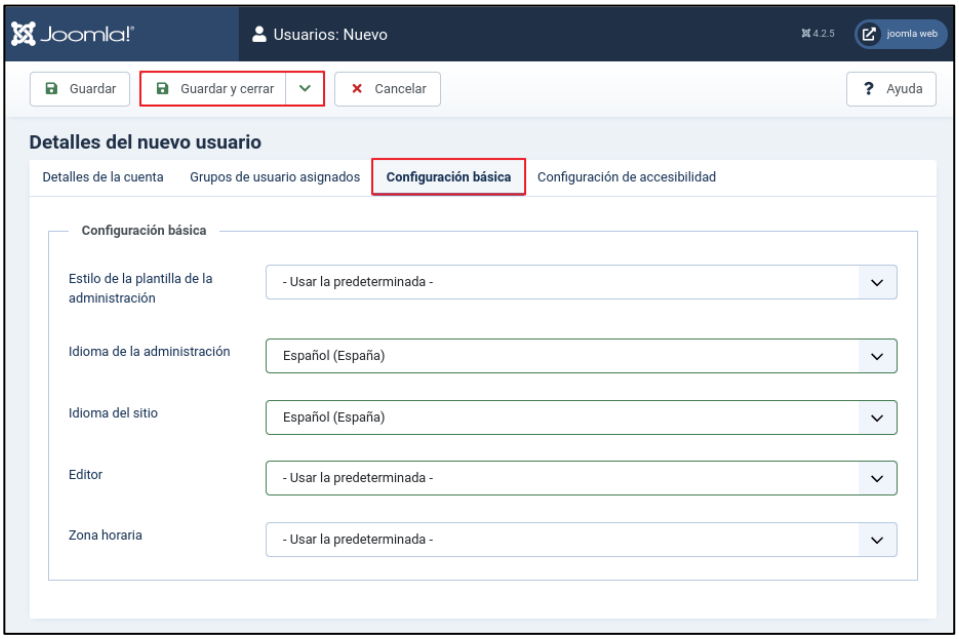
b) **[A.5.SEC-JO5]** Se crean usuarios nominales siendo estos fácilmente distinguibles.

c) **[A.5.SEC-JO6]** Para los usuarios administradores no se emplearán nomenclaturas comunes como "admin" o "administrador".

En el proceso de creación de usuarios se asignarán nombres descriptivos y únicos en el sistema, facilitando así la trazabilidad en caso de incidencias.

Paso	Descripción
16.	Accediendo al panel web de administración se iniciará sesión con un usuario con permisos de superadministrador sobre el sitio.
17.	En el proceso de creación de usuarios, se establecen nombres de usuario característicos y distintivos para cada uno de ellos. En el menú de administración, se accederá al desplegable **Usuarios**. Tras ello, pulsando sobre el símbolo **+** se podrá añadir un nuevo usuario. 

Paso	Descripción
18.	Se deben rellenar los campos relativos al nuevo usuario dentro de la pestaña **Detalles de la cuenta** utilizando para ello nombres descriptivos para cada usuario. 
19.	Se deben habilitar las opciones **Estado del usuario** y **Requerir el restablecimiento de la contraseña** ubicadas al final del formulario. 

Paso	Descripción
20.	Posteriormente se accederá a la pestaña **Grupos de usuario asignados** y se asignará el rol que va a desempeñar el nuevo usuario. 
21.	Por último, en la pestaña **Configuración básica** se pueden establecer opciones como el idioma predeterminado para el usuario o la zona horaria. Cuando se termine la configuración se guardarán los cambios como se muestra a continuación. 

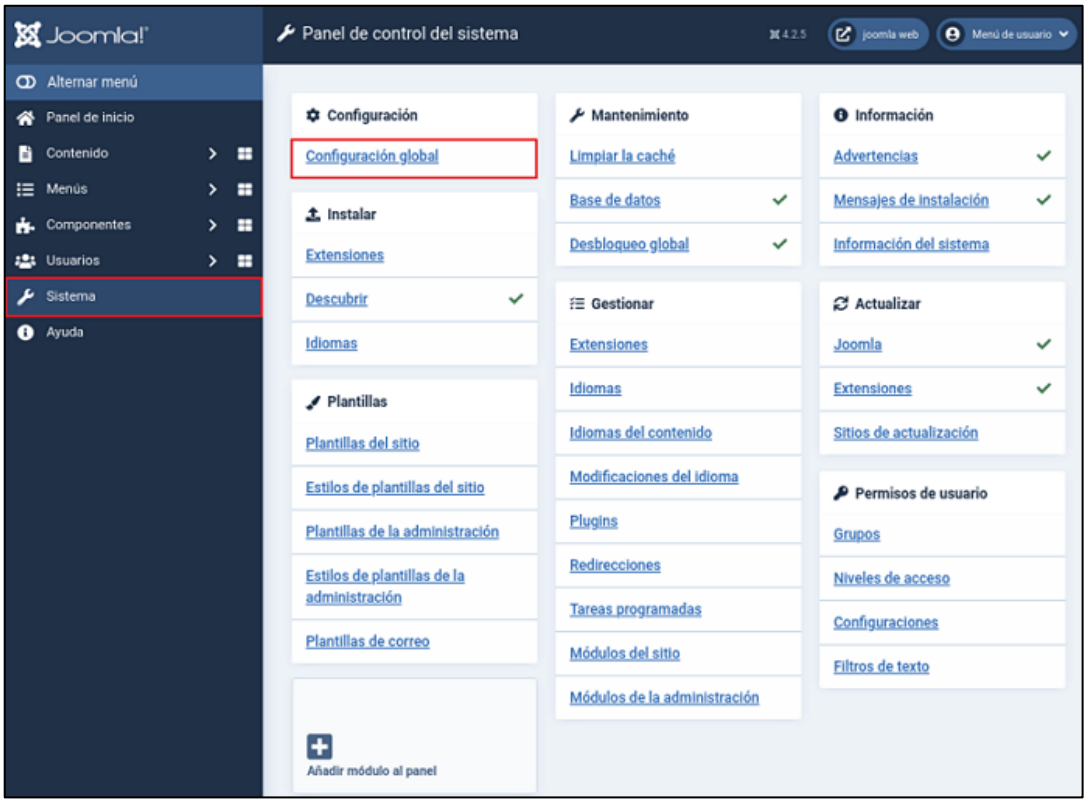
Nota: Los grupos de usuario establecen los permisos que se definirán para el usuario asignado a dicho grupo.

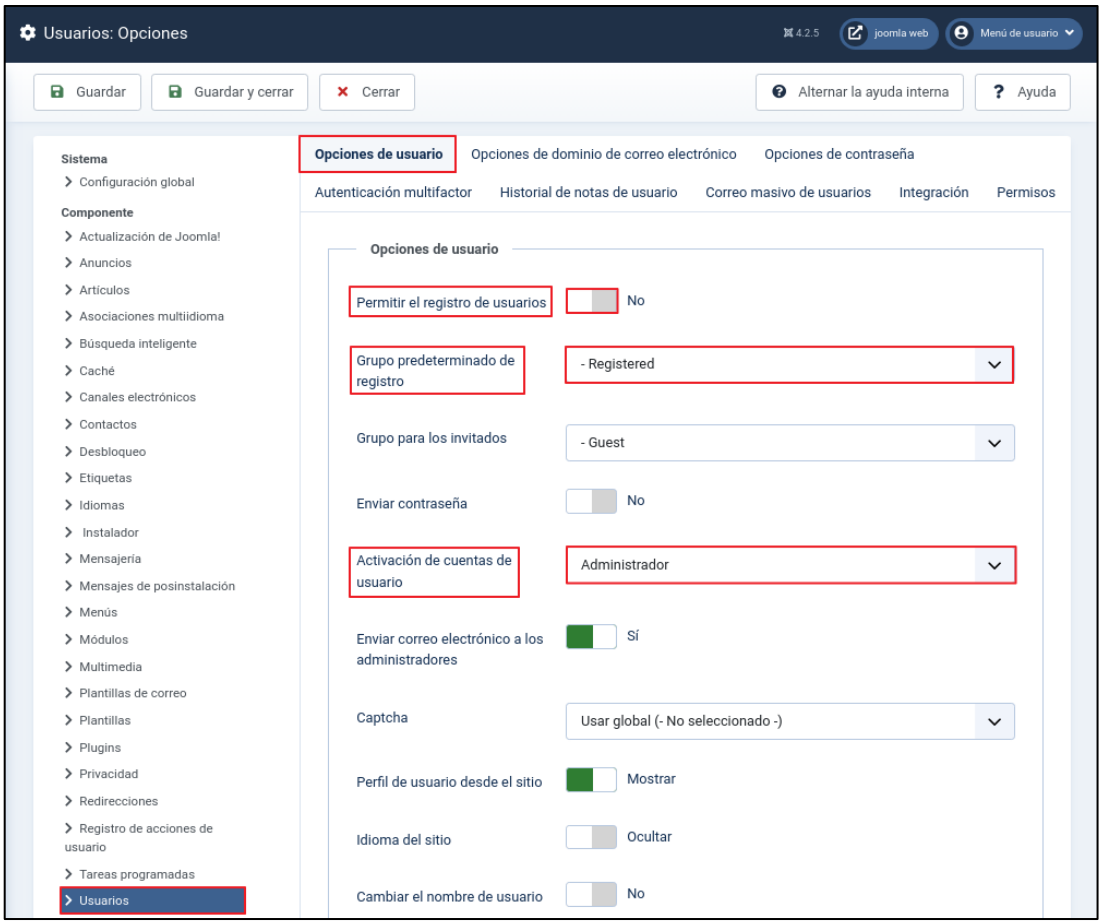
ANEXO A.3.2. DESHABILITAR REGISTRO DE USUARIOS AUTOMÁTICO

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.11.SEC-JO1]** Se deshabilita el registro automático de los usuarios.

Para establecer un buen control sobre el sitio, se deshabilita el registro automático de usuarios, teniendo que dar de alta a los mismos un usuario superadministrador.

Paso	Descripción
22.	Accediendo al panel web de administración se iniciará sesión con un usuario con permisos de superadministrador sobre el sitio.
23.	Pulsando sobre **Sistema** en el menú de administración, posteriormente se accede a **Configuración global**. 

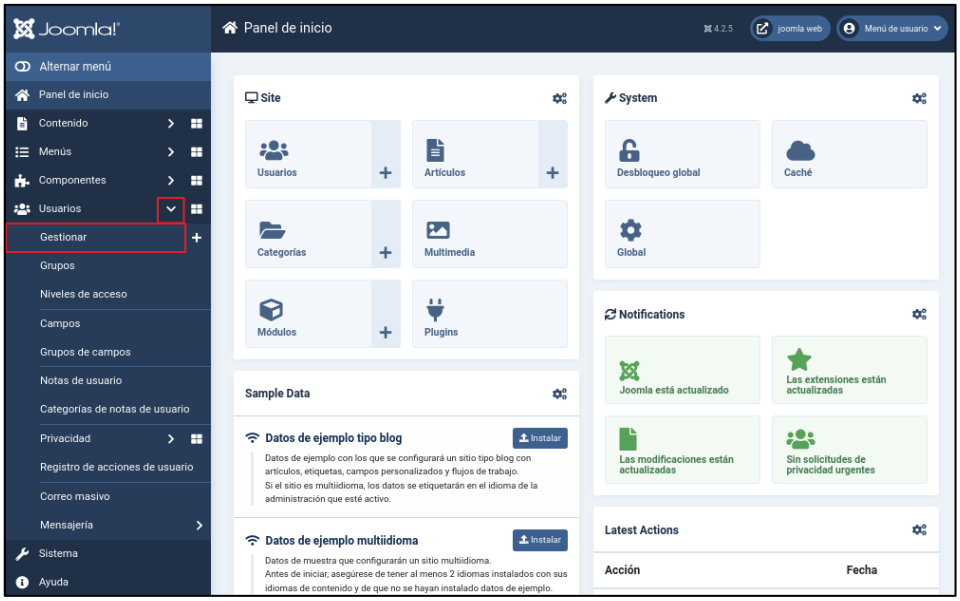
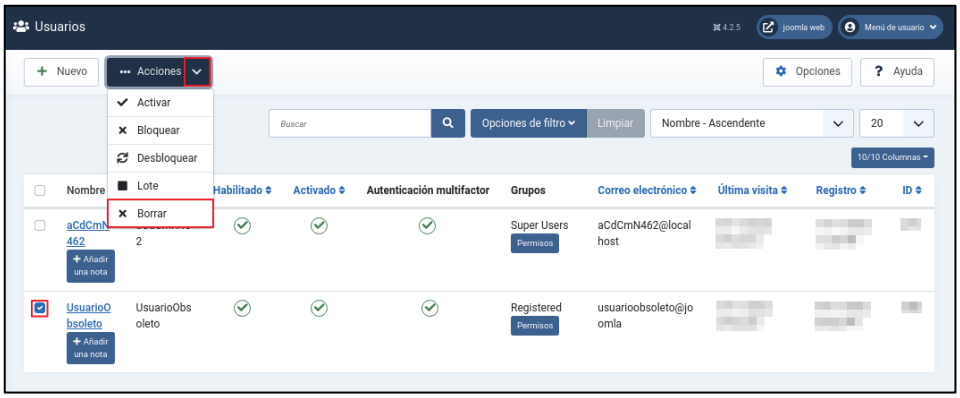
Paso	Descripción
24.	En la columna **Componente** se accederá al panel de **Usuarios** y, posteriormente, a **Opciones de usuario**. En este último desplegable, se deshabilita la opción **Permitir registro de usuarios** y se asigna el grupo por defecto **Registered**, por último, se deberá escoger el **Administrador** en **Activación de las cuentas de usuario** para la habilitación de las mismas. 

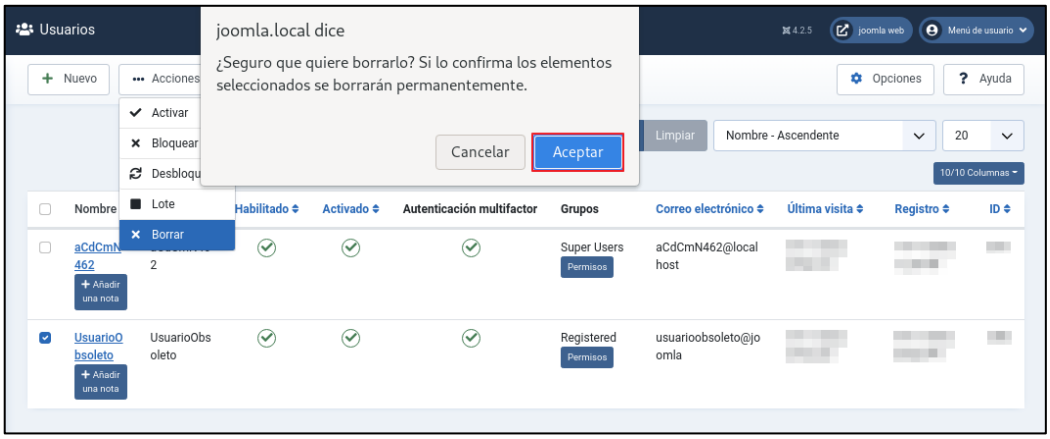
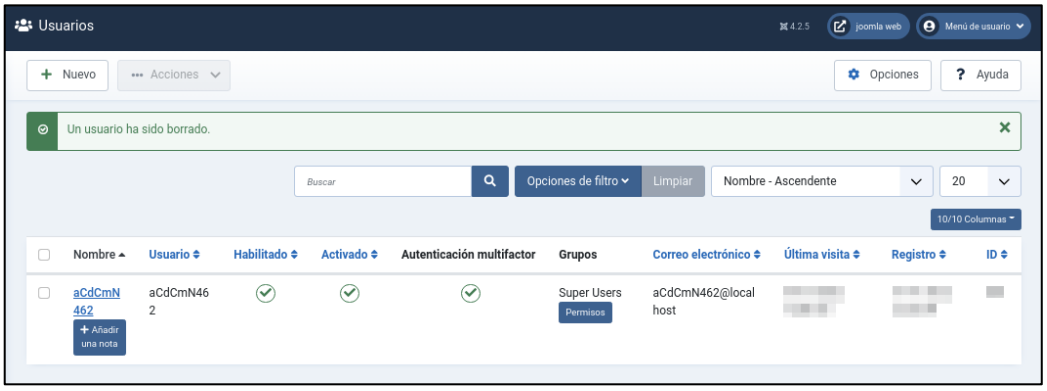
ANEXO A.3.3. BORRADO DE USUARIOS INNECESARIOS U OBSOLETOS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.6.SEC-JO2]** Se eliminan los usuarios innecesarios del producto.

Siguiendo el concepto de mínima exposición y con el propósito de mejorar la seguridad, se eliminarán los usuarios obsoletos que existan en el producto.

Paso	Descripción
25.	Si en algún momento se ha cerrado sesión, se deberá acceder al panel web de administración se inicia sesión con un usuario con permisos de superadministrador sobre el sitio.
26.	En el menú de administración, se seleccionará en el desplegable **Usuarios** haciendo uso de la flecha situada a la derecha. Posteriormente, sobre **Gestionar**. 
27.	A continuación, en el panel central, aparecerán todos los usuarios existentes en el producto. Se deberá marcar sobre la casilla en blanco a la izquierda del nombre de usuario para habilitar el check y posteriormente desplegar el menú de acciones. Por último, se deberá pulsar en **Borrar**. 

Paso	Descripción
28.	Antes de proceder a ejecutar el borrado del usuario se pedirá una confirmación mediante un cuadro de diálogo. 
29.	Finalmente, recibirá la confirmación sobre el usuario eliminado. 

ANEXO A.4. PERMISOS

ANEXO A.4.1. PERMISOS SOBRE EL DIRECTORIO DE INSTALACIÓN

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.15.SEC-JO2]** Se protegen los ficheros de configuración ante modificaciones.

Se protege el directorio de instalación de Joomla! 4 así como los ficheros que se encuentran en su interior con la intención de que no se produzcan modificaciones indeseadas.

Paso	Descripción
30.	Si en algún momento se ha cerrado sesión, se deberá abrir un terminal en el equipo que cuenta con Joomla! 4 utilizando una cuenta con permisos de administrador o "sudoers".
31.	Se accederá a la ruta donde se encuentra el directorio de instalación de Joomla! 4.

32.	Se comprobarán los permisos sobre el directorio de Joomla con el siguiente comando:
	$ ls -l /joomla
	`[aCdCmN462@joomla html]$ ls -l`
	`total 4`
	`drwxr-xr-x. 17 apache apache 4096 [redacted] joomla`

33.	Se utilizará el siguiente comando para limitar el acceso a los usuarios del sistema. **$ sudo chmod 750 /joomla** `[aCdCmN462@joomla html]$ sudo chmod -R 750 joomla/`
34.	Tras cambiar los permisos del directorio, cualquier usuario que no pertenezca al grupo "apache" no tendrá permitido acceder al directorio.
35.	Se deberá agregar el grupo propietario del directorio sobre los usuarios que van a ejercer el rol de administrador de Joomla! 4. **$ sudo usermod -a -G apache aCdCmN462** `[aCdCmN462@joomla html]$ sudo usermod -a -G apache aCdCmN462`

ANEXO A.4.2. PERMISOS DE USUARIO

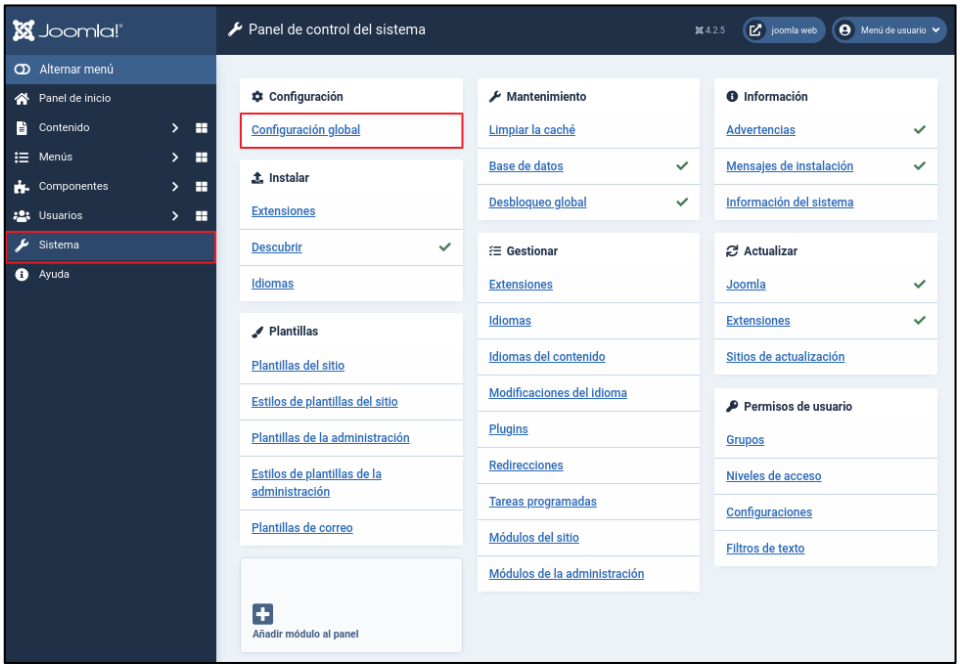
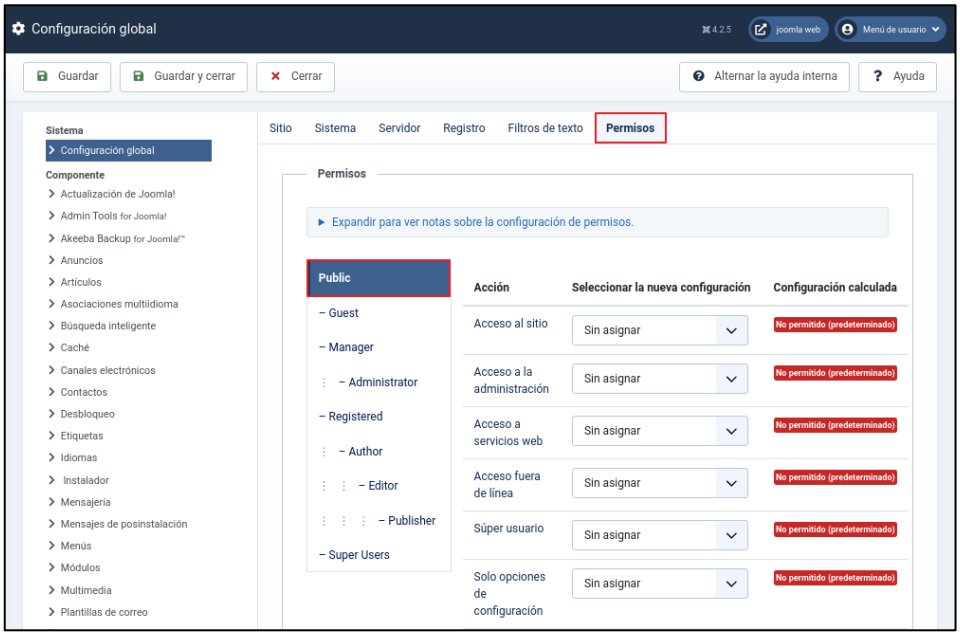
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.5.SEC-JO1]** Se controlan los permisos de inicio de sesión y suplantación de identidad.

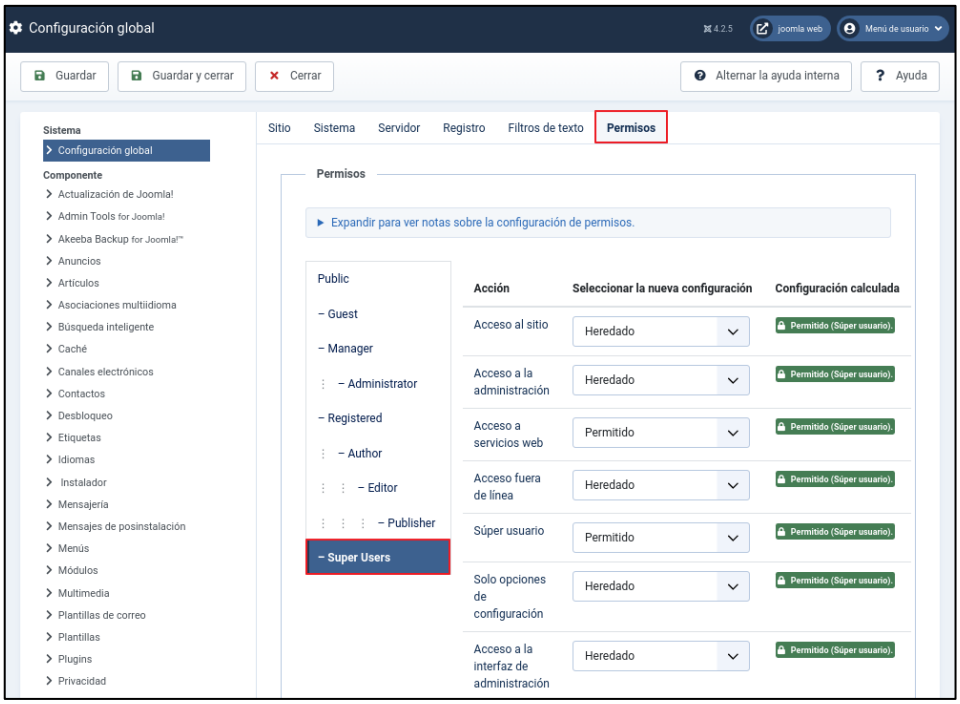
b) **[A.6.SEC-JO1]** Se delimitan de forma clara los permisos y roles de usuarios.

c) **[A.24.SEC-JO2]** Se limita la instalación de extensiones y funcionalidades a los usuarios con rol de administrador.

En el proceso de creación de usuarios, se elegirá el grupo de usuario al que va a pertenecer teniendo en consideración que el usuario heredará los permisos del grupo.

Paso	Descripción
36.	Accediendo al panel web de administración se iniciará sesión con un usuario con permisos de superadministrador sobre el sitio.
37.	Se accederá a **Sistema** en el menú de administración. Posteriormente a **Configuración global**. 
38.	En la sección central, deberá situarse sobre la pestaña **Permisos**. En la columna izquierda podrá observar los roles de usuario existentes, y en la derecha las acciones junto a la configuración para el rol seleccionado. 

Paso	Descripción
39.	Por defecto, Joomla! 4 establece una segmentación de permisos según el rol que se asigne al usuario, pero es posible modificar dicha configuración según las necesidades de la organización.



Nota: De forma predeterminada, los usuarios estándar del producto no disponen de privilegios de administración ni acceso a iniciar sesión en el panel de administración, con motivo de cumplir de forma correcta con la segregación de roles y permisos.

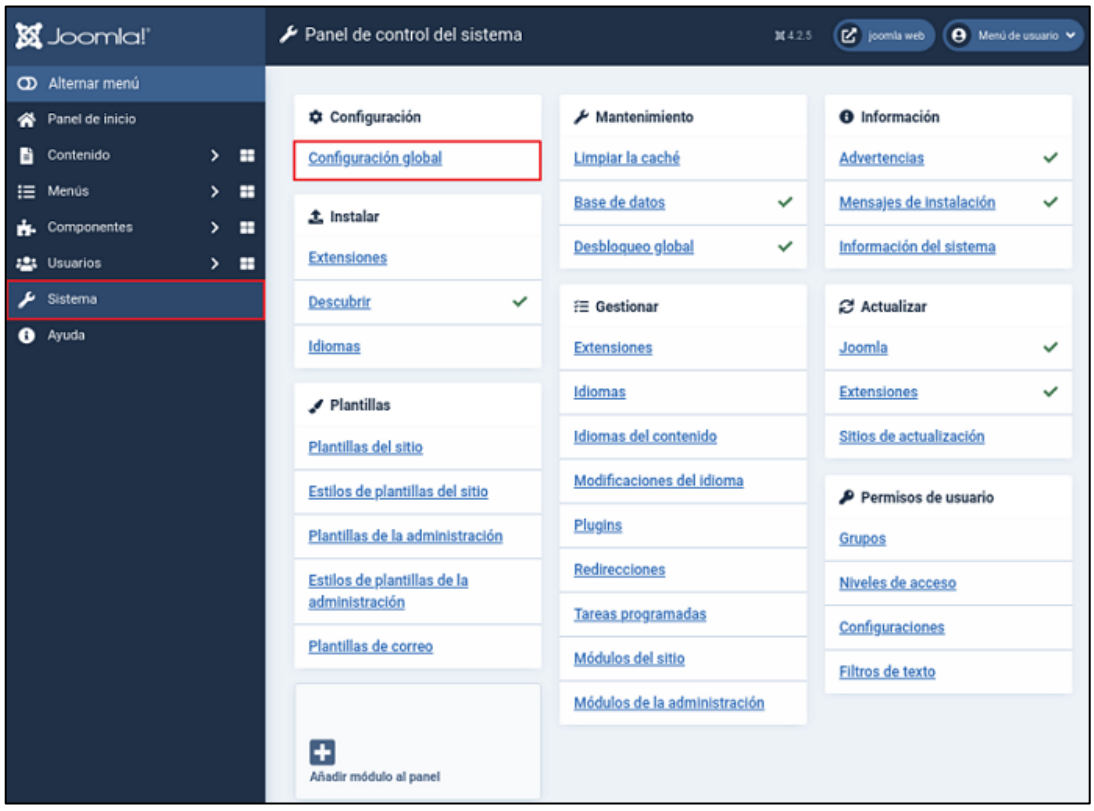
ANEXO A.5. AUTENTICACIÓN

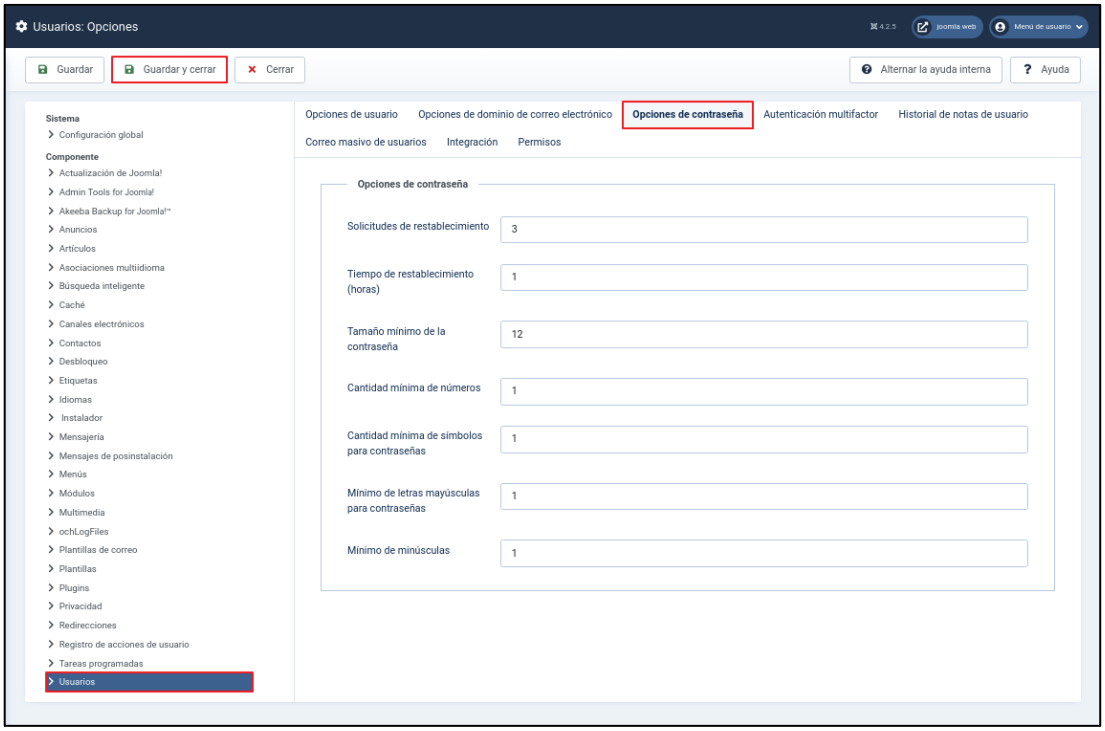
ANEXO A.5.1. POLITICA DE CONTRASEÑAS

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.5.SEC-JO2]** Se dispone de una política de credenciales robusta.

Se evitará el uso de contraseñas débiles implementando una política de contraseñas, configurando el uso obligatorio de cierto número de caracteres según las necesidades de la organización.

Paso	Descripción
40.	Si en algún momento se ha cerrado sesión, se deberá acceder al panel web de administración se inicia sesión con un usuario con permisos de superadministrador sobre el sitio.
41.	Situándose sobre **Sistema** en el menú de administración se accederá a **Configuración global**. 

Paso	Descripción
42.	A continuación, se pulsará sobre el apartado **Usuarios** al final de la columna **Componente** y se accederá a la pestaña **Opciones de contraseña** para establecer los parámetros requeridos para contraseñas de usuario. Al finalizar se pulsará sobre la opción **Guardar y cerrar**. 

Nota: Los usuarios creados con anterioridad a la implementación de la política de contraseñas no se verán afectados por la misma.

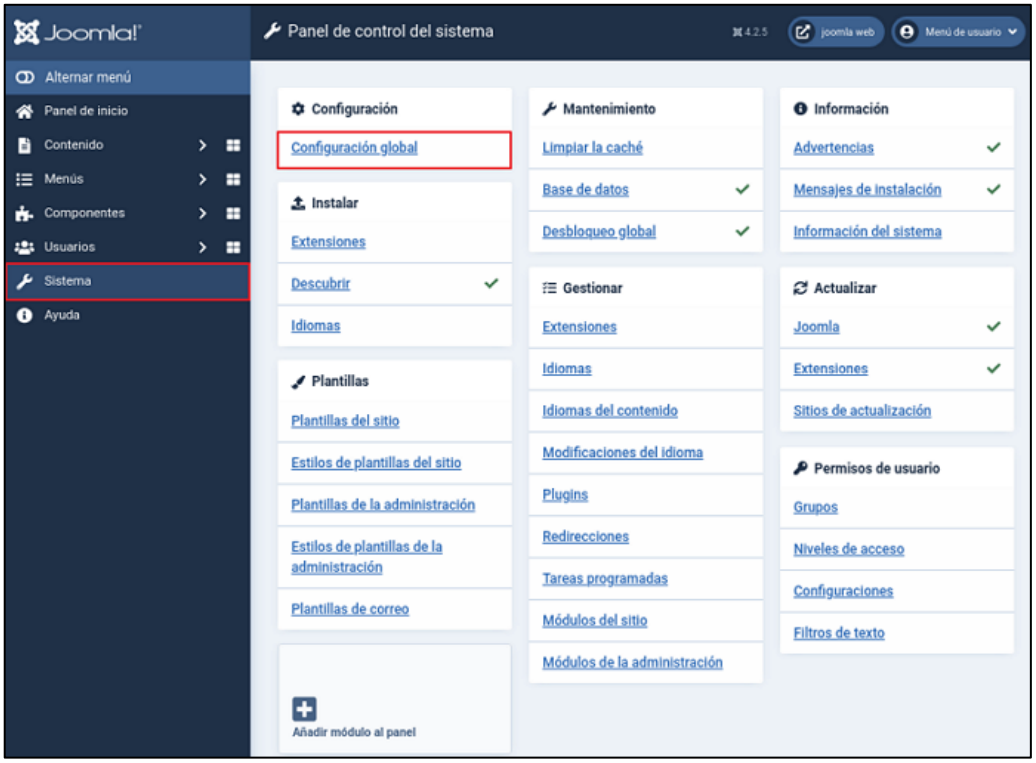
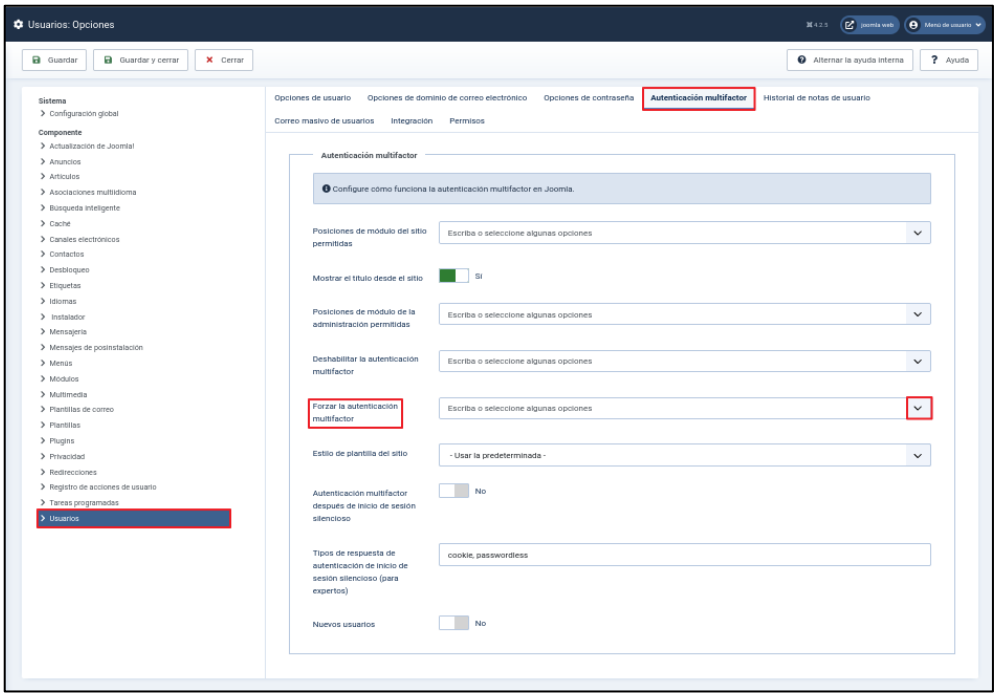
ANEXO A.5.2. DOBLE FACTOR DE AUTENTICACIÓN

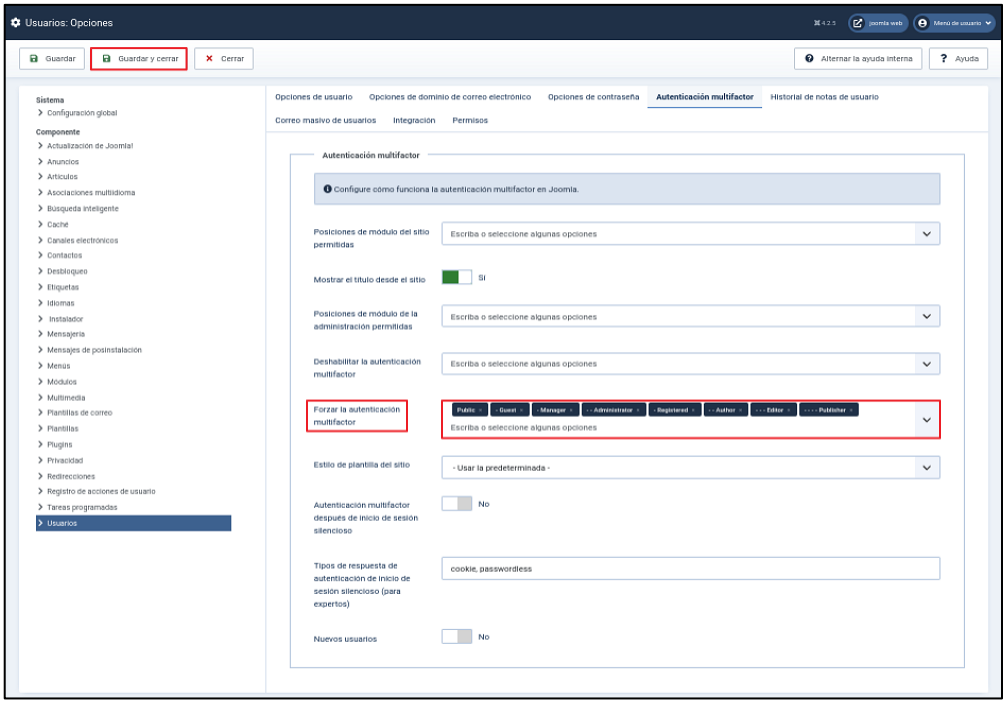
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.5.SEC-JO3]** Se utilizan métodos de doble factor de autenticación.

Con la intención de evitar accesos no deseados, se implementará un doble factor de autenticación. Existen multitud de métodos, entre ellos el de verificación mediante código, descrito en los siguientes pasos.

Paso	Descripción
43.	Si en algún momento se ha cerrado sesión, se deberá acceder al panel web de administración iniciando sesión con un usuario con permisos de superadministrador sobre el sitio.

Paso	Descripción
44.	Situándose sobre **Sistema** en el menú de administración se deberá pulsar sobre **Configuración global**. 
45.	A continuación, se accederá al apartado **Usuarios** situado al final de la columna **Componente**. Una vez en el apartado mencionado, la pantalla central cambiará mostrando la configuración genérica de los usuarios. En la pestaña **Autenticación multifactor** se establecerán los parámetros de inicio de sesión de los usuarios. 

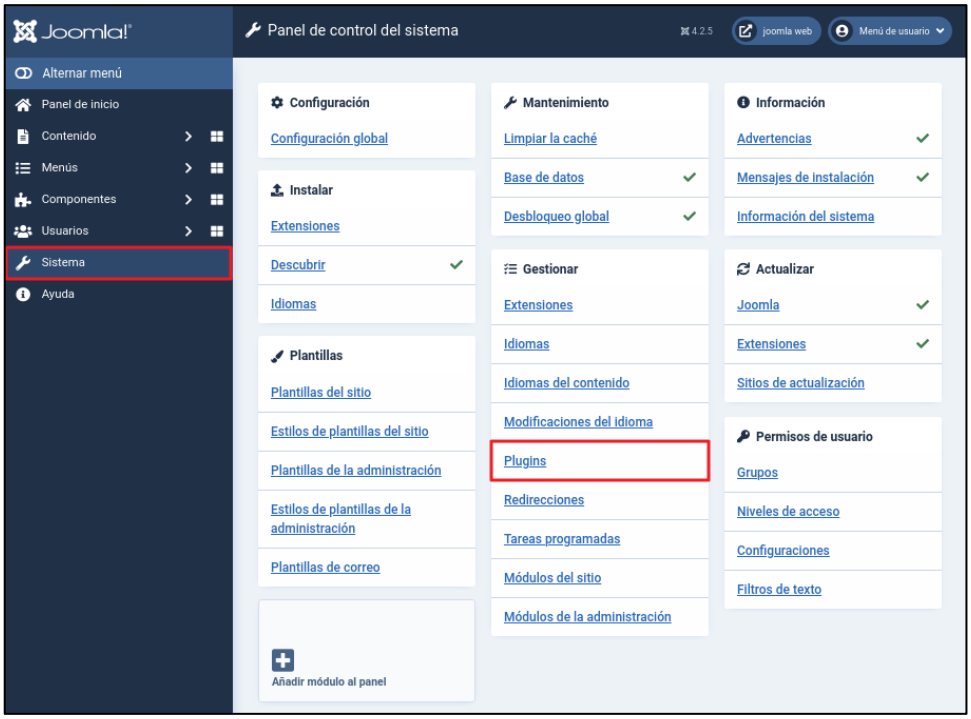
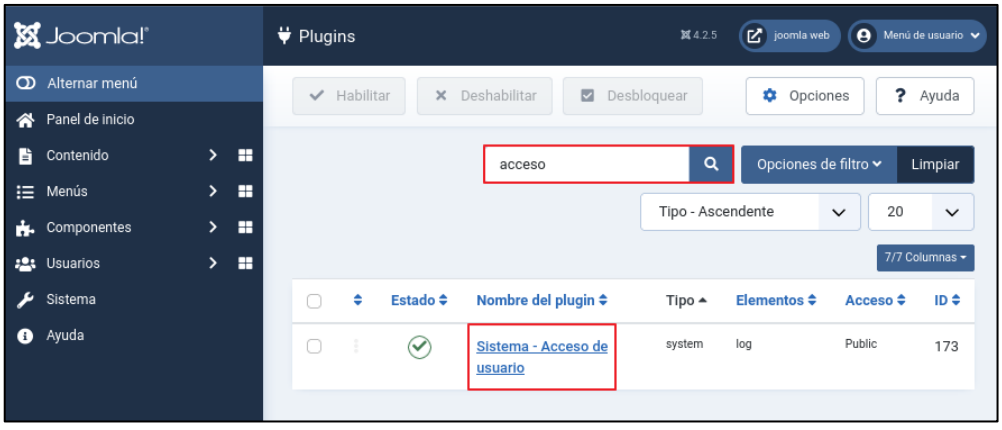
Paso	Descripción
46.	Desplegando las opciones aparecerá **Forzar la autenticación multifactor** y se deberán seleccionar los siguientes roles:" Public, Guest, Manager, Administrator, Registered, Author, Editor, Publisher". Una vez finalizado se deberá pulsar en **Guardar y cerrar**. 
47.	Una vez guardados los cambios, se les exigirá a los usuarios registrar un segundo método de autenticación. 

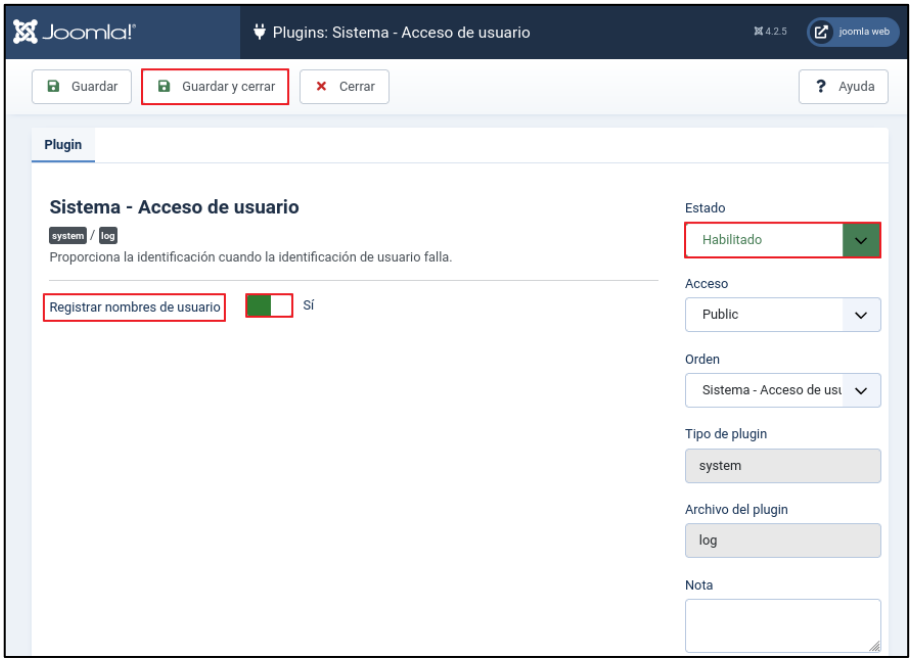
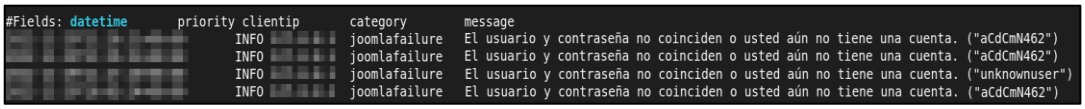
ANEXO A.5.3. HABILITAR REGISTRO DE LOG DE INICIO DE SESIÓN FALLIDO

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.3.SEC-JO1]** Se auditan los inicios de sesión fallidos.

Con la intención de poder lograr la máxima trazabilidad posible, se auditan los registros fallidos de inicio de sesión de los usuarios del producto.

Paso	Descripción
48.	Si en algún momento se ha cerrado sesión, se deberá acceder al panel web de administración iniciando sesión con un usuario con permisos de superadministrador sobre el sitio.
49.	Sobre el apartado **Sistema** en el menú de administración. Se deberá seguir el enlace **Plugins** situado en el apartado **Gestionar**. 
50.	En el buscador, se deberá escribir la palabra *"accesos"* y localizar el plugin **Sistema – Acceso de usuario**. 

Paso	Descripción
51.	Tras acceder al enlace, aparecerán las opciones para la modificación del plugin. Se marcará el check **Registrar nombres de usuario** y se comprobará que el estado se encuentra **Habilitado**, después se pulsará en **Guardar y cerrar**. 
52.	Los logs de inicio de sesión erróneos se encuentran dentro del directorio raíz de Joomla, en la ruta **/administrator/logs/error.php**. Los logs resultantes siguen el formato indicado en la imagen a continuación:  En la información del campo "*mensaje*" se encontrará el nombre del usuario que intentó iniciar sesión de forma errónea.

Nota: Es recomendable observar el incremento del tamaño del fichero programando tareas para su copia y posterior compresión en función de las políticas de conservación de logs en la organización, así como el correcto borrado o almacenado externo de los logs obsoletos para no sobrecargar el almacenamiento del sistema.

ANEXO A.6. ACL (LISTA DE CONTROL DE ACCESO)

ANEXO A.6.1. PANEL WEB DE ADMINISTRACÍON

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.15.SEC-JO3]** Se protege el acceso del panel web de administración añadiendo ACL por IP.

Es fundamental para la seguridad del sitio crear una Lista de Control de Acceso (En inglés ACL, Access Control List) para limitar mediante una lista blanca el acceso al panel web de administración del sitio.

Paso	Descripción
53.	Si en algún momento se ha cerrado sesión, se deberá abrir un terminal en el equipo que cuente con Joomla! 4 utilizando una cuenta con permisos de administrador.
54.	Se accederá al directorio **joomla/administrator**. **$ cd /[ruta]/joomla/administrator**
55.	Una vez dentro del directorio, hay que verificar si existe un fichero llamado **.htaccess** con el siguiente comando: **$ ls -la**
56.	En caso de no existir, se creará con el siguiente comando: **$ sudo touch .htaccess**
57.	A continuación, se editará el fichero teniendo en cuenta que las IP que se incluyan serán permitidas mientras que el resto de IP serán denegadas. **$ sudo vi .htaccess.** **Nota**: El punto delante del fichero es utilizado para ocultarlo ante la lectura del directorio.

58.	Añadiendo las líneas siguientes al fichero, se incluirán las IP de los equipos desde donde se va a conectar al panel web de administración. Una vez terminado se guardará el fichero.
	`Deny from All`
	`Allow from [redacted]`
	`Allow from [redacted]`
	Nota: En el campo IP, es posible añadir la dirección de localhost 127.0.0.1.

59.	Tras agregar las direcciones IP permitidas, se reiniciará el servicio web y por último se verificará que está denegada la entrada al panel web de administración desde otro equipo. **$ sudo systemctl restart httpd**

ANEXO A.7. REGISTROS DE ACTIVIDAD

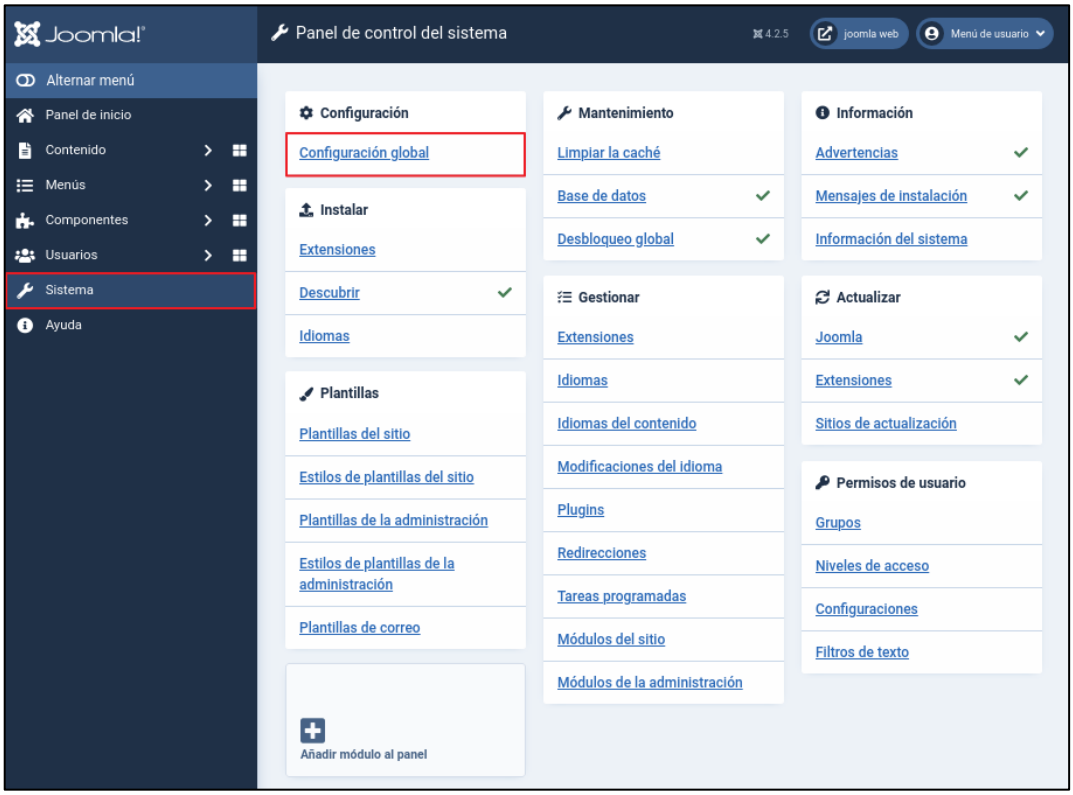
ANEXO A.7.1. TIEMPO DE INACTIVIDAD

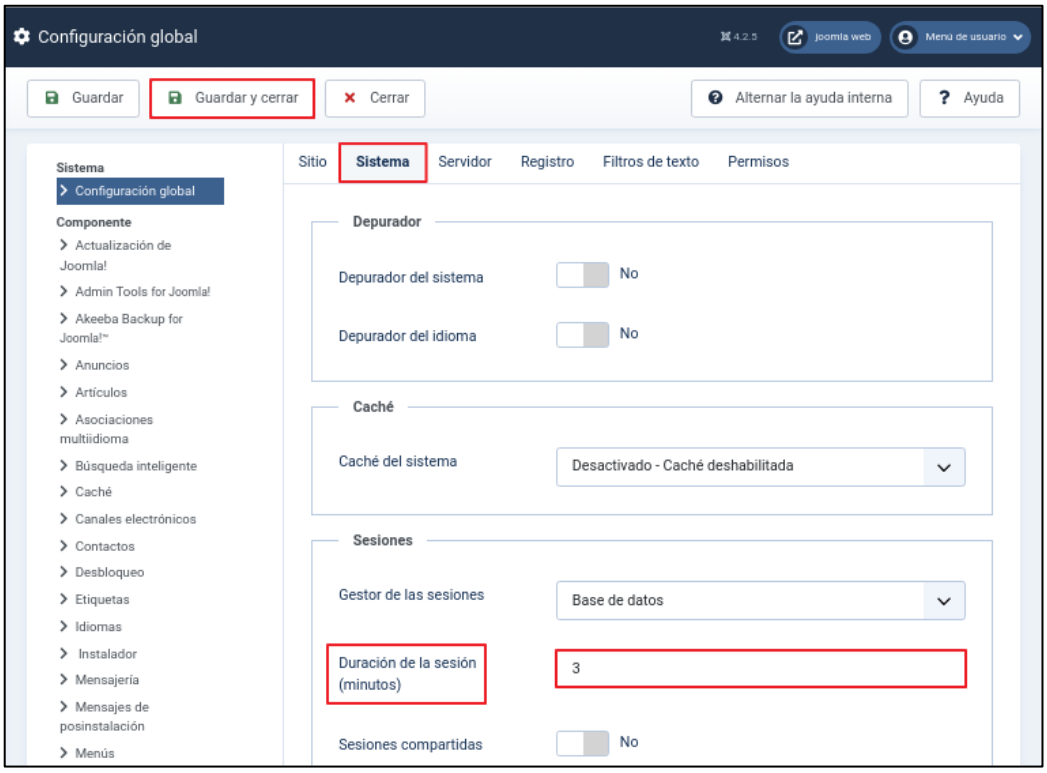
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.5.SEC-JO1]** Se controlan los permisos de inicio de sesión y suplantación de identidad.

b) **[A.5.SEC-JO4]** Se establece un tiempo máximo de sesión inactiva.

Se establece el tiempo máximo para la inactividad de las sesiones mitigando así la suplantación de identidad.

Paso	Descripción
60.	Si en algún momento se ha cerrado sesión, se deberá acceder al panel web de administración iniciando sesión con un usuario con permisos de superadministrador sobre el sitio.
61.	En el panel derecho de Joomla accediendo a **Sistema** en el menú de administración se deberá acceder a **Configuración global**. 

Paso	Descripción
62.	En la pestaña **Sistema** habrá que configurar en **Duración de la sesión,** el tiempo de inactividad máximo. Finalmente se deberá pulsar sobre **Guardar y cerrar**. 

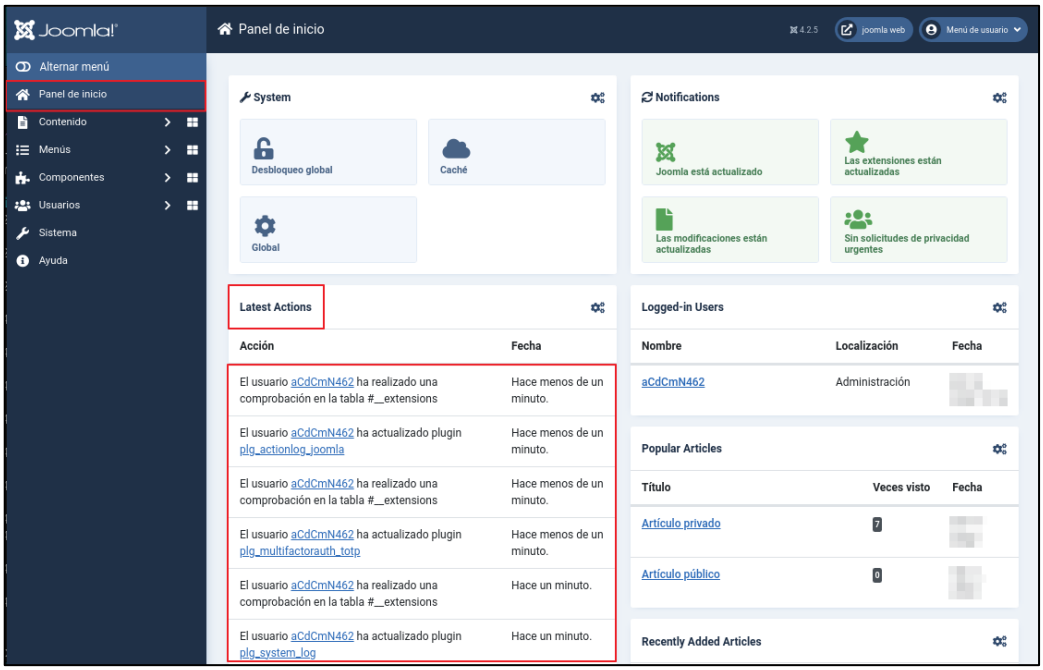
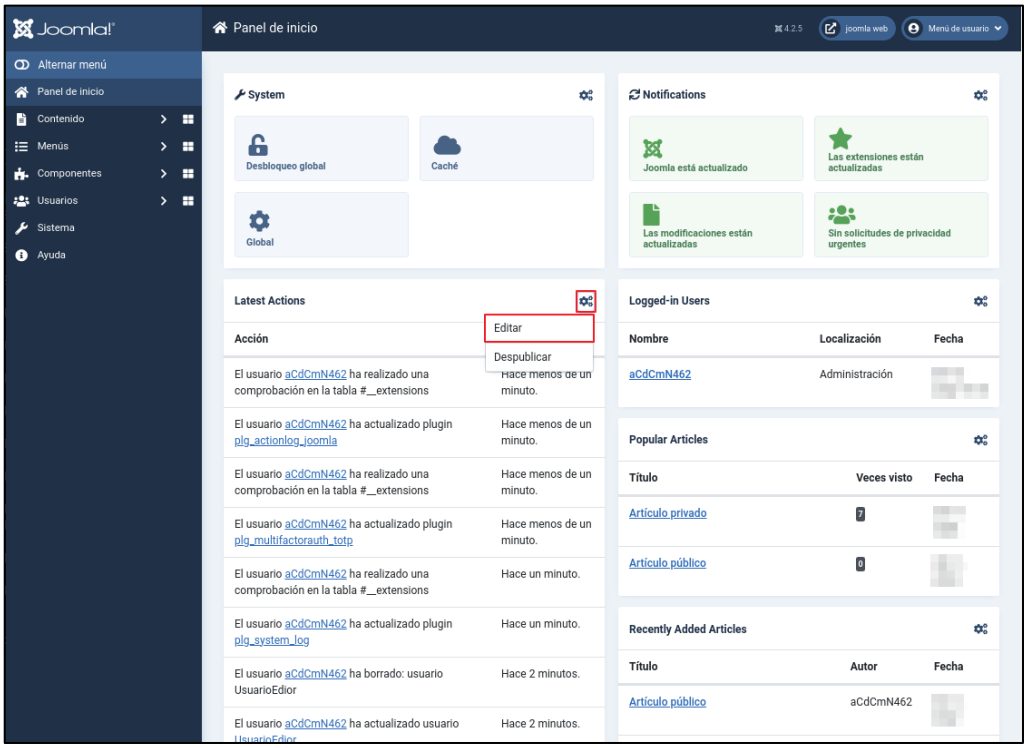
ANEXO A.7.2. AUDITAR MODIFICACIONES A OBJETOS

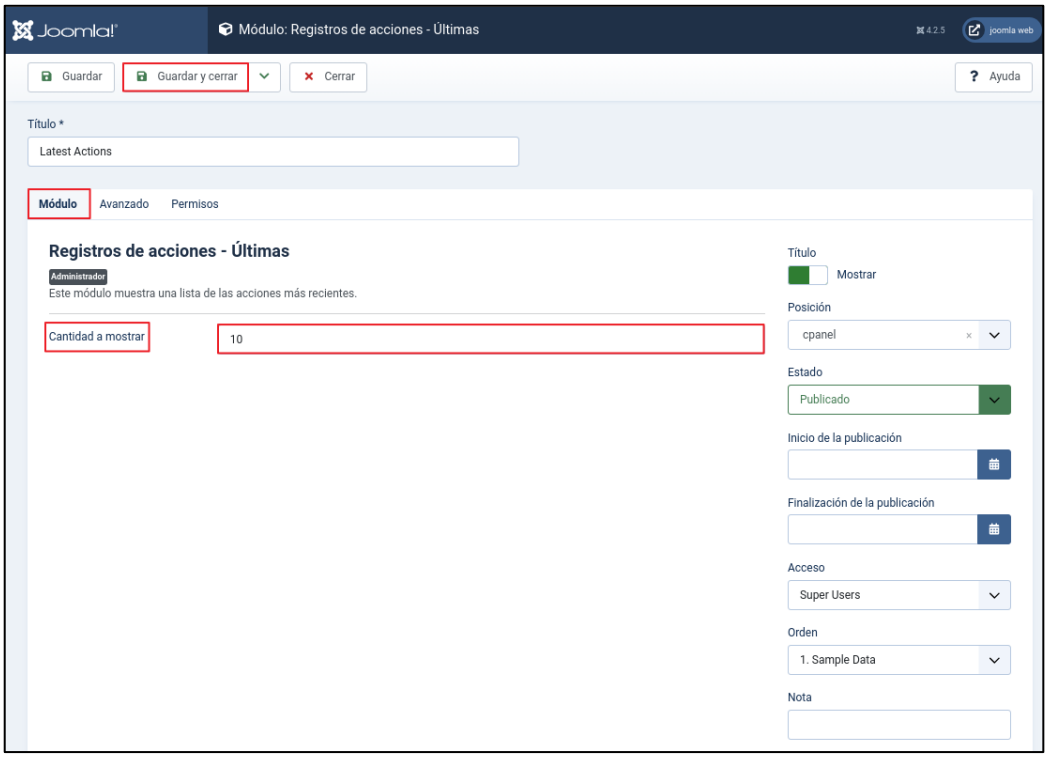
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.3.SEC-JO2]** Se auditan las modificaciones sobre los elementos del sitio.

Se habilitan los registros sobre modificaciones de extensiones y plugin del sitio de tal forma que sea posible observar qué elemento ha sido modificado.

Paso	Descripción
63.	Si en algún momento se ha cerrado sesión, se deberá acceder al panel web de administración iniciando sesión con un usuario con permisos de superadministrador sobre el sitio.

Paso	Descripción
64.	Sobre **Panel de inicio** en el menú de administración, en la pantalla central acceder a la opción **Latest Actions**. En ella se podrá observar qué cambio se realizó y qué usuario fue el responsable, e igualmente cuánto tiempo hace que fue realizado. 
65.	Es posible editar el plugin para personalizarlo. Para ello se pulsará sobre la rueda de engranaje y después sobre **Editar**. 

Paso	Descripción
66.	Al editar el plugin se podrá elegir el número de registros de acciones que se visualizarán en pantalla. Una vez configurado, se deberá **Guardar y cerrar**. 

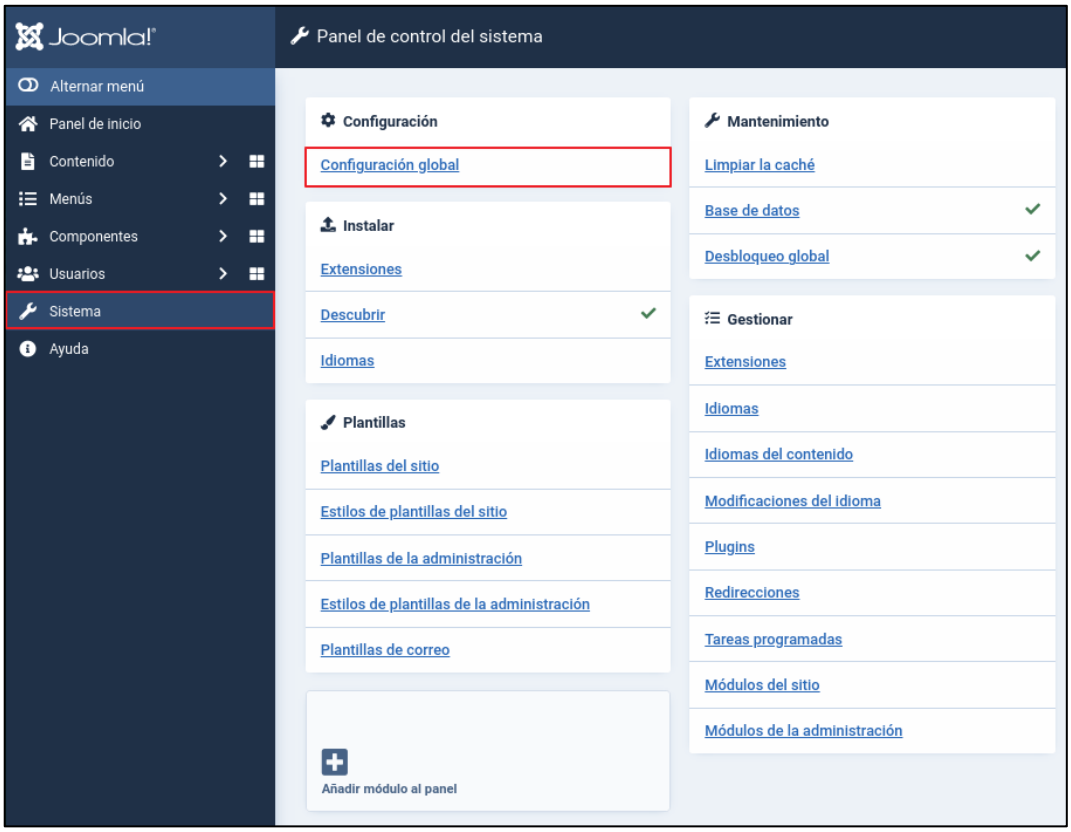
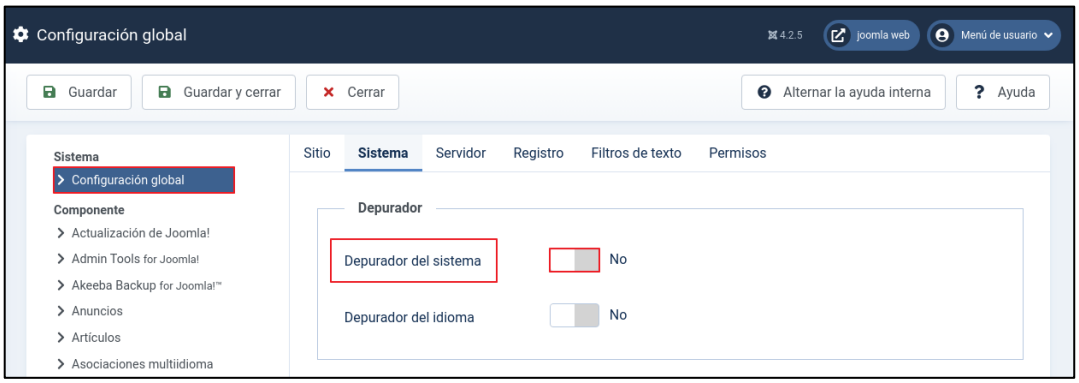
ANEXO A.7.3. DESHABILITAR DEPURACIÓN

En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

[A.19.SEC-JO2] Se deshabilita la depuración del sistema.

A continuación, se procede a deshabilitar la depuración del sistema debido a que, estando habilitada, proporciona información tanto en el "front-end" como en el "back-end" sobre consultas SQL, versión de componentes PHP, versión del servidor web, quedando expuesta esta información a cualquier usuario.

Paso	Descripción
67.	Si en algún momento se ha cerrado sesión, se deberá acceder al panel web de administración iniciando sesión con un usuario con permisos de superadministrador sobre el sitio.

Paso	Descripción
68.	Entrando en el panel web de administración y, situándose en el menú de administración se accederá a la opción **Sistema**, tras ello, a **Configuración global**. 
69.	En la sección central, se accederá a la pestaña **Sistema** donde se buscará la opción **Depurador del sistema** y se establecerá su valor en "*NO*". 

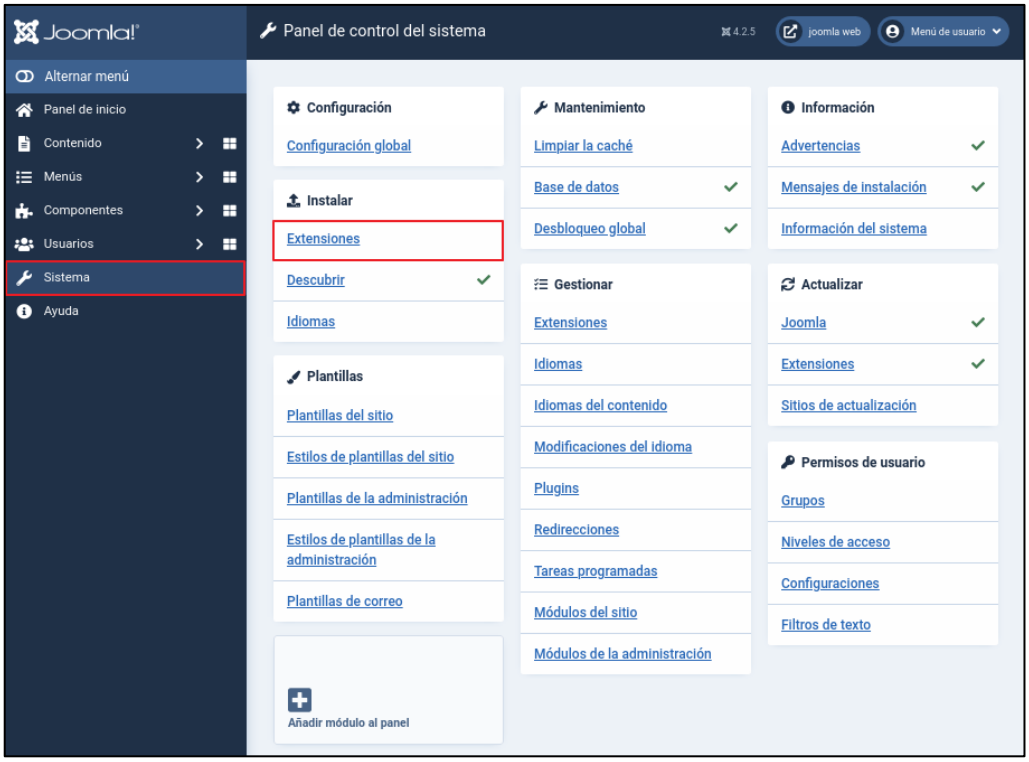
ANEXO A.8. COPIAS DE SEGURIDAD

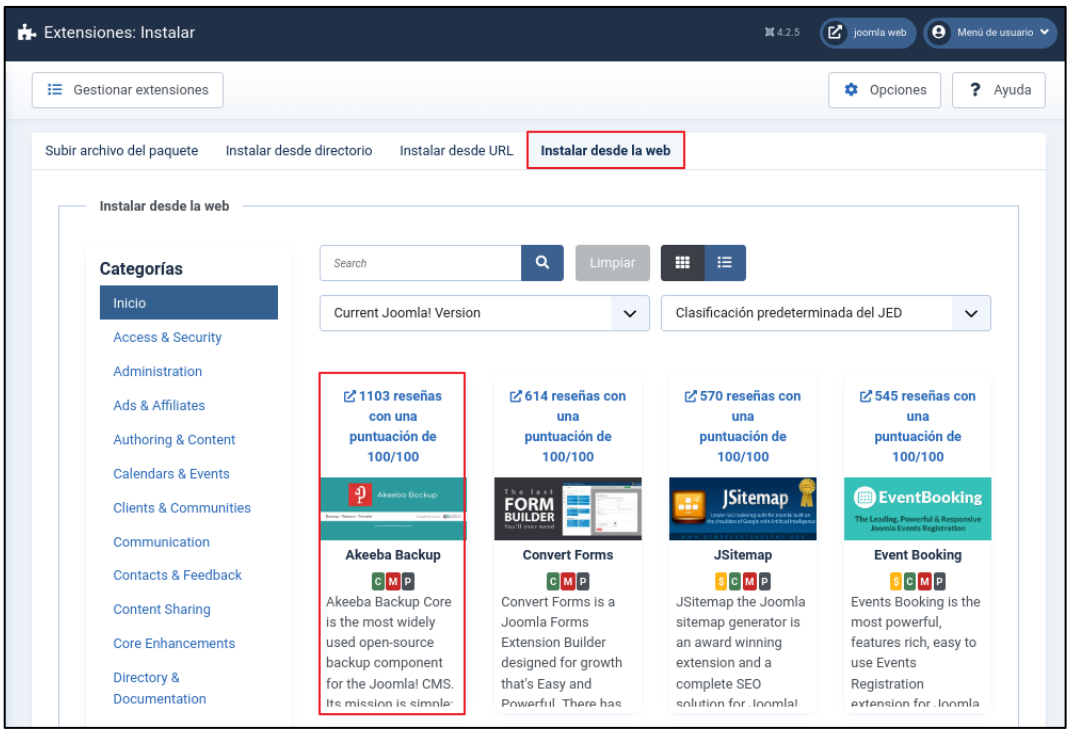
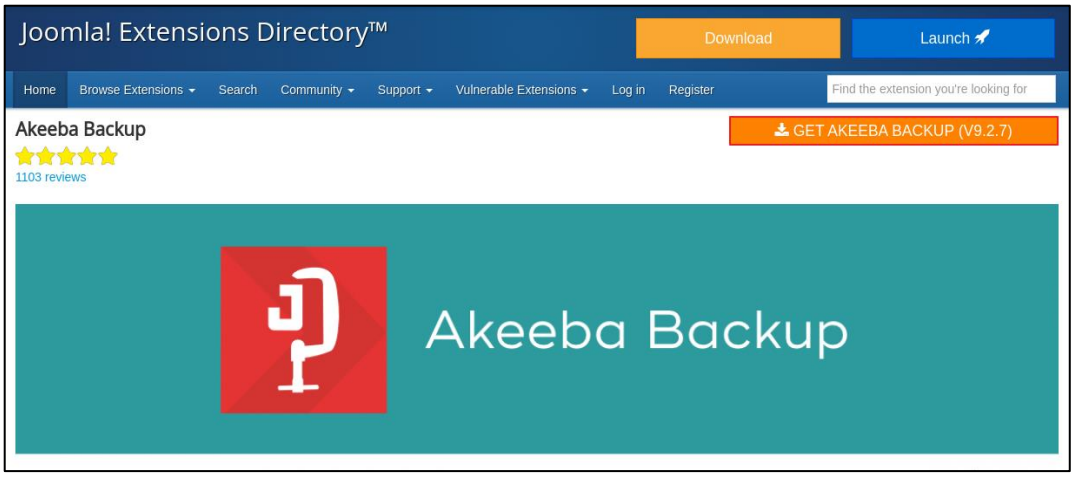
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

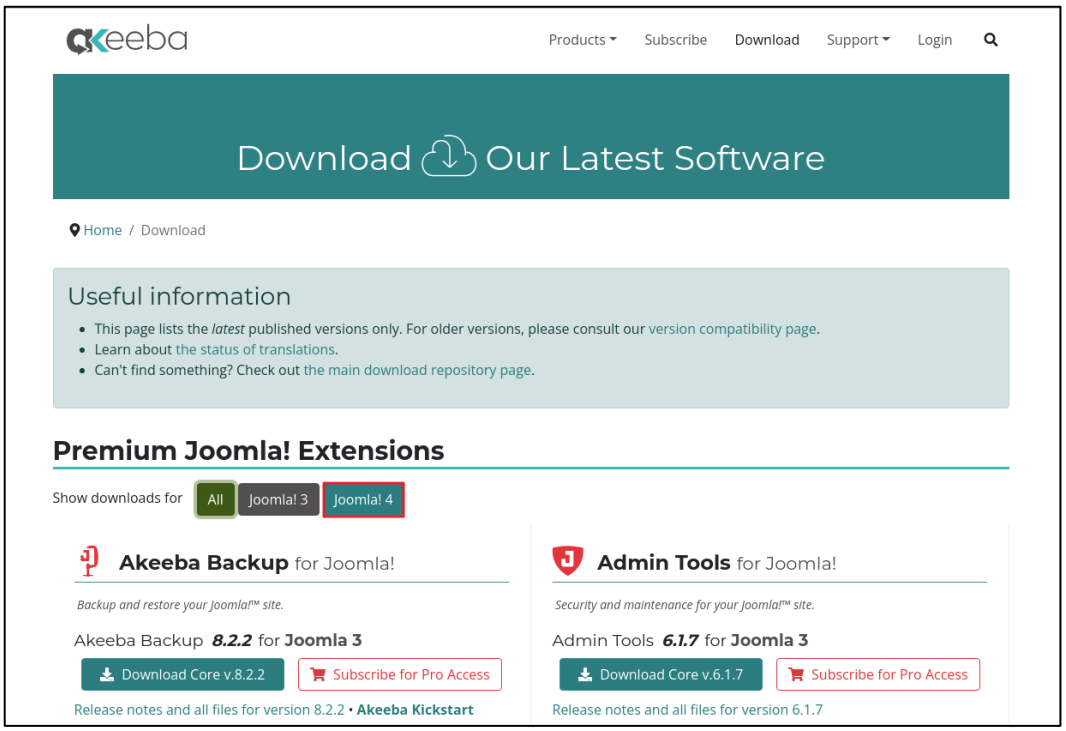
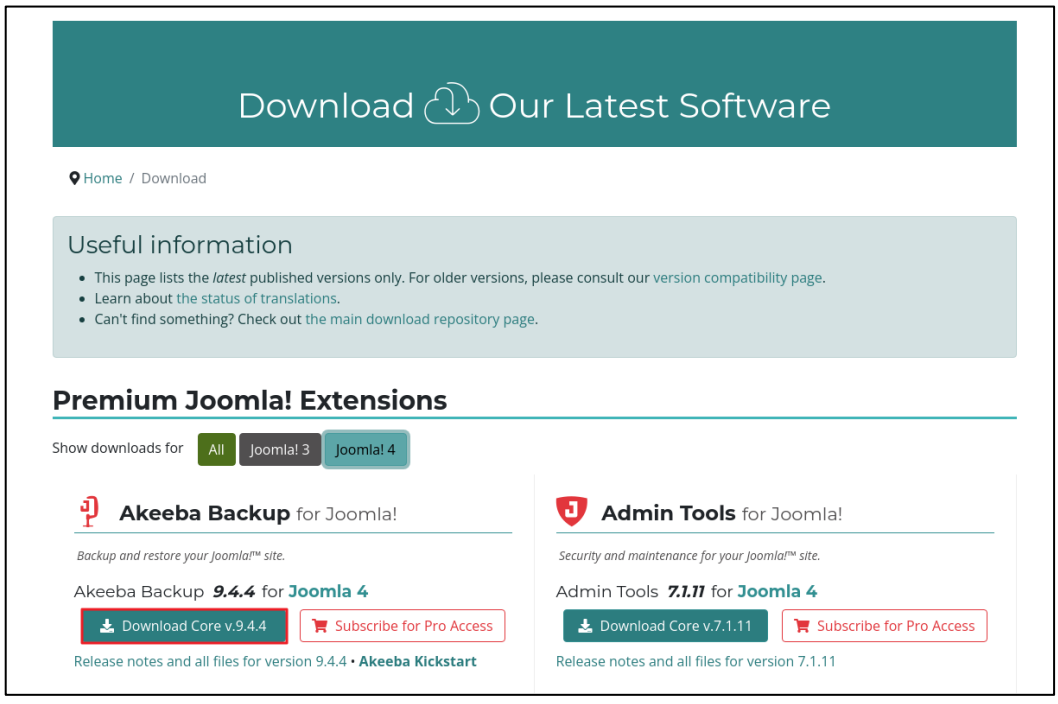
a) **[A.15.SEC-JO4]** Se realizan copias de seguridad con frecuencia.

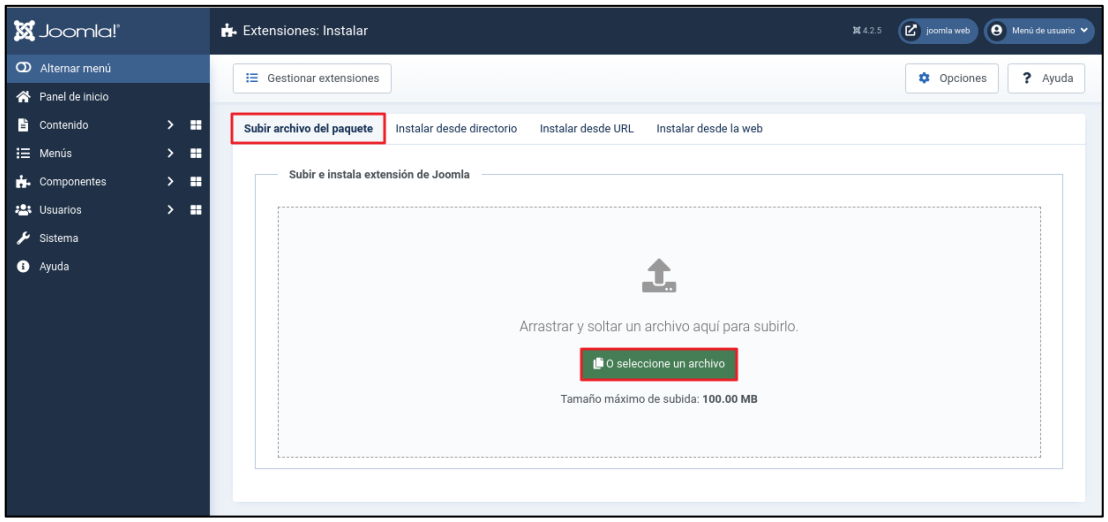
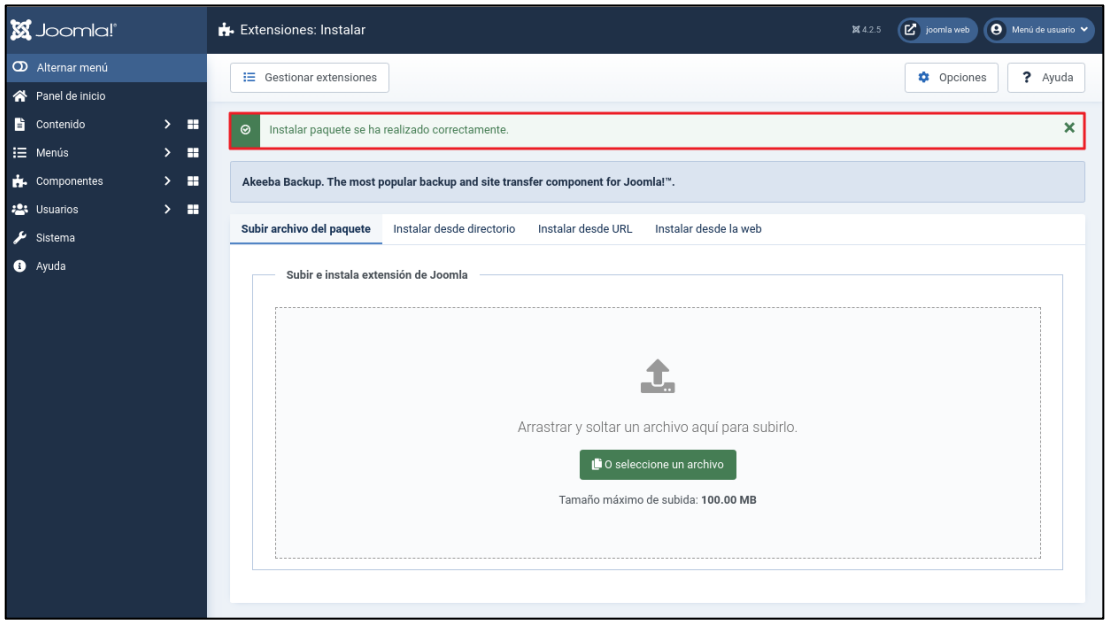
Se realizan copias de seguridad de forma periódica, imprescindibles a la hora de recuperar el contenido del sitio y las configuraciones en caso de fallo, siendo recomendable contar con una copia del último estado del gestor de contenidos en una ubicación externa al mismo.

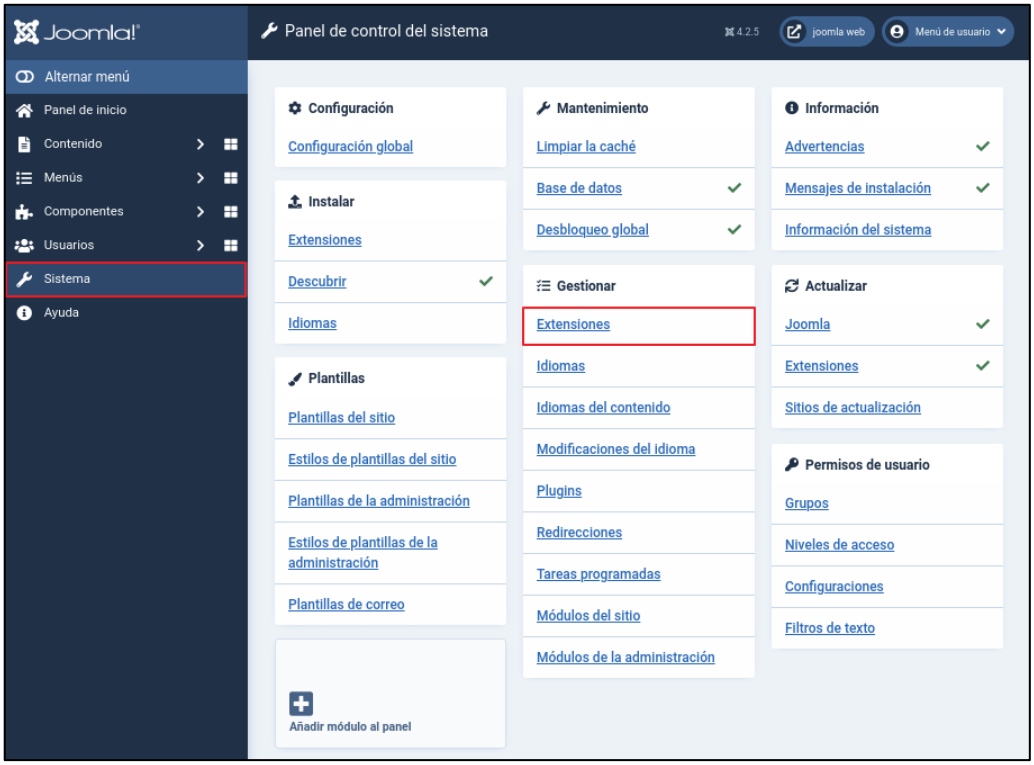
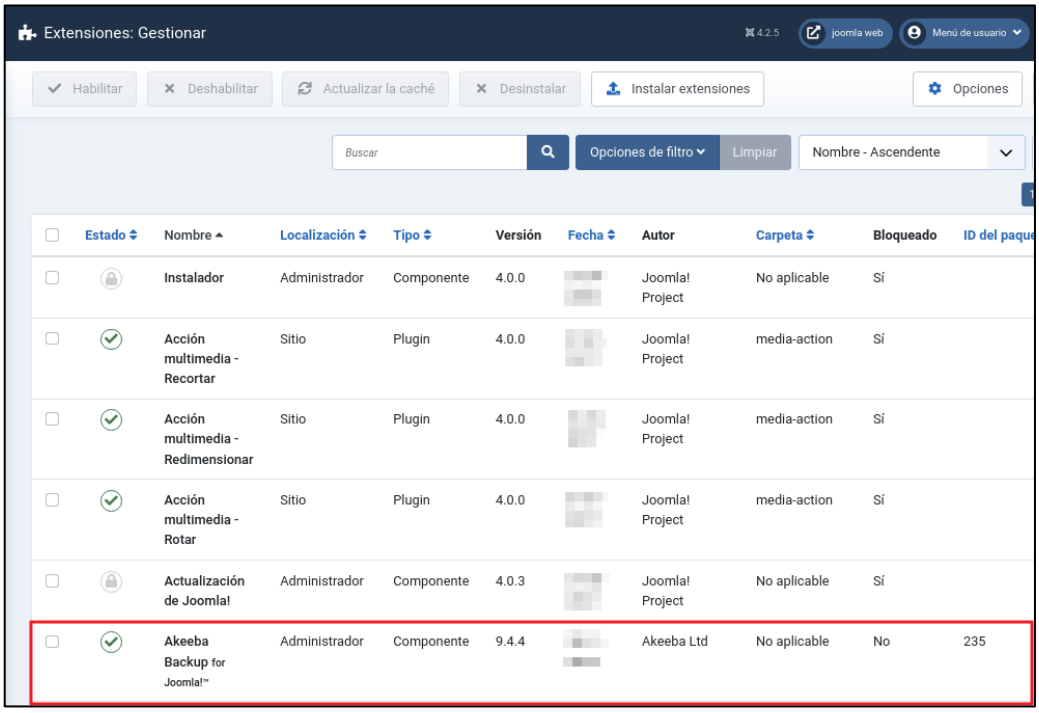
Nota: En el ejemplo mostrado a continuación se ha procedido a la instalación de "*Akeeba Backup*" como una de las posibles soluciones disponibles para la mitigación de este riesgo. Cada organización deberá valorar la solución a implementar.

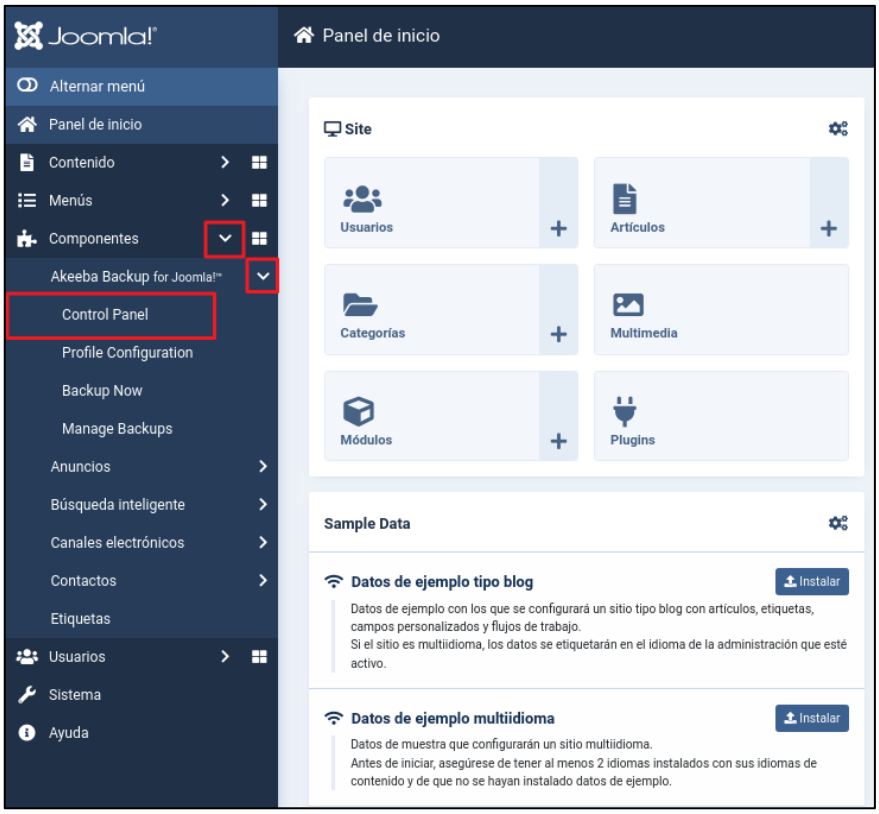
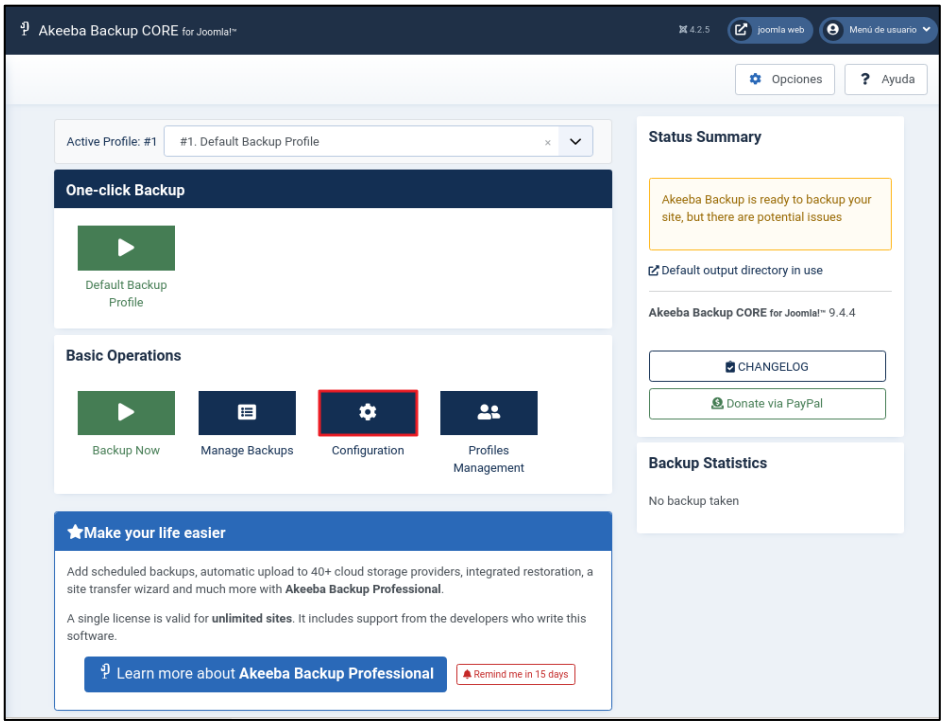
Paso	Descripción
70.	Si en algún momento se ha cerrado sesión, se deberá acceder al panel web de administración iniciando sesión con un usuario con permisos de superadministrador sobre el sitio.
71.	Entrando en el panel web de administración y, situándose en el menú de administración (**Sistema**) se accederá a la opción **Extensiones**. 

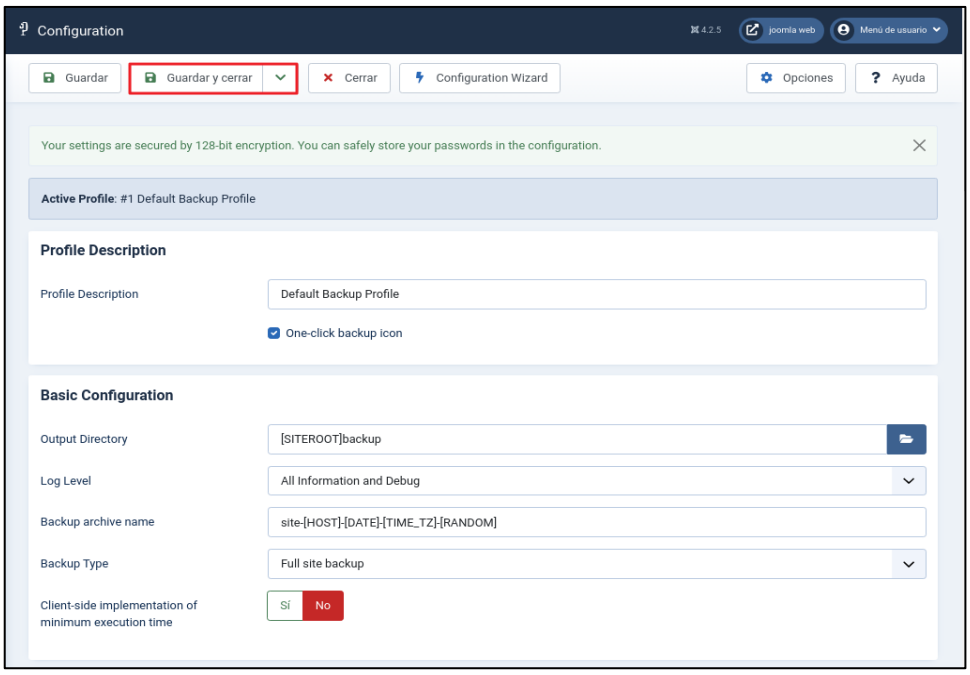
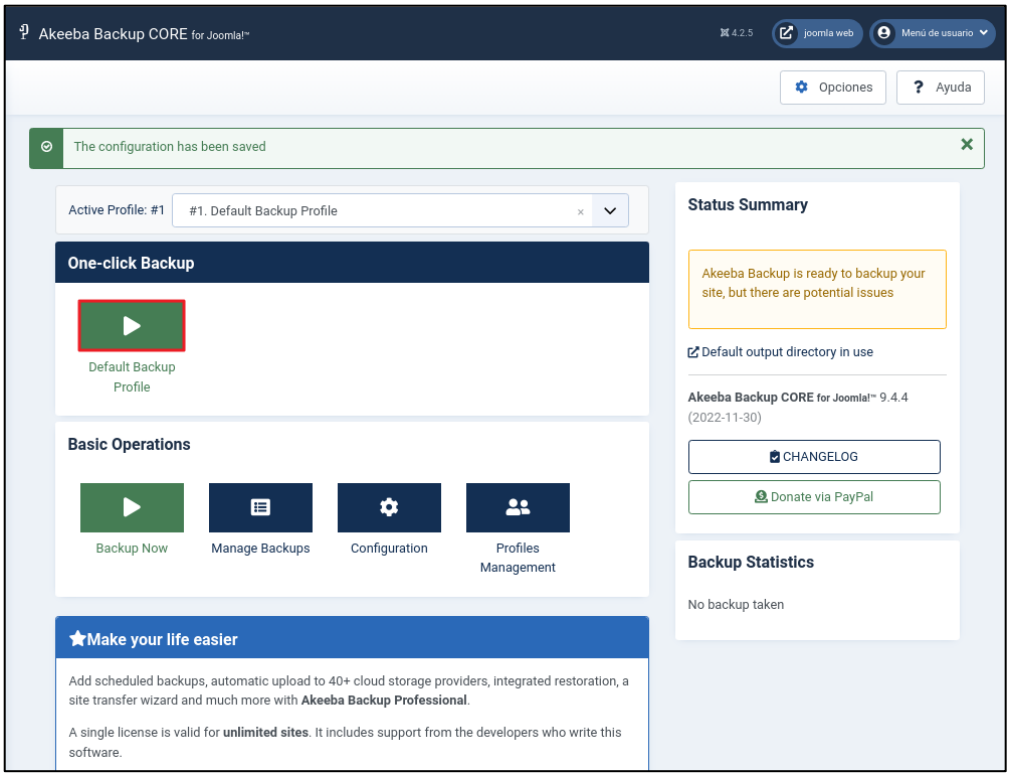
Paso	Descripción
72.	En la sección de instalación, se debe acceder a la pestaña **Instalar desde la web**. "*Akeeba Backup*" aparecerá como primera opción, en caso de no ser así, se puede ejecutar la búsqueda desde el cuadro de búsquedas. Una vez encontrada la extensión, se pulsará sobre el enlace de dicha extensión. 
73.	El enlace le redirige a la página oficial de Joomla para esa extensión. Se pulsará sobre el enlace "*GET AKEEBA BACKUP*". 

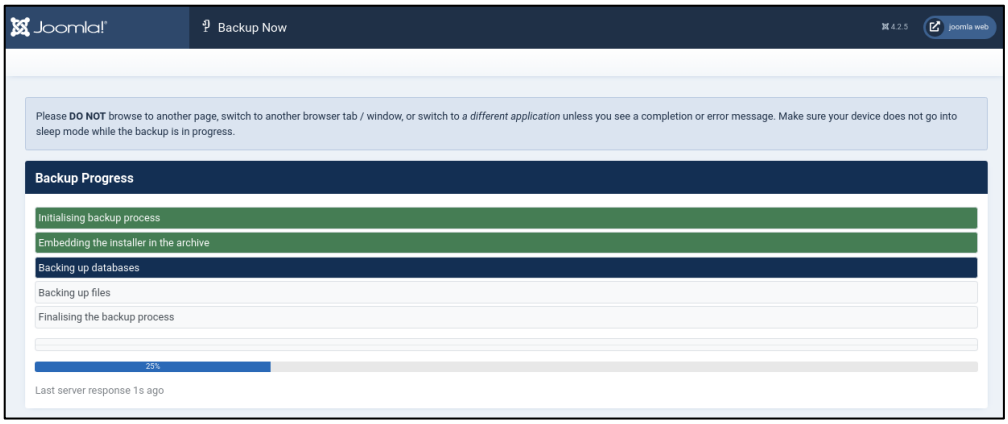
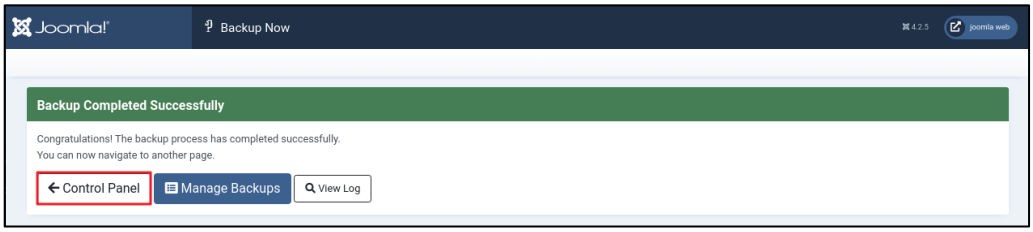
Paso	Descripción
74.	Se redirigirá esta vez a la página oficial de "*Akeeba*". En el cuadro de extensiones, para este ejemplo se descargará Joomla! 4. 
75.	Una vez seleccionada la versión de Joomla, se deberá pincha sobre el enlace de descarga de "*Akeeba Backup*". 

Paso	Descripción
76.	Situado de nuevo en la página de instalación de extensiones del gestor de contenidos, se accederá a la pestaña **Subir archivo del paquete** y, posteriormente, sobre **seleccione un archivo**, buscando la descarga realizada en su sistema de ficheros. 
77.	Una vez seleccionado el archivo el sistema se instalará la extensión. 

Paso	Descripción
78.	En el menú de administración, se accederá a **Sistema**, accediendo en el panel central en la sección **Gestionar** a la opción **Extensiones**. 
79.	Se comprobará que la extensión se encuentra instalada. 

Paso	Descripción
80.	Para ejecutar las copias de seguridad, en el menú de administración, se desplegará la opción **Componentes** y a continuación la opción de ***Akeeba Backup for Joomla!*** tras ello se accederá a **Control Panel**. 
81.	Una vez situado en el panel de control de ***Akeeba Backup***, se pulsará sobre el icono **Configuration**. 

Paso	Descripción
82.	Se ajustarán las opciones disponibles a las necesidades de la organización, entre ellas, se encuentra el directorio donde se guardan las copias de seguridad, el nombre de la copia, opciones de base de datos y opciones de cuota. Una vez definida la configuración adecuada, se pulsará sobre **Guardar y cerrar**. 
83.	Para comenzar la ejecución de la copia de seguridad, se pulsará sobre **Default Backup Profile** y comenzará el proceso de copia. 

Paso	Descripción
84.	Espere a que el proceso de copia termine. 
85.	Una vez finalizada la copia, se podrá regresar al panel de control pulsando **Control Panel**. 

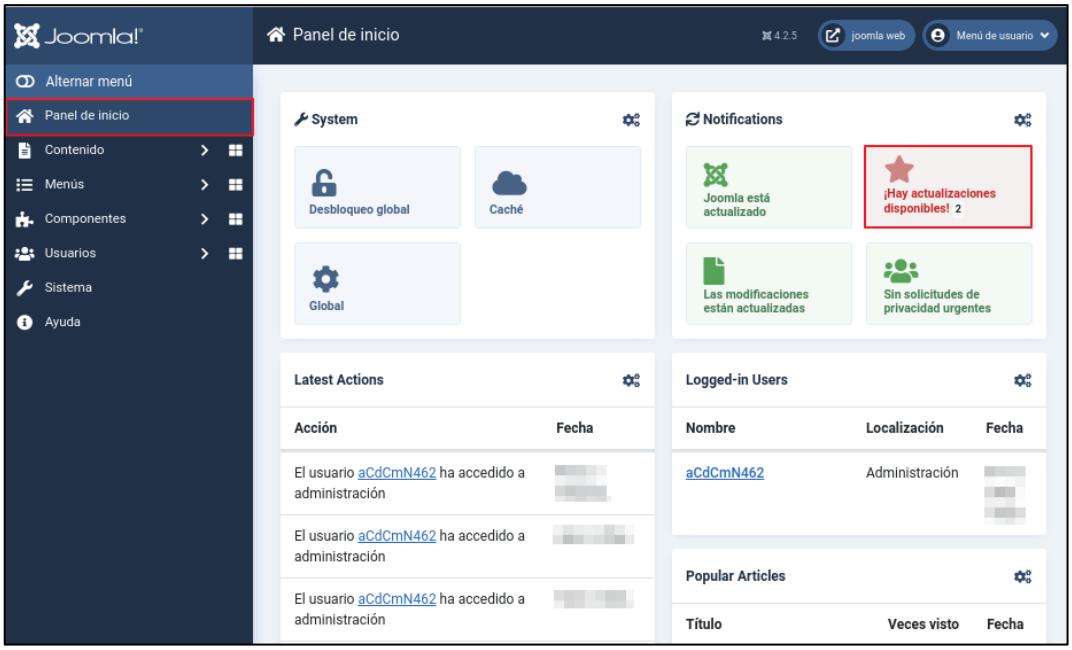
ANEXO A.9. ACTUALIZACIONES

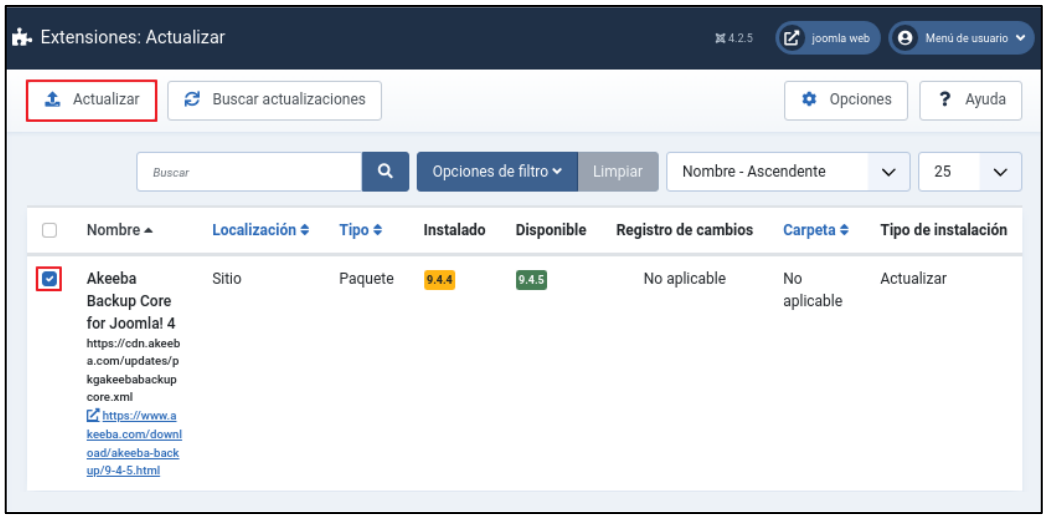
En este apartado se definen las acciones para cubrir las siguientes categorías de medidas de seguridad:

a) **[A.3.SEC-JO3]** El producto se encuentra siempre actualizado, así como los complementos que se instalen en él

El gestor de contenido o CMS (Content Management System) se encontrará siempre actualizado, así como todos los plugin o extensiones que se instalen para la mejora de sus funcionalidades.

Nota: Se recomienda hacer una copia de seguridad antes de instalar las actualizaciones para poder restablecerla en caso de no ser compatible con alguno de los componentes instalados en el producto.

Paso	Descripción
86.	Se accederá a un navegador y al panel web de administración iniciando sesión con un usuario con permisos de superadministrador sobre el sitio.
87.	Se accederá a la opción **Panel de inicio** en el menú de administración, tras ello, en la sección central, en el apartado **Notificaciones** se pulsará sobre **Actualizaciones disponibles**. 

Paso	Descripción
88.	En la nueva pantalla aparecerán las extensiones, plugin y demás complementos que se encuentran disponibles para una actualización. Es importante marcar la casilla de verificación de la extensión o plugin a actualizar y pulsar a continuación sobre **Actualizar**. 
89.	Se deberá repetir el paso anterior con la totalidad de las actualizaciones disponibles.
90.	Tras finalizar el proceso de actualización aparecerá un mensaje de verificación en pantalla. 

PUBLICACIONES DE DEFENSA

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