

Funcionalidades y mejoras ANA v.3.0



Diciembre 2021

Edita:



© Centro Criptológico Nacional, 2021

Fecha de Edición: diciembre de 2021

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN	5
2. DESCRIPCIÓN FUNCIONAL.....	5
2.1 MÓDULOS FUNCIONALES	5
2.1.1 ANA VULNERABILIDADES	5
2.1.1.1 NOVEDADES INCLUIDAS EN ANA 3.0.....	6
2.1.2 ANA MEJORA CONTINUA	6
2.1.2.1 NOVEDADES INCLUIDAS EN ANA 3.0.....	7
2.1.3 CLARA	7
2.1.3.1 NOVEDADES INCLUIDAS EN ANA 3.0.....	8
3. NUEVAS FUNCIONALIDADES	8
3.1 NUEVAS FUNCIONALIDADES ATENDIENDO A LA EXPERIENCIA DE USUARIO	8
3.1.1 NUEVO INTERFAZ GRÁFICO.....	8
3.1.1.1 CAMBIOS GENERALES.....	8
3.1.1.2 CAMBIOS GRÁFICOS EN TABLAS.....	11
3.1.1.3 CAMBIOS GRÁFICOS EN FORMULARIOS.....	12
3.1.1.4 CAMBIOS GRÁFICOS EN CUADROS MODALES.....	14
3.1.1.5 OTROS CAMBIOS.....	14
3.1.1.5.1 Indicativo de carga de datos.....	14
3.1.1.5.2 Pantalla de carga de imágenes	15
3.1.1.5.3 CLARA	15
3.1.2 NUEVO SELECTOR DE MÓDULO BASADO EN ROLES.....	16
3.1.3 NUEVO CAMPO PARA BÚSQUEDA DE AUDITORÍAS EN LA PANTALLA DE RESUMEN DEL <i>BACKEND</i>	16
3.2 NUEVAS FUNCIONALIDADES RELACIONADAS CON LA POTENCIACIÓN DE LA APLICACIÓN	17
3.2.1 NUEVOS ROLES ASOCIADOS A FUNCIONALIDADES	17
3.2.1.1 CORRESPONDENCIA ENTRE ROLES NUEVOS Y VERSIONES ANTERIORES.....	18
3.2.1.1.1 CLARA	18
3.2.1.1.2 Mejora continua.	19
3.2.1.2 ROLES DE USUARIO EN FUNCIÓN DEL MÓDULO.....	19
3.2.1.2.1 ANA Vulnerabilidades.....	19
3.2.1.2.1.1 Administrador	19
3.2.1.2.1.2 WSAdmin.....	19
3.2.1.2.1.3 WSOwner:	21
3.2.1.2.1.4 Pentester:.....	24
3.2.1.2.1.4.1 Pentester approver:	26
3.2.1.2.1.4.2 Pentester need approval:.....	26
3.2.1.2.1.4.3 Pentester audit manager:	26
3.2.1.2.1.5 Business:.....	26
3.2.1.2.1.6 Viewer:	27
3.2.1.2.1.6.1 Solver:	27
3.2.1.3 NUEVOS ROLES EN ANA.....	30
3.2.1.3.1 AuditManager.....	30
3.2.1.4 NUEVOS ROLES EN MÓDULO DE MEJORA CONTINUA (CIS)	31
3.2.1.4.1 CIS Administrator.....	31
3.2.1.4.2 CIS Auditor	31

3.2.1.4.3	CIS Viewer	31
3.2.1.5	NUEVOS ROLES EN CLARA	32
3.2.1.5.1	CLARA Administrator	32
3.2.1.5.2	CLARA Business.....	33
3.2.1.5.3	CLARA Auditor	34
3.2.1.5.4	CLARA Viewer	34
3.2.2	AUTENTICACIÓN Y NAVEGACIÓN POR ROLES.....	35
4.	MEJORAS	36
4.1	MEJORAS ATENDIENDO A LA EXPERIENCIA DE USUARIO.....	36
4.1.1	PANTALLA DE RESUMEN DEL BACKEND.....	36
4.1.2	SIMPLIFICACIÓN DE LAS VENTANAS DE IMPORTACIÓN, OBTENIENDO LAS OPCIONES DESDE LA AUDITORÍA.....	36
4.1.2.1	NESSUS.....	36
4.1.2.2	NMAP	37
4.1.2.3	CLARA.....	38
4.1.2.4	EMMA	38
4.1.2.5	CMDB	39
4.2	MEJORAS RELACIONADAS CON LA POTENCIACIÓN DE LA APLICACIÓN.....	40
4.2.1	AUDITORÍAS PADRES Y DE REGRESIÓN PUEDEN SER DE DIFERENTE TIPO	40
4.2.2	UNIFICACIÓN DE LOS PROCESOS DE IMPORTACIONES.....	40
4.2.3	AMPLIACIÓN DE LA FUNCIONALIDAD DE CREACIÓN Y EDICIÓN DE AUDITORÍAS PERMITIENDO CONFIGURAR LOS PARÁMETROS DE LAS DISTINTAS IMPORTACIONES.....	40
4.2.3.1	FUNCIONAMIENTO DE LA CONFIGURACIÓN DE IMPORTACIONES.....	41
4.2.4	MEJORAS EN LA ENTRADA DEL POC DE LAS VULNERABILIDADES Y SU SEGURIDAD	43
5.	FUNCIONALIDADES NO DISPONIBLES A PARTIR DE LA VERSIÓN 3.0	43
5.1	FUNCIONALIDADES NO DISPONIBLES	43
6.	ANEXO A: ÍNDICE DE ILUSTRACIONES.....	45

1. INTRODUCCIÓN

Este documento recoge las novedades introducidas en cada uno de los módulos de ANA versión 3.0, así como las mejoras y nuevas funcionalidades implementadas atendiendo a dos objetivos fundamentales:

- Optimizar la experiencia de usuario y facilitar el uso de la aplicación.
- Potenciar la aplicación ampliando sus capacidades.

2. DESCRIPCIÓN FUNCIONAL

ANA 3.0 es una solución modular flexible que permite incrementar la capacidad de vigilancia y conocer la superficie de exposición de los sistemas de una organización. Con esta herramienta se pretende reducir los tiempos en la gestión de la seguridad, mediante una gestión eficiente de la detección de vulnerabilidades y de la notificación de alertas, así como ofrecer recomendaciones para un tratamiento oportuno de las mismas.

2.1 MÓDULOS FUNCIONALES

2.1.1 ANA Vulnerabilidades

El módulo permite la automatización y normalización de las auditorías, mediante una gestión eficiente de los procesos de auditoría, incrementando así la capacidad de vigilancia y el conocimiento de la superficie de exposición de una organización.

Sus características principales son:

- Soporte Multi-Tenant: el uso de espacios de trabajo permite aislar la información entre diferentes clientes, organismos, departamentos, etc. de una forma rápida y segura.
- Soporte de Multi-Factor de autenticación (MFA): la información está protegida mediante capas extras de seguridad en los procesos de inicio de sesión, donde se permiten múltiples sistemas de autenticación (certificado digital de cliente, usuario y contraseña y OTP).
- Gestión centralizada de usuarios: se manejan diferentes roles de usuario para adaptarse a las necesidades de la organización. Estos usuarios y roles pueden gestionarse en la propia solución o mediante la integración con servicios de directorio, haciendo uso del protocolo LDAP.
- Gestión de vulnerabilidades: ANA vulnerabilidades permite gestionar, categorizar y normalizar los resultados de diferentes tipos de auditorías manuales y automáticas, mostrando las pruebas de concepto de las evidencias y las recomendaciones para mitigar las

vulnerabilidades, haciendo uso de metodologías de cálculo de criticidad según el nivel de exposición.

- Incorpora las bases de datos del NIST de productos y vulnerabilidades.
- Análisis de impacto en negocio: la solución permite adaptar la criticidad técnica de las vulnerabilidades según el nivel de impacto del activo y servicio al que afecta, logrando de este modo priorizar los esfuerzos en el plan de remediación.

2.1.1.1 Novedades incluidas en ANA 3.0

Los cambios principales en esta versión respecto a la anterior son:

- Mejora en la gestión de permisos y niveles de acceso gracias a los nuevos roles implementados.
- Mejora en el control, flexibilidad y gestión de las auditorías por medio de una configuración centralizada.
- Mejoras en los procesos de importación que incrementan la capacidad de normalización de los resultados provenientes de varias fuentes.
- Mejora en el proceso de seguimiento de vulnerabilidades, permitiendo al usuario interactuar con las mismas.
- Rediseño gráfico y homogeneización de la experiencia de usuario.

2.1.2 ANA Mejora continua

ANA IMPLEMENTACIONES ha cambiado su nombre a ANA MEJORA CONTINUA (CIS, por sus siglas en inglés Continuous Improvement System).

Permite el seguimiento de los procesos de inspección técnicos formales y conocer el estado de acreditación de los sistemas de la información. Permite la gestión de hallazgos identificados en las inspecciones y evaluar las conformidades técnicas resultantes, que permitirían observar el cumplimiento de compromisos y los procesos de seguridad continua.

El módulo centraliza la gestión del proceso de inspección técnica, dando soporte al mismo mediante las siguientes fases en las que los diferentes actores (Inspector/Cliente) interactúan:

1. Fase de configuración y gestión de hallazgos:

Inspector:

- Se encarga de la creación de los activos fundamentales.
- Introduce los hallazgos en base a las tablas de remediación:
 - a. Corto plazo.
 - b. Medio plazo.

c. Largo plazo.

Cliente:

- Valida los hallazgos y los acepta o rechaza.
- Introduce la información de correcciones sobre los hallazgos encontrados, incluyendo los mecanismos de corrección aplicados.

2. Fase de seguimiento y evaluación del sistema:

Inspector:

- Valida la remediación del hallazgo.
- Hace seguimiento del estado de hallazgos y determina el cumplimiento de medidas a corto, medio y largo plazo.
- El inspector determinará si en función de los resultados el sistema con respecto a la acreditación es:
 - a. Apto.
 - b. No apto.
 - c. Apto provisional.

Cliente:

- En este punto, tendrá conocimiento de los tiempos para los cuales un sistema ha sido acreditado y cuando se requiere la re-acreditación del mismo.

2.1.2.1 Novedades incluidas en ANA 3.0

Los cambios principales en la nueva versión del módulo de Mejora continua respecto a la anterior son:

- Ampliación de roles, incrementando el grado de granularidad en el manejo de las vulnerabilidades detectadas.

2.1.3 CLARA

El módulo de CLARA integrado en ANA permite llevar a cabo la evaluación de cumplimiento técnico alineado con diferentes normativas.

Adicionalmente a la valoración de si un activo o conjunto de ellos cumplen con las condiciones técnicas estipuladas, bien vengán definidas por guías técnicas como las CCN-STIC o bien por regulaciones internas de una organización, ofrece información de relevancia que puede ser válida para otros procesos operacionales de seguridad.

Entre dicha información cabe destacar la posibilidad de obtener los programas instalados, histórico de uso del activo, actividad de los usuarios, navegación, aplicaciones lanzadas, procesos en ejecución o conexiones activas, entre otras.

2.1.3.1 Novedades incluidas en ANA 3.0

Los cambios principales en la nueva versión del módulo de CLARA respecto a la anterior son:

- Ampliación de roles, incrementando el grado de granularidad en el manejo de auditorías de conformidad.
- Rediseño gráfico y homogeneización de la experiencia de usuario.

3. NUEVAS FUNCIONALIDADES

3.1 NUEVAS FUNCIONALIDADES ATENDIENDO A LA EXPERIENCIA DE USUARIO

3.1.1 Nuevo interfaz gráfico

Se ha incidido en la unificación de estilos para poder mantener una apariencia similar en los distintos módulos que componen la aplicación. Este nuevo interfaz gráfico cuenta con una elección de gama de colores, optimización del espacio y mejora en la disposición de algunos elementos, facilitando la lectura y el trabajo al usuario *pentester*.

Cabe destacar el nuevo diseño *responsive*, que facilita y mejora notablemente la experiencia de usuario al no tener que desplazarse horizontalmente para poder visualizar los datos, dado que se pueden ver en “una sola pantalla”.

3.1.1.1 Cambios generales

La gama de colores en la pantalla de autenticación está basada en azul y blanco, con un diseño más atractivo e intuitivo en los campos de usuario y contraseña.

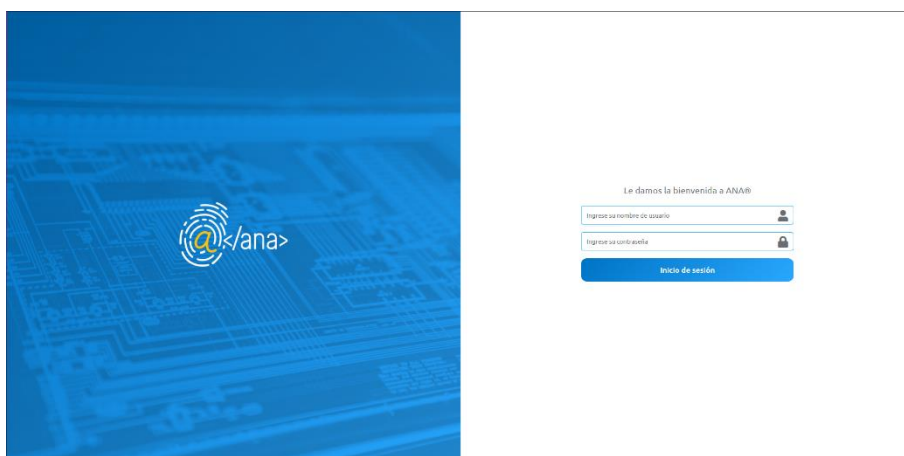


Ilustración 1. Pantalla de autenticación.

Le damos la bienvenida a ANA®

NOMBRE DE USUARIO

Ingrese su nombre de usuario

CONTRASEÑA

Ingrese su contraseña

Inicio de sesión

Ilustración 2. Campo usuario seleccionado.

Le damos la bienvenida a ANA®

Ingrese su nombre de usuario

CONTRASEÑA

Ingrese su contraseña

Inicio de sesión

Ilustración 3. Campo contraseña seleccionado.

Cuando el usuario accede a la aplicación con sus credenciales, se puede observar la disposición de los elementos en las barras de navegación:

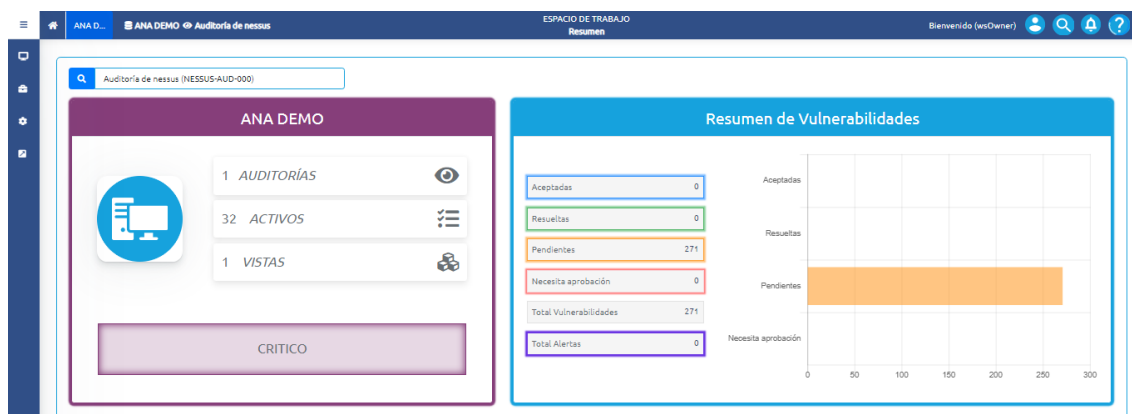


Ilustración 4. Pantalla de inicio backend.

La barra de navegación superior cuenta en la parte izquierda con la navegación de la página, el espacio de trabajo y la auditoría seleccionada:



Ilustración 5. Barra de navegación superior.

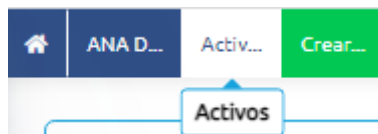
Al navegar por la aplicación, en las pantallas de crear y editar, el fondo del elemento de la navegación que indica la pantalla en la que se encuentra el usuario cambia a verde o amarillo respectivamente:



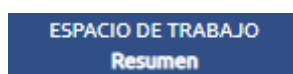
Ilustración 6. Barra de navegación crear.

*Ilustración 7. Barra de navegación editar.*

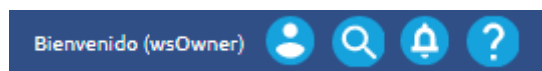
Además, estos elementos cuentan con ayuda contextual:

*Ilustración 8. Texto completo mostrado en la ayuda.*

En la parte central de la barra de navegación, se encuentra la sección y la subsección en la que se encuentra el usuario:

*Ilustración 9. Apartado sección y subsección.*

Finalmente, en la parte derecha se localizan el mensaje de bienvenida al usuario y botones de acciones:

*Ilustración 10. Botones de acciones.*

En la barra de navegación lateral, se encuentran los iconos que permiten al usuario navegar por las distintas secciones de la aplicación:

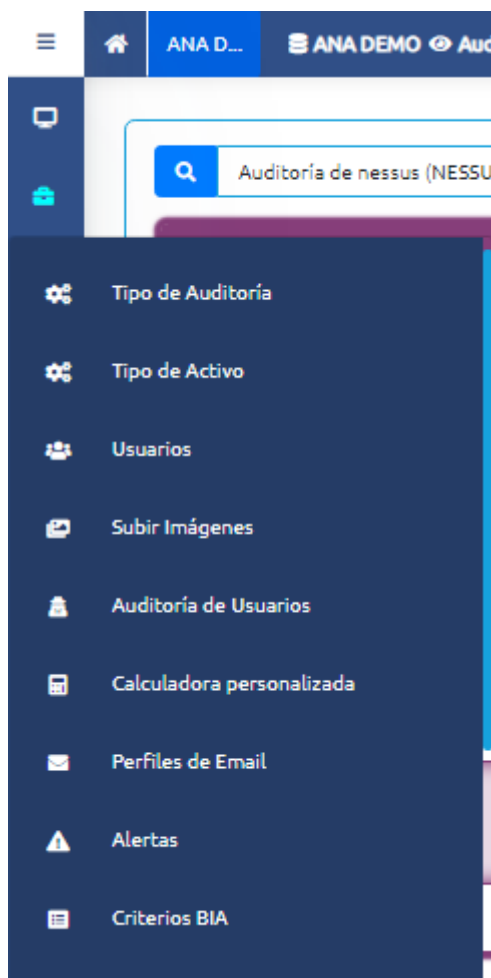


Ilustración 11. Barra de navegación lateral.

3.1.1.2 Cambios gráficos en tablas

Las tablas son uno de los elementos más importantes a la hora de tener un buen diseño, dado que la mayor parte de los datos de esta aplicación se muestran en tablas. Por este motivo, las tablas deben ser elementos fáciles de visualizar e intuitivos.

Como se puede observar en la siguiente imagen, las tablas cuentan con una combinación de colores que permiten visualizar rápidamente:

- Qué dato hay en cada columna.
- Qué hace cada filtro y si está activado o desactivado.
- La acción de los botones de la tabla de operaciones.
- La información necesaria de la tabla, cuántos registros se están mostrando y la paginación.

Filtrar por: Origen Auditoría ☒ Tipo de Auditoría ☐ Activo ☐

CRITICIDAD	NOMBRE	ID SECUNDARIO	ID DE CLIENTE	IP	TIPO DE ACTIVO	Nº COMPS.	Nº VULN.	OPERACIONES
CRITICAL	10.12.17.199	101217199	101217199	10.12.17.199	Server	20	19	CPE  
CRITICAL	10.12.17.198	101217198	101217198	10.12.17.198	Server	23	20	CPE  
CRITICAL	10.12.17.157	101217157	101217157	10.12.17.157	Server	18	27	CPE  
HIGH	liferay01.mju.es	101217155	101217155	10.12.17.155	Server	10	7	CPE  
HIGH	gridshare03.mju.es	101217203	101217203	10.12.17.203	Server	17	18	CPE  
HIGH	gridporta04.mju.es	101217205	101217205	10.12.17.205	Server	10	8	CPE  
HIGH	gridporta02.mju.es	101217201	101217201	10.12.17.201	Server	17	32	CPE  
HIGH	gridporta01.mju.es	101217200	101217200	10.12.17.200	Server	17	29	CPE  
HIGH	10.12.17.167	101217167	101217167	10.12.17.167	Server	12	8	CPE  
HIGH	10.12.17.165	101217165	101217165	10.12.17.165	Server	12	8	CPE  
HIGH	10.12.17.164	101217164	101217164	10.12.17.164	Server	12	8	CPE  
HIGH	10.12.17.162	101217162	101217162	10.12.17.162	Server	12	8	CPE  
HIGH	10.12.17.161	101217161	101217161	10.12.17.161	Server	12	8	CPE  
MEDIUM	SVR-HV-06	172161003	172161003	172.16.100.3	Server	10	5	CPE  
MEDIUM	SVR1	1721610061	1721610061	172.16.100.61	Server	7	1	CPE  

1 to 15 of 32

MTD. DE TIPOS DE ACTIVO

1 2 3 Next

NUEVO ATRAS

Ilustración 12. Ejemplo de tabla mostrando activos.

Observando estos elementos más detalladamente:

- Los filtros tienen una disposición sencilla e intuitiva para el usuario:

Filtrar por: Origen Auditoría ☒ Tipo de Auditoría ☐ Activo ☐

Ilustración 13. Detalle de filtros disponibles.

- Los nombres de las columnas cuentan con un buen contraste que facilita la lectura:

CRITICIDAD	NOMBRE	ID SECUNDARIO
------------	--------	---------------

Ilustración 14. Detalle de campos de tabla.

- Los botones de la tabla de operaciones tienen colores asociados a su acción, además de una ayuda contextual que indica qué acción realiza o por qué no se puede realizar:



Ilustración 15. Acción del botón mostrada en la ayuda.

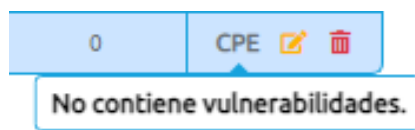


Ilustración 16. Detalle explicativo en diálogo.

3.1.1.3 Cambios gráficos en formularios

Los campos de los formularios se encuentran en una disposición óptima respecto a la etiqueta (nombre del campo) y el input que, junto al diseño de los botones, facilitan la experiencia de usuario.

Formulario de detalle de formulario con los siguientes campos:

- PERSONA AL CARGO (Owner)
- ID SECUNDARIO
- ID DE CLIENTE
- NOMBRE
- TIPO DE ACTIVO (Selecione un Tipo de Activo --)
- IP
- PROPÓSITO
- DESCRIPCIÓN

Botones: ACEPTAR, CANCELAR

Ilustración 17. Detalle de formulario.

En caso de que el usuario olvide rellenar alguno de los campos requeridos, obtendrá un mensaje o se colorearán los bordes y el nombre de la etiqueta, dependiendo de la complejidad del formulario.

ID SECUNDARIO

Campo obligatorio.

Ilustración 18. Error mostrado al usuario en mensaje.

CATEGORÍA

-- Elija una opción --

Ilustración 19. Error mostrado al usuario por color.

Además, los formularios más complejos (vulnerabilidades), cuentan con una ayuda extra en la que se indica en qué pestaña se encuentra un posible error de validación:

Formulario de identificación con las siguientes pestañas:

- RESUMEN
- DETALLES
- CVE
- CALCULADORA

Campos de identificación:

- PID (PID)
- MODO (Caja Blanca)
- CATEGORÍA (Elija una opción --)
- PRUEBA (Elija una opción --)

Indicadores de error:

- 0
- 5
- 0

Ilustración 20. Error mostrado al usuario en la pestaña.

Respecto a la disposición de los campos en los formularios, el nuevo formato es más cómodo para el usuario, optimiza el espacio y da una sensación de uniformidad que supone una gran mejora para la experiencia de usuario.

3.1.1.4 Cambios gráficos en cuadros modales

Los cuadros modales siguen la misma dinámica que el resto de la aplicación, se ha desarrollado un estilo sencillo para la visualización del usuario y con optimización del espacio y las proporciones.

CREAR NUEVO CPE PERSONALIZADO

☒ SOLO VULNERABILIDADES PENDIENTES ☐ CREAR NUEVA VERSIÓN

FABRICANTE
custom-cpe

PRODUCTO
NOMBRE FRAMEWORK

VERSIÓN
18.0.5.12

GUARDAR CANCELAR

Ilustración 21. Detalle de modal.

En caso de que la acción que se vaya a realizar en el cuadro modal pueda tener alguna consecuencia, se muestran mensajes de advertencia.

CREAR NUEVA INSTANTÁNEA DE BASE DE DATOS

NOMBRE

DESCRIPCIÓN

¡IMPORTANTE! Crear o restaurar la base de datos del workspace actual en otra base de datos eliminará las conexiones de los usuarios activos en las bases de datos origen y destino hasta que el proceso finalice.

Todas las tareas activas serán canceladas. Por favor, comuníquelo a los usuarios antes de proceder.

¡ATENCIÓN! ¡LA BASE DE DATOS CON EL NOMBRE DESTINO SERÁ DESTRUIDA Y REGENERADA CON TODOS LOS OBJETOS DE LA INSTANTÁNEA RESTAURADA!

ACEPTAR CANCELAR

Ilustración 22. Modal con información explicativa.

3.1.1.5 Otros cambios

3.1.1.5.1 Indicativo de carga de datos

Se ha implementado un sistema que consiste en mostrar una imagen de carga de datos en aquellas llamadas que consumen más tiempo de procesamiento, indicando al usuario que la aplicación está trabajando.

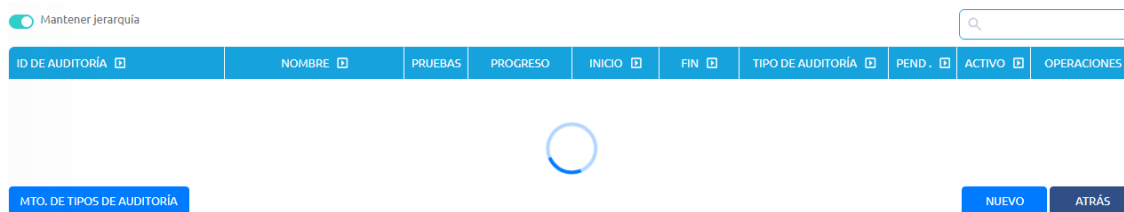


Ilustración 23. Indicativo de carga de datos en pantalla.

3.1.1.5.2 Pantalla de carga de imágenes

Se ha mejorado el diseño existente de la pantalla de carga de imágenes de versiones previas:

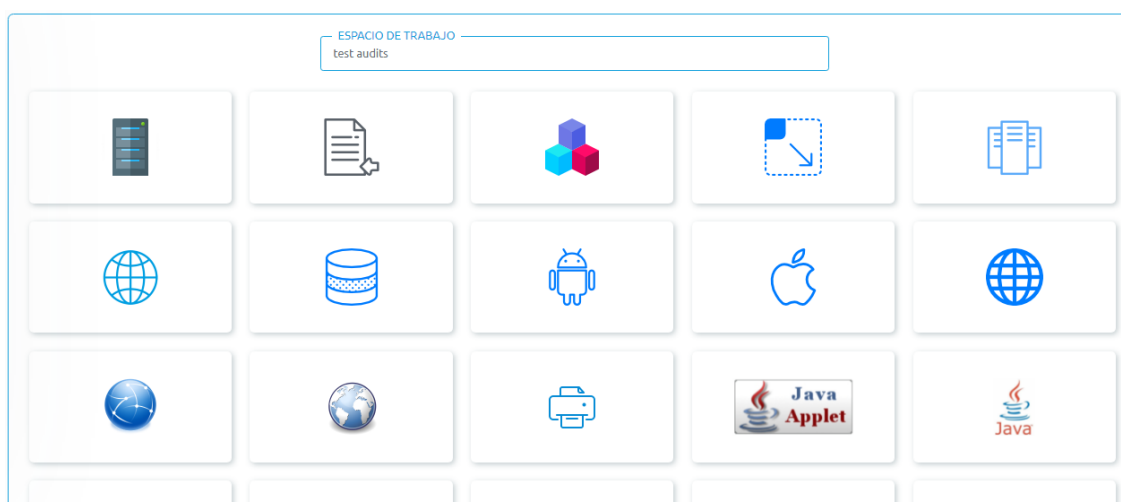


Ilustración 24. Nueva pantalla de imágenes.

3.1.1.5.3 CLARA

En CLARA se ha aplicado el nuevo interfaz gráfico, manteniendo la armonía de colores y adaptándola para una mejor visualización y comprensión.

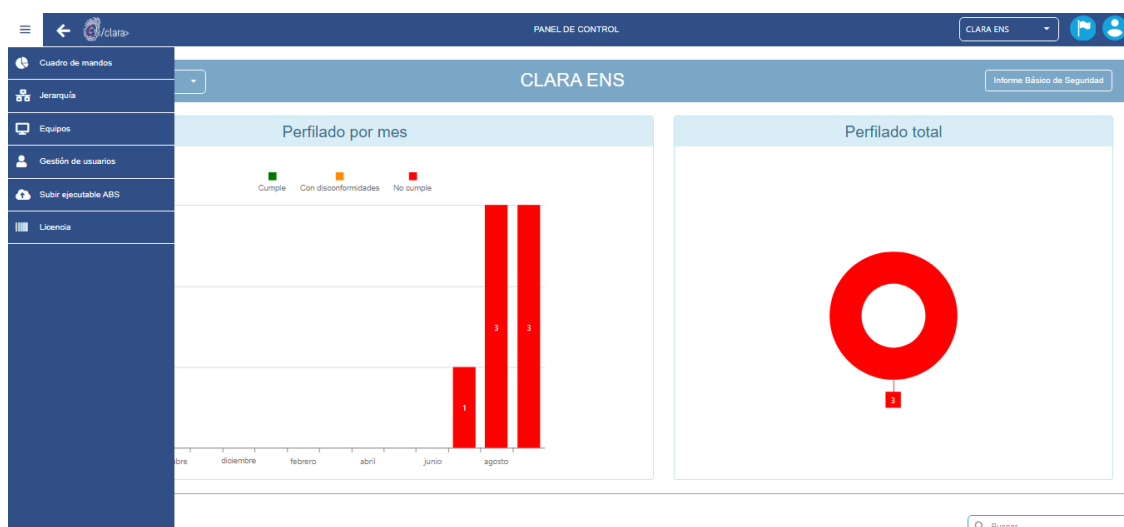


Ilustración 25. Detalle de pantalla de CLARA.

3.1.2 Nuevo selector de módulo basado en roles

Cuando un usuario tiene roles que le permiten acceder a varios módulos, se ha implementado una pantalla de selector de módulo a la que se accede inmediatamente después de introducir las credenciales.

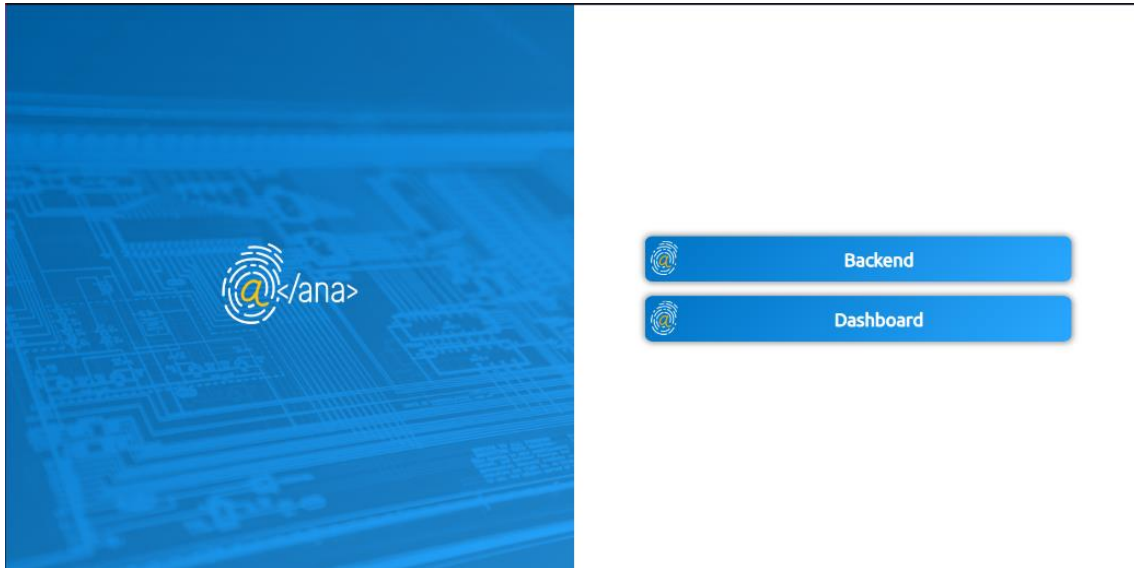


Ilustración 26. Pantalla de selector de módulo.

3.1.3 Nuevo campo para búsqueda de auditorías en la pantalla de resumen del Backend

Para facilitar al usuario la selección de una auditoría, se ha implementado un campo de búsqueda de auditorías en la pantalla de resumen.

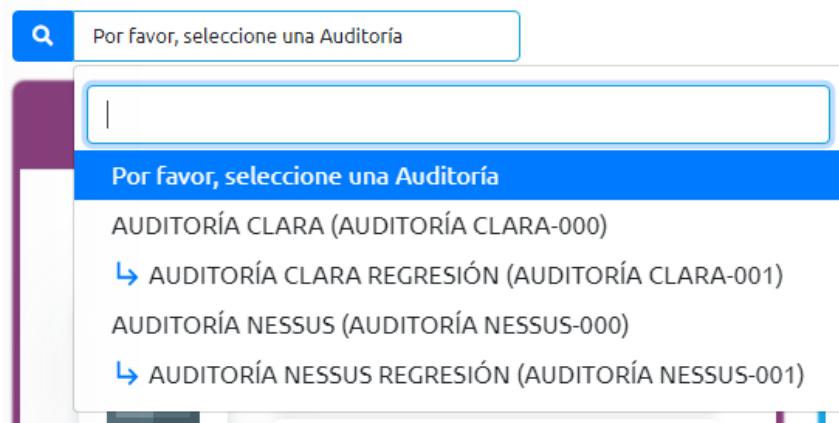


Ilustración 27. Campo de búsqueda seleccionado.

En caso de que el usuario tenga permisos en varias auditorías, se puede realizar una búsqueda por nombre o identidad de auditoría.



Ilustración 28. Campo de búsqueda con texto introducido.

3.2 NUEVAS FUNCIONALIDADES RELACIONADAS CON LA POTENCIACIÓN DE LA APLICACIÓN

3.2.1 Nuevos roles asociados a funcionalidades

La versión 3.0 de ANA incorpora nuevos roles y agrupamiento de funciones con respecto a funcionalidades anteriores. Este apartado recoge la correspondencia de roles comparándolos con los existentes en versiones anteriores.

A la hora de crear un usuario para un espacio de trabajo, se le podrán asignar diferentes roles dependiendo de los módulos activos en el espacio de trabajo.

NOMBRE DE USUARIO
Nombre de Usuario

EMAIL
Ingrese su Email

CONTRASEÑA
Ingrese su contraseña

CONFIRMAR CONTRASEÑA
Confirme su contraseña

SELECCIONA LOS ROLES DEL USUARIO

ANA

- ☐ PenTester
- ☐ Business
- ☐ Viewer
- ☐ WSOwner

MEJORA CONTINUA

- ☐ CIS Administrator
- ☐ CIS Auditor
- ☐ CIS Viewer

CLARA

- ☐ Clara Administrator
- ☐ Clara Business
- ☐ Clara Auditor
- ☐ Clara Viewer

ACEPTAR **LIMPIAR** **CANCELAR**

Ilustración 29. Cuadro modal de creación de usuario y asignación de roles.

Nota: MEJORA CONTINUA corresponde al módulo denominado ANA IMPLEMENTACIONES en las versiones anteriores. Su acrónimo en inglés CIS (Continuous Improvement System).

3.2.1.1 Correspondencia entre roles nuevos y versiones anteriores

Los roles de ANA-Vulnerabilidades se mantienen con su funcionalidad.

Será necesario reasignación de roles si se desea trabajar con los módulos de CLARA y Mejora continua.

3.2.1.1.1 CLARA

- Owner + Viewer pasa a ser CLARA Administrator.
- Pentester pasa a ser CLARA Auditor.

- Business pasa a ser CLARA Business.
- Viewer pasa a ser CLARA Viewer.

3.2.1.1.2 Mejora continua.

- Owner pasa a ser CIS Administrator.
- Pentester pasa a ser CIS Auditor.
- Viewer pasa a ser CIS Viewer.

3.2.1.2 Roles de usuario en función del módulo

3.2.1.2.1 ANA Vulnerabilidades

3.2.1.2.1.1 Administrador

- Espacios de trabajo:
 - Visualizar lista.
 - Crear.
 - Habilitar Módulos:
 - Mejora continua.
 - CLARA.
 - Editar.
 - Habilitar Módulo:
 - Mejora continua.
 - CLARA.
- Usuarios (Administrator, WSAdmin y ABS Administrator):
 - Visualizar.
 - Crear.
 - Editar (también a sí mismo).
 - Resetear contraseña (también a sí mismo).
 - Resetear segundo factor de autenticación (también a sí mismo).
 - Eliminar.
- Imágenes:
 - Visualizar.
 - Subir.
 - Eliminar.
- Configuraciones:
 - Importaciones (valores por defecto de la configuración de importaciones).
 - LDAP.
 - Autenticación.

3.2.1.2.1.2 WSAdmin

- Espacios de trabajo (de los que es administrador):
 - Visualizar.
 - Acceder.

- Usuarios (de los espacios de trabajo de los que es administrador):
 - Visualizar.
 - Crear.
 - Editar.
 - Desbloquear.
 - Resetear contraseña.
 - Resetear segundo factor de autenticación.
 - Eliminar.
- Auditoría de usuarios:
 - Visualizar registro de operaciones en un rango de fechas.
 - Descargar el registro en CSV.
- Imágenes (de los espacios de trabajo de los que es administrador):
 - Visualizar.
 - Subir.
 - Eliminar.
- Calculadora personalizada:
 - Visualizar.
 - Editar valores.
- Certificados:
 - Visualizar.
 - Crear y Descargar.
 - Editar (Nombre y contraseña. Necesario volver a generarlo).
 - Borrar/Invalidar.
 - Consultar la fecha de expiración.
- Perfiles de email (con espacio de trabajo seleccionado):
 - Visualizar.
 - Crear.
 - Editar.
 - Borrar.
- Alertas (con espacio de trabajo seleccionado y perfiles de email creados).
 - Visualizar.
 - Crear.
 - Editar.
 - Borrar.
- Auditorías:
 - Visualizar.
 - Visualizar pruebas.
 - Activos:
 - Visualizar.
 - Leer.
- Activos:
 - Visualizar.
 - Leer.
- Componentes:

- Visualizar.
 - Leer.
- Vulnerabilidades:
 - Visualizar.
 - Leer.
- Vistas:
 - Visualizar.
 - Leer.
 - Visualizar árbol (leer).

3.2.1.2.1.3 WSOwner:

- Gestión Usuarios (del espacio de trabajo del que es propietario):
 - Visualizar.
 - Crear.
 - Editar.
 - Desbloquear.
 - Resetear contraseña.
 - Resetear segundo factor de autenticación.
 - Eliminar.

Nota: Todas estas acciones también puede realizarlas para sí mismo.

- Auditoría de usuarios (del espacio de trabajo del que es propietario):
 - Visualizar registro de operaciones en un rango de fechas.
 - Descargar el registro en CSV.
- Imágenes (del espacio de trabajo del que es propietario):
 - Visualizar.
 - Subir.
 - Eliminar.
- Calculadora personalizada:
 - Editar valores.
- Perfiles de email:
 - Visualizar.
 - Crear.
 - Editar.
 - Borrar.
- Alertas (con perfiles de email creados):
 - Visualizar.
 - Crear.
 - Editar.
 - Borrar.
- Criterios BIA:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.

- Servicios BIA:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
- Snapshot:
 - Visualizar.
 - Crear.
 - Restaurar.
- Elementos borrados:
 - Restaurar activo (solo activo o con componentes y vulnerabilidades).
 - Restaurar componente (solo componente o con vulnerabilidades).
 - Restaurar vulnerabilidad.
- Aprobación masiva de vulnerabilidades:
 - Visualizar activos con vulnerabilidades pendientes.
 - Aprobar todas las vulnerabilidades pendientes de aprobación de un activo.
 - Visualizar componentes con vulnerabilidades pendientes.
 - Aprobar todas las vulnerabilidades pendientes de aprobación de un componente.
 - Visualizar vulnerabilidades pendientes.
 - Aprobar una vulnerabilidad pendiente de aprobación.
 - Visualizar vulnerabilidades pendientes desde la última actualización del NIST.
 - Añadir vulnerabilidades pendientes desde la última actualización del NIST.
- Auditorías:
 - Visualizar.
 - Visualizar pruebas.
 - Acceder a pantalla tipo de auditoría.
- Tipo de Auditoría:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
 - Acceder a las categorías de un tipo de auditoría.
- Categorías:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
 - Acceder a las pruebas de una categoría.
- Pruebas:

- Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
- Activos:
 - Visualizar.
 - Crear.
 - Editar y Leer
 - Crear CPE.
 - Eliminar.
 - Acceder a la pantalla de tipo de activo.
- Tipo de activo:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
- Componentes:
 - Visualizar.
 - Crear.
 - Editar y Leer.
 - Crear CPE.
 - Eliminar.
- Vulnerabilidades:
 - Visualizar.
 - Crear.
 - Editar y Leer.
 - Multiplicar.
 - Eliminar.
- Vistas:
 - Visualizar.
 - Crear.
 - Editar.
 - Visualizar árbol.
 - Crear y Modificar árbol.
 - Añadir grupo.
 - Vincular servicio con preguntas y respuestas a un grupo.
 - Añadir activo.
- Nessus:
 - Visualizar ficheros importados.
 - Importar fichero.
 - Consultar información de importación.
 - Descargar ficheros JSON:
 - Anonimizados.
 - Contadores.
 - Validaciones.

- Filtración.
 - Agrupación.
 - Ignorados.
- Nmap:
 - Visualizar ficheros importados.
 - Importar fichero.
 - Consultar información de importación.
 - Descargar ficheros JSON.
 - Anonimizados:
 - Contadores.
 - Validaciones.
 - Filtración.
 - Agrupación.
 - Ignorados.
- CLARA:
 - Visualizar ficheros importados.
 - Importar:
 - Seleccionando fichero.
 - Sin seleccionar (se conecta a la instancia por defecto de CLARA).
 - Consultar información de importación.
 - Tarea programada.
- EMMA:
 - Visualizar ficheros importados.
 - Importar fichero.
 - Consultar información de importación.
 - Descargar ficheros JSON:
 - Ignorados.
 - Resultados.
- CMDB:
 - Visualizar ficheros importados.
 - Importar fichero.
 - Consultar información de importación.
 - Configuraciones.
- LDAP.

3.2.1.2.1.4 Pentester:

- Auditorías:
 - Visualizar.
 - Visualizar pruebas.
 - Actualizar estado de pruebas (seleccionar cuál hay que hacer y cuál está hecha).
- Activos:
 - Visualizar.
 - Crear.

- Editar y Leer.
 - Eliminar.
- Componentes:
 - Visualizar.
 - Crear.
 - Editar y Leer.
 - Eliminar.
- Vulnerabilidades:
 - Visualizar.
 - Crear.
 - Editar y Leer.
 - Multiplicar.
 - Eliminar.
- Nessus:
 - Visualizar ficheros importados.
 - Importar fichero.
 - Consultar información de importación.
 - Descargar ficheros JSON:
 - Anonimizados.
 - Contadores.
 - Validaciones.
 - Filtración.
 - Agrupación.
 - Ignorados.
- Nmap:
 - Visualizar ficheros importados.
 - Importar fichero.
 - Consultar información de importación.
 - Descargar ficheros JSON:
 - Anonimizados.
 - Contadores.
 - Validaciones.
 - Filtración.
 - Agrupación.
 - Ignorados.
- CLARA:
 - Visualizar ficheros importados.
 - Importar:
 - Seleccionando fichero.
 - Sin seleccionar, se conecta a la instancia por defecto de CLARA.
 - Consultar información de importación.
 - Tarea Programada.
- EMMA:
 - Visualizar ficheros importados.

- Importar fichero.
 - Consultar información de importación.
 - Descargar ficheros JSON:
 - Ignorados.
 - Resultados.
- CMDB:
 - Visualizar ficheros importados.
 - Importar fichero.
 - Consultar información de importación.

3.2.1.2.1.4.1 Pentester approver:

Todas las acciones del pentester, añadiendo o modificando:

- Auditorías:
 - Aprobar vulnerabilidades pendientes.
- Activos:
 - Crear CPE.
 - Componentes.
 - Crear CPE.
- Vulnerabilidades:
 - Editar.
 - Aprobar vulnerabilidad pendiente.

3.2.1.2.1.4.2 Pentester need approval:

Todas las acciones del Pentester, añadiendo o modificando:

- Vulnerabilidades.
- Crear (crea las vulnerabilidades como “Pendiente de aprobación”).

3.2.1.2.1.4.3 Pentester audit manager:

Todas las acciones del pentester, añadiendo o modificando:

- Auditorías:
 - Crear.
 - Editar.
 - Cambiar activos.
 - Dar permisos a usuarios.
 - Desactivar.
 - Eliminar.

3.2.1.2.1.5 Business:

- Vistas:
 - Visualizar.
 - Crear.
 - Editar.

- Visualizar árbol.
- Crear o modificar árbol.
- Añadir Grupo.
- Vincular servicio con preguntas y. respuestas a un grupo.
- Añadir activo.

3.2.1.2.1.6 Viewer:

- Visualizar el dashboard.
- Servicios BIA:
 - Activar o desactivar.
- Informes:
 - Generar informe:
 - De la vista:
 - Técnico.
 - Ejecutivo.
 - Auditoría.
- KPI:
 - Visualizar.
- Vulnerabilidades:
 - Descargar CSV.
 - Visualizar detalles.
 - Vulnerabilidades más comunes.
 - Descargar CSV.
 - CVE más comunes.
 - Descargar CSV.
- Componentes:
 - Descargar CSV.
- Auditorías intervinientes (en un activo).
 - Descargar CSV.

3.2.1.2.1.6.1 Solver:

Todas las acciones del Viewer, añadiendo o modificando:

- Vulnerabilidades.
 - Marcar para revisión.

Roles	Administrador	WSAdmin	WSOwner	Pentester	Pentester Approver	Pentester Need Approval	Pentester Audit Manager	Business	Viewer	Viewer Solver
Gestión de Acceso										
Acceso a Backend	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Acceso a Dashboard	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓
Acceso a la Gestión de Activos	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗
Acceso a la Gestión de Auditorías	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗
Acceso a la Gestión de Componentes	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗
Acceso a la Gestión de Vistas	✗	✓	✓	✗	✗	✗	✗	✓	✗	✗
Acceso a la Gestión de Vulnerabilidades	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗
Acceso a la Zona de Administración	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Acceso a la Zona de Inicialización	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Acceso a la Zona de Trabajo	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗
Gestión de entidades										
Creación, Edición y Eliminación de Categorías	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Creación, Edición y Eliminación de Componentes	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗
Creación, Edición y Eliminación de Definiciones de Alerta	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Creación, Edición y Eliminación de Perfiles de Email	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Creación, Edición y Eliminación de Pruebas	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Creación, Edición y Eliminación de Tipos de Activos	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Creación, Edición y Eliminación de Tipos de Auditoría	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Creación, Edición y Eliminación de un Activo	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗

Roles	Administrador	WSAdmin	WSOwner	Pentester	Pentester Approver	Pentester Need Approval	Pentester Audit Manager	Business	Viewer	Viewer Solver
Creación, Edición y Eliminación de una Auditoría	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
Creación, Edición y Eliminación de una Vista	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗
Creación, Edición y Gestión de Espacios de Trabajo	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Creación, Edición y Eliminación de Criterios BIA	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Creación, Edición y Eliminación de Servicios BIA	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Importación de Ficheros										
Importación de Imágenes	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Importación de Nessus	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗
Importación de Nmap	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗
Importación de CLARA	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗
Importación de EMMA	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗
Importación de CMDB	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗
Gestión de usuarios										
Creación y Edición de Usuarios	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
Creación y Edición de Usuarios Administradores	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Creación y Edición de Usuarios WSAdmin	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Creación de Usuarios WSOwner	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Creación, Edición y Eliminación de Usuarios Business	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Creación, Edición y Eliminación de Usuarios Pentester	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Creación, Edición y Eliminación de Usuarios Viewer	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Edición del propio Usuario: Cambio de contraseña	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Edición del propio Usuario: Reseteo de contraseña	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗

Roles	Administrador	WSAdmin	WSOwner	Pentester	Pentester Approver	Pentester Need Approval	Pentester Audit Manager	Business	Viewer	Viewer Solver
Edición y Eliminación de Usuarios WSOwner	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Configuraciones										
Configuración inventariado de	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗
Configuración autoevaluación de	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗
Configuración LDAP	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗
Configuración importaciones de	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗
Configuración del Login	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Otras Tareas										
Realización y restauración de Snapshots	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Administración de objetos borrados	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Aprobación masiva de vulnerabilidades	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Gestión de Certificados	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
Gestión de Calculadora personalizada	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗
Gestión de Auditoría de usuarios	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗

3.2.1.3 Nuevos roles en ANA

3.2.1.3.1 AuditManager

El rol de AuditManager está pensado para gestionar auditorías, desde su creación hasta su edición, así como la asignación de los pentester a las mismas.

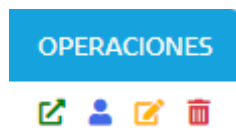


Ilustración 30. Operaciones disponibles de un AuditManager.

3.2.1.4 Nuevos roles en módulo de Mejora continua (CIS)

3.2.1.4.1 CIS Administrator

Puede crear sistemas, programas y hallazgos desde el Backend:

- Sistemas/Programas:
 - Crear.
 - Editar.
 - Eliminar.
- Hallazgos:
 - Crear.
 - Editar.
 - Eliminar.

3.2.1.4.2 CIS Auditor

Puede crear hallazgos desde el Backend:

- Sistemas/Programas:
 - Ver.
- Hallazgos:
 - Crear.
 - Editar.
 - Eliminar.

3.2.1.4.3 CIS Viewer

Tiene acceso al Dashboard:

- Visualizar el Dashboard:
- Informes:
 - Generar.

Roles	CIS Administrator	CIS Auditor	CIS Viewer
Gestión de Acceso			
Acceso a Backend	✓	✓	✗
Acceso a Dashboard	✗	✗	✓
Acceso a la Gestión de Sistemas/Programas	✓	✓	✗
Acceso a la Gestión de Hallazgos	✓	✓	✗
Gestión de entidades			
Creación, Edición y Eliminación de Sistemas/Programas	✓	✗	✗
Creación, Edición y Eliminación de Hallazgos	✓	✓	✓

3.2.1.5 Nuevos roles en CLARA

3.2.1.5.1 CLARA Administrator

Puede realizar TODAS las acciones:

- Visualizar el panel de control.
- Análisis:
 - Visualizar.
 - Visualizar importación.
 - Importar.
- Jerarquías:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
- Equipos:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
 - Analizar.
 - Parar análisis.
- Plantillas de análisis:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
- Configuración de comunicación:

- Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
- Cumplimiento de CLARA:
 - Calcular.
- Catálogo de actualizaciones de seguridad de Microsoft:
 - Actualizar.
- Configuración de tareas programadas:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
- Configuración de alertas:
 - Editar
- Contactos:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
- Informes:
 - Visualizar.

3.2.1.5.2 CLARA Business

Puede realizar las siguientes acciones:

- Visualizar el panel de control.
- Análisis:
 - Visualizar.
- Jerarquías:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
- Equipos:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
- Plantillas de análisis:
 - Visualizar.
- Configuración de comunicación:
 - Visualizar.
 - Crear.
 - Editar.

- Eliminar.
- Cumplimiento de CLARA:
 - Calcular.

3.2.1.5.3 CLARA Auditor

Puede realizar las siguientes acciones:

- Visualizar el panel de control.
- Análisis:
 - Visualizar.
 - Visualizar importación.
 - Importar.
- Jerarquías:
 - Visualizar.
- Equipos:
 - Visualizar
 - Crear.
 - Editar.
 - Eliminar.
 - Analizar.
 - Parar análisis.
- Plantillas de análisis:
 - Visualizar.
 - Crear.
 - Editar.
 - Eliminar.
- Configuración de comunicación:
 - Visualizar.
- Configuración de tareas programadas:
 - Visualizar.
- Contactos:
 - Visualizar.

3.2.1.5.4 CLARA Viewer

Puede realizar las siguientes acciones:

- Visualizar el panel de control.
- Jerarquías:
 - Visualizar.
- Equipos:
 - Visualizar.

Roles	CLARA Administrator	CLARA Business	CLARA Auditor	CLARA Viewer
Gestión de acceso				
Acceso a Backend	✓	✓	✓	✓
Acceso a Dashboard	✓	✓	✓	✓
Acceso a la Gestión de Análisis	✓	✓	✓	✗
Acceso a la Gestión de Importación de Análisis	✓	✗	✓	✗
Acceso a la Gestión de Jerarquías	✓	✓	✓	✓
Acceso a la Gestión de Equipos	✓	✓	✓	✓
Acceso a la Gestión de Plantillas de Análisis	✓	✓	✓	✗
Acceso a la Gestión Configuración de Comunicación	✓	✓	✓	✗
Acceso a la Gestión de Cumplimiento de CLARA	✓	✓	✗	✗
Acceso a la Gestión de Configuración de Tareas Programadas	✓	✗	✓	✗
Acceso a la Gestión de Configuración de Alertas	✓	✗	✗	✗
Acceso a la Gestión de Contactos	✓	✗	✓	✗
Gestión de entidades				
Importación de Análisis	✓	✗	✓	✗
Visualización de Importaciones de Análisis	✓	✗	✓	✗
Creación, Edición y Eliminación de Jerarquías	✓	✓	✗	✗
Creación, Edición y Eliminación de Equipos	✓	✓	✓	✗
Análisis y Detención de Análisis de Equipos	✓	✗	✓	✗
Creación, Edición y Eliminación de Plantillas de Análisis	✓	✗	✓	✗
Creación, Edición y Eliminación de Configuración de comunicación	✓	✓	✗	✗
Calcular Cumplimiento de CLARA	✓	✓	✗	✗
Actualización del Catálogo de Actualizaciones de Seguridad de Microsoft	✓	✗	✗	✗
Creación, Edición y Eliminación de Configuración de Tareas Programadas	✓	✗	✗	✗
Edición de Configuración de Alertas	✓	✗	✗	✗
Creación, Edición y Eliminación de Contactos	✓	✗	✗	✗
Otras Tareas				
Visualización de Informes Técnicos	✓	✗	✗	✗

3.2.2 Autenticación y navegación por roles

Se ha implementado una nueva funcionalidad que permite el acceso a las aplicaciones sin tener que navegar de unas a otras, siempre y cuando el usuario solo

tenga el rol o roles asociados a una aplicación; en caso contrario, se mostrará el selector de aplicaciones mencionado anteriormente.

4. MEJORAS

Se han desarrollado mejoras asociadas a la experiencia de usuario y a la potenciación de la aplicación.

4.1 MEJORAS ATENDIENDO A LA EXPERIENCIA DE USUARIO

4.1.1 Pantalla de resumen del backend

Esta mejora se corresponde con el buscador de auditorías. Se ha incluido tanto en nuevas funcionalidades como en mejoras, ya que sigue siendo un selector de auditorías, pero se ha mejorado incluyendo una nueva funcionalidad que permite buscar las auditorías facilitando la selección de estas.

4.1.2 Simplificación de las ventanas de importación, obteniendo las opciones desde la auditoría

Como se ha visto en la creación y edición de auditorías, se pueden configurar las importaciones para cada auditoría. Además de las mejoras que esto supone a nivel de aplicación, es una gran ayuda para el usuario a la hora de importar ficheros de Nessus, CLARA, Nmap, EMMA o CMDB.

Antes solo se podían importar estos ficheros para auditorías de infraestructura en las que el usuario tenía permisos. Ahora se ha ampliado este rango a todas las auditorías, sin importar el tipo, en las que el usuario tiene permisos y tienen configurada dicha importación.

4.1.2.1 Nessus

Se permitirá elegir una auditoría que tenga habilitada la opción de importación de Nessus:

Ilustración 31. Modal de importación de Nessus.

Una vez seleccionada la auditoría, se cargarán los campos configurados en la misma. Se podrá modificar la fecha de detección de la vulnerabilidad:

Ilustración 32. Modal de importación de Nessus, campos rellenos.

4.1.2.2 NMAP

Se mostrarán las mismas opciones y funcionamiento que en la importación de Nessus:

*Ilustración 33. Modal de importación de NMAP.*

4.1.2.3 CLARA

Se mostrarán las mismas opciones y funcionamiento que en la importación de Nessus:

*Ilustración 34. Modal de importación de CLARA.*

4.1.2.4 EMMA

Se mostrarán las mismas opciones y funcionamiento que en la importación de Nessus:

The screenshot shows a web form titled "IMPORTAR ARCHIVO EMMA". It contains the following fields and controls:

- AUDITORÍA**: A dropdown menu with "DEMO-IMPORTACIONES" selected.
- FECHA DE DETECCIÓN DE LA VULNERABILIDAD**: A date input field showing "06/09/2021".
- MODO DE AUDITORÍA**: A dropdown menu with "CAJA NEGRA/GRIS" selected.
- ID .**: A text input field with "IP" entered.
- CREDENCIALES**: A toggle switch that is currently turned on.
- SOFTWARE**: A toggle switch that is currently turned on.
- VULN .**: A toggle switch that is currently turned on.
- SELECCIONE FICHERO DE EMMA**: A button to select a file.
- File type**: A text field showing "*.emma, *.json".
- IMPORTAR**: A blue button to import the file.
- CERRAR**: A red button to close the modal.

Ilustración 35. Modal de importación de EMMA.

4.1.2.5 CMDB

En este caso, se podrá seleccionar la auditoría que tiene habilitada la importación de CMDB:

The screenshot shows a web form titled "IMPORTAR ARCHIVO CMDB". It contains the following fields and controls:

- AUDITORÍA**: A dropdown menu with "DEMO-IMPORTACIONES" selected.
- MODO DE AUDITORÍA**: A dropdown menu with "CAJA NEGRA/GRIS" selected.
- CREDENCIALES**: A toggle switch that is currently turned on.
- SOFTWARE**: A toggle switch that is currently turned on.
- TIPO DE ESTRUCTURA**: A dropdown menu with "Posición" selected.
- SEPARADOR**: A text input field.
- TIPO DE ARCHIVO**: A dropdown menu with "Activos y Componentes" selected.
- ID DEL PADRE**: A text input field with the placeholder "Introduce numero ordinal".
- ID DE CLIENTE**: A text input field with the placeholder "Introduzca numero ordinal".
- ID SECUNDARIO**: A text input field with the placeholder "Introduzca numero ordinal".
- NOMBRE**: A text input field with the placeholder "Introduzca numero ordinal".
- DIRECCIÓN IP**: A text input field with the placeholder "Introduzca numero ordinal".
- PERSONA AL CARGO**: A text input field with the placeholder "Introduzca numero ordinal".
- TIPO DE ACTIVO**: A text input field with the placeholder "Introduzca numero ordinal".
- DESCRIPCIÓN**: A text input field with the placeholder "Introduzca numero ordinal".
- PROPÓSITO**: A text input field with the placeholder "Introduzca numero ordinal".
- SELECCIONE FICHERO DE CMDB**: A button to select a file.
- File type**: A text field showing "*.csv".
- IMPORTAR**: A blue button to import the file.
- CERRAR**: A red button to close the modal.

Ilustración 36. Modal de importación de CMDB.

4.2 MEJORAS RELACIONADAS CON LA POTENCIACIÓN DE LA APLICACIÓN

4.2.1 Auditorías padres y de regresión pueden ser de diferente tipo

Se ha eliminado la restricción de que la auditoría padre y la de regresión sean del mismo tipo, dando un margen más amplio a la hora de realizar auditorías de regresión.

ID DE AUDITORÍA	NOMBRE	PRUEBAS
AUDITORÍA NESSUS (000)	AUDITORÍA NESSUS	Pruebas
AUDITORÍA NESSUS (001)	AUDITORÍA NESSUS REGRESIÓN	Pruebas
AUDITORÍA NESSUS (002)	AUDITORÍA NESSUS REGRESIÓN	Pruebas

PROGRESO	INICIO	FIN	TIPO DE AUDITORÍA
	06/09/2021	07/09/2022	Auditoría iOS
	06/09/2021	07/09/2022	Auditoría iOS
	06/09/2021	07/09/2022	Auditoría Android

Ilustración 37. Auditoría padre y sus dos auditorías de regresión.

4.2.2 Unificación de los procesos de importaciones

Se han unificado los procesos de importación de Nessus, CLARA, Nmap, EMMA y CMDB, consiguiendo que todas las importaciones tengan el mismo flujo de procesado, diferenciando los aspectos singulares de cada una de ellas.

4.2.3 Ampliación de la funcionalidad de creación y edición de auditorías permitiendo configurar los parámetros de las distintas importaciones

Se ha ampliado la funcionalidad de la creación y edición de auditorías:

- Añadiendo la configuración de las importaciones (recuadrado en rojo) dentro de cada una de ellas, enfocado a la automatización de auditorías dentro de la aplicación.
- Añadiendo un campo “Número de secuencia” compuesto por 3 números (recuadrado en verde):
 - Si una auditoría no tiene auditoría padre, el valor de este campo será 000.
 - Si una auditoría tiene padre, el valor de este campo aumentará de 1 en 1 por cada auditoría de regresión de dicha auditoría padre. (Si es la primera hija, será 001, si es la segunda, 002 y así sucesivamente).

- Se ha modificado el campo “Modo” (recuadrado en morado) que antes era un campo de texto y ahora es un selector que permite elegir:
 - Caja Blanca.
 - Caja Negra.
 - Caja Gris.
 - Caja Negra/Gris.
- Al seleccionar una auditoría padre, se cargarán los datos del padre para todos los campos menos para el nombre de la auditoría:
 - Todos los campos serán modificables menos:
 - Id de auditoría, que será el del padre y se diferenciará de este y del resto de auditorías de regresión del mismo padre mediante el número de secuencia.
 - Número de secuencia: viene determinado por el número de auditorías de regresión de la auditoría padre.

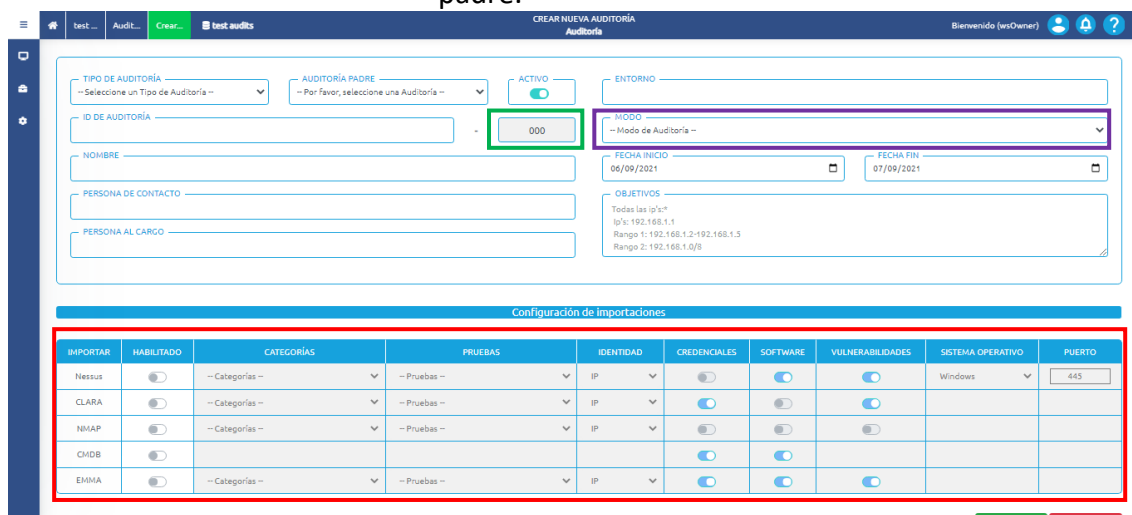


Ilustración 38. Pantalla de creación de auditoría.

4.2.3.1 Funcionamiento de la configuración de importaciones

Se puede configurar la importación de Nessus, CLARA, Nmap, CMDB y EMMA.

Para poder configurar las importaciones se requieren dos pasos previos:

- 1º. Seleccionar un tipo de auditoría: esto es necesario porque, como se verá a continuación, para las importaciones en las que hay vulnerabilidades, se tiene que seleccionar una categoría y una prueba y, la categoría depende del tipo de auditoría (y la prueba depende de la categoría).
- 2º. Activar el botón “HABILITADO” correspondiente a la importación que se quiera configurar.

IMPORTAR	HABILITADO
Nessus	<input type="checkbox"/>
CLARA	<input type="checkbox"/>
NMAP	<input type="checkbox"/>
CMDB	<input type="checkbox"/>
EMMA	<input type="checkbox"/>

Ilustración 39. Botones para habilitar las importaciones.

IMPORTAR	HABILITADO	CATEGORÍAS
Nessus	<input checked="" type="checkbox"/>	-- Categorías --
CLARA	<input type="checkbox"/>	-- Seleccione un Tipo de Auditoría --

Ilustración 40. Mensaje explicativo de acción requerida.

IMPORTAR	HABILITADO	CATEGORÍAS	PRUEBAS
Nessus	<input checked="" type="checkbox"/>	-- Categorías --	-- Pruebas --
CLARA	<input type="checkbox"/>	-- Categorías --	Por favor, seleccione una categoría

Ilustración 41. Mensaje explicativo de acción requerida.

Los siguientes parámetros para configurar son:

- Identidad: indica qué campo lleva la identidad de los activos que se van a importar (nombre o IP).
- Software: activar si se quiere importar software.
- Vulnerabilidades: activar si se quieren importar vulnerabilidades.
- Sistema operativo: Windows o Linux.
- Puerto: por defecto para Windows 445 y para Linux 22 aunque se puede escribir el que el usuario quiera (dentro del rango de puertos que existen).

IDENTIDAD	CREDENCIALES	SOFTWARE	VULNERABILIDADES	SISTEMA OPERATIVO	PUERTO
IP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Windows	445
IP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
IP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
IP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Ilustración 42. Ejemplo de una importación.

Todas y cada una de las restricciones que existen y que no dejen modificar al usuario algún dato de interés, se le notificarán mediante ayuda en línea:

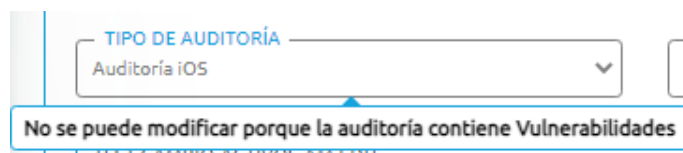
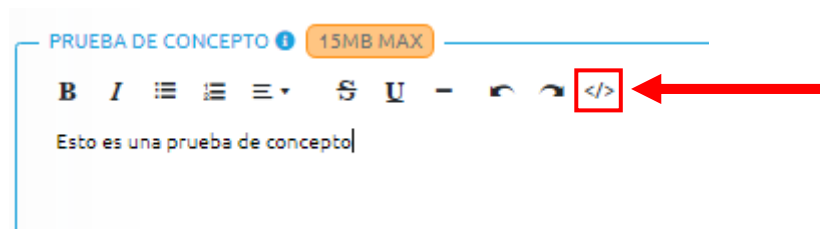
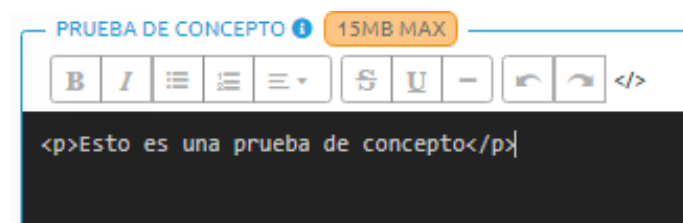


Ilustración 43. Mensaje explicativo de acción requerida.

4.2.4 Mejoras en la entrada del PoC de las Vulnerabilidades y su seguridad

Se ha añadido un botón para poder ver el código *html* del propio campo.

Ilustración 44. Botón para mostrar el código *html* del campo.Ilustración 45. Código *html* mostrado.

Se ha mejorado la sanitización (seguridad), mostrando un listado de etiquetas no permitidas.

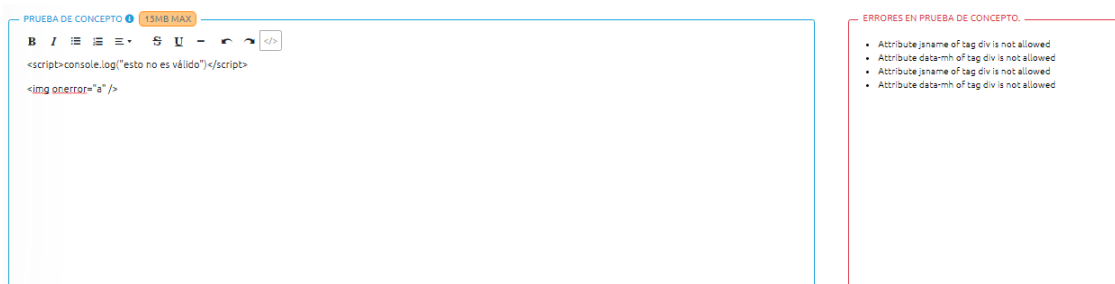


Ilustración 46. Errores en prueba de concepto.

5. FUNCIONALIDADES NO DISPONIBLES A PARTIR DE LA VERSIÓN 3.0

A continuación, se recopilan las funcionalidades de ANA que ya no estarán disponibles a partir de la versión 3.0.

5.1 FUNCIONALIDADES NO DISPONIBLES

El módulo de actualizaciones deja de estar disponible para las actualizaciones de software y CPE/CVE. A partir de ahora, cualquiera de estos dos tipos de

actualizaciones, se llevará a cabo a través de archivos ISO. Estos archivos ISO deberán añadirse a la unidad de disco virtual de la máquina virtual de ANA, para proceder a la actualización.

Dicho archivo ISO se descargará desde la plataforma LORETO, a través del enlace <http://ccn-cert.net/ana-actualizaciones>, cuya contraseña de acceso ha de solicitarse en la dirección de correo electrónico ana@ccn-cert.cni.es.

6. ANEXO A: ÍNDICE DE ILUSTRACIONES

Ilustración 1. Pantalla de autenticación.....	8
Ilustración 2. Campo usuario seleccionado.....	9
Ilustración 3. Campo contraseña seleccionado.....	9
Ilustración 4. Pantalla de inicio backend.....	9
Ilustración 5. Barra de navegación superior.	9
Ilustración 6. Barra de navegación crear.....	9
Ilustración 7. Barra de navegación editar.	10
Ilustración 8. Texto completo mostrado en la ayuda.	10
Ilustración 9. Apartado sección y subsección.	10
Ilustración 10. Botones de acciones.....	10
Ilustración 11. Barra de navegación lateral.....	11
Ilustración 12. Ejemplo de tabla mostrando activos.....	12
Ilustración 13. Detalle de filtros disponibles.....	12
Ilustración 14. Detalle de campos de tabla.....	12
Ilustración 15. Acción del botón mostrada en la ayuda.....	12
Ilustración 16. Detalle explicativo en diálogo.	12
Ilustración 17. Detalle de formulario.	13
Ilustración 18. Error mostrado al usuario en mensaje.....	13
Ilustración 19. Error mostrado al usuario por color.....	13
Ilustración 20. Error mostrado al usuario en la pestaña.....	13
Ilustración 21. Detalle de modal.	14
Ilustración 22. Modal con información explicativa.	14
Ilustración 23. Indicativo de carga de datos en pantalla.	15
Ilustración 24. Nueva pantalla de imágenes.	15
Ilustración 25. Detalle de pantalla de CLARA.....	15
Ilustración 26. Pantalla de selector de módulo.....	16
Ilustración 27. Campo de búsqueda seleccionado.....	16
Ilustración 28. Campo de búsqueda con texto introducido.....	17
Ilustración 29. Cuadro modal de creación de usuario y asignación de roles.....	18
Ilustración 30. Operaciones disponibles de un AuditManager.	30
Ilustración 31. Modal de importación de Nessus.....	37
Ilustración 32. Modal de importación de Nessus, campos rellenados.	37
Ilustración 33. Modal de importación de NMAP.....	38
Ilustración 34. Modal de importación de CLARA.	38
Ilustración 35. Modal de importación de EMMA.....	39
Ilustración 36. Modal de importación de CMDB.....	39
Ilustración 37. Auditoría padre y sus dos auditorías de regresión.....	40
Ilustración 38. Pantalla de creación de auditoría.....	41
Ilustración 39. Botones para habilitar las importaciones.	42
Ilustración 40. Mensaje explicativo de acción requerida.....	42

Ilustración 41. Mensaje explicativo de acción requerida.....	42
Ilustración 42. Ejemplo de una importación.	42
Ilustración 43. Mensaje explicativo de acción requerida.....	43
Ilustración 44. Botón para mostrar el código html del campo.	43
Ilustración 45. Código html mostrado.....	43
Ilustración 46. Errores en prueba de concepto.....	43