Funcionalidades y mejoras
ANA v.3.1

Abril 2022

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Fecha de Edición: abril de 2022

ÍNDICE

1. INTRODUCCIÓN

Este documento recoge las novedades introducidas en ANA versión 3.1, 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 es una solución modular flexible que permite incrementar la capacidad de vigilancia y efectuar diagnósticos de seguridad sobre los sistemas de una organización. Con esta solución 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.

En esta nueva versión, se han incluido las siguientes funcionalidades y mejoras:

- **Nuevo módulo de automatización para el diagnóstico de la seguridad**.
- Nuevo rol de usuario Viewer Master, para el uso del diagnóstico de seguridad desde ANA *Dashboard*.
- Cambios de nomenclatura:
  - Mejora Continua pasa a llamarse CONFORMIDADES.
  - CLARA pasa a llamarse CUMPLIMIENTO.
- Mejoras de rendimiento en todos los módulos de ANA:
  - ANA vulnerabilidades: *Backend* y *Dashboard*.
  - CONFORMIDADES.
  - CUMPLIMIENTO.
- Implementación de la ayuda en línea en todos los módulos de ANA.

3. NUEVO MÓDULO FUNCIONAL. AUTOMATIZACIÓN DEL DIAGNÓSTICO DE SEGURIDAD

Se ha añadido un módulo de automatización para el diagnóstico de la seguridad, cuya finalidad es poder configurar análisis automáticos, que recopilarán información

del estado de seguridad de los sistemas analizados. Estos análisis irán creando auditorías, con sus activos, componentes y hallazgos correspondientes.

Esta funcionalidad puede ser utilizada:

- Desde ANA *Backend*, por un usuario que posea el rol Pentester AuditManager.
- Desde ANA *Dashboard*, por un usuario que posea el nuevo rol creado al efecto, Viewer Master.

Estos roles pueden ser asignados a cualquier usuario del espacio de trabajo mediante un usuario que tenga rol WsOwner.

3.1 ELEMENTOS INCLUIDOS EN LA AUTOMATIZACIÓN

Los elementos incluidos en esta nueva funcionalidad son:

- Nuevo rol *Viewer Master*: creado para el uso del nuevo módulo de diagnóstico de la seguridad desde ANA *Dashboard*.
- Certificado de licencia. Para el uso de la funcionalidad es necesario incluir en ANA un certificado de licencia. La carga de este certificado se realiza a través del punto de menú “Certificado de licencia de automatización”. Este punto de menú sólo es visible para usuarios con rol *Administrador* o *WsOwner*.
- Configuración de análisis: accesible sólo desde el módulo de *Backend* de ANA por usuarios con rol *Pentester-AuditManager*. En esta pantalla se configuran los diferentes análisis que se lanzarán atendiendo a su periodicidad.
- Histórico de análisis: accesible sólo desde el módulo de *Backend* de ANA por usuarios con rol *Pentester-AuditManager*. En esta pantalla se puede consultar el estado de los análisis que actualmente están en ejecución, así como el reporte final del mismo una vez haya finalizado.
- Botón de análisis bajo demanda: accesible sólo desde el módulo de *Dashboard* de ANA para usuarios con rol *Viewer Master*. Este botón invoca un tipo específico de análisis hacia los objetivos que se especifiquen, sin posibilidad de configuración.
- Auditorías de automatización. Los análisis crearán auditorías automáticamente, donde se cargarán los resultados del análisis para su posterior tratamiento.

- Vistas de automatización. Los análisis crearán vistas automáticamente, donde se cargarán los activos descubiertos en los análisis.

3.2 INTRODUCCIÓN DEL CERTIFICADO DE LICENCIA

Para usar la funcionalidad de automatización se requiere un certificado de licencia, que autentica y autoriza a una organización a utilizar el módulo de automatización de auditorías. Para solicitar el acceso a dicho módulo, se debe contactar con el CCN-CERT a través del correo electrónico ana@ccn-cert.cni.es.

Una vez autorizado, se proporcionará un certificado digital, la contraseña de importación y una URL. Estos archivos y datos serán solicitados más adelante en el apartado de Certificado de Licencia de automatización.

Nota: los organismos adheridos a ANA Central no necesitan solicitar el certificado para poder utilizar el servicio.

El certificado puede ser instalado a través del menú como se muestra en la siguiente ilustración, visible únicamente para usuarios con rol *Administrador* o *WsOwner*.

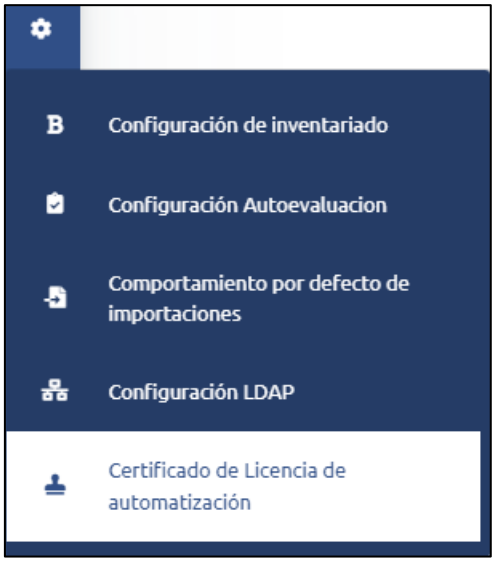

Ilustración 1. Gestión del certificado en el menú principal.

Existen dos formas de instalar el certificado:

- Con un usuario con rol *Administrador*: de esta forma el certificado validará a todos los espacios de trabajo que existan en la instancia de ANA.
- Con un usuario con rol *WsOwner*: de esta forma el certificado validará sólo al espacio de trabajo donde se instale.

Ilustración 2. Formulario de introducción de Certificado de Licencia de Automatización.

Los campos que se muestran en esta pantalla son:

- Seleccione certificado de licencia: el cual abrirá el explorador de archivos para seleccionar el certificado (extensión “pfx” o “p12”).
- Contraseña: se deberá incluir la contraseña facilitada junto con el certificado.
- URL: se deberá introducir el enlace o dirección IP correspondiente donde se encuentra el servicio de automatización, facilitados junto con el certificado.

3.3 CONFIGURACIÓN DE ANÁLISIS AUTOMÁTICOS

Una vez instalado correctamente el certificado de autenticación, se pueden crear configuraciones de análisis automáticos.

La configuración de los análisis está únicamente disponible para usuarios con el rol *AuditManager*, a través del menú lateral izquierdo “Más aplicaciones” de ANA *Backend*, tal y como muestra la siguiente imagen:

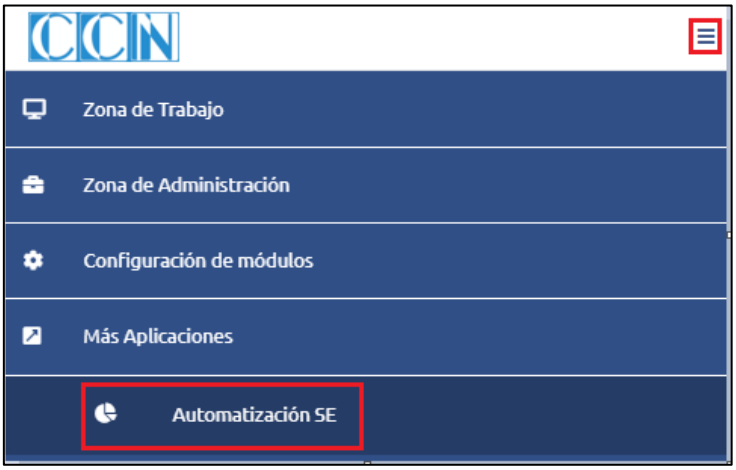

Ilustración 3. Acceso al nuevo módulo de automatización.

Actualmente, existen tres tipos de análisis que pueden ser configurados desde ANA *Backend*:

- **Pasivo / OSINT**: cuyo objetivo son los dominios que se especifiquen. En este análisis se intenta encontrar todos los subdominios asociados a los dominios objetivos.
- **No intrusivo / NMAP**: cuyo objetivo son direcciones IP o rangos de direcciones IP. En este análisis se intentará descubrir los servicios y puertos abiertos asociados a las direcciones IP objetivo. Este análisis puede encontrar vulnerabilidades que se darán de alta en el módulo correspondiente de ANA.
- **Pasivo no intrusivo**: la combinación de los dos análisis anteriores. Dirigido a dominios, primero efectúa el análisis OSINT y, posteriormente, realiza el análisis NMAP a los subdominios que se darán de alta en el módulo correspondiente de ANA.

Hay que tener en cuenta que el inicio de la ejecución de los análisis configurados, tanto inmediatos como programados, dependerá del volumen de análisis que se estén ejecutando en ese momento en la solución ANA y, por tanto, de los análisis en cola de ejecución.

En caso de que existiera algún fallo a la hora de lanzar o configurar un análisis, se mostrarán los avisos correspondientes en pantalla.

En la pantalla de configuración de análisis, se muestra una tabla con los análisis configurados en la que se puede observar las siguientes columnas:

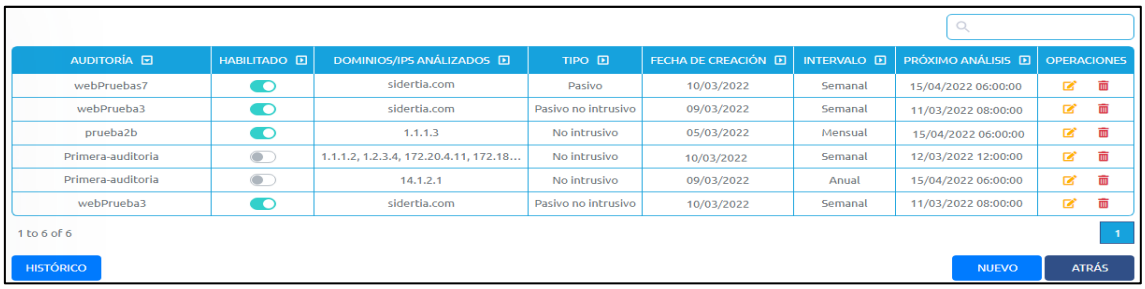

Ilustración 4. Pantalla de configuración de análisis automatizados.

- Auditoría: muestra el nombre de la auditoría que tiene configurada un análisis automatizado. Al definir una configuración de análisis automático, se creará una auditoría con el nombre que se indique en el formulario de configuración de nuevo análisis.
- Habilitado: muestra si el análisis está habilitado o deshabilitado. Mediante el interruptor se puede cambiar de estado, lo que permite tener análisis configurados, pero deshabilitada su ejecución. Un análisis

configurado con una periodicidad inmediata, permanecerá habilitado mientras está en ejecución, pero una vez termine se deshabilitará automáticamente.

- Dominios/IPs analizados: muestra todos los dominios o direcciones IP objeto del análisis.
- Tipo: muestra el tipo de análisis automatizado (pasivo, no intrusivo o pasivo no intrusivo).
- Fecha de creación: muestra la fecha en la se creó la configuración del análisis automatizado.
- Intervalo: muestra la periodicidad para la ejecución de los (inmediato, semanal, mensual o anual).
- Próximo análisis: muestra la fecha y hora de la próxima ejecución del análisis configurado para la auditoría automática. En el caso de ser una configuración de auditoría inmediata este campo aparecerá vacío.
- Operaciones: muestran las opciones de edición y eliminación de la configuración del análisis automatizado desde los botones correspondientes a ese análisis. Se podrá editar o borrar con las siguientes consideraciones:
    - Si se edita un análisis que está en ejecución, este se cancelará e iniciará otro automáticamente con la nueva configuración.
    - Si se borra un análisis que está en ejecución, se cancelará.

La pantalla de configuración de análisis también permite:

- Crear una nueva configuración de análisis, desde el botón “NUEVO”.
- Volver a la página principal de ANA *Backend*, pulsando el botón “ATRÁS”.
- Acceder a la pantalla Histórico de análisis automatizados, a través del botón “HISTÓRICO”.

3.3.1 Creación de nuevo análisis

A través del botón “NUEVO” existente en la pantalla de configuración de análisis, se accederá a la creación de un nuevo análisis automatizado.

En la pantalla que aparecerá existen dos secciones principales:

- Configuración técnica: donde se han de especificar los parámetros del análisis, como por ejemplo el tipo de análisis a realizar.

- Configuración de ejecución: donde se establecen los parámetros temporales del análisis, como por ejemplo si es un análisis inmediato o mensual.

En las configuraciones de análisis, existen cuatro apartados que son comunes a todos:

- Habilitado: determina si el análisis que estamos configurando estará, de inicio, habilitado o no.
- Tipo: la elección del tipo modifica el formulario para adaptarse a los requisitos del tipo de análisis elegido.
- Auditoría: determina el nombre de la auditoría que se creará automáticamente y donde se darán de alta los resultados del análisis. En nombre de la auditoría ha de ser único y no se puede repetir. Una vez pulsado el botón "ACEPTAR" este nombre no se podrá editar.
- Periodicidad: la elección de la periodicidad modifica el formulario para adaptarse a los requisitos del tipo de periodicidad elegida.

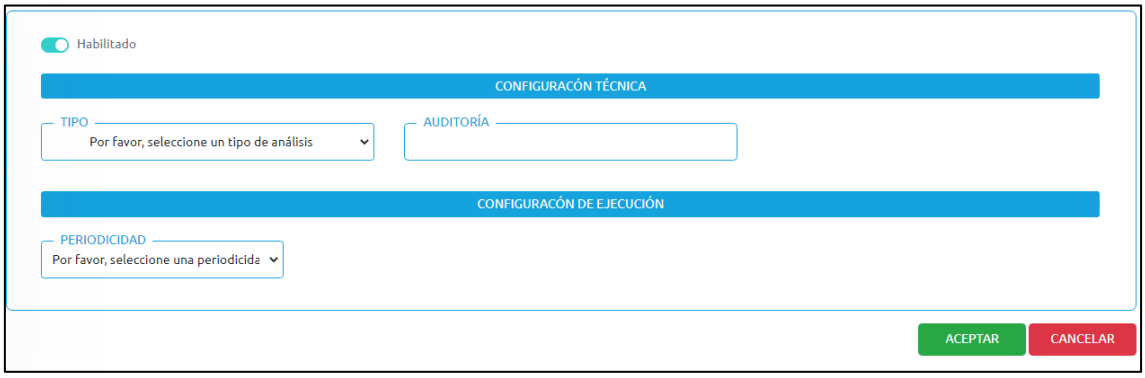

Ilustración 5. Pantalla inicial de creación de nuevo análisis.

Tal y como se ha especificado anteriormente, los campos tipo y periodicidad, modifican el formulario en función de la opción elegida. A continuación, se detallan las diferentes configuraciones a establecer según las opciones elegidas.

3.3.1.1 Configuración de análisis de tipo pasivo

El análisis pasivo se realiza consultando datos de fuentes abiertas. En este tipo de análisis los objetivos serán dominios.

Al seleccionar pasivo, aparecerá un nuevo campo llamado "Dominios" donde se deberán escribir estos, separados por comas en caso de ser varios. Por ejemplo "ccn.es" o "ccn.es, ccn-cert.es".

Una vez escritos, se deberá pulsar el botón "Añadir" para que queden registrados en la configuración.

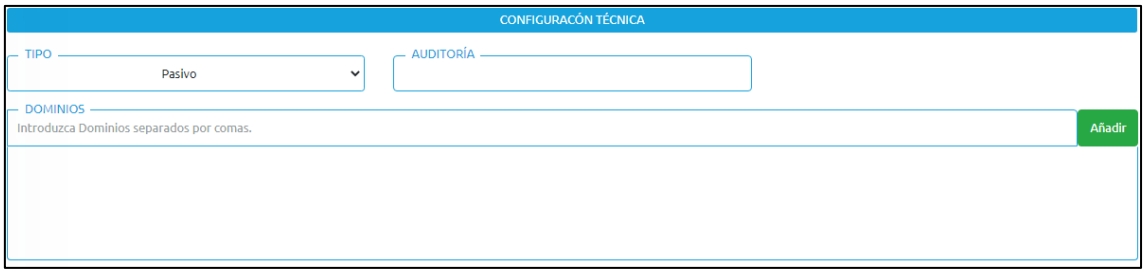

Ilustración 6. Configuración de análisis de tipo pasivo.

No se permite añadir varias veces el mismo dominio, aunque sí se permite añadir subdominios del primero, por ejemplo: “ccn.es, subdomain.ccn.es”.

Se puede configurar otro análisis para los mismos dominios, pero estos pertenecerán a la nueva auditoría que se generará.

Los activos que se den de alta en las auditorías creadas por los análisis pueden ser modificados por usuarios con rol *Pentester.*

3.3.1.2 Configuración de análisis de tipo no intrusivo

Este análisis se realiza con la herramienta NMAP. Es un análisis enfocado al descubrimiento de servicios y puertos abiertos. En este caso, los objetivos serán direcciones IP.

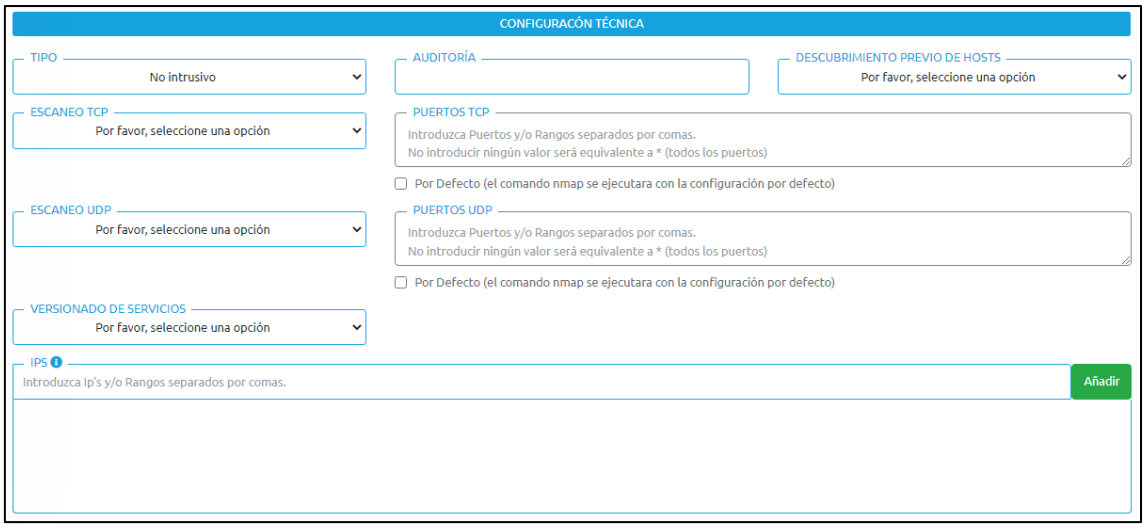

Ilustración 7. Configuración de análisis de tipo no intrusivo.

Al seleccionar el tipo no intrusivo, se observará que aparecen más campos a establecer que en un análisis pasivo. Se explican a continuación:

- Descubrimiento previo de hosts: también conocido como sondeo ping. Se basa en determinar la disponibilidad de un dispositivo de red, servidor web o interfaz utilizando una solicitud de eco. Si se selecciona la opción SÍ, se realizará esta acción y, en caso de que el resultado sea negativo, no

continuará con ese host. Por el contrario, si se selecciona la opción NO, no se realizará esta comprobación y se seguirá con el escaneo.

- Escaneo TCP: al seleccionar SÍ, se escanearán rangos de puertos TCP configurados en la sección de puertos TCP. Al seleccionar NO, no se escanearán puertos TCP:
    - Puertos TCP: si se selecciona la opción "Por Defecto", se escanearán los 1000 puertos más comunes. Si se selecciona esta opción o se elige un rango de puertos muy amplio, el análisis podría requerir un tiempo elevado de ejecución. Los puertos podrán introducirse individualmente (por ejemplo, 389), por rangos (por ejemplo, 443-449) o separándolos con comas: 443,444,445). Se permite también saltos de línea o espacios para separar los puertos.
- Escaneo UDP: al seleccionar SÍ, se escanearán rangos de puertos UDP configurados en la sección puertos UDP. Al seleccionar NO, no se escanearán puertos UDP:
    - Puertos UDP: si se selecciona la opción "Por Defecto", se escanearán los 1000 puertos más comunes. Si se selecciona esta opción o se elige un rango de puertos muy amplio, el análisis podría requerir un tiempo elevado de ejecución. Los puertos podrán introducirse individualmente (por ejemplo, 389), por rangos (por ejemplo, 443-449) o separándolos con comas: 443,444,445). Se permite también saltos de línea o espacios para separar los puertos.
- Versionado de servicios: al seleccionar SÍ, en los puertos que se encuentren abiertos, se intentará reconocer los distintos servicios (software ejecutando) y sus versiones. Por ejemplo, si se encuentra abierto el puerto 25/TCP, normalmente se corresponderá con un servidor de correo (SMTP), pero con esta opción se intentará comprobar que efectivamente es ese servicio y no otro el que está escuchando. También generará el correspondiente identificador CPE en los componentes dados de alta para ese activo, si se encuentra correspondencia con los CPE almacenados en ANA. En caso de encontrar el CPE, no se darán de alta sus vulnerabilidades CVE asociadas, aunque pueden añadirse manualmente por un usuario con rol *Pentester*. Al seleccionar NO, no se analizará el versionado de servicios.

- IP: en este campo se establecerán las direcciones IP objetivo del análisis. Puede introducirse una dirección IP, rangos, o rangos separados por comas. Ejemplos: “13.95.12.55”, “19.55.22.11-19.55.22.13”. Al igual que con los dominios de un análisis pasivo, en el mismo análisis no se pueden repetir direcciones IP, pero pueden ser configuradas las mismas en un análisis diferente.

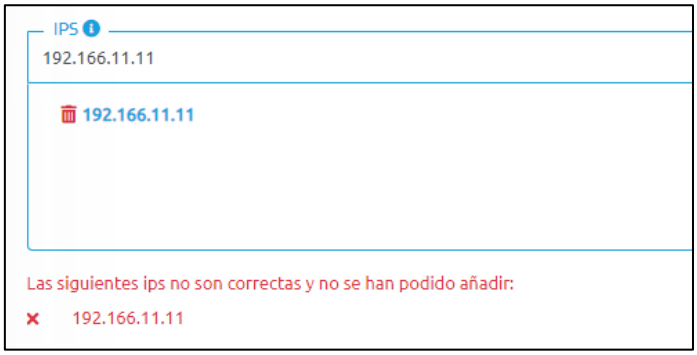

Ilustración 8. Mensaje de advertencia para una dirección IP repetida.

3.3.1.3 Configuración de análisis de tipo pasivo no intrusivo

En este tipo de análisis se realizará inicialmente un análisis pasivo al dominio o dominios seleccionados, obteniéndose los subdominios asociados a estos y, posteriormente, se ejecutará un análisis no intrusivo a cada dirección IP asociada a cada subdominio, realizando así una combinación de los dos análisis anteriores con una única configuración de análisis.

La configuración es equivalente a la del tipo *no intrusivo*, pero en lugar de seleccionar direcciones IP objetivos, se introducirán dominios.

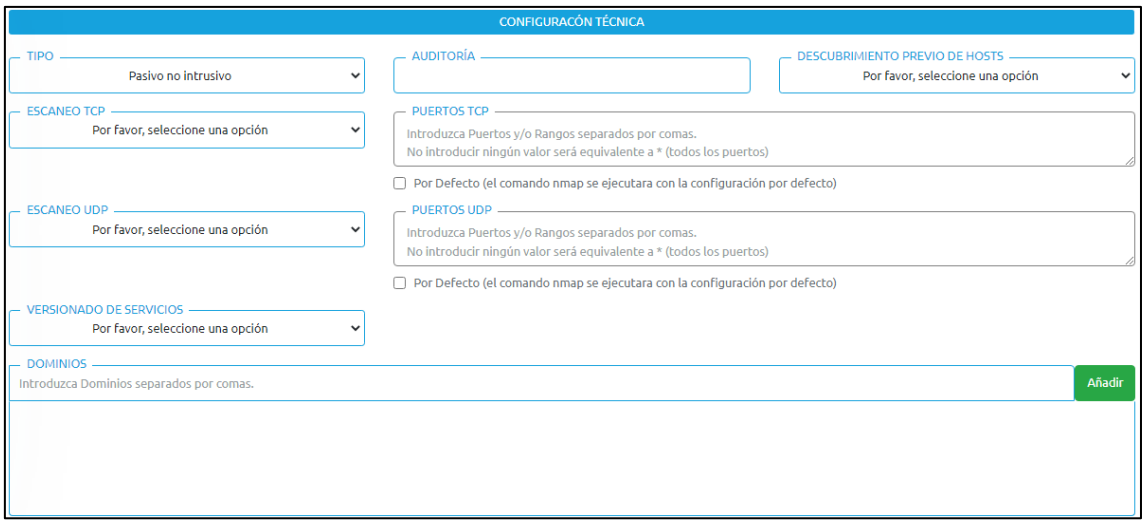

Ilustración 9. Configuración de análisis de tipo pasivo no intrusivo.

Al igual que el análisis *no intrusivo*, se darán de alta, si se encuentran, los CPE asociados a los servicios. Estos podrán ser modificados posteriormente por un usuario con rol *Pentester*.

3.3.2 Periodicidad de los análisis

Los análisis pueden ser configurados con diferentes tipos de periodicidad.

Uno de los tipos que se podrá elegir es el tipo *inmediato*. Este análisis se ejecutará, si la carga del servidor de análisis lo permite, inmediatamente después de pulsar el botón "ACEPTAR" en la configuración de análisis.

En caso de que se establezca una periodicidad diferente de *inmediato*, habrá que cumplimentar los siguientes campos:

Ilustración 10. Configuración de periodicidad de ejecución.

- Fecha inicio: fecha el que comenzará el primer análisis. No se puede establecer una fecha anterior a la fecha actual.
- Hora inicio: hora en la que se iniciará el análisis. Si se especifica una hora anterior a la actual, y el día especificado es el actual, el análisis comenzará de manera inmediata si la hora de fin no se ha superado. No se puede configurar un análisis nuevo con una fecha de inicio anterior al día actual.
- Hora fin: hora tope que tiene el análisis para comenzar a ser ejecutado. En el caso de que el análisis esté en curso, este seguirá ejecutándose, aunque se sobrepase la hora de fin. En caso de que el análisis no se haya podido ejecutar dentro de su rango temporal por sobrecarga del servidor de análisis, este se ejecutaría lo antes posible y se programaría para la siguiente ejecución que le correspondiera.

Ejemplos: Día y hora actuales 12/04/2022 17:00 H:

Análisis semanal con fecha de inicio 12/04/2022 hora inicio 15:00 H hora fin 23:59H

Primer análisis inmediato, al ser la hora de inicio anterior a la actual y no haberse superado la hora de fin.

Siguiente análisis 19/04/2022 a las 15:00 H.

Análisis mensual con fecha de inicio 20/04/2022 hora inicio 16:00 H hora fin 23:59 H:

Primer análisis el 20/04/2022 a las 16:00 H.

Siguiente análisis el 20/05/2022 a las 16:00 H.

Análisis anual con fecha de inicio 13/04/2022 hora inicio 00:00 H hora fin 05:00 H e interruptor deshabilitado:

El primer análisis tendría lugar a las 00:00 H del 13/04/2022, pero como estará deshabilitado este se planifica para el 13/04/2023 a las 00:00 H.

Análisis mensual fecha de inicio 12/03/2022 hora de inicio 17:00 H hora de fin 18:00 H:

El análisis se configuró el 10/03/2022 para que se lanzara el primer análisis dos días después. El primer análisis se lanzó el mes pasado a la hora y día indicados.

Sobrecarga en el servidor de análisis el día actual y se superan las 18:00 H. El análisis quedaría en cola para ejecución. Se libera dicha cola el 13/04/2022 a las 10:00 H. El análisis se ejecuta en ese momento, pero su siguiente ejecución es la establecida por el usuario, es decir, el 12/05/2022.

Nota: la hora para la configuración / ejecución de los análisis está expresada en UTC.

3.3.3 Modificación de configuración de análisis

La pantalla de modificación de una configuración de análisis funciona exactamente de la misma forma que la de creación, pero no se permite el cambio del nombre de la auditoría. Los cambios realizados se aplicarán de manera inmediata.

Como se ha especificado anteriormente, si se edita un análisis que está en ejecución, este se cancelará y comenzará inmediatamente uno nuevo con la nueva configuración establecida.

3.3.4 Eliminación de configuración de análisis

Al pulsar en el botón de eliminar una configuración de análisis en la tabla, se mostrará el modal correspondiente a la confirmación de eliminación.

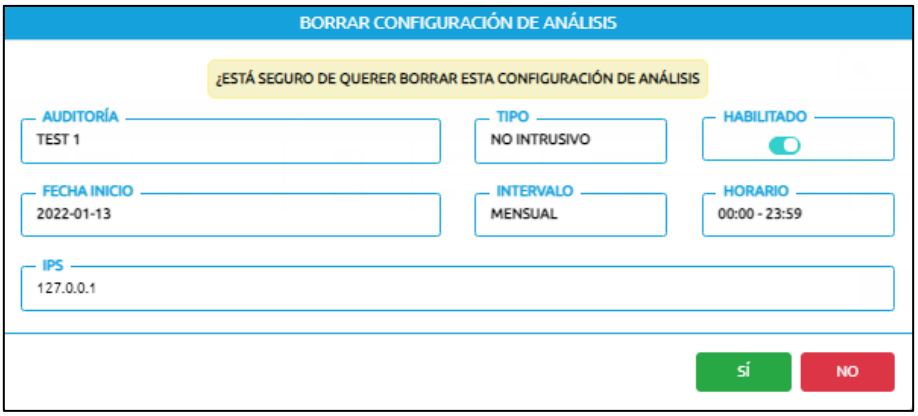

Ilustración 11. Ventana modal de eliminación de análisis.

Al borrar una configuración de análisis, si ya se había realizado alguno, se mantendrán accesibles y visibles las auditorías creadas y sus activos, componentes y vulnerabilidades encontrados, así como las ejecuciones correspondientes en el apartado histórico.

Si se borra una configuración de un análisis que se encuentra en ejecución, este se cancelará.

3.4 HISTÓRICO DE ANÁLISIS

Se podrá acceder a esta pantalla a través del botón "HISTÓRICO", situado en la parte izquierda de la pantalla de configuración de análisis automáticos.

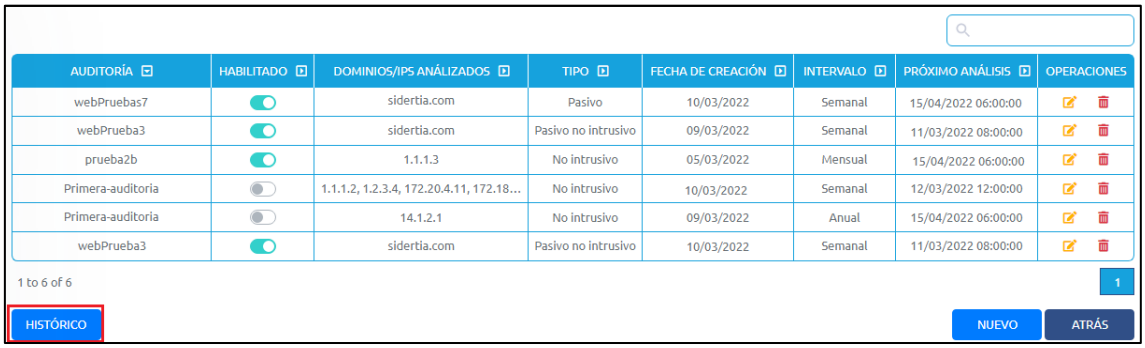

Ilustración 12. Acceso a histórico a través del botón.

Una vez se ha accedido a la pantalla se mostrará información de los análisis que se hayan ido ejecutando a lo largo del tiempo en nuestro espacio de trabajo.

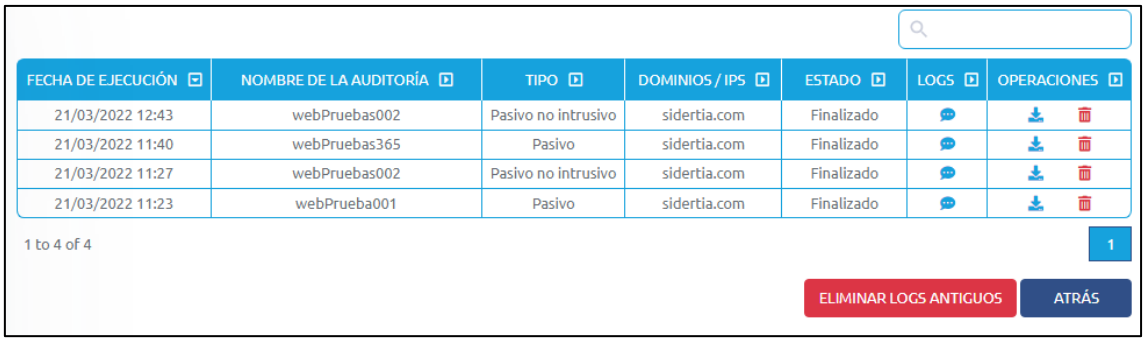

Ilustración 13. Pantalla histórico de análisis.

Por cada análisis realizado, independientemente de si pertenecen a una misma configuración, se muestra una fila.

Los campos que se pueden observar son:

- Fecha de ejecución: Fecha y hora en la que terminó ese análisis.
- Nombre de la auditoría: nombre especificado por el usuario cuando se creó la configuración del análisis.
- Tipo: tipo de análisis en esa ejecución.
- Dominios / IP: objetivos de los análisis en esa ejecución.
- Estado: estado en el que se encuentra el análisis. Cuatro posibles:
  - En ejecución.
  - Cancelando.
  - Cancelado.
  - Finalizado.
- Logs: este botón abre una ventana modal que muestra información relativa al proceso de análisis.

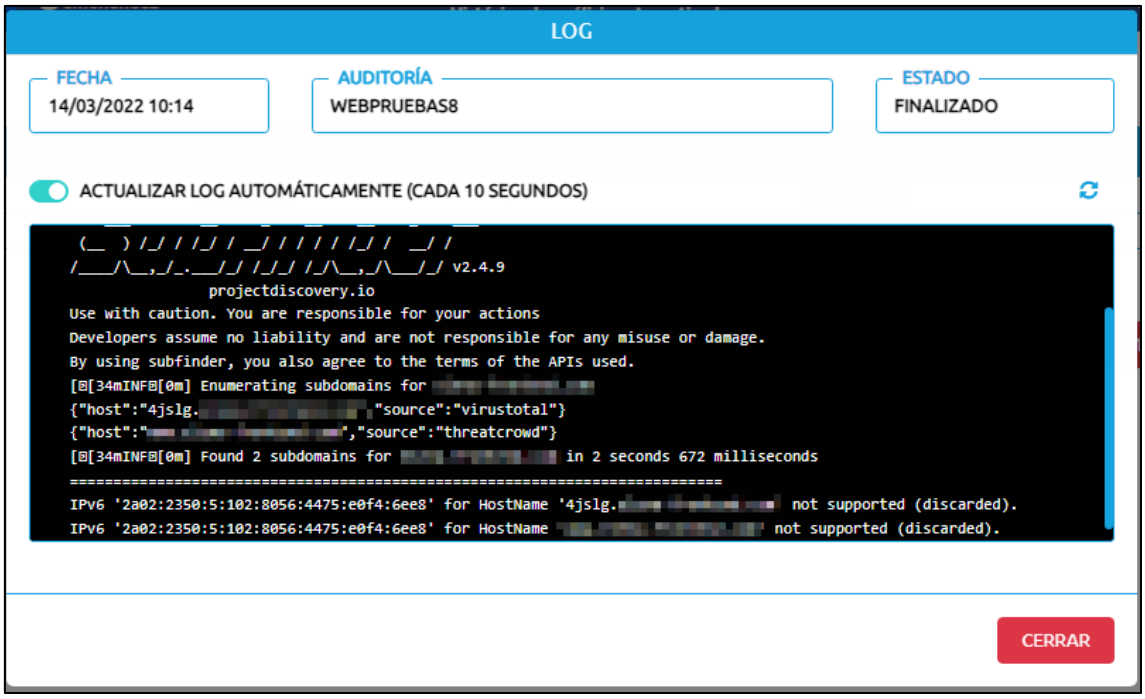

Ilustración 14. Ventana modal de información del análisis.

- En esta ventana modal, se puede ver el proceso de análisis.
- Si el análisis está en ejecución, esta ventana mostrará la parte final del log y se actualizará cada diez segundos, aunque esta opción se refresco se puede deshabilitar con el botón tipo interruptor.
- Se puede forzar el refresco con el botón de actualizar :

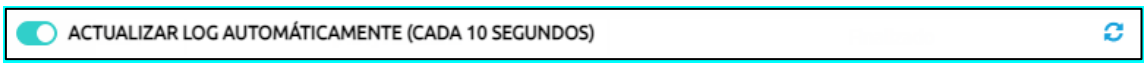

Ilustración 15. Botones de acciones disponibles en información del análisis.

- Si el análisis ha finalizado, el reporte comenzará por la primera línea y el refresco estará deshabilitado. En lugar de aparecer el botón , tendremos la posibilidad de descargar el fichero de log correspondiente al análisis .

- Operaciones: acciones que se pueden realizar en los análisis. Existen dos tipos de grupos de acciones:
  - En tiempo de ejecución:
    - Es posible cancelar un análisis que se encuentra en ejecución. Para ello se deberá pulsar sobre el aspa roja ✖ y aceptar el cuadro de diálogo emergente.

FECHA DE EJECUCIÓN	NOMBRE DE LA AUDITORÍA	TIPO	DOMINIOS / IPS	ESTADO	LOGS	OPERACIONES
22/03/2022 10:24	webPrueba1234	Pasivo	sidertia.com	En ejecución		
21/03/2022 12:43	webPruebas002	Pasivo no intrusivo	sidertia.com	Finalizado		
21/03/2022 11:40	webPruebas365	Pasivo	sidertia.com	Finalizado		
21/03/2022 11:27	webPruebas002	Pasivo no intrusivo	sidertia.com	Finalizado		
21/03/2022 11:23	webPrueba001	Pasivo	sidertia.com	Finalizado		

Ilustración 16. Ejemplo de un análisis que puede ser cancelado.

- En análisis finalizados: si el análisis ha finalizado normalmente o si se canceló, se podrán realizar las siguientes acciones:

Ilustración 17. Botones de operaciones de análisis finalizados.

  - Descargar fichero de log: pulsando sobre el icono azul , se podrá descargar el fichero que contiene la salida de lo realizado durante el análisis.
  - Eliminar el histórico de este análisis: pulsando sobre el icono rojo , se podrá eliminar este histórico.

Es posible eliminar los log con más de un mes de antigüedad. Al pulsar el botón "ELIMINAR LOGS ANTIGUOS", se realizará esta acción. Se necesita confirmación en la ventana modal emergente para realiza el borrado.

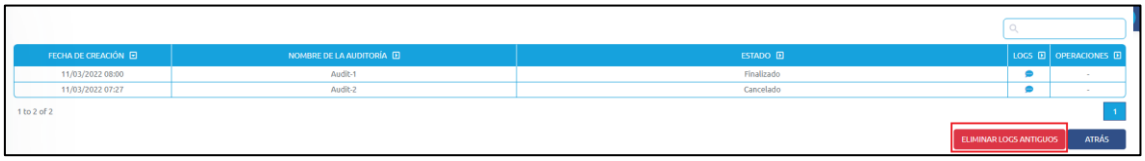

Ilustración 18. Botón de eliminación de log con más de un mes de antigüedad.

3.5 COMPORTAMIENTO DE LAS AUDITORÍAS CREADAS AUTOMÁTICAMENTE

Como ya se ha comentado, al establecer una nueva configuración de análisis, es necesario especificar un nombre de auditoría único.

Al pulsar el botón "ACEPTAR", automáticamente se creará una auditoría en el apartado auditorías de ANA *Backend*, sobre la cual tendrá permisos el usuario que da de alta el análisis. Posteriormente se pueden asignar permisos a más usuarios sobre esa auditoría.

En esta auditoría se irán añadiendo los activos, componentes y vulnerabilidades que descubran los análisis.

Estas auditorías no pueden ser editadas, pero sí pueden ser borradas, eliminándose también la configuración de análisis que creó esta auditoría, permaneciendo los datos de la pantalla histórico que se hayan podido crear. Para borrar una auditoría es necesario que esta no contenga ni activos, ni componentes, ni vulnerabilidades.

Si los análisis llegan a la fecha de siguiente ejecución por periodicidad, o se vuelve a habilitar un análisis inmediato, se creará una nueva auditoría de regresión, que actualizará los activos de su auditoría padre. En el nombre de esta auditoría de regresión figurará una (R), así como el identificador incremental que le corresponda, que será aumentado en uno respecto a la auditoría padre, si es la primera de regresión, o por el contrario uno más que la anterior auditoría de regresión.

Los resultados dados de alta en las auditorías se pueden modificar.

Para acceder a los resultados de un análisis, se ha de seleccionar la auditoría correspondiente en la pantalla principal de ANA *Backend* y posteriormente pulsar en activos.

Ilustración 19. Activos creados por un análisis automatizado.

Como se puede apreciar en la ilustración, la carga de activos y cómo se muestra la información, no varía con respecto a una auditoría normal.

Los activos dados de alta por un análisis automático tendrán el identificador AUT 

.

Los componentes se añaden a cada activo. Si en la configuración de análisis se seleccionó el versionado de servicios, los componentes pueden identificarse con su correspondiente CPE. Los CVE asociados a los CPE podrán ser añadidos manualmente por un usuario con rol *Pentester,* ya que el sistema no los dará de alta de forma automática.

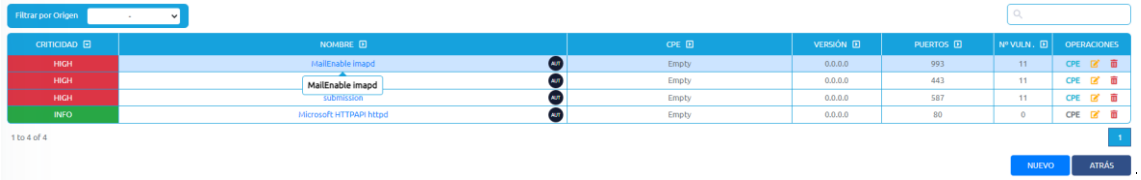

Ilustración 20. Componentes asociados a un activo.

Los tipos de análisis que dan de alta componentes y vulnerabilidades son: *no intrusivo* y *pasivo no intrusivo*. El tipo *pasivo* únicamente crea activos.

3.6 COMPORTAMIENTO DE LAS VISTAS AUTOMÁTICAS

Al igual que se crean auditorías de manera automática, los análisis automatizados, a medida que vaya avanzando su ejecución, irán agrupando en vistas los resultados para que puedan ser visualizados desde el módulo de ANA *Dashboard*.

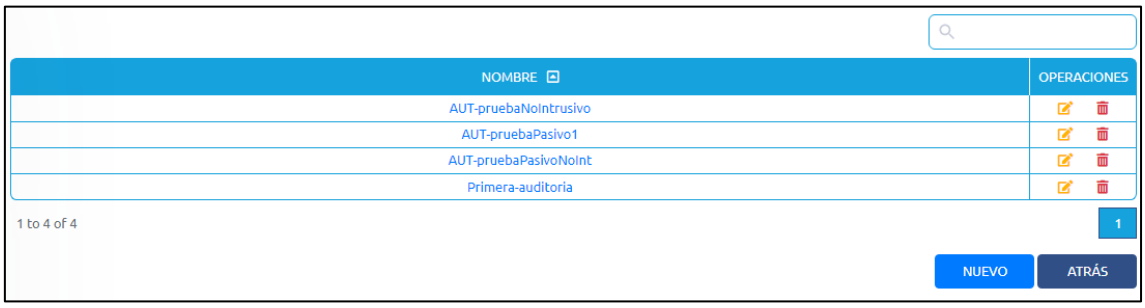

Ilustración 21. Pantalla de gestión de vistas.

A diferencia de las auditorías, las vistas sí se pueden modificar y borrar.

El nombre que tendrán estas vistas será el nombre que especificó el usuario para la auditoría, con el prefijo "AUT-" para facilitar la identificación de las vistas que han sido creadas por análisis automatizados.

Sobre estas vistas tendrán permisos de visualización los siguientes usuarios:

- El *AuditManager* que dio de alta el análisis desde ANA *Backend*, si en el momento en el que se cree la vista posee rol *Viewer Master*.
- El *Viewer Master* que dio de alta el análisis desde el botón correspondiente en el módulo de ANA *Dashboard*.

Posteriormente a la creación automática de la vista, si se quiere asignar más usuarios a las vistas, un usuario con rol WsOwner o Business podrá añadir a los usuarios con rol *Viewer* que se desee.

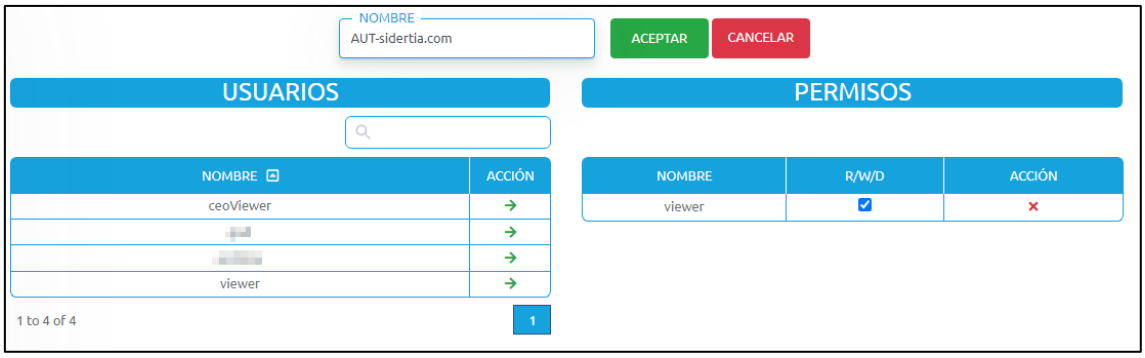

Ilustración 22. Pantalla de permisos de vistas.

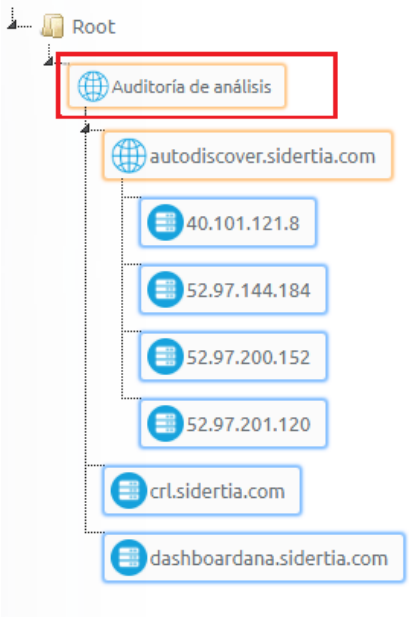

Ilustración 23. Detalle de una vista generada automáticamente.

Como se puede apreciar, los activos que se descubran, serán añadidos a la vista dentro un grupo que tendrá por nombre el nombre de la auditoría.

En caso de que se descubran múltiples activos con el mismo nombre, pero que tienen diferente dirección IP, se creará un grupo dentro del grupo principal cuyo nombre será el nombre del dominio que posee múltiples direcciones IP y dentro estarán agrupados los activos con nombre su dirección IP, tal y como se puede ver en la anterior ilustración en el grupo “autodiscover.sidertia.com”.

3.7 ANÁLISIS AUTOMATIZADOS DESDE ANA DASHBOARD

Es posible lanzar un análisis automatizado de diagnóstico de seguridad desde el módulo de ANA *Dashboard*, sin más requisitos que especificar los objetivos del análisis.

Esta acción únicamente puede ser realizada por un nuevo rol creado para este fin, el *Viewer Master*. Si el usuario que accede a ANA *Dashboard* posee este rol, le aparecerá un botón en la barra de herramientas con forma de diana.

Ilustración 24. Botón para lanzar análisis desde ANA Dashboard.

Al pulsar el botón se abre una ventana modal en la que se deberá introducir un dominio o una dirección IP o rango de direcciones IP:

- Si se introduce un **dominio**, el análisis a realizar será equivalente a un ***pasivo no intrusivo***, analizando los 1000 puertos más comunes TCP y con descubrimiento de servicios.
- Si se introduce una **dirección IP o rango de direcciones IP**, se realizará un análisis ***no intrusivo***, analizando los 1000 puertos más comunes TCP y con descubrimiento de servicios.

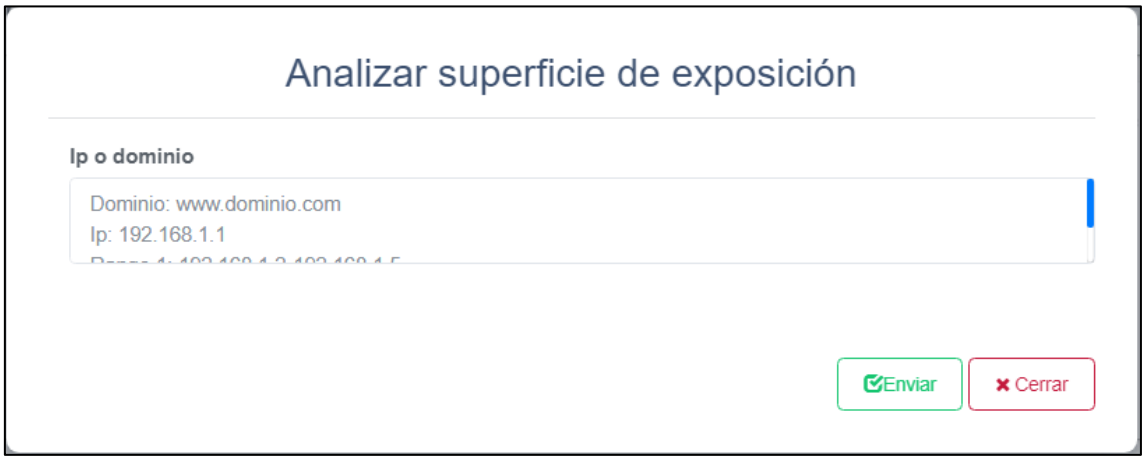

Ilustración 25. Ventana modal de inicio de diagnóstico de seguridad desde ANA Dashboard.

Al pulsar el botón enviar se ejecutará el análisis.

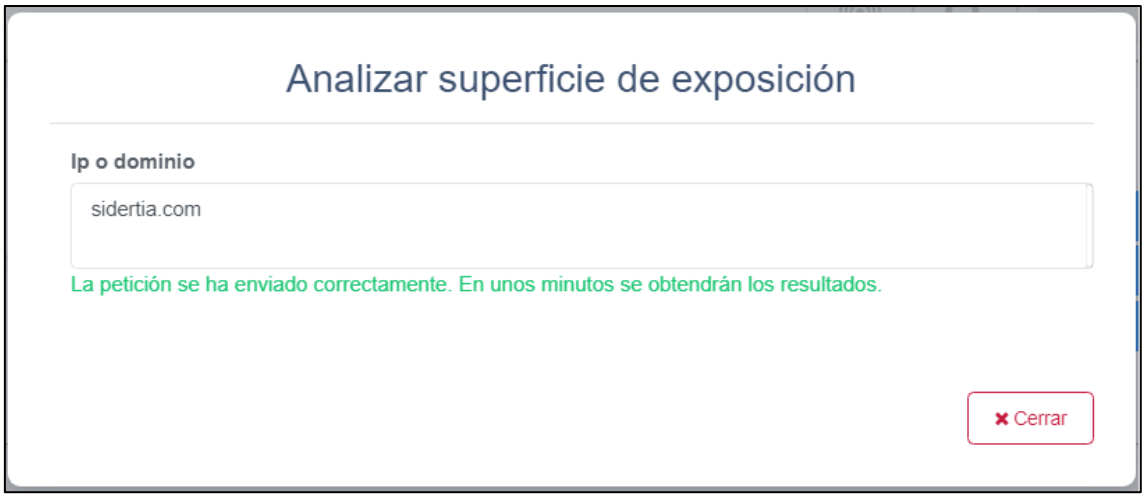

Ilustración 26. Diagnóstico de la seguridad iniciado.

Los análisis enviados desde ANA *Dashboard* se ejecutan de manera inmediata y quedarán configurados con una periodicidad mensual.

No se podrán solicitar análisis sobre los mismos objetivos especificados anteriormente en otro análisis lanzado desde ANA *Dashboard*. En caso de que el usuario lo intente se mostrará un error.

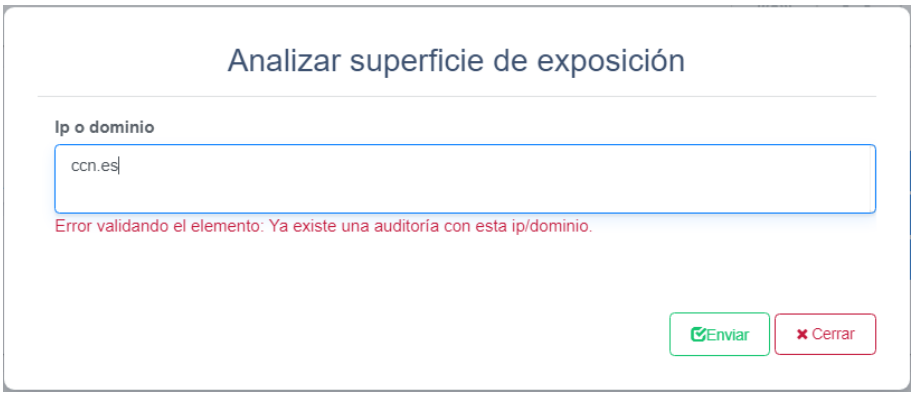

Ilustración 27. Error de inicio de análisis.

La configuración de un análisis enviado desde ANA *Dashboard* puede ser modificada desde la pantalla de configuración de análisis de ANA *Backend*, por un usuario con rol *AuditManager*.

Una vez comenzado el análisis, se visualizará una alerta que mostrará la evolución; la duración del análisis varía en función de la extensión de los objetivos a analizar.

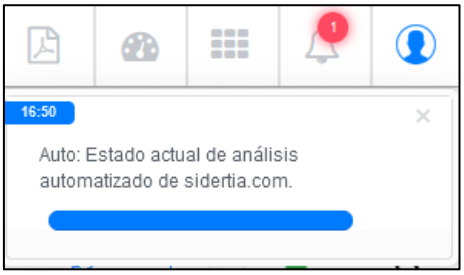

Ilustración 28. Notificación de análisis en curso.

3.7.1 Comportamiento de creación de vistas

Al igual que los análisis configurados desde ANA *Backend*, los análisis creados desde ANA *Dashboard* también crean auditorías y vistas de manera automática.

Como se ha especificado anteriormente, un análisis lanzado por un usuario *Viewer Master*, automáticamente le otorga permisos de lectura sobre la vista generada, por lo que este usuario podrá ver en el *Dashboard* el resultado del análisis, sin necesidad de solicitar permisos sobre la vista. También es posible dar permisos a otros usuarios sobre esta vista.

Ilustración 29. Vista de un análisis de diagnóstico de seguridad.

4. IMPLEMENTACIÓN DE AYUDA EN LA APLICACIÓN

La ayuda en línea se ha añadido en todos aquellos módulos que no disponían de ella.

A modo de ejemplo, a continuación se muestran unas ilustraciones:

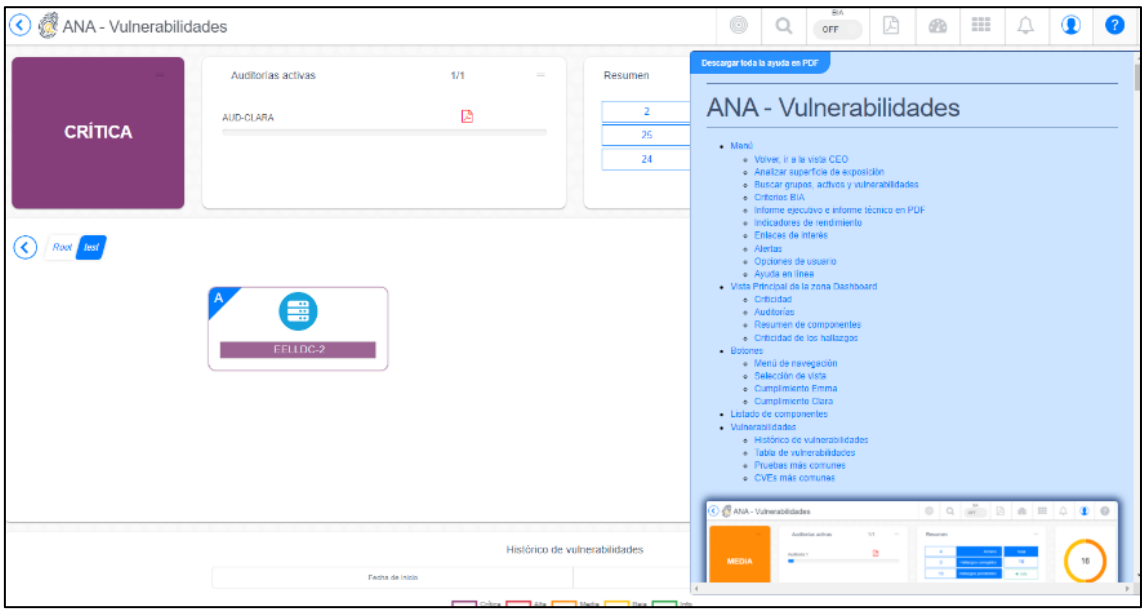

Ilustración 30. Ayuda en línea en ANA vulnerabilidades Dashboard.

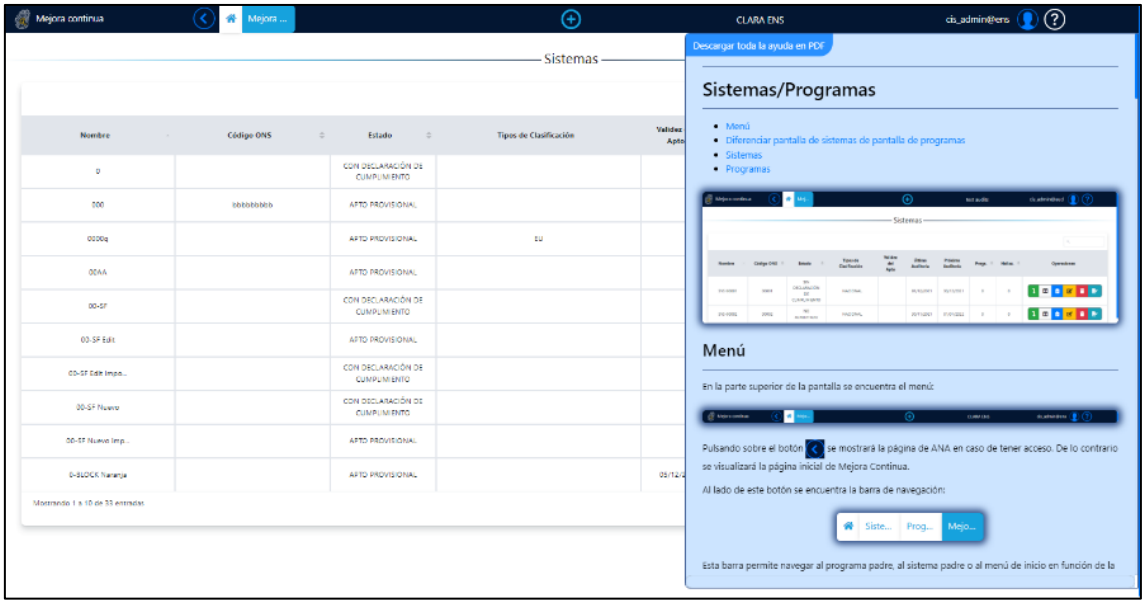

Ilustración 31. Ayuda en línea en Conformidades Backend.

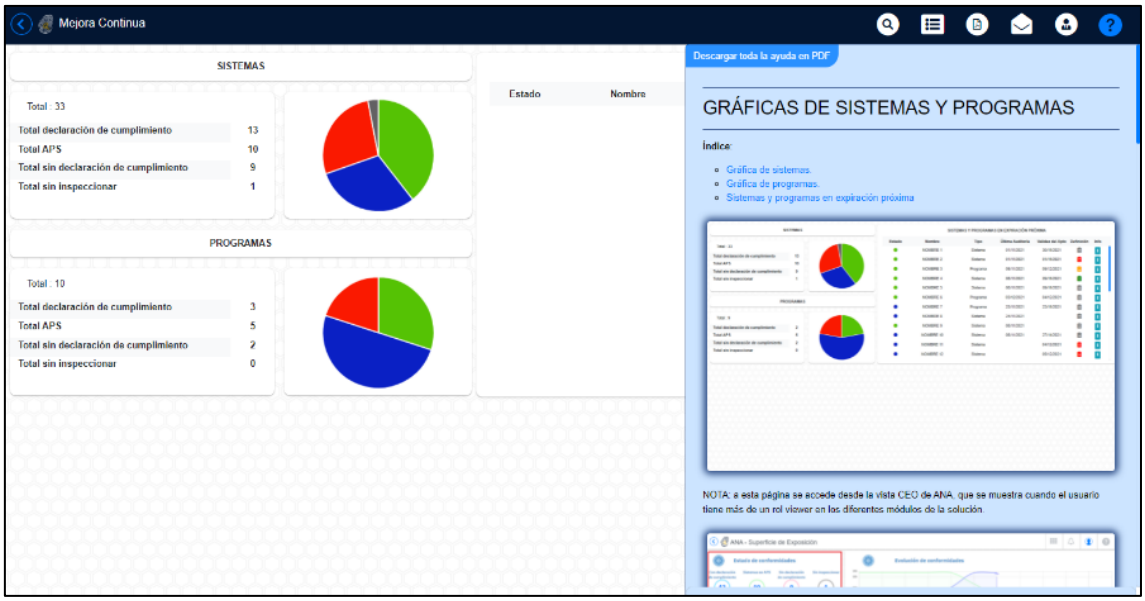

Ilustración 32. Ayuda en línea en Conformidades Dashboard.

Ilustración 33. Ayuda en línea en Cumplimiento.

5. OTROS CAMBIOS REALIZADOS EN LA VERSIÓN 3.1

Conformidades:

- Cambio del texto "Total certificado" por "Total declaraciones de cumplimiento".
- Cambio del texto "Total no certificado" por "Total sin inspeccionar".
- Cambio del texto "No apto" por "Sin declaración de cumplimiento".

- Cambio del texto "Info" por "Sin relevancia (SR)". En aquellos elementos gráficos donde el texto completo no quepa, se mostrará sólo "SR".
- Mostrar un pop-up en el *Dashboard* de Conformidades con la información del sistema o programa al sobrevolar el icono  .
- Se implementa la funcionalidad de "Cerrar sesión" desde el módulo de Conformidades.
- Se alinean los textos de la ayuda en el *Backend* de la vista tabla de hallazgos.
- Se afina la precisión de los campos de fechas en los formularios.
- En la tabla de subsanación, se cambia el cursor para que el usuario sepa que se pueden arrastrar los paneles.
- Mejora visual en el ajuste de los campos que se muestran en la tabla de subsanación.

Servicio de análisis de CLARA:

- Se optimiza la obtención de recursos necesarios para el funcionamiento del servicio de CLARA, para sólo actualizar aquellos que hayan cambiado. Sólo para sistemas clasificados.
- Se separa la obtención de recursos ENS y Sistemas Clasificados, para no traer recursos innecesarios.

6. ANEXO A: ÍNDICE DE ILUSTRACIONES