Automatización y Normalización de Auditorias

Propiedades

ANA es una aplicación para la gestión y evolución de los niveles de exposición a los que se encuentra sometida una entidad. De este modo, ANA proporciona la capacidad de medir estos niveles, ayudando a reducir las probabilidades de explotación de vulnerabilidades por un elemento externo.

- Solución "back-end" para la gestión continua de seguridad sobre el conjunto de activos de un organismo.
- Procesos automatizados para inventariado de activos, permitiendo también el descubrimiento de servicios a través de regresiones periódicas.
- Categorización de activos y normalización de los resultados de diferentes tipos de auditorías, manuales o automáticas.
- Metodología de Cálculo de Criticidad según nivel de exposición.
- Gestión de tiempos de resolución y cálculo de tiempo máximo de resolución de vulnerabilidades.
- Pruebas de Concepto de evidencias y recomendaciones para la mitigación de vulnerabilidades identificadas.
- Control y seguimiento de vulnerabilidades identificadas, incorporando un proceso de auditoría continua a través de históricos de evolución de estas.
- Panel de Control, según estrategia de roles de usuarios, que permite la configuración de cuadros de mando para la navegación granular en función de agrupaciones de activos, peligrosidad y/o estado, así como su evolución en el tiempo.
- Sistema de alertas para el seguimiento de los tiempos de respuesta para la mitigación y evolución de vulnerabilidades.
- Generación de indicadores clave de rendimiento (KPI´s).
- Generación automática de informes tipo "Ejecutivo", atendiendo a la configuración de los Paneles de Control en base a requisitos previamente establecidos.
- Informes de tipo "Técnico" de resultados de auditorías con evolución en el tiempo.
- Aislamiento entre organismos, solución escalable y rápido despliegue, así como distintas modalidades de despliegue (ANA-ON PREMISE o ANA-CENTRAL).

Funcionalidades

El organismo adquiere la solución ANA para evaluar de forma continua sus sistemas, definiendo el alcance y la profundidad de los análisis (revisiones de salud, auditorías completas de aplicaciones o redes, seguimiento continuo, etc.). Dependiendo de la modalidad de implantación, se despliega la solución ANA en las infraestructuras del organismo o se utiliza ANA-CENTRAL, previa validación por parte del CCN-CERT.

Según el alcance definido, se llevarán a cabo las diferentes tareas de auditoría (manualmente, programadas a través de ANA o mediante el uso de herramientas de terceros), cuyos resultados pasarán a integrarse y normalizarse en ANA.

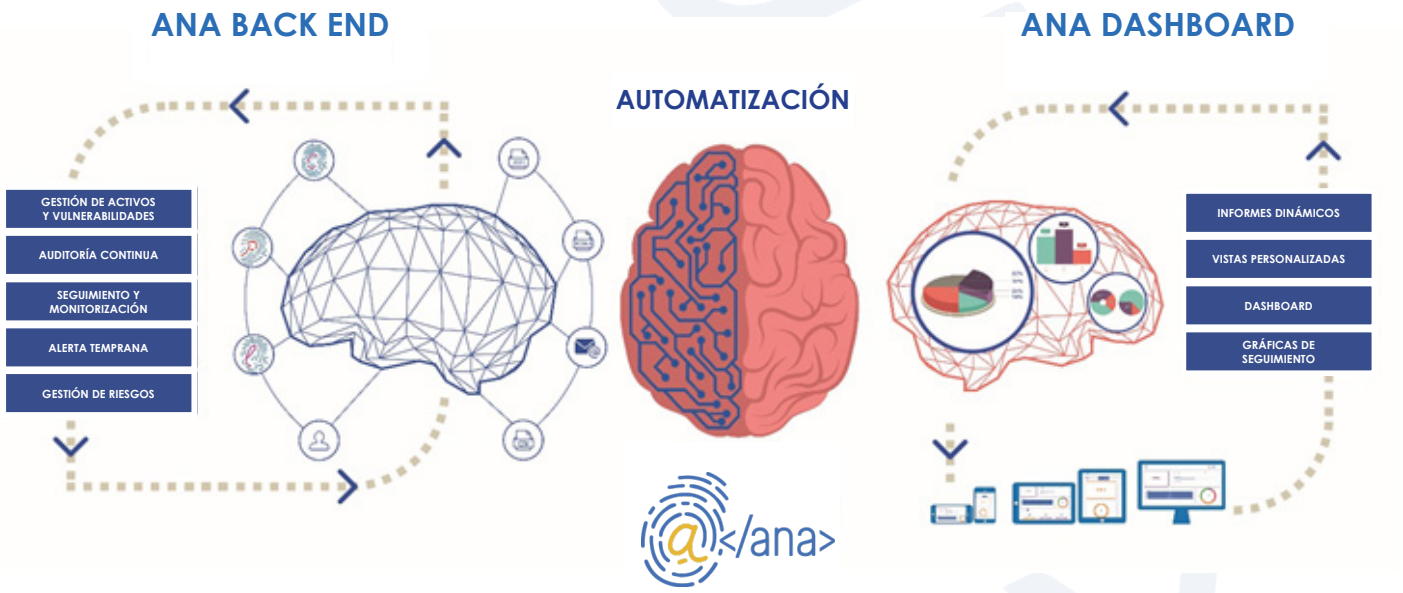
El organismo accede a la solución ANA para configurar el modelo de presentación que más le interese para la generación de los cuadros de mando y tener la capacidad de evaluar en el tiempo el avance del estado y evolución continua de seguridad de sus activos por granularidad, vulnerabilidades localizadas, recomendaciones de mitigación y descarga de informes, tanto ejecutivos como técnicos.

Secciones

La solución se encuentra dividida, de forma global, en dos (2) bloques diferentes:

ANA BACK-END. Donde se parametrizan todos los aspectos asociados a los diferentes organismos y donde se realiza toda la explotación: carga de activos, identificación de vulnerabilidades, integración con otras soluciones, etc.

ANA DASHBOARD. Donde se conectan los diferentes organismos para visualizar el estado de sus activos, vulnerabilidades, paneles de control de evolución y estadísticas, descargar informes, etc. durante todo el ciclo de vida de los activos.



Modalidades de despliegue de ANA

ANA-ON PREMISE

ANA-ON PREMISE se presenta como virtual *appliance* en el formato de máquina virtual. Se implementa mediante la instalación de una máquina virtual en la infraestructura de la organización. Por lo tanto, este despliegue puede llevarse a cabo en cualquiera de las siguientes plataformas de virtualización:

- VMWare
- Hyper-V

Para desplegar ANA bajo esta modalidad será necesario contar con los siguientes requisitos técnicos para instalar el virtual appliance:

- 16 GBytes de RAM
- 4 procesadores virtuales
- 128 GBytes disco SSD
- 1 Interfaz de red virtual
- 1 dirección IP fija
- 2 entradas DNS para ANA-Backend y ANA-Dashboard

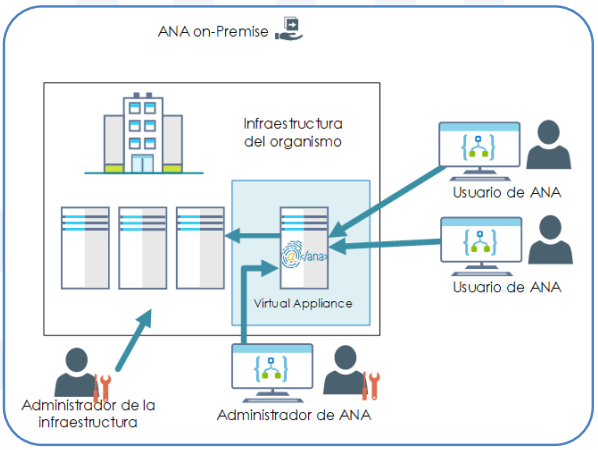


Fig. 1.- Acceso a ANA mediante Appliance en infraestructuras de la organización

ANA-CENTRAL

Se aprovecha la infraestructura de nube privada administrada por el CCN-CERT. El organismo que decida implantar ANA en la modalidad ANA-CENTRAL, deberá solicitarlo al CCN-CERT a través de los canales oficiales (soporte_auditorias@ccn.cni.es). El CCN-CERT se encargará de orquestar todos los procedimientos necesarios para la creación de una nueva instancia de ANA y proporcionar acceso al organismo solicitante.

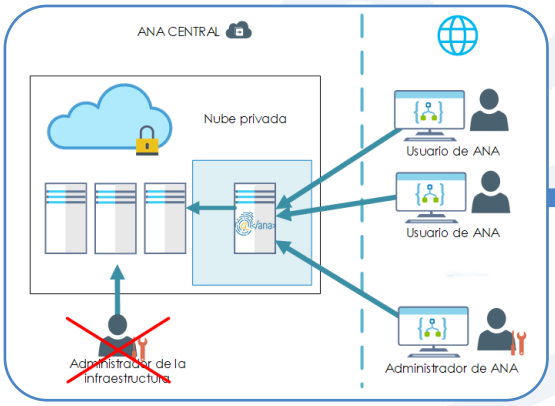


Fig. 2.- Asignación de WorkSpace a la Organización y su modo de acceso

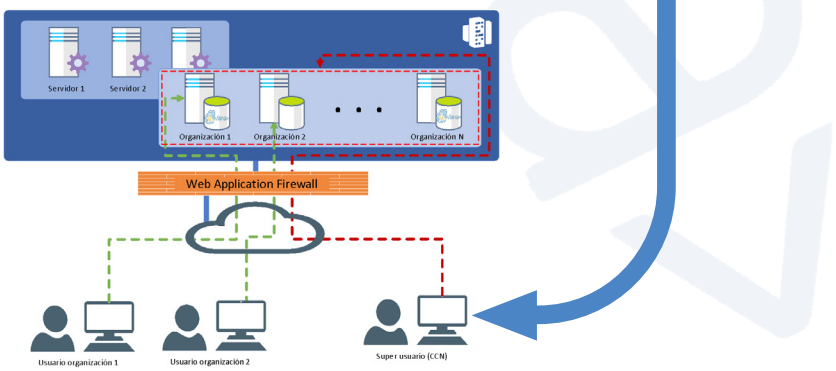


Fig. 3.- Esquema de acceso desde distintas Organizaciones

Comparativa entre ANA-ON PREMISE y ANA-CENTRAL

	ANA-ON PREMISE	ANA-CENTRAL
Instalación y configuración inicial	✓	✓
Administración de usuarios	✓	✓
Configuración de ANA	✓	✓
Acceso a Back-end	✓	✓
Acceso a Dashboard	✓	✓
Informes Ejecutivos/Técnicos	✓	✓
Notificación de alertas	✓	✓
Automatización de pruebas *	✓	✓
No necesita hardware propio	✗	✓
Frecuencia de actualizaciones de la herramienta	Semestral	Continua
Frecuencia de actualizaciones de CPE y CVE	Manual	Diaria
Copia de seguridad de la base de datos	✗	✓
Custodia de los datos de las auditorías	Organismo	CCN-CERT
Soporte incluido (8x5)	✗	✓
Canal de comunicación con el equipo de soporte	Email	Email + Teléfono
Mantenimiento de la infraestructura	✗	✓
Integración con LUCÍA (notificación de alertas)	✗	✓
Soporte respuesta a incidentes CCN-CERT	✗	✓

* ANA-CENTRAL - Solo para recursos accesibles desde internet

Beneficios

1. Control centralizado del estado de los activos del organismo.
2. Seguimiento continuo de los activos y vulnerabilidades para mejorar los tiempos de resolución.
3. Normalización de todas las auditorías realizadas.
4. Sistema de alertas.
5. Evaluación de vulnerabilidades en tiempo real.
6. Histórico de evolución de medidas correctivas.
7. Generación de informes ejecutivos y técnicos, según evolución en el tiempo.
8. Diferentes vistas técnicas y ejecutivas del estado de los sistemas y misiones del organismo.
9. Reducción de tiempos en la gestión de la seguridad.

Integración con otras soluciones CCN-CERT

</clara>
Auditoría de cumplimiento

</lucía>
Gestión de ciberincidentes

</pilar>
Solución de análisis y gestión de riesgos

</ana>

soporte_auditorias@ccn.cni.es

www.ccn-cert.cni.es

CCN-CERT
centro criptológico nacional