XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva

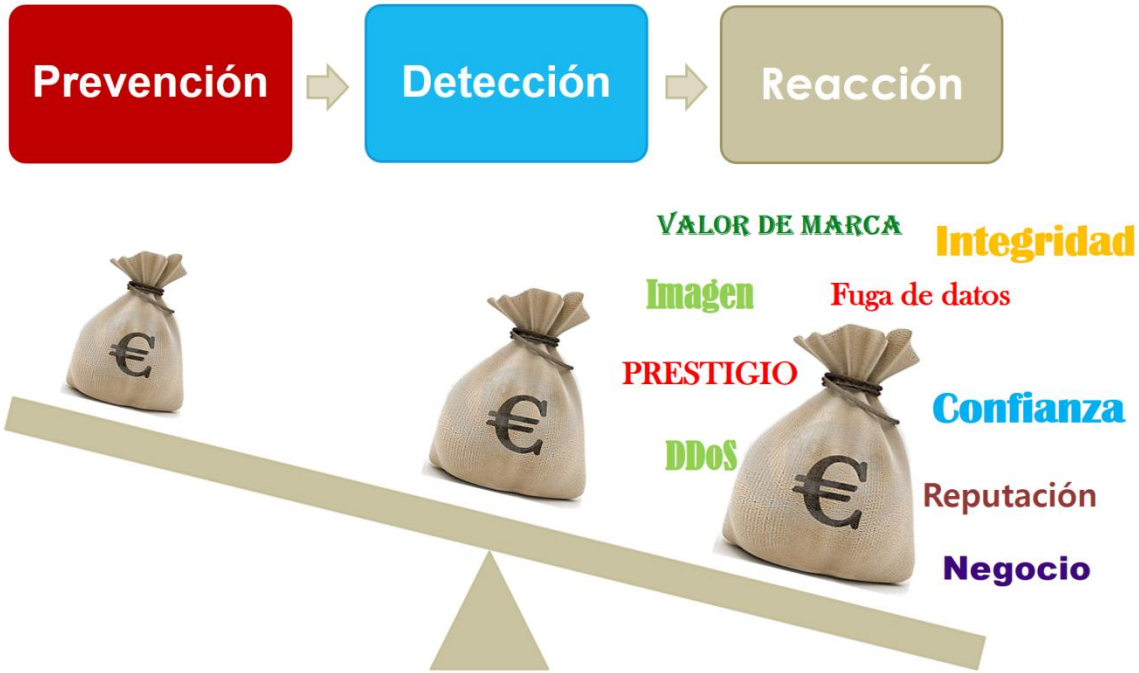
ANA
Automatización y Normalización de Auditorías

centro criptológico nacional

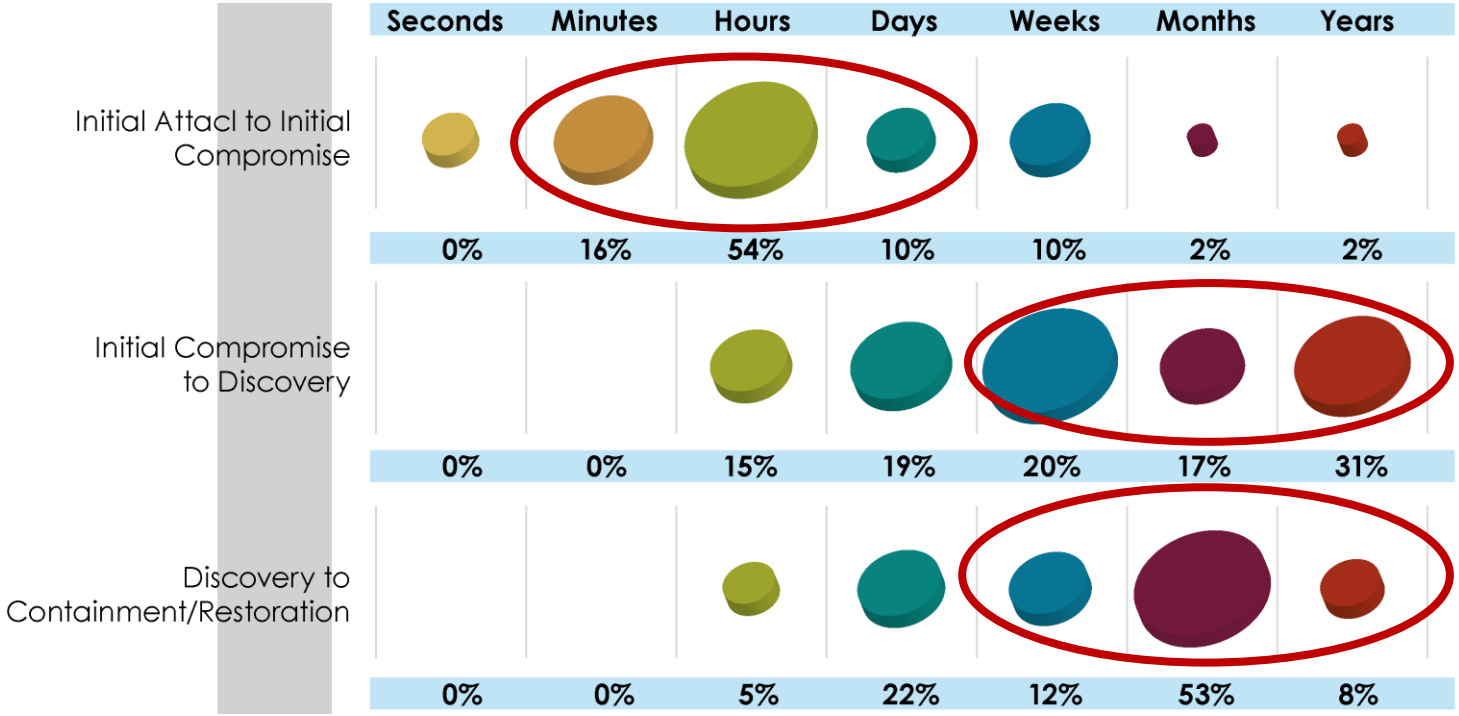
- Pablo López
- Centro Criptológico Nacional
- ccn@ccn.cni.es

- Pedro-Castor Valcárcel Lucas
- Gerencia Informática de la Seguridad Social
- pedro-castor.valcarcel@seg-social.es

Necesidad de Evaluación Continua



Necesidad de Evaluación Continua

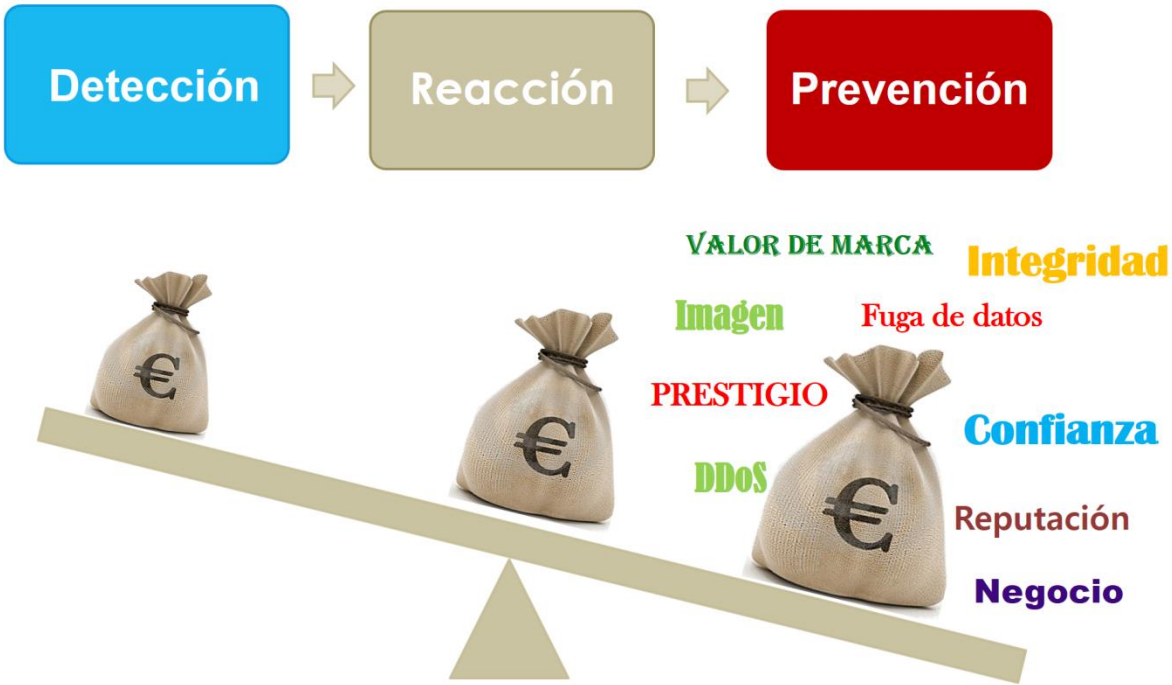


Las **víctimas** de ciberataques **siguen sufriendo ataques** a lo largo del tiempo

Necesidad de Evaluación Continua

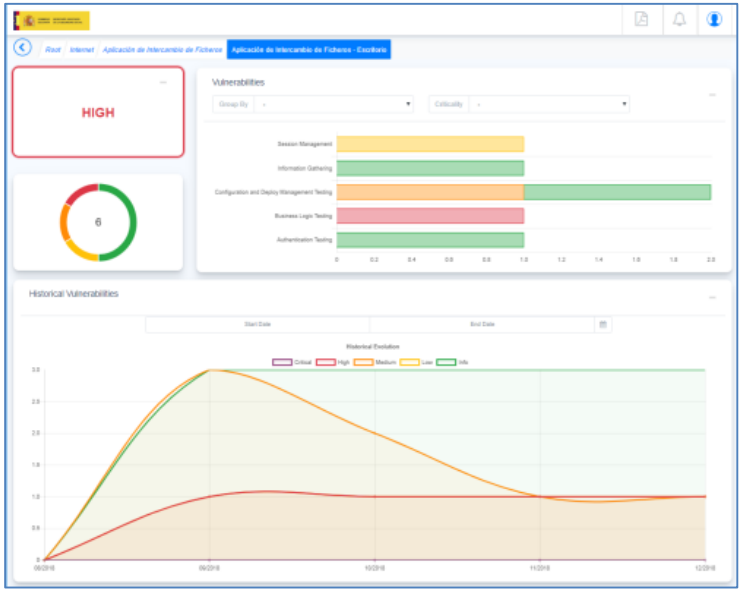
La adaptación a las nuevas amenazas implica **mejorar las capacidades de vigilancia** y diseñar respuestas cada vez más eficaces frente a los ataques

Necesidad de Evaluación Continua



Necesidad de Evaluación Continua

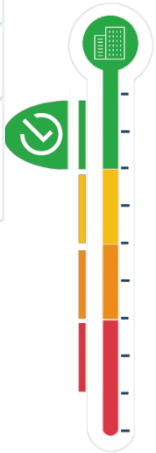
El objetivo es **gestionar y medir de manera continua la evolución de activos** auditados respecto a niveles de seguridad y riesgo definidos, posibilitando con la **priorización de recursos** disponibles la **capacidad de reacción y mitigación** ante posibles defectos de configuración y vulnerabilidades detectadas.



Capacidad de medir la **SEGURIDAD** de exposición de la Organización

Ayudar a reducir la exposición de **VULNERABILIDADES** al exterior de la Entidad

Automatización y Normalización de Auditorías (ANA)



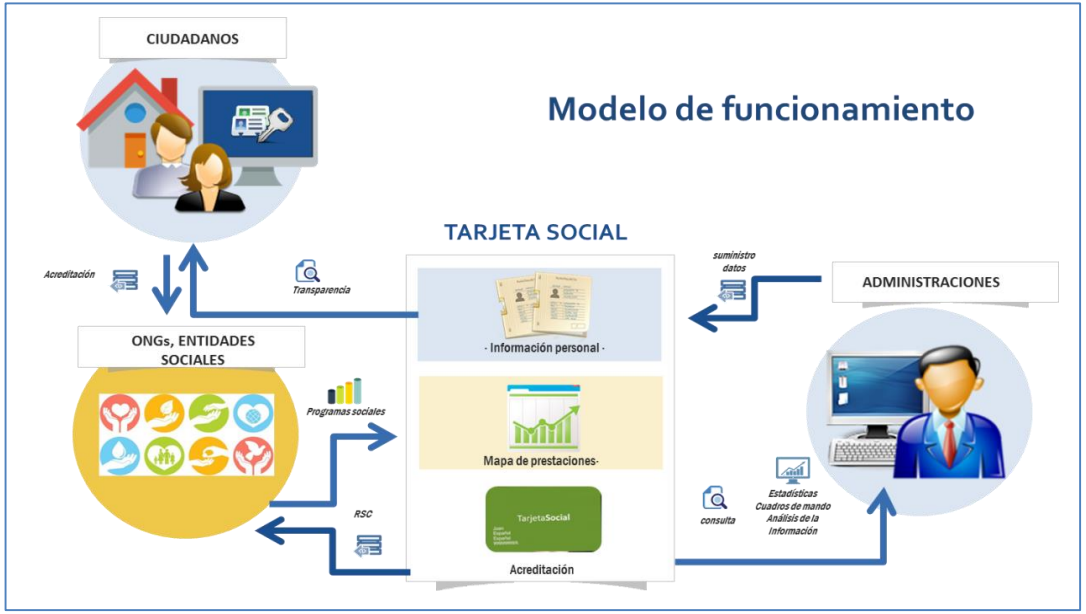
@</ana>

- Acceder en tiempo real a problemas localizados, reproducirlos y seguir su evolución en el tiempo
- Generar dinámicamente informes del estado real de la entidad por departamento, servidor, aplicación o cualquier activo definido
- Organizar la información proporcionando múltiples vistas/cuadro de mandos a los usuarios
- Centralizar y normalizar todas las inspecciones de seguridad realizadas
- Alerta temprana mediante interacción directa y detallada de los problemas encontrados permitiendo una notificación oportuna sin dilación indebida

CASO PRÁCTICO

La Tarjeta Social Universal (TSU) del Ministerio de Empleo y Seguridad Social

Llave de acceso a un catálogo de prestaciones públicas que permite conocer el estado detallado de las prestaciones de contenido económico que percibe una persona en un momento determinado



Gerencia de Informática de la Seguridad Social

@</ana>

CASO PRÁCTICO

PROCEDIMIENTO DE GESTIÓN DE VULNERABILIDADES			
	Tarea	Responsable	Entregable
1	Comunicar vulnerabilidades	Equipo auditor	**Detalle** de las vulnerabilidades
2	Elaborar resumen de vulnerabilidades	Equipo auditor	**Informe general** **Informes parciales** (por tipos de activos)
3	Comunicar resumen de vulnerabilidades	Responsable de seguridad	Informe general (reunión con alta dirección) Informes parciales (reunión con responsables técnicos)

CASO PRÁCTICO

PROCEDIMIENTO DE GESTIÓN DE VULNERABILIDADES			
	Tarea	Responsable	Entregable
4	Asignar responsable de resolver	Responsable de seguridad	Asignar a cada vulnerabilidad las **tareas** a realizar y un **responsable** por cada una
5	Estrategia de resolución	Responsable técnico	Buscar **vulnerabilidades comunes y repetitivas**
6	Asignar fecha de compromiso de resolución	Responsable técnico	Asignar a cada tarea una **fecha de compromiso de resolución**
7	Comprobar que las tareas están resueltas	Responsable de seguridad	Preguntar al responsable técnico y **actualizar su estado** (cierre, pendiente, etc.)

CASO PRÁCTICO

Gerencia de Informática de la Seguridad Social

Demostración

@.</ana>

CASO PRÁCTICO

PROCEDIMIENTO DE GESTIÓN DE VULNERABILIDADES			
	Tarea	Sin ANA	Con ANA
1	Comunicar vulnerabilidades	Aprox. 10 días (esperar a la finalización de las pruebas + preparar reunión de presentación)	Inmediato Sin intermediarios Información detallada y no distorsionada Alertas Canal seguro
2	Elaborar resumen de vulnerabilidades	2 días desde la finalización de las pruebas	Inmediato Resumen por grupos de activos
3	Comunicar resumen de vulnerabilidades	5 días (preparación de reuniones de presentación)	Esta tarea sobra. Ya está recogida en la anterior

CASO PRÁCTICO

PROCEDIMIENTO DE GESTIÓN DE VULNERABILIDADES			
	Tarea	Sin ANA	Con ANA
4	Asignar responsable de resolver	Con otra herramienta	Integración con sistema de ticketing
5	Estrategia de resolución	Con otra herramienta	Informe de vulnerabilidades más comunes
6	Asignar fecha de compromiso de resolución	Con otra herramienta	Asignación inicial por nivel de criticidad
7	Comprobar que las tareas están resueltas	Con otra herramienta	Automatización parcial y alertas

Automatización y Normalización de Auditorías (ANA)

Integración con otras soluciones

Automatización y Normalización de Auditorías (ANA)

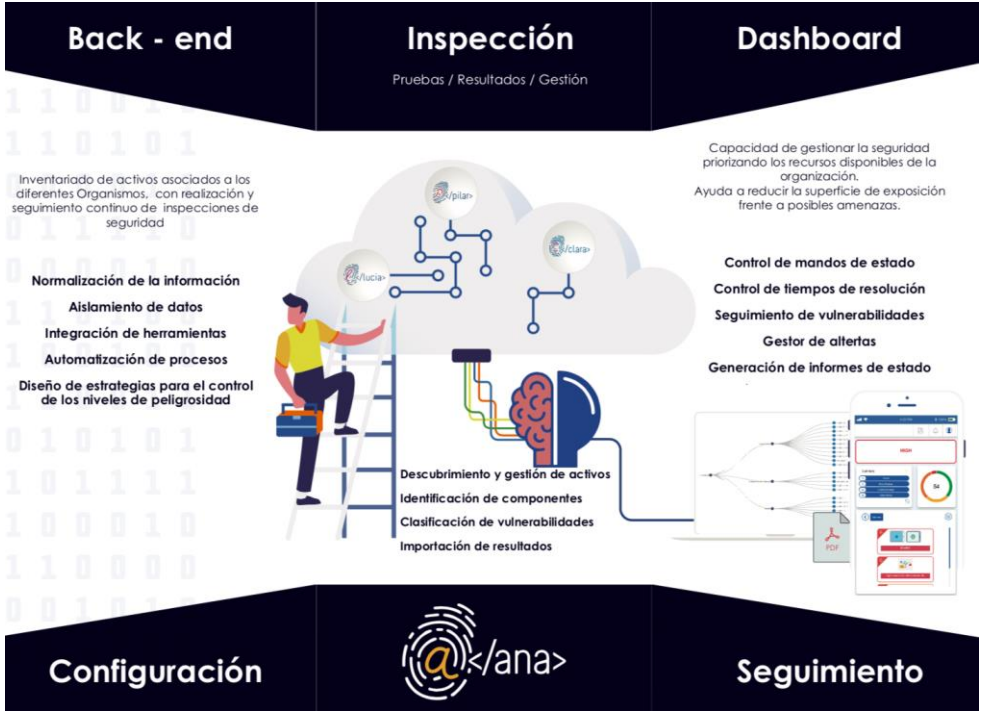
Automatización y Normalización de Auditorías (ANA)

ANA - CENTRAL

ANA - LOCAL

- Capacidad de medir la seguridad y la superficie de exposición.
- Gestión de activos. (integración con CLARA)
- Control y seguimiento de vulnerabilidades.
- Alertas asociadas a vulnerabilidades. (notificación ~~LUCIA~~ / correo electrónico)
- Cálculo automático del estado del riesgo. (integración PILAR)
- Correlación de resultados. (~~gestión centralizada~~)
- Sincronización ~~diaria~~ de CVE (NIST).
- Generación de informes ejecutivo y técnico.
- Cuadro de mandos y alerta temprana.
- Soporte de ~~Respuesta a Incidentes CCN-CERT~~.

Automatización y Normalización de Auditorías (ANA)



- Necesidad de la evaluación permanente del estado de seguridad.
- La gestión de la seguridad consume tiempo y recursos y ANA ha venido a reducir tiempos.
- ANA implementa una gestión eficiente de la detección de vulnerabilidades y notificación de alertas.
- ANA proporciona recomendaciones para un tratamiento oportuno de la superficie de exposición.

@</ana>

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectiva

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional