



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

El arte de la ciberresiliencia.

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: M Soraya Artiles Burgos

DIRECTORES: Javier Vales Alonso
Miguel Rodelgo Lacruz

CURSO ACADÉMICO: 2023-2024

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

El arte de la ciberresiliencia.

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de Telecomunicación

UniversidadeVigo

RESUMEN

La capacidad para anticipar, resistir, recuperarse y adaptarse a ciberataques a las infraestructuras TIC de Defensa es crucial para el normal desarrollo de las misiones de Defensa Nacional, las cuales se desarrollan en un escenario mayoritario de tecnologías de la información y la comunicación (TIC). Este trabajo pretende estudiar las estrategias y acciones que se tienen que llevar a cabo para reducir la superficie de exposición en las infraestructuras TIC de Defensa, y que son aplicables al contexto de sistemas de información complejos en grandes organizaciones. Estas acciones se basan tanto en la experiencia de la Jefatura de Ciberseguridad del Ministerio de Defensa como en las recomendaciones de la Agencia de Ciberseguridad (NCIA) de la OTAN.

El objetivo de este trabajo es la definición de un conjunto de acciones de automatización de tareas de ciberresiliencia gracias al desarrollo de una plataforma de gestión continua de la superficie de exposición a amenazas. Además, se plantea el desarrollo de un modelo de aprendizaje automático para reconocer el estado de riesgo de la superficie. Este algoritmo aprenderá de la inseguridad observada a diario y contribuirá a priorizar las acciones de mitigación. Asimismo, se proponen acciones para fortalecer la seguridad de los activos y garantizar el cumplimiento normativo en ciberseguridad.

Junto con estas acciones de automatización, que deben ejecutarse dentro de una plataforma con acceso restringido en la infraestructura TIC de Defensa, se implementan asimismo acciones manuales de seguimiento, coordinación y comunicación por parte de diversos roles de la organización para la reducción de la superficie de exposición. En síntesis, el objetivo final de este Trabajo Final de Máster (TFM) es el análisis y diseño de desarrollos innovadores que aborden la construcción de un entorno ciberresiliente para la reducción de la superficie de exposición. Esto se logrará mediante la implementación del conjunto de acciones de ciberresiliencia y su despliegue en una infraestructura TIC heterogénea y compleja, de forma que se pongan en juego todas las capacidades de automatización y coordinación de los actores que defienden y fortifican la columna vertebral digital de la Defensa.

PALABRAS CLAVE

Ciberresiliencia¹, resiliencia², ciberseguridad, superficie, vulnerabilidad

¹ La Real Academia Española (RAE) contempla términos que han sido conformados con el elemento compositivo ciber, para expresar terminología relacionada con el mundo de las computadoras u ordenadores y de la realidad virtual, y recomienda su uso en la creación de términos pertenecientes al ámbito de las comunicaciones por internet (<https://www.rae.es/dpd/ciber>). Algunos ejemplos del elemento compositivo ciber pueden ser ciberresiliencia, ciberseguridad, ciberataque, ciberamenaza, ciberinteligencia, ciberincidente o ciberdefensa, siendo ciberespacio y cibernauta entradas incluidas en el propio diccionario de la lengua española de la RAE.

² En su segunda acepción, la RAE define resiliencia como la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido.

AGRADECIMIENTOS

A mi familia, a mi marido, por los momentos de ausencia y por su apoyo incondicional.

A mis tutores, por mejorar cada idea... por sus acertadas correcciones.

A la fábrica de sueños de SUPERFICIE.

CONTENIDO

Contenido	1
Índice de Figuras	4
Índice de Tablas.....	6
1 Introducción y objetivos	7
1.1 Marco conceptual	7
1.2 Motivación	9
1.3 Objetivos	12
1.3.1 OBJ.1 – Definición de acciones de comunicación y coordinación para la reducción de la superficie de exposición en infraestructuras TIC	13
1.3.2 OBJ.2 – Desarrollo de un entorno ciberresiliente que permite reducir la superficie de exposición en infraestructuras TIC.....	14
1.3.3 OBJ.3 – Cumplimiento con la normativa en ciberseguridad	15
1.4 Estructura y contenidos	16
2 Estado del arte	18
2.1 Topología de la superficie de exposición.....	18
2.1.1 Superficie interna.....	19
2.1.2 Superficie externa	20
2.1.3 Superficie oculta	21
2.1.4 Superficie obsoleta.....	22
2.1.5 Superficie vulnerable	22
2.1.6 Superficie señuelo.....	24
2.2 Gestión de la superficie de exposición.....	25
2.2.1 Evolución de la gestión de la superficie de exposición	27
2.2.2 Roles de la superficie de exposición.....	29
2.3 Herramientas para la gestión de la superficie de exposición	30
2.3.1 HER.1 – Herramientas de evaluación (ASCA)	32
2.3.2 HER.2 – Herramientas de gestión de la superficie de ataque de ciberactivos (CAASM)	33
2.3.3 HER.3 – Herramientas de gestión de la superficie externa (EASM)	34
2.3.4 HER.4 – Herramientas de detección y respuesta extendida ante amenazas (XDR)	35
2.3.5 HER.5 – Herramientas de simulación de amenazas (BAS).....	36
2.3.6 HER.6 – Servicios de Protección de Riesgos Digitales (DRPS)	37
2.3.7 HER.7 – Herramientas de detección y respuesta de red (NDR).....	38
2.3.8 HER.8 – Herramientas de gestión de eventos de seguridad (SIEM).....	39

2.3.9 HER.9 – Herramientas de gestión de vulnerabilidades (VM)	40
2.3.10 HER.10 – Herramientas de gestión TIC y configuración (ITSM y CMDB).....	41
2.3.11 HER.11 – Herramientas de control de acceso a red (NAC)	42
2.4 Tipos de vulnerabilidades en la superficie de exposición	43
2.4.1 VUL.1 – Vulnerabilidades y Exposiciones Comunes (CVE).....	43
2.4.2 VUL.2 – Enumeración de Vulnerabilidad Comunes (CWE)	44
2.4.3 VUL.3 – Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP).....	44
2.4.4 VUL.4 – Configuraciones inseguras.....	44
2.5 Normativa de ciberseguridad relativa a la superficie de exposición.....	45
2.5.1 NOR.1 – Esquema Nacional de Seguridad (ENS).....	45
2.5.2 NOR.2 – Ley de Ciberseguridad de la Unión Europea	46
2.5.3 NOR.3 – Ley de ciberresiliencia de la Unión Europea.....	46
3 Acciones de ciberresiliencia	47
3.1 Trazabilidad entre estrategias, objetivos y acciones de ciberresiliencia	47
3.2 Desarrollo de las acciones de ciberresiliencia.....	48
3.2.1 ACC.1.1, 1.2 – Creación de grupos de trabajo (Principio de la unidad – Unir para vencer)	49
3.2.2 ACC.2.1 – Identificación de la superficie de exposición (Principio del conocimiento – Conocimiento del enemigo y del entorno)	50
3.2.3 ACC.2.2 – Detección de vulnerabilidades de la superficie de exposición (Principio de adaptación – Conocer las debilidades propias)	52
3.2.4 ACC.2.3 – Priorización de acciones de mitigación en la superficie de exposición (Principio de la economía – Priorizar los esfuerzos).....	53
3.2.5 ACC.2.4 – Monitorización de agentes en la infraestructura (Principio del terreno – Disponer los mensajeros sobre el terreno)	54
3.2.6 ACC.2.5 – Telemetría de seguridad de la infraestructura (Principio de la planificación – Planificar y reflexionar).....	54
3.2.7 ACC2.6 – Creación de una infraestructura señuelo (Principio del engaño – Fingir debilidad).....	56
3.2.8 ACC2.7 – Evaluación de amenazas (Principio de sorpresa – Evaluación constante)	57
3.2.9 ACC3.1, 3.2, 3.3 – Bastionado de activos, ENS y Ley de Ciberresiliencia (Principio de defensa – Defender en profundidad)	58
4 Metodología, implementación y validación	59
4.1 Metodología de desarrollo	59
4.1.1 Pruebas de concepto para la selección de herramientas de ciberseguridad	59
4.1.2 Recogida de información a través de APIs	60
4.1.3 Desarrollo ágil de la plataforma	61
4.2 Implementación de una plataforma CTEM.....	62

4.2.1 Recopilación nocturna de datos de las herramientas de ciberseguridad.....	63
4.2.2 Descubrimiento de activos (superficie interna)	65
4.2.3 Descubrimiento de activos (superficie externa)	66
4.2.4 Trazabilidad superficie interna-externa	67
4.2.5 Listado de Vulnerabilidades	68
4.2.6 Riesgos de la identidad digital	69
4.2.7 Información estratégica de la superficie de exposición	69
4.2.8 Comunicación del Equipo de Seguridad Defensiva con el resto de gestores de vulnerabilidades.....	70
4.2.9 Conectividad de los agentes.....	71
4.2.10 Gestión de usuarios.....	72
4.2.11 Seguridad de la plataforma CTEM	72
4.3 Cuantificación de la superficie anómala	73
4.4 Verificación de los KPI con la plataforma CTEM.....	76
4.5 Validación de la plataforma SUPERFICIE como enfoque CTEM.....	79
5 Conclusiones y líneas futuras	86
5.1 Conclusiones	86
5.2 Líneas futuras	87
6 Bibliografía.....	88
Anexo I: Acrónimos	91

ÍNDICE DE FIGURAS

Figura 1 Principios estratégicos de Sun Tzu aplicados a la ciberresiliencia [Fuente propia]	9
Figura 2 Cronograma de los ataques de Rusia en la guerra de Ucrania [5]	10
Figura 3 Proceso de gestión de vulnerabilidades a través de enumeración de activos, configuración segura y parcheo [Fuente propia].....	11
Figura 4 Objetivos para la reducción de la superficie de exposición [Fuente Propia]	13
Figura 5 Topología de la superficie de exposición [Fuente propia realizada con Blender].....	18
Figura 6 Superficie interna [Fuente propia realizada con Blender]	19
Figura 7 Superficie externa [Fuente propia realizada con Blender].....	20
Figura 8 Superficie oculta [Fuente propia realizada con Blender].....	21
Figura 9 Superficie obsoleta [Fuente propia realizada con Blender]	22
Figura 10 Superficie vulnerable [Fuente propia realizada con Blender]	23
Figura 11 Superficie señuelo [Fuente propia realizada con Blender]	24
Figura 12 Etapas del programa CTEM [18]	27
Figura 13 Evolución: De la gestión de la superficie de exposición a la gestión continua de la exposición a amenazas (CTEM) [Fuente propia]	28
Figura 14 Roles para la gestión continua de la superficie de exposición a amenazas (CTEM) [Fuente propia]	30
Figura 15 Ciclo de Hype para operaciones de seguridad, 2023 (Gartner) [25].....	31
Figura 16 Trazabilidad estrategias, objetivos, y acciones de ciberresiliencia para la reducción de la superficie de exposición [Fuente propia]	48
Figura 17 Acciones de ciberresiliencia [Fuente Propia].....	49
Figura 18 Capacidades necesarias para la gestión de la superficie de exposición a amenazas (CTEM) [39]	63
Figura 19 Herramientas para alimentar la gestión de la superficie de exposición a amenazas (CTEM) [Fuente propia].....	64
Figura 20 SUPERFICIE – Enumeración de activos internos (servidores) [Fuente SUPERFICIE] ...	65
Figura 21 SUPERFICIE – Vulnerabilidades y acciones en un activos interno (servidor) [Fuente SUPERFICIE]	66
Figura 22 SUPERFICIE – Enumeración de activos externos (dominios) [Fuente SUPERFICIE]	66
Figura 23 SUPERFICIE – Información de activos externos (direcciones IP) [Fuente SUPERFICIE]	67
Figura 24 SUPERFICIE – Enumeración de activos externos (certificados) [Fuente SUPERFICIE]	67
Figura 25 SUPERFICIE – Listado de vulnerabilidades [Fuente SUPERFICIE].....	68
Figura 26 SUPERFICIE – Vulnerabilidad con los activos afectados [Fuente SUPERFICIE]	69
Figura 27 SUPERFICIE – Riesgos de la identidad digital [Fuente SUPERFICIE]	69

Figura 28 SUPERFICIE – Panel estratégico [Fuente SUPERFICIE].....	70
Figura 29 SUPERFICIE – Panel táctico-operativo [Fuente SUPERFICIE].....	71
Figura 30 SUPERFICIE – Panel táctico y operativo con notificaciones a los gestores de vulnerabilidades [Fuente SUPERFICIE].....	71
Figura 31 SUPERFICIE – Panel de monitorización [Fuente SUPERFICIE].....	72
Figura 32 SUPERFICIE – Roles y privilegios [Fuente SUPERFICIE].....	72
Figura 33 Algoritmo de regresión lineal múltiple – Valores de entrenamiento [Fuente propia]	75
Figura 34 Algoritmo de regresión lineal múltiple – Valores reales vs. reales predichos [Fuente propia]	75
Figura 35 Modelo de madurez de alto nivel para un programa CTEM [16].....	86
Figura 36 Líneas futura para la reducción de la superficie de exposición – Mejora de la ciberresiliencia	87

ÍNDICE DE TABLAS

Tabla 1 Indicadores clave de rendimiento del Objetivo 1 [Fuente propia]	13
Tabla 2 Indicadores clave de rendimiento del Objetivo 2 [Fuente propia]	15
Tabla 3 Indicadores clave de rendimiento del Objetivo 3 [Fuente propia]	16
Tabla 4 Trazabilidad entre objetivos y acciones [Fuente propia].....	47
Tabla 5 Indicadores clave de rendimiento para medir la superficie de exposición [Fuente Propia]	79
Tabla 6 Validación de la plataforma SUPERFICIE como CTEM [17]	85

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Marco conceptual

Cuando una infraestructura de Tecnologías de la Información y Comunicaciones (TIC) se ve afectada por una vulnerabilidad que, en solo 3 días tiene más de 60 variantes de ciberataques, lo primero que uno se pregunta es cómo se ha visto afectada esa infraestructura. Y la respuesta es la misma que se lleva contestando el ser humano desde que defiende infraestructuras físicas: depende de la superficie expuesta.

En el mundo militar, el concepto de superficie de exposición fue acuñado para referirse a todo aquello que era visible por el enemigo. El concepto de mínima superficie de exposición busca reducir al máximo lo que sea visible para el enemigo. En términos de la defensa de infraestructuras físicas nos referimos tanto a la ocultación de posiciones defensivas como a la protección y encubrimiento de los propios activos que "habitan" la infraestructura. No obstante, cuando hablamos de la seguridad de infraestructuras lógicas o ciberseguridad, las actuaciones no son tan diferentes. Para minimizar la superficie de exposición de una infraestructura TIC, el objetivo principal será reducir al mínimo la visibilidad de todos sus activos (datos, redes...): ocultarlos, eliminar los obsoletos y cortar los caminos de ataque.

Una infraestructura TIC habita en el ciberespacio, que no es más que un entorno de información [1], por lo que la reducción al mínimo de la visibilidad de los activos que "pueblan" esa infraestructura conllevará intrínsecamente la fortificación de ese entorno de información. Esta fortificación incluye la mitigación de vulnerabilidades en los activos presentes, la ocultación de aquellos que no interesa que estén expuestos por no dar un servicio hacia el exterior, y el descubrimiento de todo activo que en un principio haya pasado desapercibido para el propio dueño de la infraestructura.

Por ende, las acciones destinadas a la protección de las redes y sistemas de información se desarrollan en el ciberespacio, y requieren claramente la reducción de la superficie de exposición. Estas acciones tienen que ver menos con actuaciones intrincadas y laberínticas, y más con algunos principios básicos como los definidos por el general, estratega militar y filósofo de la antigua china Sun Tzu [2]. Estos principios se aplican exclusivamente a la propia defensa de una infraestructura TIC:

1. **Principio de la unidad - Unir para vencer:** Sun Tzu fomentaba la colaboración entre diferentes equipos con distintas responsabilidades. En el ámbito de la ciberseguridad, la colaboración entre las diferentes unidades de una organización, como el Equipo de Seguridad, personal de tecnologías de la información y otros departamentos, permite obtener una visión unificada de los puntos débiles de la infraestructura. Esta colaboración mejora la visión conjunta y contribuye a la reducción de la superficie de exposición ante posibles amenazas.
 - *El supremo arte de la guerra es someter al enemigo sin luchar. La oportunidad de derrotar al enemigo está en tus manos; no en la oportunidad que el enemigo te brinda.*
2. **Principio del conocimiento - Conocimiento del enemigo y del entorno:** Sun Tzu enfatizaba la importancia de conocer a tu enemigo y el terreno en el que te enfrentas. En ciberresiliencia, esto se traduce en la necesidad de conocer todos los elementos de la infraestructura, comprender las ciberamenazas, los posibles actores maliciosos y las vulnerabilidades en la infraestructura TIC.
 - *Conoce al adversario y sobre todo concóctete a ti mismo y serás invencible.*
 - *La información es poder.*
3. **Principio de adaptación - Conocer las debilidades propias:** Sun Tzu abogaba por la inteligencia para la adaptación en la estrategia. En ciberresiliencia, esto significa que las organizaciones deben ser capaces de ajustar sus estrategias y defensas en base a las vulnerabilidades encontradas y conforme evolucionan las ciberamenazas.
 - *Sé flexible y reflexiona antes de realizar un movimiento.*

- *No debes depender de las condiciones favorables, ni de las condiciones desfavorables, sino que debes estar preparado para adaptarte a las condiciones.*
 - *La invencibilidad está en uno mismo, la vulnerabilidad en el adversario.*
4. **Principio de la economía** - *Priorizar los esfuerzos*: Sun Tzu aconsejaba utilizar los recursos de manera eficiente. En ciberresiliencia, esto significa asignar recursos de seguridad de manera eficaz, centrándose en áreas críticas de la infraestructura.
- *Si se envían refuerzos a todas partes, se es débil en todas partes.*
 - *Grandes resultados pueden ser conseguidos con pequeños esfuerzos.*
5. **Principio de terreno** - *Disponer los mensajeros sobre el terreno*: Sun Tzu argumenta que tener espías o agentes secretos bien ubicados en el campo de batalla es esencial para obtener información valiosa sobre el enemigo, sus movimientos, su moral y sus planes. Esto permite a un comandante tomar decisiones informadas. En ciberseguridad, esto se traduce en el despliegue de agentes por toda la infraestructura y a todos los niveles para poder obtener información de debilidades, amenazas a través de la simulación, configuraciones y potenciales caminos de ataque. La comunicación efectiva es clave para la ciberresiliencia.
- *La disposición de las tropas es clave para lograr la victoria, ya que una disposición adecuada puede maximizar las fortalezas y minimizar las debilidades de los soldados.*
 - *Sólo cuando conoces cada detalle de la condición del terreno puedes maniobrar y luchar.*
 - *Los que no saben tener mapas, hacer reconocimientos o utilizar guías locales, son incapaces de obtener ventaja del terreno.*
6. **Principio de la planificación** - *Planificar y reflexionar*: Sun Tzu enfatizaba la importancia de la planificación cuidadosa y la estrategia. En ciberresiliencia, esto se traduce en la necesidad de acumular la mayor cantidad de datos sobre el terreno de forma que se puedan planificar planes de respuesta a incidentes y estrategias de recuperación en caso de un ataque.
- *Reflexionar antes de hacer un movimiento.*
 - *Resolver dificultades antes de que surjan.*
 - *Las tácticas sin estrategia son el ruido antes de la derrota.*
7. **Principio del engaño** - *Fingir debilidad*: Sun Tzu hablaba sobre la importancia de confundir al enemigo. En ciberseguridad, esto implica la utilización de tácticas de señuelo y detección temprana para identificar posibles amenazas.
- *Conocer al enemigo y utilizar al enemigo para derrotar al enemigo.*
 - *Para conocer a tu enemigo debes convertirte en tu enemigo.*
 - *Engaña al enemigo moviendo algo que él está obligado a observar.*
8. **Principio de sorpresa** - *Evaluación constante*: Sun Tzu hacía hincapié en la importancia de la valoración estratégica de las tropas, el enemigo y el terreno como parte fundamental de la ejecución de una campaña militar. En ciberresiliencia la realización de evaluaciones regulares de riesgos y vulnerabilidades en la infraestructura TIC consigue mantener un ciclo de mejora continua en la ciberdefensa de esta infraestructura.
- *La manera de evitar lo que es seguro es estar en guardia, lo que es probable es estar preparado, pero lo que es completamente inesperado es ser completamente desconcertante.*
9. **Principio de la defensa** - *Defender en profundidad*: Sun Tzu recomendaba la construcción de defensas en profundidad para protegerse contra los ataques enemigos. En ciberseguridad, esto se traduce en el bastionado y securización³ de los activos de la infraestructura. Por otra parte, se

³ La Fundación del Español Urgente ([FundeuRAE](http://FundeuRAE.org)), promovida por la Real Academia Española y la Agencia EFE, recomienda utilizar el verbo securizar que resulta más adecuado que securizar con el significado de ‘hacer que un ordenador o una operación realizada por internet sean seguros’.

incluye el cumplimiento con normativa específica de seguridad para llegar a una defensa casi total.

- *La defensa es para tiempos de escasez, el ataque para tiempos de abundancia.*

Si bien no se pueden aplicar los principios de Sun Tzu directamente a la ciberresiliencia, su enfoque en la estrategia, la adaptación y el conocimiento del enemigo puede proporcionar una base sólida para abordar los desafíos de ciberseguridad a los que se enfrenta una infraestructura TIC hoy en día.

La ciberresiliencia de una infraestructura se puede entender como la capacidad para trascender (anticiparse, resistir, recuperarse, adaptarse) a cualquier amenaza en una infraestructura TIC. En este sentido, se entiende que la ciberresiliencia se fundamenta en la capacidad de una organización para aplicar principios estratégicos con el objetivo de proteger sus activos y garantizar la continuidad operativa en un entorno cibernético en constante evolución. Las estrategias de ciberresiliencia basadas en los principios de Sun Tzu, que cualquier organización debe adoptar para fortalecer su capacidad de mantener la continuidad operativa y minimizar el impacto de posibles ciberataques, se resumen en los siguientes pasos mostrados en la figura a continuación:



Figura 1 Principios estratégicos de Sun Tzu aplicados a la ciberresiliencia [Fuente propia]

1.2 Motivación

La capacidad para anticipar, resistir, recuperarse y adaptarse a ciberataques [3] en las infraestructuras TIC de Defensa es crucial para el normal desarrollo de las misiones de Defensa

Nacional, las cuales se desarrollan en un escenario híbrido en el que el ciberespacio juega un papel decisivo.

Un ejemplo de actualidad, y que ha marcado nuevas reglas en el arte de la guerra, es la propia guerra de Ucrania en la que el conjunto de acciones hostiles van dirigidas a escenarios cibernéticos, a la propia economía o incluso al establecimiento de vectores de influencia en internet, redes sociales o localizaciones físicas, llevando incluso a la creación de una armada IT por parte de Ucrania en febrero de 2022 para abordar las amenazas en el ciberespacio [4]. A continuación, se muestra la Figura 2 que ilustra un ejemplo de campañas de phishing respaldadas por el Gobierno Ruso antes y durante la Guerra de Ucrania:

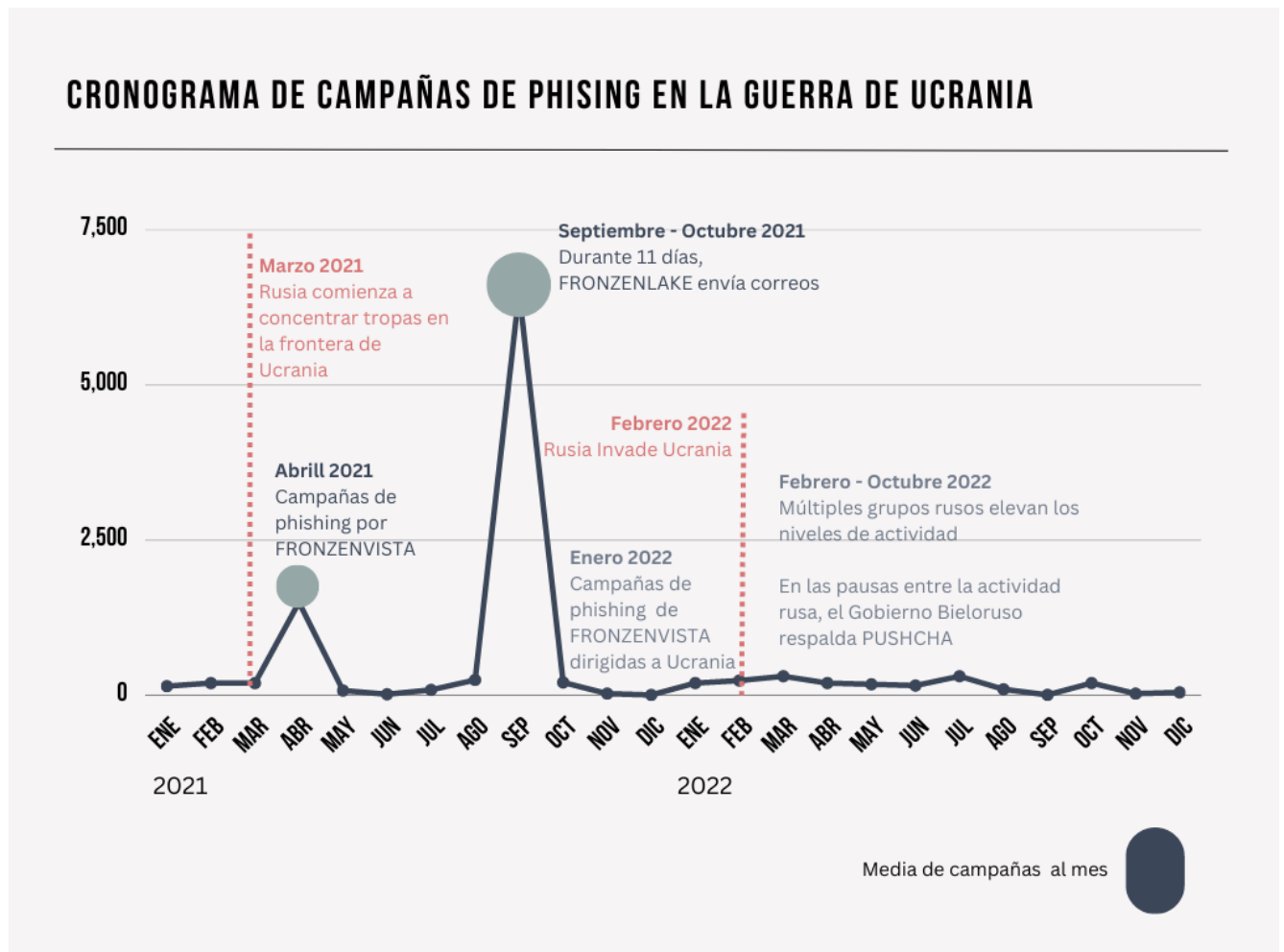


Figura 2 Cronograma de los ataques de Rusia en la guerra de Ucrania [5]

Las capacidades de ciberresiliencia de una infraestructura TIC requieren inevitablemente la reducción de la superficie de exposición mediante estrategias de seguridad efectivas. Esto incluye la automatización de procesos relacionados con la configuración y actualización de software de los activos, mejorando intrínsecamente el cumplimiento normativo y logrando una infraestructura más eficiente y fácil de gestionar [6]. Esta reducción implica una disminución en la cantidad de sistemas, aplicaciones y servicios que necesitan ser monitorizados y protegidos. A largo plazo, se espera una disminución en el número de ciberataques, lo que conlleva un menor tiempo y coste dedicado a mitigar incidentes de seguridad.

Este trabajo pretende estudiar las estrategias y acciones que se tienen que llevar a cabo para reducir la superficie de exposición en las infraestructuras TIC de Defensa, y que son aplicables al contexto de sistemas de información complejos en grandes organizaciones. Estas acciones se basan, por una parte

en las propia experiencia dentro de la Jefatura de Ciberseguridad del Ministerio de Defensa, y por otra parte en las recomendaciones de la Agencia de Ciberseguridad (NCIA⁴) de la OTAN.

Concretamente, la experiencia de la Jefatura de Ciberseguridad es un elemento primordialmente práctico, que conlleva un trabajo de análisis diario y revisión periódica de los avances llevados a cabo en la gestión de vulnerabilidades a través del desarrollo de una plataforma de gestión de vulnerabilidades, así como la mejora continua de éste desarrollo a través de su revisión de todos los actores involucrados en el proceso.

En cuanto a la estrategia de la NCIA relativa a la gestión de vulnerabilidades, ésta se lleva a cabo a través de la identificación de activos, gestión de la configuración y aplicación de parches. Todas estas acciones se establecen como elementos imprescindibles para la mejora de la ciberresiliencia de las organizaciones de Defensa (ACPV⁵) [7]. Gracias a la consecución de esta estrategia ACPV, la gestión de vulnerabilidades se basa en un enfoque informado sobre riesgos que permite una toma de decisiones priorizada de las acciones de mitigación de vulnerabilidades debidamente justificada. A continuación, se muestra la Figura 3 que desglosa el conjunto de acciones para cada uno de los tres elementos ACPV (i.e., Activos, Configuración y Parches).

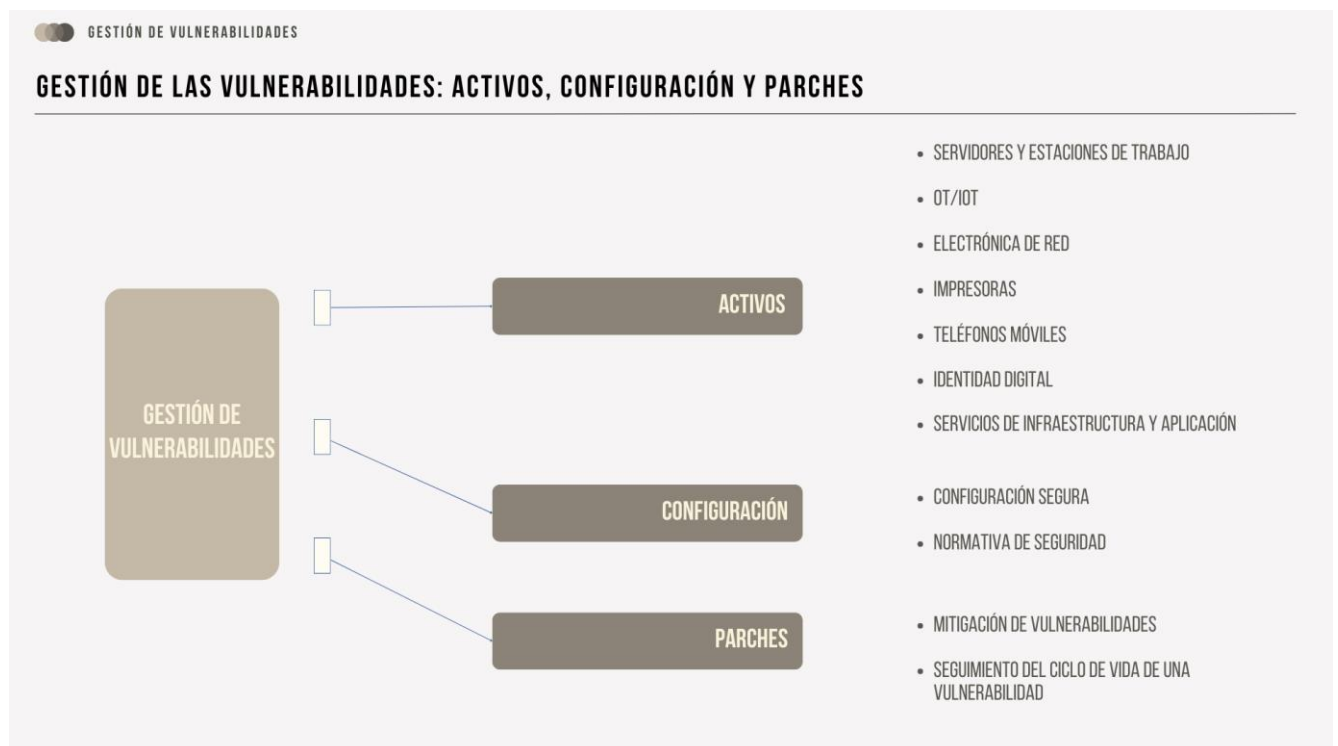


Figura 3 Proceso de gestión de vulnerabilidades a través de enumeración de activos, configuración segura y parcheo [Fuente propia]

Tanto la perspectiva eminentemente práctica de la Jefatura de Ciberseguridad como el abordaje procedimental de la NCIA se complementan para llevar a cabo una serie de acciones que permiten mejorar la ciberresiliencia de una infraestructura TIC. Es importante entender que la propia Unión Europea, en su regulación de ciberseguridad [8] establece la importancia de la creación de ciberresiliencia por parte de sus Estados miembros, por lo que este trabajo tiene como objetivo aportar un granito de arena para incrementar la protección de las redes y sistemas de información, desarrollar y

⁴ NCIA, NATO (North Atlantic Treaty Organization) Communication and Information Agency.

⁵ ACPV, nomenclatura OTAN para activos, configuración, parches y vulnerabilidad, por sus siglas en inglés.

mejorar la ciberresiliencia, así como la capacidad de respuesta, y despliegue de competencias en el ámbito de la ciberseguridad.

1.3 Objetivos

Reducir la superficie de exposición de una infraestructura conlleva necesariamente la reducción de la superficie de ataque, siendo ésta un aspecto crítico para garantizar la ciberseguridad, y consiguientemente se constituye como una estrategia clave para la mejora de la ciberresiliencia en una infraestructura TIC. Esta estrategia se refiere a la disminución de la cantidad de activos, sistemas de información y datos que están directamente expuestos a ciberamenazas.

La reducción de la superficie de ataque y la reducción de la superficie de exposición son conceptos relacionados en el ámbito de la ciberseguridad y la gestión de riesgos. Ambos se centran en minimizar las oportunidades y puntos de vulnerabilidad que podrían ser explotados por atacantes, pero se enfocan en diferentes aspectos de seguridad.

1. **Reducción de la superficie de ataque:** este concepto se refiere a la implementación de estrategias y medidas para disminuir las oportunidades y puntos de entrada que podrían ser explotados por atacantes. Esto implica fortalecer la seguridad de sistemas, redes y aplicaciones para limitar el acceso no autorizado y prevenir la explotación exitosa de vulnerabilidades. Las estrategias para reducir la superficie de ataque incluyen parcheo y actualización de software, segmentación de red, control de acceso y autenticación multifactor⁶, entre otros.
2. **Reducción de la superficie de exposición:** este concepto se centra en minimizar la cantidad de activos que se exponen al entorno lógico y, por lo tanto, a posibles amenazas. Esto implica la identificación y eliminación de activos no utilizados, la limitación de la visibilidad de ciertos activos a través de técnicas como segmentación de red y la protección adecuada de activos críticos. Al reducir la superficie de exposición, se disminuyen los puntos que los atacantes podrían utilizar como camino de entrada.

En resumen, mientras que la reducción de la superficie de ataque se centra en fortalecer la seguridad para prevenir la explotación de vulnerabilidades, la reducción de la superficie de exposición se centra en minimizar la cantidad de activos que podrían ser blanco de ataques. Ambos enfoques son complementarios y forman parte de una estrategia integral de ciberseguridad para reducir el riesgo de incidentes y mejorar la resiliencia de una organización.

Por otra parte, los Indicadores Clave de Rendimiento (KPI⁷) desempeñan un papel fundamental en la medición y seguimiento del progreso hacia la reducción de la superficie de exposición. Los KPI son métricas medibles que proporcionan información sobre el rendimiento y efectividad de las medidas de seguridad. Gracias a estos indicadores, se puede evaluar el éxito en la consecución de los esfuerzos en la mejora de la ciberresiliencia, así como en tomar decisiones basadas en datos objetivos que informan en tiempo real del estado de la superficie de exposición.

En consecuencia, la definición de los objetivos de este trabajo requiere del análisis de su cumplimiento con la situación actual de la infraestructura, y el contraste de los resultados y rendimiento en un futuro planificado. Por lo que se deberá llevar a cabo la recolección de datos actuales, y se establecerán metas futuras que permitirán ajustar los valores obtenidos para ir cumpliendo los objetivos establecidos. El resultado del cumplimiento de los KPI se verá en la sección (4.4 Verificación de los KPI con la plataforma CTEM).

⁶ La autenticación multifactor (MFA) es un proceso de registro en varios pasos que requiere que los usuarios ingresen algo más de información que simplemente una contraseña.

⁷ KPI, por sus siglas en inglés (*Key Performance Indicators*).

En la Figura 4 se resume el contenido de los objetivos para la reducción de la superficie de exposición junto con los indicadores clave de rendimiento:



Figura 4 Objetivos para la reducción de la superficie de exposición [Fuente Propia]

A continuación, se detallan los objetivos fundamentales de este trabajo, los cuales han sido establecidos en la figura anterior, incluyendo además, cuáles son los indicadores clave de rendimiento actuales y los que se deberían alcanzar para alcanzar un nivel adecuado de ciberresiliencia en la infraestructura TIC de Defensa.

1.3.1 OBJ.1 – Definición de acciones de comunicación y coordinación para la reducción de la superficie de exposición en infraestructuras TIC

El trabajo propone la definición de acciones de comunicación transparente y coordinación efectiva con todas las partes interesadas para la reducción de la superficie de exposición de las infraestructuras TIC de Defensa, teniendo en cuenta que esta reducción implica la disminución de los puntos de acceso y las vulnerabilidades que podrían ser aprovechadas por los potenciales atacantes.

Id KPI	Descripción	Actual	Objetivo	Comentarios (Actual)
KPI.1.1	Número de actuaciones de seguimiento de la superficie de exposición	Anual	Mensual	Se convoca una reunión anual de seguimiento de la Política de Seguridad de la Información
KPI.1.2	Número de actuaciones de seguimiento de desarrollo de la plataforma de ciberseguridad	Ninguna	Semanal	No existen reuniones periódicas para el seguimiento de desarrollos de ciberseguridad

Tabla 1 Indicadores clave de rendimiento del Objetivo 1 [Fuente propia]

1.3.2 OBJ.2 – Desarrollo de un entorno ciberresiliente que permite reducir la superficie de exposición en infraestructuras TIC

Por otra parte, el trabajo proporciona el desarrollo de una plataforma basada en un enfoque distribuido que recolecta información del ecosistema de agentes desplegados en los activos de la organización. Toda la información obtenida será analizada, cohesionada y centralizada para permitir una toma de decisiones rápida y eficaz.

Id KPI	Descripción	Actual	Meta	Comentarios (Actual)
KPI.2.1	Estado de la superficie de exposición	Sin visibilidad	Visibilidad completa	El valor de medición corresponde al riesgo global
KPI.2.2	Porcentaje de activos identificados y controlados	30%	99.9%	Se lleva un control manual (i.e. hoja Excel) de los activos
KPI.2.3	Porcentaje de activos parcheados	30%	99.9%	Principalmente a través de actualizaciones de seguridad de grandes fabricantes
KPI.2.4	Método de descubrimiento de activos TIC	Manual	Automático	Actualmente se descubren de forma manual
KPI.2.5	Método de comprobación del cumplimiento de configuración segura de los activos TIC	Local	Distribuido	Actualmente se comprueba la configuración mediante el despliegue de la herramienta CLARA ⁸ [9] de forma local
KPI.2.6	Priorización de las acciones de mitigación de vulnerabilidades en los activos TIC	No existe	Automatizada	Se mitigan vulnerabilidades en base a actualizaciones proporcionadas por los fabricantes
KPI.2.7	Tiempo medio de mitigación de una vulnerabilidad (MTTC ⁹)	No se controla	Control diario	No se contempla ningún tipo de seguimiento de la tasa de corrección de vulnerabilidades
KPI.2.8	Número de tecnologías integradas para obtener	+5	1	Las herramientas no tienen comunicación

⁸ CLARA es una herramienta proporcionada por el CCN para analizar las características de seguridad técnicas definidas en las guías CCN-STIC.

⁹ También se denomina tiempo media de corrección (MTTC, por sus siglas en inglés, *Mean Time to Contain*), en este caso de vulnerabilidades, siendo una métrica que se utiliza en ciberseguridad para medir el tiempo promedio de mitigación de una amenaza una vez ha sido detectada.

	información de la superficie expuesta			entre sí, por lo que se pretenda integrar y centralizar la información proporcionada por cada herramienta
KPI.2.9	Monitorización de la conectividad de los distintos agentes de seguridad desplegados en la Organización	Mala	Muy buena	No se conoce el estado de despliegue de los agentes
KPI.2.10	Control de la telemetría de seguridad	Dispersa	Centralizada	Si bien se mandan logs a la plataforma de gestión de incidentes, existen logs de aplicaciones que se pierden
KPI.2.11	Número de servicios utilizados para obtener ciberinteligencia que permita una adecuada predicción de las ciberamenazas	+20	-3	No existe un equipo de evaluación de amenazas

Tabla 2 Indicadores clave de rendimiento del Objetivo 2 [Fuente propia]

1.3.3 OBJ.3 – Cumplimiento con la normativa en ciberseguridad

Finalmente, el trabajo proporciona un análisis del cumplimiento con la normativa de ciberseguridad existente en la propia infraestructura de la organización. Esta normativa puede referirse a: guías de configuración segura (por ejemplo CCN-STIC¹⁰), legislación nacional en materia de seguridad (por ejemplo, el Esquema Nacional de Seguridad [10]), y reglamentos europeos en materia de ciberseguridad y ciberresiliencia (por ejemplo, Directiva 2016/1148 [11] y Reglamento 2019/881 [8]).

Id KPI	Descripción	Actual	Objetivo	Comentarios (Actual)
KPI.3.1	Porcentaje de activos bastionados (cumplen configuración segura según guías CCN ¹¹ -STIC)	60%	99.9%	Se lleva a cabo la configuración segura de forma manual
KPI.3.2	Tasa de cumplimiento del Esquema Nacional de Seguridad (ENS)	1%	99.9%	Existen servicios en proceso de certificación del ENS

¹⁰ Índice de guías CCN-STIC (<https://www.ccn-cert.cni.es/guias/indice-de-guias.html>).

¹¹ El CCN es el organismo responsable de garantizar la seguridad de los servicios de tecnologías de la información y comunicaciones en las diferentes entidades de la Administración Pública, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.

KPI.3.3	Tasa de cumplimiento con regulación europea	30%	99.9%	Se están empezando a incluir cláusulas en las licitaciones contemplando regulaciones de certificación y cualificación de productos
---------	---	-----	-------	--

Tabla 3 Indicadores clave de rendimiento del Objetivo 3 [Fuente propia]

1.4 Estructura y contenidos

Una vez establecido el marco conceptual, delineada la motivación del autor y expresados los objetivos perseguidos con este trabajo, se aspira a haber generado la curiosidad necesaria para adentrarse más profundamente en la comprensión de la protección de las infraestructuras TIC de organizaciones críticas frente a las emergentes amenazas híbridas y su compleja evolución. Si aún así, esta curiosidad o incertidumbre no parece haber calado en el ánimo del lector, se realizan a continuación una serie de preguntas, para que, en caso de ser contestadas negativamente, conduzcan a la lectura del resto del trabajo en búsqueda de soluciones para mejorar la ciberresiliencia de una infraestructura TIC:

- ¿Proporciona información integrada el ecosistema de herramientas de ciberseguridad que pueblan tu infraestructura TIC?
- ¿Existe una visibilidad completa de la superficie de exposición, incluyendo la superficie interna, la externa, e incluso la oculta? ¿se pueden trazar los activos de la interna a la externa? ¿se pueden conocer los servidores detrás de cada sistema de información? ¿existen activos no controlados?
- ¿Se pueden priorizar los esfuerzos de mitigación de ciertas vulnerabilidades basándose en aquellas más abundantes o las que pudieran impactar en los activos más importantes?
- ¿Se aprovecha la telemetría de seguridad generada en el día a día para anticipar posibles amenazas?
- ¿Se analizan todas las rutas de ataque que puedan llevar a los activos más prioritarios?
- ¿Se mitigan las vulnerabilidades de manera precisa, continuada, y se aplican aquellas configuraciones de seguridad exigidas por normativa específica?
- ¿Puede asegurar el responsable de la infraestructura el nivel de riesgo ante ciberataques en tiempo real?
- ¿Se lleva a cabo una asignación de recursos optimizada para la mejora de la ciberseguridad basada en datos objetivos?
- ¿Existe alguna infraestructura externa a modo de señuelo que permita estudiar el modus operandi de los ciberatacantes?

Seguidamente, en el capítulo del estado del arte se revisa aquella literatura bajo la temática de ciberseguridad que analiza la evolución de la gestión de vulnerabilidades hacia una gestión continua de la superficie de exposición a amenazas de una infraestructura TIC, incluyendo la descripción de la topología de la superficie de exposición, su gestión y roles, las herramientas de apoyo, las vulnerabilidades que afectan a la superficie, así como la normativa aplicable.

A continuación, En el capítulo 3, se detallan las acciones de ciberresiliencia que constituyen el núcleo de este trabajo de investigación. Estas acciones están diseñadas para cumplir con los objetivos planteados y, de manera inherente, resultan en la reducción efectiva de la superficie de exposición de una infraestructura TIC. Se abordan diversas acciones que buscan la comunicación efectiva entre equipos, aquellas que siguen los principios de preparación y detección temprana (mediante la identificación de activos y sus vulnerabilidades) para la recuperación y restauración de la infraestructura a un estado de riesgo aceptable. También se incluyen acciones orientadas al aprendizaje y mejora continua, la resolución prioritaria de problemas de seguridad en los activos de la infraestructura, el incremento de flexibilidad y adaptabilidad mediante el estudio continuo de la superficie de ataque, así

como acciones que implican la monitorización de la infraestructura a través del despliegue de agentes, la gestión de la telemetría de seguridad para la detección temprana de amenazas y el despliegue de señuelos para aprender de los propios atacantes. Además, se consideran acciones para obtener ciberinteligencia que permita una adecuada predicción de las ciberamenazas y garantizar el cumplimiento normativo en materia de ciberseguridad y ciberresiliencia.

En el capítulo 4, se expone la implementación práctica de una plataforma que lleva a cabo todas las acciones propuestas en el capítulo 3. Esto incluye la explicación de la metodología del desarrollo de la plataforma en base a las acciones de ciberresiliencia propuestas, su proceso de implementación, el análisis de un algoritmo de aprendizaje automático para el reconocimiento del estado de la superficie de exposición, la verificación de los indicadores de rendimiento definidos previamente en el capítulo 1 y aplicados en el propio despliegue de la plataforma, así como la validación de la plataforma como un enfoque innovador para la monitorización continua de amenazas.

Finalmente, se exponen las conclusiones y se señalan las líneas futuras para mejorar el desarrollo propuesto, con el objetivo de perfeccionar aquellos indicadores de rendimiento que no han experimentado mejoras significativas con la plataforma propuesta.

2 ESTADO DEL ARTE

2.1 Topología de la superficie de exposición

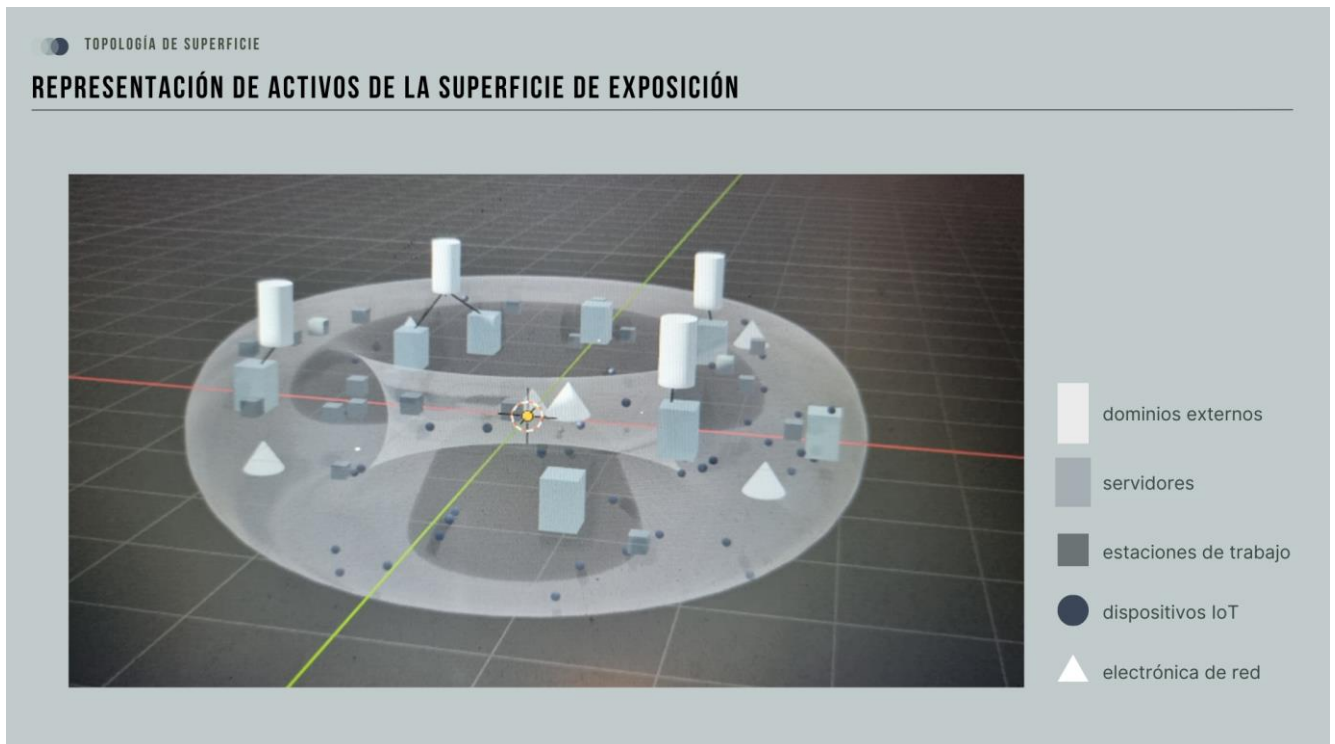


Figura 5 Topología de la superficie de exposición [Fuente propia realizada con Blender¹²]

La superficie de exposición de una infraestructura de tecnologías de la información y comunicación (TIC) se refiere al conjunto de activos, sistemas de información, datos y conexiones que son visibles y accesibles desde el entorno digital, y que, por lo tanto, pueden ser considerados como vectores de ataque por parte de un atacante para explotar una vulnerabilidad. En otras palabras, es el área en la que los activos de una organización están expuestos a posibles riesgos y ataques en el entorno de ciberseguridad, pudiendo considerar la superficie de ataque como la suma de los diferentes vectores de ataque [12].

A continuación, se detallan los distintos tipos de “superficies” que conforman la superficie de exposición de una infraestructura TIC, concibiendo ésta superficie como un toroide¹³. Si bien un toroide es una superficie cerrada, puede presentar variaciones o regiones específicas que definen diversos elementos y propiedades dentro de esta estructura tridimensional (ver Figura 5). En esta representación, los activos de la superficie externa se muestran como cilindros, mientras que los activos de la superficie interna, como los servidores se representan como ortoedros, las estaciones de trabajo como cubos, los dispositivos IoT¹⁴ como esferas y la electrónica de red como conos.

¹² Blender es una herramienta de software de código abierto utilizada para la creación de contenido 3D, incluyendo modelado, animación, renderizado, simulación, composición (blender.org).

¹³ Un toroide es una superficie geométrica tridimensional que se forma al rotar un círculo alrededor de un eje que no pasa por su centro, creando una estructura anular o de "rosquilla". En términos matemáticos, se puede describir mediante ecuaciones paramétricas que definen sus coordenadas en el espacio tridimensional.

¹⁴ IoT, por sus siglas en inglés (*Internet of Things*).

2.1.1 Superficie interna

Cuando hablamos de la "superficie interna de exposición" en el contexto de una infraestructura TIC, nos referimos a los activos digitales, sistemas y recursos que están dentro de la red interna de una organización y que podrían ser vulnerables o susceptibles a amenazas y ataques desde el interior de la red. Estos activos pueden ser explotados por personas que ya tienen acceso a la red, ya sea de manera legítima (como empleados) o de manera malintencionada (como atacantes internos).

En otras palabras, la superficie interna de exposición comprende los componentes de la infraestructura TIC que están dentro de la red de una organización y que podrían ser objetivos de amenazas y ataques desde dentro. Esto puede incluir:

- Servidores internos: los servidores que no son directamente accesibles desde Internet pero que aún están dentro de la red de la organización.
- Estaciones de trabajo y dispositivos finales: ordenadores y dispositivos utilizados por los usuarios dentro de la red interna.
- Dispositivos IoT (Internet de las cosas) internos: dispositivos conectados a la red interna, como cámaras de seguridad y dispositivos industriales [13].
- Electrónica de red: dispositivos para la gestión y mantenimiento de redes de comunicación, como routers, switches, cortafuegos...
- Sistemas de almacenamiento y otros recursos compartidos: almacenamiento interno utilizado para almacenar datos y archivos, bases de datos internas, así como otros recursos dentro de la red utilizados para colaborar y compartir información.
- Segmentos de red internos: redes internas que no están directamente conectadas a Internet, pero que aún pueden ser accesibles para atacantes internos.

La Figura 6 muestra el concepto de superficie interna, que incluye la representación de los servidores, estaciones de trabajo, IoTs y electrónica de red como figuras geométricas.

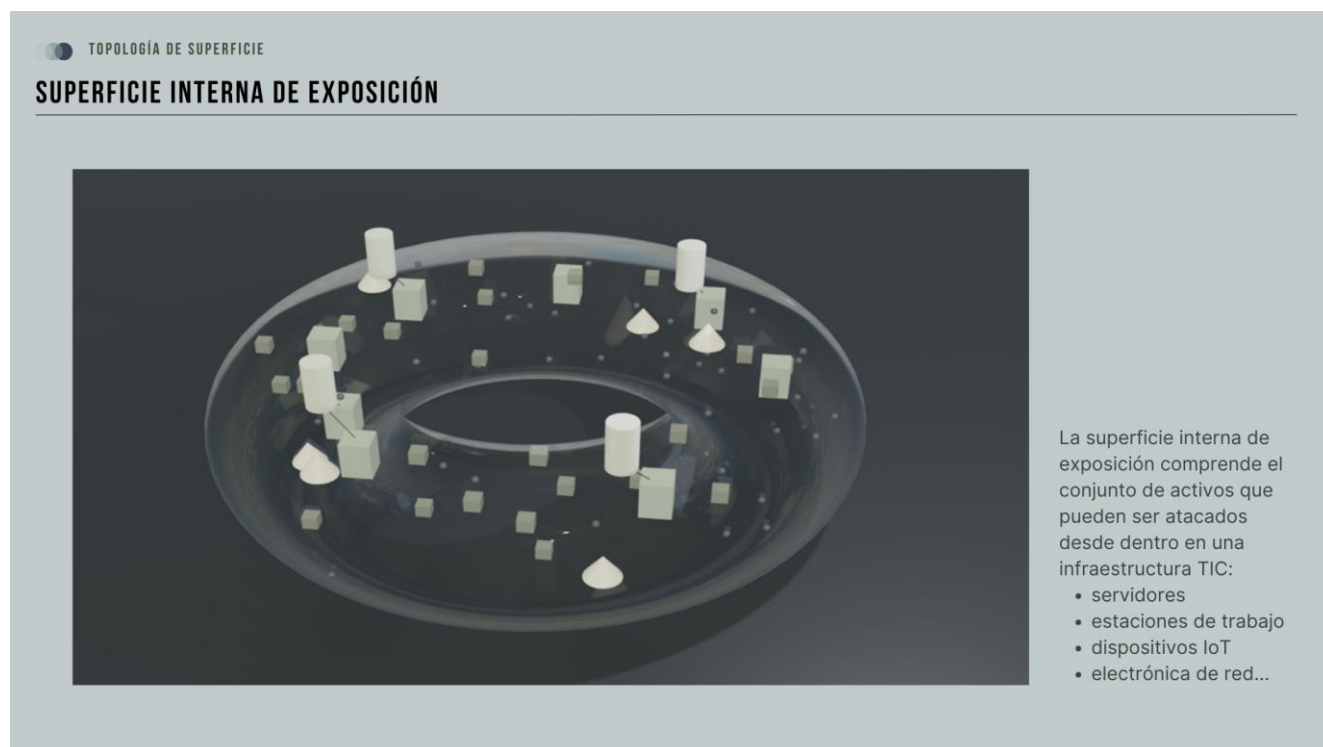


Figura 6 Superficie interna [Fuente propia realizada con Blender]

2.1.2 Superficie externa

Cuando hablamos de la "superficie externa de exposición" en el contexto de una infraestructura TIC, nos referimos a todos los activos digitales, sistemas y recursos que están directamente accesibles y expuestos al entorno externo, como Internet. Estos activos son potencialmente visibles y accesibles para cualquier persona o entidad que tenga conexión a la red, incluidos atacantes.

En otras palabras, la superficie externa de exposición comprende los componentes de la infraestructura TIC que están accesibles desde fuera de la red de la organización y que podrían ser puntos de entrada para amenazas y ataques. Esto puede incluir:

- Servidores web: los servidores que alojan sitios web y aplicaciones web accesibles desde Internet.
- Aplicaciones públicas: cualquier aplicación en línea que sea accesible a través de Internet, como aplicaciones móviles, servicios en la nube y plataformas en línea.
- Direcciones IP públicas: las direcciones IP públicas asignadas a los activos de la organización que están expuestos directamente a Internet.
- Infraestructura de red: componentes de red que están conectados directamente a Internet, como enrutadores, cortafuegos y puntos de acceso inalámbrico públicos.
- Bases de datos accesibles: bases de datos que se pueden acceder desde Internet para consultar o manipular información.
- Interfaces de administración remota: interfaces que permiten la administración remota de sistemas y dispositivos.
- Dispositivos IoT: dispositivos conectados a Internet, como cámaras IP y dispositivos domésticos inteligentes [13].

La Figura 7 muestra el concepto de superficie externa, que incluye la representación de activos expuestos (aplicaciones web, dominios, direcciones IP, certificados...).



Figura 7 Superficie externa [Fuente propia realizada con Blender]

2.1.3 Superficie oculta

La "superficie oculta de exposición" en el contexto de una infraestructura TIC se refiere a los activos, sistemas y recursos que siendo directamente accesibles desde el exterior de la red, como Internet, o estando dentro de la superficie interna, no han sido debidamente controlados por el responsable de la infraestructura, y podrían ser vulnerables a amenazas y ataques si son descubiertos y explotados por atacantes desde el exterior, por ejemplo Internet, o bien desde el interior si ya han obtenido acceso a la red interna. Identificar y proteger estos elementos es crucial para prevenir ataques.

En otras palabras, la superficie oculta de exposición comprende aquellos componentes de la infraestructura TIC que, aun no habiendo sido debidamente enumerados y controlados, representan posibles objetivos de amenazas y ataques si los atacantes logran encontrarlos o infiltrarse en la red interna. Esto puede incluir:

- Sistemas de respaldo: equipos y servidores utilizados para almacenar copias de seguridad de datos y sistemas.
- Recursos en desuso: sistemas y servicios que ya no están activos o en uso, pero siguen activos.
- Equipos desconectados: dispositivos que no están conectados permanentemente a la red, pero que aún pueden ser potencialmente vulnerables si se conectan en algún momento.
- Recursos restringidos: activos y sistemas que solo son accesibles para un grupo limitado de usuarios autorizados y no están visibles para todos los usuarios en la red.
- Recursos aislados: activos y sistemas que están aislados y protegidos dentro de la red, pero que aún podrían ser descubiertos y explotados si los atacantes logran acceder a la red interna.

La Figura 8 muestra el concepto de superficie oculta, que incluye la representación de activos que de alguna manera no son controlados (falta la instalación de agentes, ya no se utilizan, son elementos con poca visibilidad, aislados...).

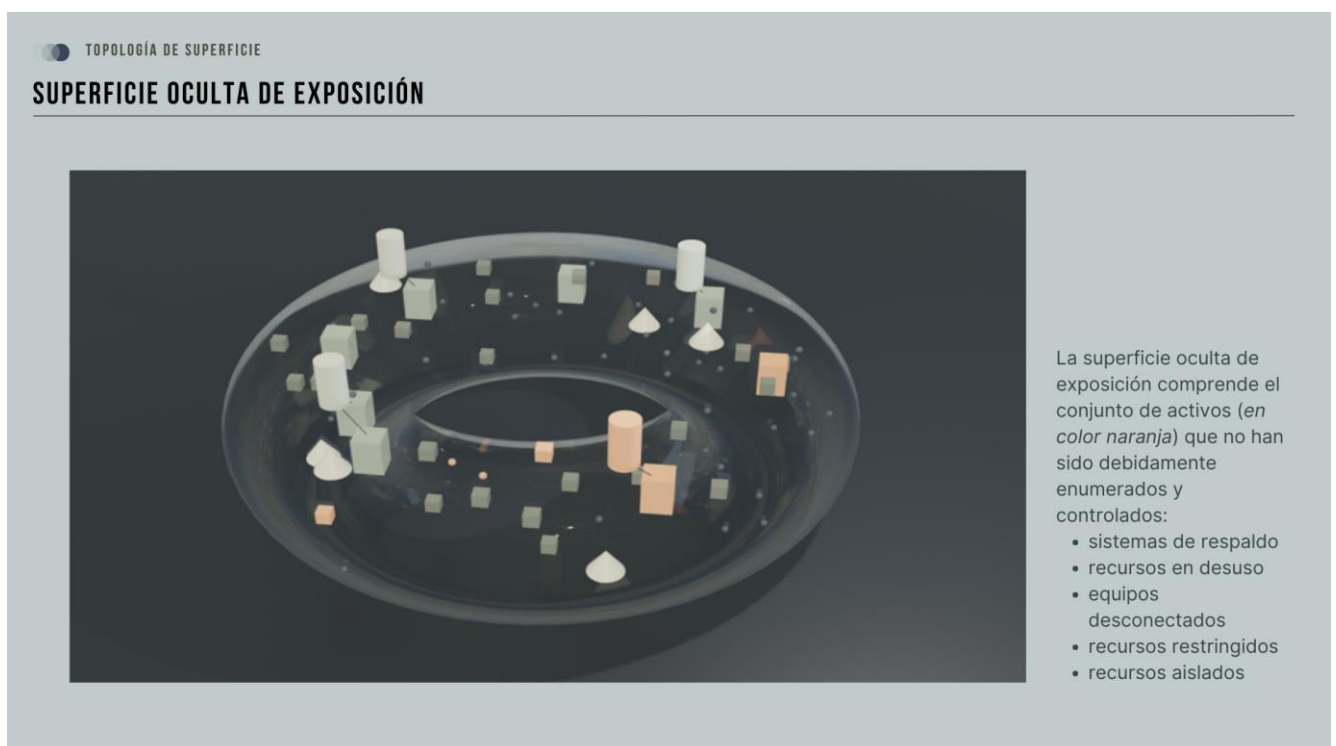


Figura 8 Superficie oculta [Fuente propia realizada con Blender]

2.1.4 Superficie obsoleta

La “superficie obsoleta” de una infraestructura de TIC se refiere a las partes o componentes de esa infraestructura que han quedado desactualizados o que están en estado de obsolescencia. Esto significa que estos componentes ya no son compatibles con las tecnologías más recientes, no reciben actualizaciones de seguridad o soporte del fabricante y, por lo tanto, son más vulnerables a ciberamenazas.

La superficie obsoleta puede incluir sistemas operativos antiguos, aplicaciones descontinuadas, hardware que ya no se fabrica, o cualquier otro componente de la infraestructura que haya llegado al final de su ciclo de vida útil y no se ha actualizado. Estos componentes obsoletos pueden representar un riesgo significativo para la ciberseguridad de la infraestructura, ya que los ciberatacantes a menudo buscan aprovechar las vulnerabilidades en sistemas antiguos y desactualizados.

Para mantener la ciberseguridad, es importante identificar y gestionar la superficie obsoleta de una infraestructura TIC, lo que implica reemplazar o actualizar los componentes obsoletos, aplicar parches de seguridad siempre que sea posible y tomar medidas para reducir los riesgos asociados con estas partes de la infraestructura.

La Figura 9 muestra el concepto de superficie obsoleta, que incluye la representación de activos que han quedado desactualizados en la infraestructura.



Figura 9 Superficie obsoleta [Fuente propia realizada con Blender]

2.1.5 Superficie vulnerable

La “superficie vulnerable” de una infraestructura de TIC se refiere a las áreas, componentes o puntos de acceso en esa infraestructura que son más susceptibles a amenazas y vulnerabilidades. Este término se distingue de la superficie de exposición en general, ya que esta última abarca tanto los activos expuestos vulnerables como los no vulnerables. La superficie vulnerable se considera el punto más débil o expuesto de la infraestructura que podrían ser explotados por actores maliciosos.

La superficie vulnerable puede incluir, pero no se limita a:

- Sistemas operativos desactualizados: los sistemas operativos que no han recibido actualizaciones de seguridad pueden ser vulnerables a *exploits* conocidos.
- Software no parcheado: las aplicaciones y software que no se han actualizado con parches de seguridad son un objetivo común para los atacantes.
- Configuraciones incorrectas: configuraciones inseguras o incorrectas de servidores y dispositivos pueden dejar puntos de acceso abiertos.
- Puertos abiertos: los puertos de red abiertos sin protección adecuada pueden ser un punto de entrada para ataques.
- Contraseñas débiles: las contraseñas inseguras o predeterminadas son un riesgo para la seguridad.
- Dispositivos IoT: los dispositivos del Internet de las cosas (IoT) a menudo carecen de medidas de seguridad sólidas y pueden ser vulnerables.
- Acceso remoto no seguro: acceso remoto a la infraestructura sin medidas de seguridad adecuadas.
- Fallos en la gestión de parches: la falta de una política de gestión de parches efectiva puede dejar sistemas sin actualizar.
- Usuarios con permisos inadecuados: usuarios con permisos excesivos o inadecuados pueden comprometer la seguridad.

La Figura 10 muestra el concepto de superficie vulnerable, que muestra la representación de posibles caminos de ataque por los que un atacante podría vulnerar activos (por ejemplo, porque tienen vulnerabilidades, configuración insegura...).

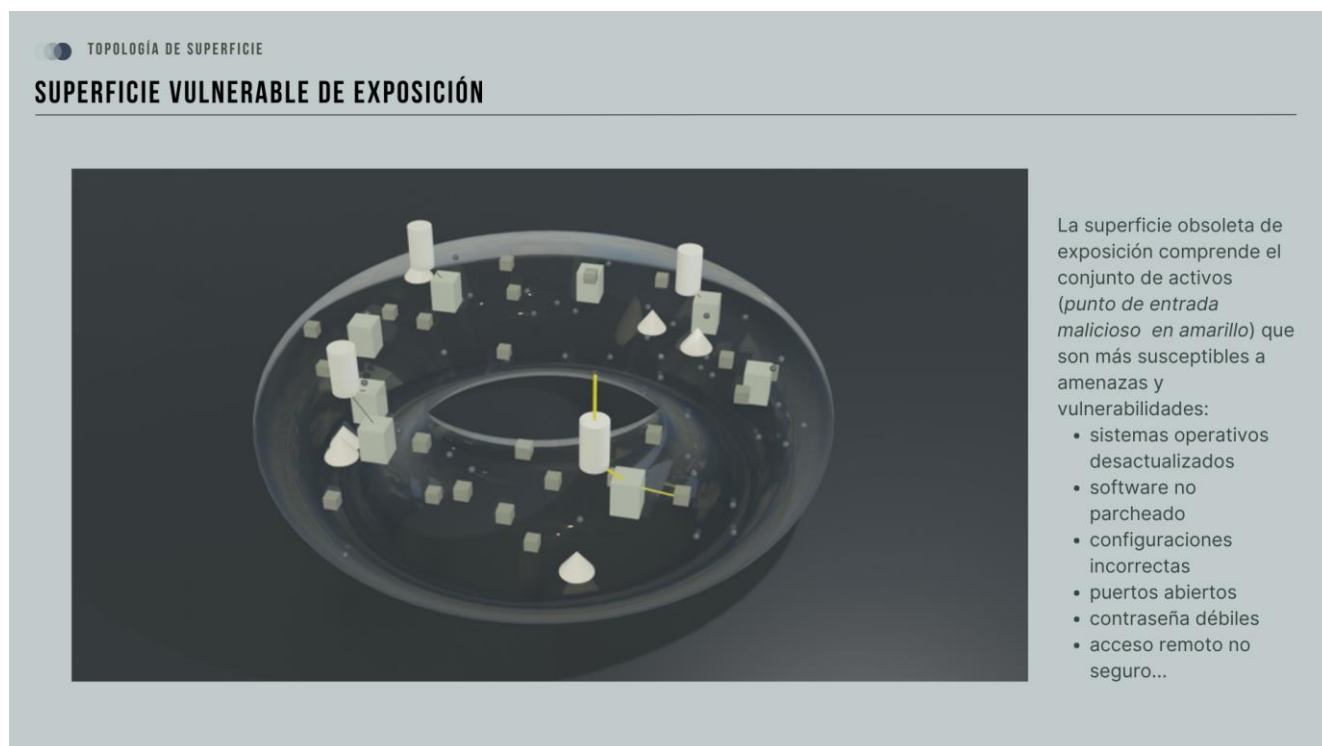


Figura 10 Superficie vulnerable [Fuente propia realizada con Blender]

Al igual que con la “superficie oculta” y la “superficie obsoleta”, identificar y gestionar la superficie vulnerable es esencial para garantizar la ciberseguridad. Esto implica implementar prácticas de seguridad sólidas, aplicar parches y actualizaciones, configurar sistemas de manera segura y mantener una estrategia de ciberseguridad efectiva para reducir los riesgos y proteger la infraestructura TIC.

2.1.6 Superficie señuelo

La “superficie señuelo de exposición” en el contexto de una infraestructura TIC se refiere a una técnica de seguridad que implica crear activos digitales, sistemas o recursos falsos y atractivos para atraer a posibles atacantes y desviar su atención de los activos reales y valiosos. Estos señuelos o *honeypots* están diseñados para simular vulnerabilidades o recursos interesantes que podrían atraer la atención de los atacantes [14].

En otras palabras, la superficie señuelo de exposición abarca aquellos componentes de la infraestructura TIC que se establece intencionalmente para atraer a los atacantes, aprender de ellos y mantenerlos ocupados y lejos de los activos críticos y valiosos. Los objetivos principales de los señuelos son:

- Recolección de información: los señuelos pueden ser configurados para recopilar información sobre las tácticas y técnicas utilizadas por los atacantes, lo que puede ser valioso para mejorar las defensas y prevenir futuros ataques.
- Detección temprana: al observar los intentos de ataque dirigidos a los señuelos, las organizaciones pueden identificar amenazas antes de que lleguen a los sistemas reales y tomar medidas para detenerlas. Además, al proporcionar objetivos falsos y atractivos, los señuelos pueden desviar la atención de los atacantes, dando tiempo a organizarse.
- Aprendizaje y análisis: los señuelos permiten a los equipos de seguridad analizar las tácticas y técnicas de ataque utilizadas y desarrollar mejores estrategias de defensa.
- Investigación forense: los señuelos pueden ser utilizados para recopilar evidencia y datos forenses sobre los atacantes, con el objetivo de identificar la fuente y el propósito de los ataques.

La Figura 11 ilustra el concepto de superficie señuelo que muestra la representación de la superficie señuelo diseñada para “atacar” la superficie principal y evaluar sus capacidades de resiliencia. Esta superficie adicional, anexa a la infraestructura principal, contiene vulnerabilidades colocadas intencionalmente para atraer a posibles atacantes, permitiendo así el estudio de sus métodos y técnicas.

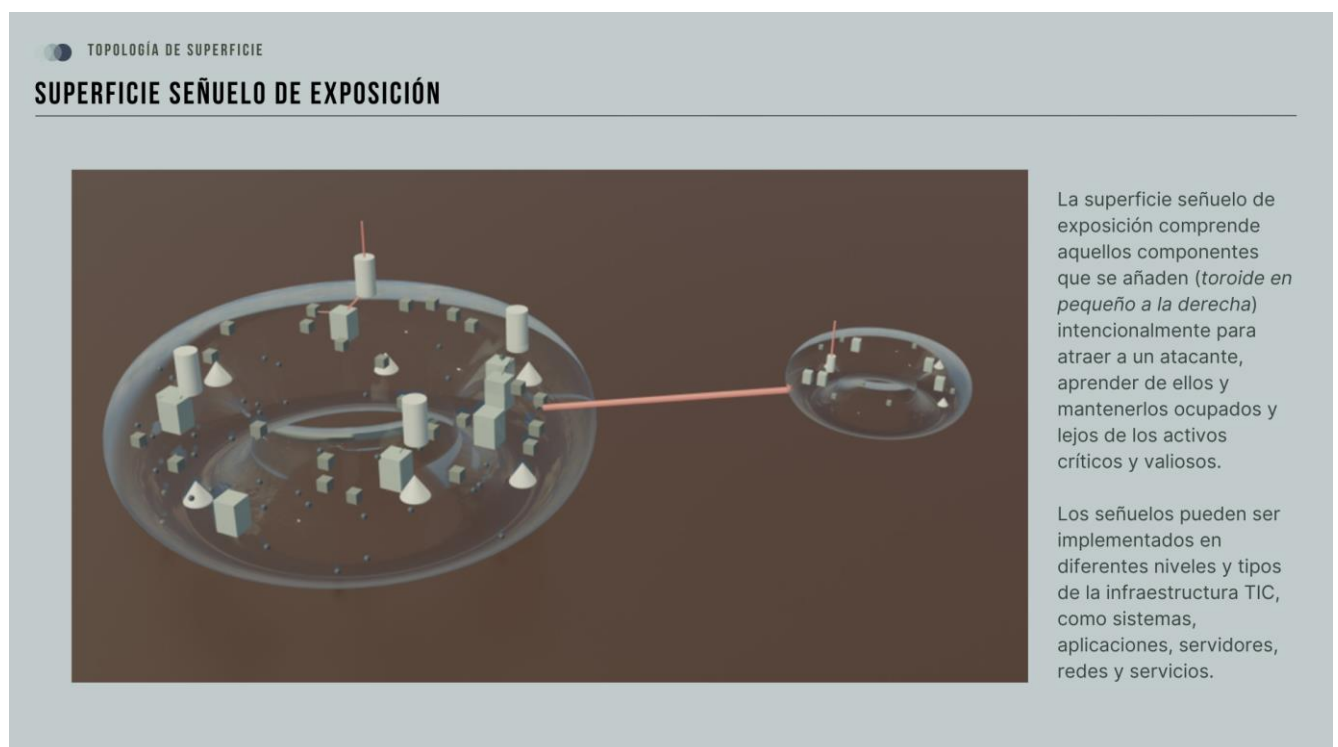


Figura 11 Superficie señuelo [Fuente propia realizada con Blender]

2.2 Gestión de la superficie de exposición

Las infraestructuras TIC de las grandes organizaciones se han vuelto cada vez más complejas, distribuidas e híbridas, albergando incluso nubes propias y trasladando servicios a nubes ajenas. Estas complicadas superficies de exposición en constante expansión ven incrementados sus puntos ciegos¹⁵ y debilidades, por lo que la inclusión de todo un ecosistema de herramientas de ciberseguridad no es suficiente para evitar ciberataques, se necesita cohesionar el resultado de todas a ellas en un único punto de avistamiento con capacidades de integración. La gestión de esta superficie en este punto de cohesión se refiere a la vigilancia continua necesaria para mitigar todas las ciberamenazas actuales y futuras e incluye todas las evaluaciones de riesgo y medidas de seguridad que se utilizan para identificar y proteger la superficie de exposición, reduciendo las posibilidades de un ataque con éxito [15].

Es precisamente con la combinación de diversas tecnologías ya presentes en la infraestructura TIC en una sola plataforma la que facilita la recopilación de información de forma exhaustiva. Por ejemplo, el programa de Gestión Continua de la Exposición a Amenazas (CTEM¹⁶) de la firma de investigación y consultoría tecnológica Gartner [16] subraya la importancia de este enfoque en el proceso de pensamiento para lograr un ciberresiliencia duradera y robusta. Asimismo, este programa resalta la necesidad del liderazgo ejecutivo del CISO¹⁷ con el objetivo de emitir informes periódicos para el estudio de la evolución del estado de riesgo de la superficie de exposición, lo que mejora el rendimiento con el tiempo, así como el control de desviaciones. Según Gartner, “Para el año 2026, las organizaciones que prioricen sus inversiones en seguridad basadas en un programa de gestión continua de exposición serán tres veces menos propensas a sufrir un ciberataque”.

Más concretamente, y tal y como expone el documento de desmitificación de la gestión continua de la exposición a amenazas [17], la complejidad en cuanto al despliegue excesivo de herramientas de ciberseguridad puede provocar a su vez brechas significativas en la comunicación, lo que conduce a respuestas fragmentadas ante amenazas y tiempos prolongados para la mitigación de vulnerabilidades. Por ello, el paradigma CTEM permite abordar una estrategia de reducción del riesgo que unifica la evaluación de riesgos y priorización de problemas a través de toda la información proporcionada por diversas fuentes, así como la coordinación de personas, procesos y tecnología (las personas y procesos llevan a cabo funciones específicas y bien definidas; y la tecnología permite la automatización de los procesos).

Por todo ello, a través del ciclo de vida del enfoque CTEM definido por Gartner, se pone en marcha la maquinaria para la ejecución continua de dos etapas con una serie de pasos en cada una de ellas que permite la mejora de la ciberresiliencia de una infraestructura TIC. A continuación, se detallan todos estos pasos que ponen a prueba la resiliencia de esta infraestructura gracias a colaboración entre las distintas unidades de una organización [18]:

- A. **Diagnóstico:** identificar todos los factores relevantes de forma que se facilite la comunicación entre los órganos decisorios y el personal TIC, garantizando que hablen un lenguaje común y entendible, mediante la implementación de los pasos que se detallan a continuación.
 - **Definición del alcance:** consiste en definir qué segmentos de la infraestructura serán incluidos en el proceso, involucrando a personal del Centro de Operaciones de Seguridad junto con personal TIC. De esta forma, se produce una cooperación que marca los objetivos

¹⁵ En el contexto de la infraestructura de tecnologías de la información y comunicación (TIC), un "punto ciego" se refiere a un área o aspecto que no está visible o no está siendo monitoreado adecuadamente. Es un componente, dispositivo o parte de la red que no está siendo supervisado o auditado, lo que puede representar un riesgo de seguridad o una falta de visibilidad sobre posibles problemas.

¹⁶ CTEM, por sus siglas en inglés (*Continuous Threat Exposure Management*).

¹⁷ CISO, por sus siglas en inglés (*Chief Information Security Officer*).

de riesgo y se establecen las bases de seguridad que puedan servir de base para monitorizar tendencias en ciclos sucesivos. Se recomienda para definir este alcance llevar a cabo un mapeo de la superficie de ataque externa.

- **Descubrimiento:** que se caracteriza por realizar un mapeo de la infraestructura TIC y su evaluación de la resiliencia interna. Esto conlleva la creación de un inventario completo de todos los activos, así como el mapeo de su interconexión tanto interna con la externa. Este descubrimiento no es solamente una identificación de vulnerabilidades, sino que incluye la emulación de una amplia gama de escenarios de ataque, por ejemplo con la inclusión de todas las tácticas, técnicas y procedimientos (TTPs¹⁸) definidos en la base de conocimiento de MITRE ATT&CK [19] para el desarrollo de modelos y metodologías de amenazas. Además, una parte crucial del proceso de descubrimiento implica obtener de manera automatizada la estructura organizativa, es decir, contar con una herramienta que proporcione contexto sobre la propia organización y que entregue esta información mediante una interfaz de programación de aplicaciones (API) [20].
- **Priorización:** donde se lleva a cabo la priorización de tareas (especialmente la mitigación de vulnerabilidades y cumplimiento con la configuración segura) y definición de la tolerancia al riesgo. Basándose en las prioridades de negocio definidas en el primer paso, el CISO y el Responsable del Centro Operativo de Seguridad (COS¹⁹) se definen los datos y procesos críticos, su valor respectivo o grado de sensibilidad, además de cómo es de esencial para dar apoyo a los objetivos y criterios decisivos de la organización. El proceso de priorización debe ser automático, periódico y sin llevar a cabo la interrupción de los Servicios. Además, la periodicidad será mayor o menor según la importancia del activo.

B. **Acciones:** se llevan a cabo a través de los dos pasos que se detallan a continuación.

- **Validación:** recopila toda la información recogida durante la fase de diagnóstico. Requiere la implementación de diversas técnicas, desde pruebas de penetración hasta simulación de ataques y ejercicios de *red teaming*²⁰. Este proceso debería cumplir con los siguientes objetivos:
 - a. Evaluación de la probabilidad de éxito, confirmando realmente si un atacante puede explotar la superficie descubierta como vulnerable.
 - b. Estimación del impacto potencial más alto, gracias a la exploración de todos los caminos de ataque hacia un activo crítico para la organización.
 - c. Identificación de si el proceso de mitigación de una vulnerabilidad en concreto puede ser suficientemente rápido y adecuado para los objetivos operativos de la organización.
- **Movilización:** en este último paso se llevan a cabo las de medidas correctivas. Este proceso debe estar alineado según el resultado obtenido en el proceso de validación anterior, llevando a cabo la implementación de las medidas correctivas de la forma más optimizada, fluida y rápida posible.

¹⁸ TTPs, por sus siglas en inglés (*Tactics, Techniques, and Procedures*).

¹⁹ El Centro Operativo de Seguridad (SOC, por sus siglas en inglés, *Security Operations Center*) se encarga de supervisar y gestionar la seguridad de la información en tiempo real. Dentro de sus funciones principales se encuentra la gestión de ciberincidentes.

²⁰ El *red teaming* es una práctica en ciberseguridad que implica simular un ataque desde la perspectiva de un adversario. En lugar de realizar pruebas de seguridad convencionales que se centran en identificar y corregir vulnerabilidades conocidas, el *red teaming* busca evaluar la resistencia general de un sistema o red al replicar las tácticas, técnicas y procedimientos que un atacante real podría emplear.

La Figura 12 resume las etapas detalladas arriba, las cuales deberían ser cumplidas por una plataforma CTEM que aspirara a reducir su superficie de exposición, consiguiendo una mejora intrínseca de su ciberresiliencia.



Figura 12 Etapas del programa CTEM [18]

2.2.1 Evolución de la gestión de la superficie de exposición

La gestión de la exposición [21], que permite tener un único punto de observación donde obtener una vista destacada del paisaje de activos, es la evolución natural de la gestión de vulnerabilidades que se llevaba a cabo a través de diversas herramientas disponibles en el mercado, que habían funcionado hasta ahora de forma aislada y sin relacionarse entre ellas. Dado que un ciberatacante explora la superficie de exposición buscando vulnerabilidades y configuraciones erróneas, pasando de una zona de la superficie a otra, la propia infraestructura necesita una plataforma que se constituya en mirador y que disponga de un lugar predominante para poder defenderse de cualquier amenaza.

Según la predicción de Gartner, "la gestión de la exposición es un desafío para todas las organizaciones, incluso para aquellas de alta madurez y grandes empresas, debido a que la superficie de ataque sigue cambiando y expandiéndose" [22]. De hecho, se expande más allá de la capacidad de aplicar parches y bloquear comportamientos anómalos, por lo que se necesita una estrategia innovadora para la reducción de la superficie de exposición, que logre limitar el nivel de complejidad de la infraestructura.

A continuación, se presenta la Figura 13 que ilustra la evolución de la gestión convencional de vulnerabilidades hasta la gestión continua de la exposición a amenazas (CTEM). En ella se destaca la necesidad de introducir procesos más avanzados como son: la identificación de la superficie oculta, la incorporación de una superficie señuelo, la identificación de los servicios que se ejecutan sobre los activos, la dependencia entre activos, la trazabilidad entre los activos externos o expuestos y los internos, la introducción de KPI que permitan medir la evolución de la superficie y la priorización de los esfuerzos de mitigación de vulnerabilidades.

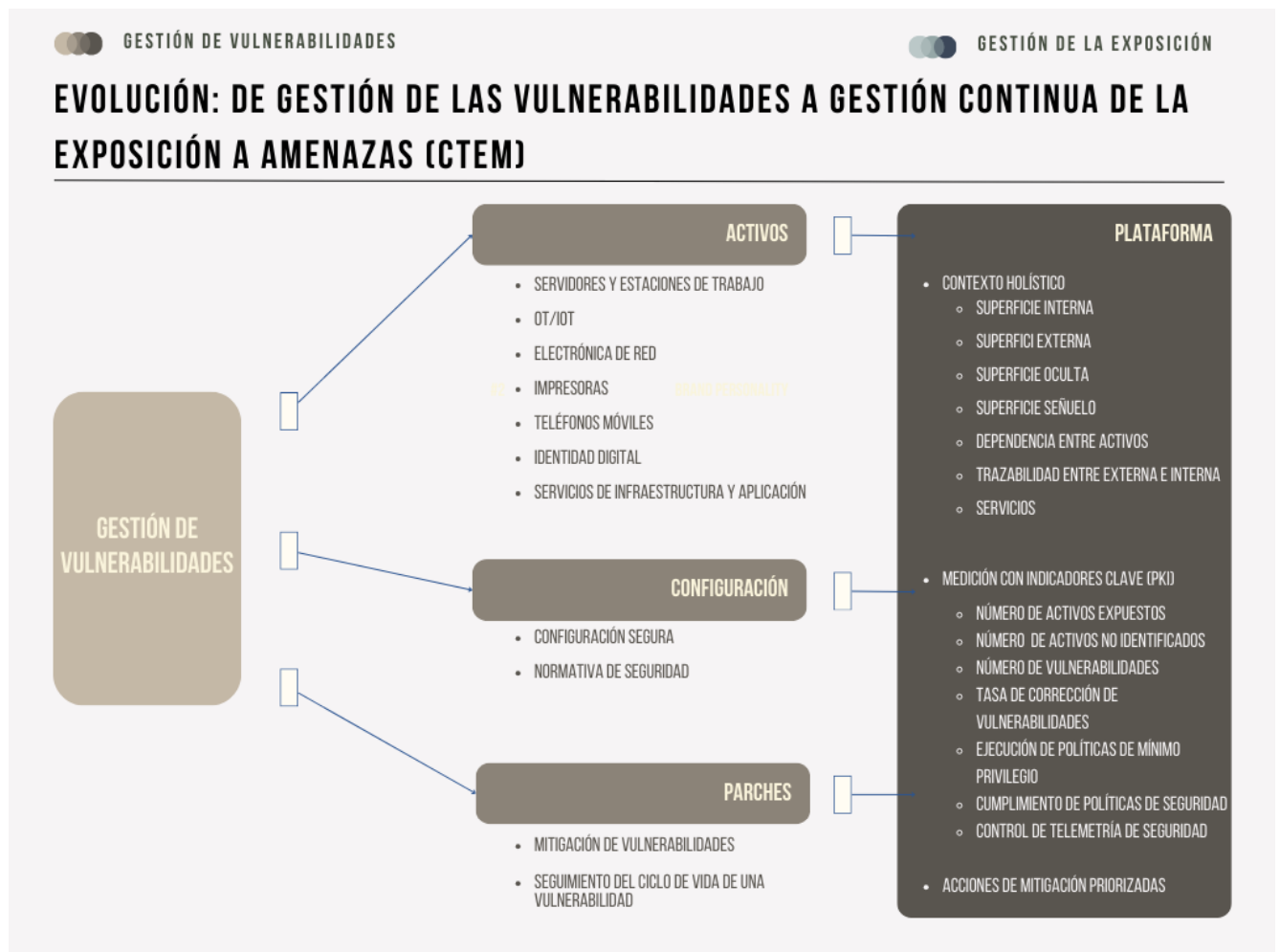


Figura 13 Evolución: De la gestión de la superficie de exposición a la gestión continua de la exposición a amenazas (CTEM) [Fuente propia]

Por tanto, el desafío para proteger una infraestructura TIC radica en realizar una gestión efectiva de la superficie de exposición a través de un único puesto de mando y control, evolucionando de la gestión de vulnerabilidades a la gestión continua de la exposición a amenazas. Este punto centralizado, con capacidad de comunicarse mediante los interfaces de programación de aplicaciones (API²¹) con las herramientas de ciberseguridad desplegadas previamente en la infraestructura y otros elementos externos de apoyo, proporcionaría las siguientes capacidades:

1. **Vista unificada** de los datos proporcionados por las herramientas de ciberseguridad desplegadas en la infraestructura y otros elementos externos, incluyendo el levantamiento de activos de más alto nivel que agrupen varios activos de más bajo nivel.
2. **Predicción de ciberataques y priorización de las acciones de mitigación** para poder gestionar los esfuerzos en ciberseguridad basado en datos objetivos y que permitan prever la dedicación del personal TIC a tareas concretas.
3. **Cuadros de mando y control** para llevar a cabo el análisis evolutivo del riesgo de ciberataques en la infraestructura.

²¹ Una interfaz de programación de aplicaciones (API), por sus siglas en inglés (*Application Programming Interface*) es un conjunto de reglas y herramientas que permite a diferentes software comunicarse entre sí. Proporciona un conjunto de funciones y procedimientos que permiten la creación de aplicaciones y facilitan la interacción entre diferentes componentes de software.

Finalmente añadir, que existen soluciones emergentes que proporcionan, además de las capacidades citadas anteriormente, el control de activos para obtener una visibilidad unificada de todos los activos de una organización. Éstas herramientas se denominan CAASM²², para la Gestión de la Superficie de Ataque de Activos Cibernéticos [23], e integran una amplia variedad de fuentes de datos para proporcionar a los equipos de seguridad una visión completa, unificada y actualizada de sus activos. Además, este tipo de soluciones pueden medir la efectividad de la gestión de la superficie de ataque a través del seguimiento de varios indicadores clave de rendimiento (KPI) y métricas, lo que permitiría ayudar a identificar áreas de mejora. Algunos KPI y métricas importantes a considerar incluyen: cobertura de activos, Tiempo Medio de Identificación (MTTI²³), Tiempo Medio de Detección (MTTD²⁴) y Tiempo Medio de Respuesta (MTTR²⁵), o niveles de cumplimiento con configuración segura.

2.2.2 Roles de la superficie de exposición

Todas las capacidades descritas anteriormente pueden ser aprovechadas por los siguientes actores de la infraestructura para poder llevar a cabo la gestión continua de la superficie de exposición a amenazas (CTEM), según su nivel de responsabilidad:

- **Administradores de la superficie de exposición:** disponen de privilegios de lectura y escritura sobre la gestión de la superficie, y pueden mejorar su capacidad en las siguientes tareas en su ámbito o área de actuación:
 - Llevar a cabo una evaluación de riesgos que permita una toma de decisiones basada en datos objetivos para la adquisición de nuevas herramientas de ciberseguridad.
 - Crear nuevos usuarios, ámbitos y áreas de actuación.
 - Mejorar el cumplimiento de normativa nacional, europea e internacional en ciberseguridad y ciberresiliencia.
 - Disponer de métricas para ayudar a medir, comparar y comunicar el riesgo de ciberseguridad a Unidades TIC y a entidades jerárquicas superiores de su organización, así como a organismos dedicados a la mejora de la ciberseguridad y la ciberresiliencia.
 - Obtener una vista unificada del riesgo en ciberseguridad con indicadores clave de rendimiento para medir el progreso de reducción de la superficie de ataque.
 - Llevar a cabo un seguimiento del despliegue de agentes de las herramientas de ciberseguridad a través de paneles de monitorización.
- **Gestores de la superficie de exposición:** disponen de privilegios de lectura y escritura sobre la gestión de la superficie, y pueden mejorar su capacidad en las siguientes tareas en su ámbito o área de actuación:
 - Identificar claramente los activos de la superficie, la trazabilidad entre los externos e internos, los servicios de alto nivel, y poder dedicar recursos priorizados en su mitigación.
 - Conocer con claridad las acciones de mitigación de vulnerabilidades y su priorización.
 - Anticipar los posibles ciberataques a los que se verá sometida la infraestructura.
 - Visualizar los usuarios de la superficie y su papel en la reducción de la superficie de exposición.
 - Disponer de métricas para hacer un seguimiento del progreso de la reducción de la superficie de exposición.

²² CAASM, por sus siglas en inglés, (*Cyber Asset Attack Surface Management*).

²³ MTTI, por sus siglas en inglés (*Mean Time to Identify*).

²⁴ MTTD, por sus siglas en inglés (*Mean Time to Detect*).

²⁵ MTTR, por sus siglas en inglés (*Mean Time to Respond*).

- Comprender el riesgo, cómo reducirlo y establecer de forma precisa las amenazas a las que se ve sometida la infraestructura.
- **Visores de la superficie de exposición:** disponen de privilegios de lectura sobre la gestión de la superficie, y pueden mejorar su capacidad en las siguientes tareas en su ámbito o área de actuación:
 - Disponer de visibilidad completa de la superficie de ataque.
 - Disponer de una vista unificada de todos los activos, sin puntos ciegos y la agrupación de activos que constituyen a su vez activos más alto nivel.
 - Identificar los cuadros de mando para la reducción de la superficie de exposición que les son de utilidad, tanto a nivel estratégico como táctico u operativo.

A continuación, se muestra la Figura 14 con los roles para la gestión continua de la superficie de exposición a amenazas, así como sus privilegios concedidos en esta gestión:

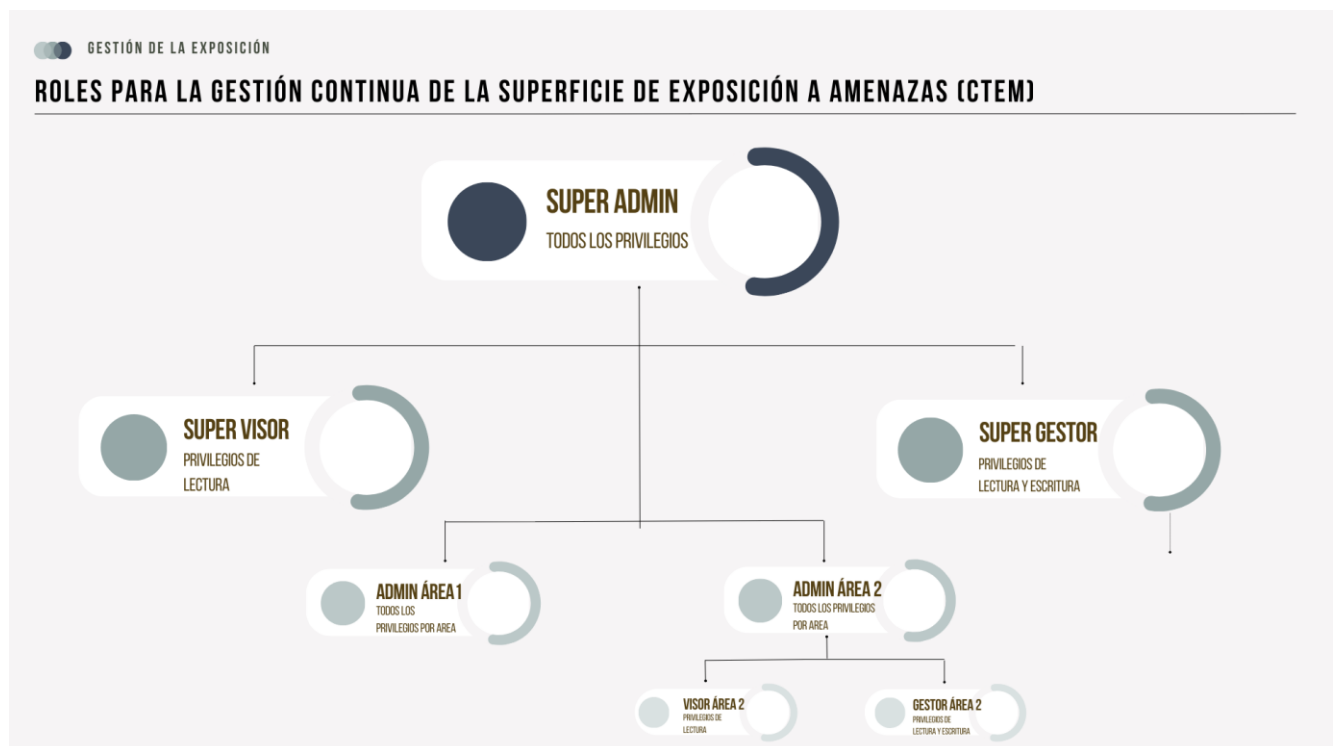


Figura 14 Roles para la gestión continua de la superficie de exposición a amenazas (CTEM) [Fuente propia]

2.3 Herramientas para la gestión de la superficie de exposición

La idea que subyace a la hora de entender y controlar la superficie de exposición de una infraestructura TIC radica en recopilar la mayor información posible de todos elementos que están desplegados en esa infraestructura, extraer de ellos todos los datos, correlacionarlos, y gracias a ello crear conocimiento. Estos elementos, en su mayoría, aunque no de manera exclusiva, son herramientas típicas de ciberseguridad diseñadas con funciones específicas para garantizar la integridad y protección de la infraestructura.

Por tanto, las herramientas de ciberseguridad [24] desplegadas en la infraestructura TIC proporcionan los datos que serán posteriormente cohesionados por una plataforma de gestión de la superficie de exposición, lo que permitirá obtener una comprensión completa de la superficie de exposición y conseguir una gestión precisa y eficaz de la infraestructura. Estas herramientas son típicamente de ciberseguridad, aunque algunas de ellas podrían tener una vocación de gestión de

servicios y cambios (ITSM²⁶), o bien de gestión de elementos de configuración en una infraestructura TIC a través de una base de datos de gestión de configuración (CMDB)²⁷.

Con respecto a la implantación de herramientas de seguridad, Gartner define el concepto de Hype Cycle™ [25] como una metodología de investigación, con el objetivo de representar la madurez y adopción de aplicaciones en el mercado a lo largo del tiempo, evolucionando desde el “desencadenante de innovación”, pasando por “pico de expectativas”, “desilusión”, y “declive”, hasta la “meseta de productividad”. Gracias a este tipo de investigaciones una organización puede alcanzar a comprender cuándo adoptar ciertas tecnologías y cuándo esperar su madurez y estabilización. Concretamente, en el estudio para las operaciones de seguridad, se recomienda la implementación de la gestión continua de la exposición a amenazas (CTEM), y específicamente la comprensión y gestión de la superficie de ataque incluyendo el uso de la inteligencia artificial, junto con la priorización de las acciones de mitigación. A continuación, se muestra la Figura 15 del Ciclo de Hype para Operaciones de Seguridad del año 2023 que indica por ejemplo, el uso actual de herramientas ASCA²⁸, CAASM y EASM²⁹ como “desencadenante de innovación”, herramientas XDR³⁰ y BAS³¹ en su “pico de expectativas”, DRPS³² en su fase de “desilusión”, NDR³³ en “declive”, y finalmente SIEM³⁴ y VM³⁵ en su “meseta de productividad”.

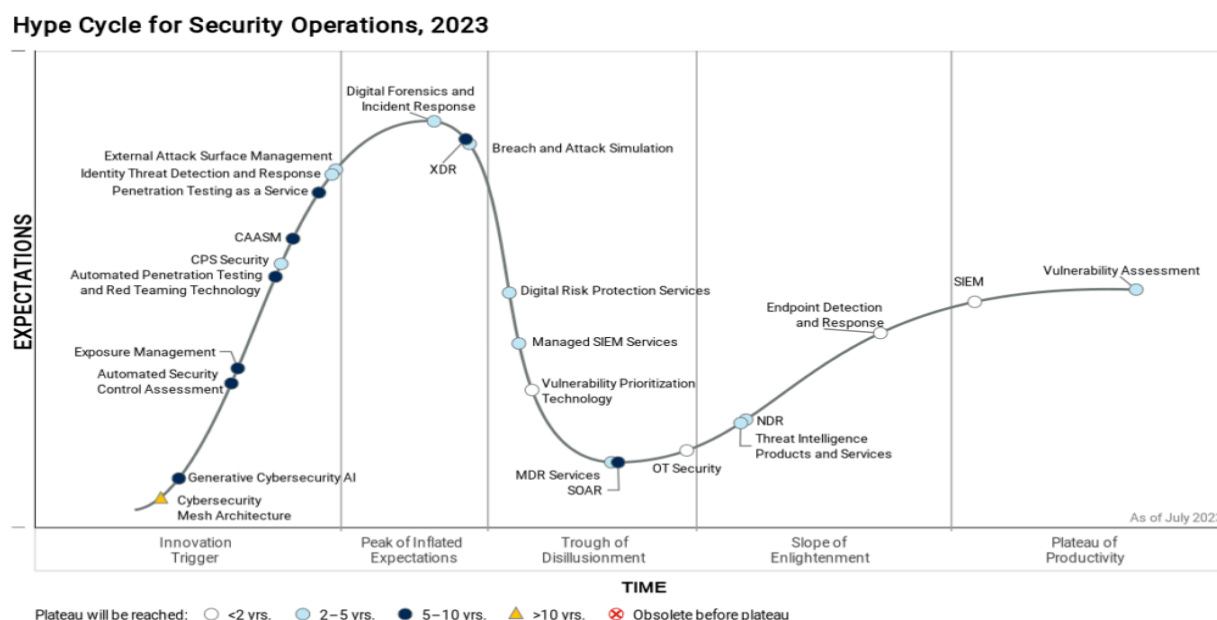


Figura 15 Ciclo de Hype³⁶ para operaciones de seguridad, 2023 (Gartner) [25]

²⁶ ITSM, por sus siglas en inglés (*Information Technology Service Management*).

²⁷ CMDB, por sus siglas en inglés (*Configuration Management Database*).

²⁸ ASCA, por sus siglas en inglés (*Automated Security Control Assessment*).

²⁹ EASM, por sus siglas en inglés (*External Attack Surface Management*).

³⁰ XDR, por sus siglas en inglés (*Extended Detection and Response*).

³¹ BAS, por sus siglas en inglés, (*Breach and Attack Simulation*).

³² DRPS, por sus siglas en inglés (*Digital Risk Protection Services*).

³³ NDR, por sus siglas en inglés (*Network Detection and Response*).

³⁴ SIEM, por sus siglas en inglés (*Security Information and Event Management*).

³⁵ VM, por sus siglas en inglés (*Vulnerability Management*).

³⁶ Hype en marketing es una estrategia de usar publicidad extrema. El hype como estrategia de marketing moderna está estrechamente asociado con las redes sociales. El marketing a través de la exageración a menudo utiliza la escasez

A continuación, se describen todos los posibles tipos de herramientas, muchos de ellos mostrados en la figura anterior, que pueden ser parte de esa base de conocimiento que proporciona información a la plataforma de gestión de la superficie de exposición. Aquellas herramientas que no se muestran en la figura anterior, y que también forman parte de la base de conocimiento, no son específicas de seguridad y se utilizan para el inventario propiamente de activos y servicios (i.e. ITSM, CMDB) o para el acceso de dispositivos a la red (i.e. NAC³⁷). Sin embargo, es importante señalar, que estos tipos de herramientas que proporcionan funcionalidad diversa en una red o sistema de información, están cada vez más orientadas a la seguridad, encontrando soluciones extendidas, proporcionadas por los propios fabricantes, que si que proporcionan seguridad aún no siendo ésta su vocación inicial.

2.3.1 HER.1 – Herramientas de evaluación (ASCA)

Las herramientas de evaluación automatizada de controles de seguridad, comúnmente conocidas como ASCA, funcionan mediante la automatización de la evaluación y prueba de los controles de seguridad en un entorno de tecnologías de la información. Estas herramientas están diseñadas para identificar posibles vulnerabilidades, debilidades en la configuración y otras deficiencias en los sistemas y redes de una organización. Si bien las soluciones de evaluación automática de controles de seguridad son valiosas, no reemplazan las prácticas de evaluación de amenazas o *red teaming*³⁸. Los ejercicios llevados a cabo por este tipo de equipos red funcionan de forma similar a la de un atacante, ajustando tácticas en tiempo real según los datos recopilados, lo que emula una amenaza genuina. Sin embargo, gracias las herramientas ASCA se pueden obtener evaluaciones continuas y automatizadas de ciberseguridad [26]. Algunas de las más importantes del mercado son capaces de trabajar en varios niveles para obtener:

1. **Análisis automático:** realizan escaneos y análisis automáticos en los sistemas y redes de una organización. Estos escaneos pueden incluir la identificación de puertos abiertos, servicios en ejecución y otras características de la infraestructura.
2. **Análisis de configuración:** Examinan la configuración de los sistemas para asegurarse de que cumpla con las mejores prácticas de seguridad. Esto puede incluir la revisión de configuraciones de cortafuegos, políticas de seguridad, configuraciones de servidores y más.
3. **Identificación de vulnerabilidades:** buscan activamente vulnerabilidades conocidas en sistemas, aplicaciones y servicios. Utilizan bases de datos actualizadas de vulnerabilidades para comparar las configuraciones y la versión del software con las amenazas conocidas.
4. **Pruebas de penetración automatizadas:** realizan pruebas de penetración automatizadas para simular ataques y evaluar cómo los sistemas responden a posibles amenazas.

Algunas de las herramientas más utilizadas para la evaluación automatizada de controles de seguridad son:

- **Picus Security**, utiliza una variedad de técnicas para simular amenazas y ciberataques, incluyendo las tácticas, técnicas y procedimientos (TTP) utilizados en ataques reales. La plataforma ejecuta estas simulaciones de amenazas contra la infraestructura de una organización en un entorno controlado y seguro. Además, evalúa la capacidad de los sistemas y las defensas de seguridad para detectar, prevenir y mitigar estos ataques simulados. Por otra parte, es capaz de entrenar a personal de ciberseguridad en la detección y respuesta.

artificial para inducir la demanda

³⁷ NAC, por sus siglas en inglés (*Network Access Control*).

³⁸ *Red teaming*, en inglés, es una práctica en ciberseguridad que simula un enfoque adversarial para evaluar la seguridad de un sistema, red, aplicación o entidad. En lugar de utilizar métodos convencionales de prueba de seguridad que se centran en identificar vulnerabilidades conocidas, este tipo de prácticas adopta la perspectiva de un atacante real y busca descubrir debilidades que podrían pasar desapercibidas en evaluaciones tradicionales.

2.3.2 HER.2 – Herramientas de gestión de la superficie de ataque de ciberactivos (CAASM)

Las herramientas de gestión de la superficie de ataque de ciberactivos, comúnmente conocidas como CAASM, son aplicaciones de ciberseguridad diseñadas para descubrir, evaluar y gestionar la superficie de ataque de una infraestructura TIC. Su propósito principal es proporcionar visibilidad integral de todos los activos digitales, desde servidores y dispositivos móviles hasta recursos en la nube, identificando continuamente nuevos activos y evaluando las vulnerabilidades asociadas. Al ofrecer una comprensión detallada de la postura de seguridad de una organización, una herramienta CAASM facilita la gestión proactiva de riesgos, la toma de decisiones informada y la respuesta rápida a posibles amenazas, contribuyendo así a fortalecer la ciberseguridad y reducir la exposición a riesgos en un entorno tecnológico en constante evolución. Algunas de las más importantes del mercado son capaces de trabajar en varios niveles para obtener:

1. **Visibilidad integral:** proporciona una visibilidad integral de los activos digitales de una organización, incluyendo dispositivos, redes, sistemas, aplicaciones y datos. Esta visibilidad se extiende tanto a entornos locales como a entornos en la nube.
2. **Descubrimiento continuo:** Identificar de manera continua nuevos activos que entran en la infraestructura digital de la organización y realizar un seguimiento de cualquier cambio en la superficie de ataque.
3. **Evaluación de riesgos:** evaluar y priorizar los riesgos asociados con los activos y las vulnerabilidades detectadas, permitiendo a la organización concentrarse en las áreas más críticas desde el punto de vista de la seguridad.
4. **Gestión de vulnerabilidades:** detectar y clasificar vulnerabilidades en los activos, proporcionando información detallada sobre las debilidades y permitiendo una gestión efectiva para la mitigación de riesgos.
5. **Cumplimiento normativo:** ayudar a garantizar que la organización cumple con los requisitos legales y normativos al evaluar y mejorar constantemente la seguridad de sus activos.
6. **Reducción de la superficie de ataque:** identificar y reducir la superficie de ataque al mitigar activos no utilizados o innecesarios que podrían representar riesgos de seguridad.
7. **Respuesta rápida a incidentes:** facilitar la detección temprana de incidentes de seguridad y proporcionar información para una respuesta rápida y eficaz ante amenazas y ataques.
8. **Optimización de recursos de seguridad:** ayudar a las organizaciones a asignar eficientemente recursos de seguridad, centrándose en los activos y áreas de mayor riesgo.
9. **Integración con otras soluciones:** integrarse de manera efectiva con otras herramientas y soluciones de ciberseguridad para proporcionar una visión más completa y coordinada de la postura de seguridad de la organización.
10. **Mejora continua:** facilitar la mejora continua de la seguridad al proporcionar análisis y retroalimentación sobre la eficacia de las medidas de seguridad implementadas y proponer recomendaciones para fortalecer la postura de seguridad en curso.

Algunas de las herramientas más utilizadas para la gestión de la superficie de ataque de activos cibernéticos son:

- runZero, es una es una solución integral de gestión de activos que permite descubrir, inventariar y gestionar todo tipo de activos de tecnologías de la información, desde servidores, estaciones de trabajo y dispositivos móviles hasta activos de IoT y basados en la nube. Es capaz de identificar activos que no están en uso activo para mitigar riesgos de seguridad. Además, crea un inventario de activos recopilando datos clave, como nombre, dirección IP, sistema operativo, software instalado y configuraciones, facilitando la gestión

efectiva de activos, el seguimiento de cambios y la identificación de posibles vulnerabilidades de seguridad [27].

- Lansweeper, es una plataforma de gestión de integral de activos IT, que permite un descubrimiento de activos automático, escaneos para recopilar información de cada activo (sistema operativo, configuraciones hardware, software instalado, direcciones IP...) y alertas de posibles cambios en su configuración.
- Axonius, es una plataforma que proporciona una visión completa de los activos de la infraestructura, la relación entre ellos, y su contexto dentro de la lógica de negocio. Es capaz de conectarse a cientos de fuentes de datos y agregar, normalizar, eliminar duplicados y correlacionar datos sobre dispositivos, identidades, servicios en la nube, software, aplicaciones SaaS³⁹, vulnerabilidades, controles de seguridad y sus interrelaciones. También se pueden automatizar acciones para el control de los activos.

2.3.3 HER.3 – Herramientas de gestión de la superficie externa (EASM)

Las herramientas de gestión de la superficie de exposición externa, comúnmente conocidas como EASM, son soluciones diseñadas para identificar y evaluar posibles vulnerabilidades en la superficie de exposición externa de una infraestructura TIC, lo que permite obtener un mapa completo de todos sus elementos expuestos [28]. Algunas de las más importantes del mercado son capaces de trabajar en varios niveles para obtener:

1. **Descubrimiento de activos visibles:** realizan un análisis automatizado para descubrir todos los activos digitales visibles desde el exterior de la infraestructura gracias a fuentes de información como DNS pasivo, Wikipedia, datos financieros públicos, whois, y bases de datos de certificados. Si bien, el análisis puede estar determinado por la búsqueda en un rango de IPs determinado. Este análisis puede encontrar activo [29]s como dominios, subdominios, servicios en la nube, aplicaciones web y otros recursos accesibles públicamente, además de desconocidos o sin monitorizar. La evaluación se puede realizar de forma periódica para asegurarse de que la exposición digital se mantenga bajo control, lo que ayuda a detectar nuevos activos y cambios en la exposición con el tiempo.
2. **Evaluación de vulnerabilidades:** una vez que se identifican los activos, evalúan la exposición de estos activos visibles a amenazas potenciales y vulnerabilidades conocidas y configuraciones inseguras, y problemas de privacidad. Utilizan bases de datos de vulnerabilidades y patrones de ataque para medir el riesgo asociado con cada activo. Incluso, a través de evaluaciones avanzadas se llevan a cabo pruebas de seguridad de aplicaciones dinámicas (DAST⁴⁰), se detectan vulnerabilidades y exposiciones comunes (CVEs), código de aplicaciones explotables, configuraciones incorrectas del sistema, datos expuestos, credenciales predeterminadas, y problemas de validez de certificados.
3. **Priorización:** utilizan diversos enfoques para la priorización de acciones de mitigación, con el objetivo de abordar primero los riesgos más críticos y reducir la exposición digital de manera efectiva. Algunas de las formas en que llevan a cabo la priorización de acciones son: gravedad de la vulnerabilidad, riesgo asociado, capacidad de explotación, valor del activo, impacto en la superficie de exposición, recomendaciones de cumplimiento, conjunto de políticas, y capacidad de ataque.
4. **Acciones correctivas:** proponen acciones correctivas para abordar los riesgos y las vulnerabilidades detectadas, como por ejemplo: recomendaciones detalladas, escenarios de

³⁹ SaaS, por sus siglas en inglés (*Software as a Service*).

⁴⁰ DAST, por sus siglas en inglés (*Dynamic Application Security Testing*).

mitigación e incluso la automatización de ciertas acciones correctivas, como la aplicación de parches o la modificación de configuraciones.

Algunas de las herramientas más utilizadas para la gestión de la superficie de externa son:

- Acunetix, diseñada para evaluar y mitigar vulnerabilidades en aplicaciones web y sitios web. Funciona en cualquier aplicación web o sitio web a través del navegador y utiliza el protocolo estándar HTTP/HTTPS. También analiza software y aplicaciones web que utilizan JavaScript.
- Cycognito, es una plataforma de seguridad para identificar, analizar y mitigar vulnerabilidades de los activos expuestos, como sitios web, aplicaciones e infraestructuras de red. Lleva a cabo descubrimiento de activos, mapeo de la superficie de ataque, evaluación de riesgos y monitorización continua.
- Tenable Attack Surface Management (Tenable.asm), es parte de la plataforma de seguridad de Tenable y permite obtener visibilidad integral de los activos, servicios y aplicaciones conectados a Internet. Además, permite realizar una evaluación de la superficie de ataque, una evaluación de riesgos y priorización de las acciones correctivas, así como la integración con otras soluciones de Tenable.

2.3.4 HER.4 – Herramientas de detección y respuesta extendida ante amenazas (XDR)

Las herramientas de detección y respuesta extendida ante amenazas, comúnmente conocidas como XDR, permiten una detección temprana y una respuesta efectiva ante ciberamenazas. Algunas de las más punteras del mercado proporcionan la siguiente funcionalidad:

1. **Recopilación y correlación de datos y eventos:** recopilan y correlacionan datos de múltiples fuentes de la infraestructura, principalmente referidos a los activos tipo dispositivo final, como servidores y estaciones de trabajo. Además, recopilan información del registro de eventos, datos de tráfico de red y la actividad de cada usuario. Analizan y correlacionan eventos en toda la organización para identificar patrones y cadenas de eventos que podrían indicar un ataque en curso.
2. **Análisis de comportamiento y respuesta automatizada:** utilizan análisis de comportamiento avanzado para identificar patrones y actividades anómalas en la infraestructura. Pueden detectar actividades sospechosas, como movimientos laterales (cuando un atacante o malware se propaga desde un punto de entrada al resto de la red), comunicaciones maliciosas y acceso no autorizado. Pueden automatizar la respuesta para llevar a cabo acciones inmediatas ante amenazas, como bloquear direcciones IP sospechosas o aislar sistemas comprometidos. Además, pueden integrarse con otras soluciones de seguridad y herramientas de gestión para un flujo de trabajo más eficiente y una respuesta más efectiva.
3. **Detección de amenazas:** utilizan bases de datos de indicadores de compromiso (IoC⁴¹) y firmas de malware para identificar en tiempo real ciberamenazas conocidas, como malware, direcciones IP maliciosas y dominios sospechosos. Asimismo, emplean técnicas de análisis de comportamiento y análisis heurístico, y en algunos casos algoritmos de Inteligencia Artificial, para detectar ciberamenazas nuevas y desconocidas que no coinciden con las firmas tradicionales

⁴¹ IoC, por sus siglas en inglés (*Indicator of Compromise*) se refiere a información específica que puede indicar la presencia de actividad maliciosa en un sistema o red. Estos indicadores son utilizados en el ámbito de la ciberseguridad para identificar posibles compromisos de seguridad y para tomar medidas correctivas. Los IOC pueden ser tanto técnicos como contextuales, y algunos ejemplos incluyen direcciones IP, nombres de dominio, dominios de internet, hash de archivos, patrones de comportamiento, firmas de malware, credenciales comprometidas, reglas de detección de IDS/IPS...

de malware. Además, clasifican las amenazas identificadas según su gravedad y riesgo potencial para ayudar a los analistas de seguridad a enfocarse en las amenazas más críticas primero.

4. **Análisis forense:** proporcionan herramientas para investigar incidentes y analizar a fondo la naturaleza y el alcance de una amenaza. Los analistas pueden profundizar en los datos, identificar el vector de ataque y evaluar el impacto. Además, pueden generar informes detallados sobre amenazas identificadas, ciberincidentes y resultados de análisis para mejorar la visibilidad y la toma de decisiones.

Algunas de las herramientas más utilizadas para la detección y respuesta ante amenazas son:

- Cortex XDR, identifica automáticamente ataques activos mediante la instalación de agentes en los servidores y en las estaciones de trabajo, y enviando la información proporcionada por estos agentes a la nube donde se lleva a cabo el análisis. Utiliza aprendizaje automático para establecer comportamientos anómalos por parte del usuario y del propio dispositivo.
- CrowdStrike, es una plataforma de ciberseguridad con protección de dispositivos finales a través de inteligencia artificial y aprendizaje automático, además de implementación de reglas en cortafuegos y controles en aplicaciones para prevenir el acceso no autorizado y la ejecución de programas maliciosos. Los datos de seguridad se recopilan y analizan en tiempo real en la nube, lo que facilita la administración desde cualquier ubicación.
- Microsoft Defender XDR, es una solución integral de seguridad que protege tanto el entorno multinube como multiplataforma y permite obtener una visibilidad completa de las ciberamenazas gracias al uso de inteligencia artificial y aprendizaje automático. Analiza dispositivos finales e identidad digital. Permite agilizar la respuesta a incidentes a través de un proceso de investigación centralizado y automatizado que incluye correlación de eventos. Lleva integrado también las capacidades SIEM.
- TRENDMicro Deep Discovery, es un conjunto de herramientas para la detección de comportamiento anómalo desplegada a través de agentes que se comunican con un manager, e incluye un módulo para actuar como parcheado virtual antes de que actúe propiamente el EDR, llevando a cabo una protección activa contra CVEs conocidas. Implementa una capa de seguridad de políticas y reglas de seguridad que evitan la explotación de una vulnerabilidad determinada.
- SentinelOne, es una plataforma de protección de dispositivos finales, con un despliegue típico de agentes en estos activos y con análisis de comportamiento a través de algoritmos de IA para procesos en ejecución. Como capacidad de respuesta es capaz de realizar aislamiento de la red, inmunización automática de los activos, reversión al punto anterior, incluyendo reversión de *ransomware*.

2.3.5 HER.5 – Herramientas de simulación de amenazas (BAS)

Las herramientas de simulación de amenazas, comúnmente conocida como BAS, son aplicaciones diseñadas para probar y mejorar la ciberseguridad de una infraestructura TIC al simular amenazas y ataques de una manera controlada, ayudando a identificar vulnerabilidades, evaluar su ciberresiliencia y llevar a cabo medidas de seguridad para fortalecer su ciberseguridad, siendo una de las herramientas fundamentales para implementar un programa continuo de gestión de exposición de amenazas [29]. Algunas de las más importantes del mercado son capaces de trabajar en varios niveles para obtener:

1. **Simulaciones de ataques:** permiten simular una variedad de ciberataques, como *phishing*, *ransomware*, explotación de vulnerabilidades y más, para evaluar la efectividad de sus defensas. Además, son capaces de evaluar la efectividad de las defensas de seguridad existentes y cómo responden a las amenazas simuladas. Esto ayuda a identificar brechas en la seguridad y áreas de mejora.

2. **Evaluación de la superficie de ataque:** al igual que las herramientas de análisis de la superficie de exposición externa, analizan este tipo de superficie de exposición pero incluyendo además la superficie interna, encontrando los puntos de entrada potenciales para los ciberataques así como todo tipo de vulnerabilidades. Además, permiten evaluar cómo funcionan las defensas de seguridad existentes ante amenazas simuladas. Esto revela si las soluciones de seguridad son efectivas o si necesitan mejoras.
3. **Medición de ciberresiliencia:** ayudan a comprender su capacidad para resistir y recuperarse de ciberamenazas, proporcionando métricas de riesgo que ayudan a comprender qué amenazas y vulnerabilidades representan el mayor riesgo para la infraestructura, permitiendo priorizar las acciones de mitigación.

Algunas de las herramientas más utilizadas para la simulación de amenazas y validación automatizada de seguridad son:

- Cymulate, es una plataforma de gestión de la exposición a amenazas, simulando todo tipo de amenazas y vulnerabilidades conocidas (como lo haría un ciberatacante). Prioriza las debilidades detectadas en función de su gravedad y riesgo potencial, permitiendo además validar las acciones de mitigación, como parches y configuraciones seguras, para comprobar si realmente se resuelven los problemas de seguridad. También proporciona simulaciones de ataques configurables y trazabilidad con la matriz MITRE ATT&CK [19].
- Pentera, es una plataforma de cobertura continua de ciberseguridad que evalúa tanto la superficie de exposición interna como externa. No utiliza agentes para llevar a cabo la validación en tiempo real de la ciberseguridad de la infraestructura. Además, emula ataques, incluyendo las últimas tácticas, técnicas y procedimientos presentes en el ciberespacio.
- XM Cyber, es una solución para la gestión continua de la exposición con capacidad para descubrir conexiones ocultas entre configuraciones incorrectas, vulnerabilidades e identidades excesivamente permisivas que comprometen activos críticos. Permite obtener una vista única de todas las redes locales y en la nube para reducir continuamente la exposición al riesgo. Detecta oportunidades de movimiento lateral y visualiza el enfoque de un atacante mediante un modelo basado en gráficos.

2.3.6 HER.6 – Servicios de Protección de Riesgos Digitales (DRPS)

Los servicios de protección de riesgos digitales abordan la necesidad de proteger activos digitales y mitigar riesgos en entornos del ciberespacio. Este tipo de servicios supervisan la superficie web, la *dark web*⁴², plataformas de redes sociales y mercados de aplicaciones para identificar amenazas. Algunas de las más punteras del mercado proporcionan la siguiente funcionalidad:

1. **Monitorización de amenazas en la web:** estos servicios monitorizan la *dark web* en busca de información comprometida, datos filtrados, cuentas falsas en redes sociales, credenciales filtradas o robadas, información de tarjetas de crédito, de propiedad intelectual y código, o bien amenazas específicas contra la organización.
2. **Protección de marca en el ciberespacio:** rastrean y protegen la marca de una organización en línea, identificando actividades fraudulentas, dominios falsos que se hacen pasar por una marca u organización o dominios ilegítimos que han sido comprometidos, falsificación de sitios web y uso no autorizado de la marca.

⁴² La *dark web* o internet oscura es el contenido de la *World Wide Web* que existe en o redes oscuras, redes que se superponen a la internet pública y requieren de software específico y configuraciones o autorización para acceder.

3. **Gestión de reputación en línea:** estos servicios ayudan a monitorear y gestionar la reputación en línea de una organización, respondiendo proactivamente a comentarios negativos y mitigando posibles riesgos para la reputación.
4. **Detección de fugas de datos:** las soluciones DLP⁴³ ayudan a prevenir la fuga de datos confidenciales y proporcionan capacidades de detección y respuesta ante amenazas.
5. **Protección contra *phishing* y fraude en el ciberespacio:** estas plataformas utilizan análisis avanzado para detectar y prevenir ataques de *phishing* y actividades fraudulentas en línea.
6. **Monitorización de actividad en redes sociales:** estas herramientas rastrean la actividad en redes sociales para identificar amenazas, comentarios negativos o actividades maliciosas relacionadas con la organización.

Algunas de las herramientas o servicios más utilizadas para la protección de riesgos digitales son:

- Allure Security Technology, proporciona servicios de protección de marca [30] utilizando inteligencia artificial para analizar millones de fuentes en el ciberespacio y encontrar dominios falsos, sitios web fraudulentos, ataques de *phishing*, perfiles falsos en redes sociales y otras estafas, todo ello sin ningún esfuerzo manual.
- Fortirecon, es un servicio SaaS que incluye la protección de la marca y reputación en el ciberespacio, detectando y eliminando los riesgos cibernéticos asociados. Por ejemplo, sitios web falsos, cuentas en redes sociales, aplicaciones móviles y credenciales en venta.

2.3.7 HER.7 – Herramientas de detección y respuesta de red (NDR)

Las herramientas de detección y respuesta de red, comúnmente conocidas como NDR, están diseñadas para detectar ciberamenazas en redes corporativas utilizando inteligencia artificial (IA), aprendizaje automático (ML) y análisis de datos. Algunas de las más punteras del mercado proporcionan la siguiente funcionalidad:

1. **Detección de amenazas:** utilizan inteligencia artificial (IA), aprendizaje automático (ML) y análisis de datos para identificar patrones de tráfico anómalos o sospechosos que podrían indicar la presencia de ciberamenazas. Además, proporcionan información contextual sobre amenazas, incluyendo detalles sobre la naturaleza de la amenaza, el vector de ataque y la posible magnitud del impacto.
2. **Modelado del comportamiento normal:** construyen modelos de comportamiento normal analizando continuamente el tráfico de red tanto en la dirección norte/sur (que cruza el perímetro de la empresa) como en la dirección este/oeste (tráfico lateral dentro de la red).
3. **Análisis de tráfico:** examinan el tráfico de red en tiempo real para identificar actividades inusuales, comunicaciones no autorizadas o comportamientos que podrían indicar una violación de seguridad. Permiten además, investigar incidentes de seguridad, permitiendo a los analistas examinar el tráfico pasado y entender la naturaleza y el alcance de una amenaza.
4. **Alertas y notificaciones:** generan alertas y notificaciones automáticas en tiempo real cuando se detectan patrones de tráfico anómalos, para poder responder de manera inmediata ante posibles amenazas.

Algunas de las herramientas más utilizadas para la detección y respuesta de red son:

- Darktrace, es una plataforma de seguridad que utiliza inteligencia artificial y aprendizaje automático para detectar y responder a amenazas en la red en tiempo real, tal y como lo realiza el sistema inmunológico humano. Su enfoque se basa en la detección de anomalías y

⁴³ DLP, por sus siglas en inglés (*Data Loss Prevention*).

comportamientos inusuales en la red y los sistemas, siendo capaz de realizar acciones llevando a cabo las menos agresivas para contener cada amenaza.

- *Horizon NDR Check Point*, es una solución para redes en la nube privada y pública, así como para redes locales, que proporciona visibilidad integral de la red, inteligencia de amenazas y capacidades de detección de amenazas que podrían haber eludido otras soluciones de seguridad.

2.3.8 HER.8 – Herramientas de gestión de eventos de seguridad (SIEM)

Las herramientas de gestión de eventos se comportan como sistemas de gestión de seguridad que recopilan, analizan y presentan información y eventos relacionados con la seguridad de una infraestructura. Algunas de las más punteras del mercado proporcionan la siguiente funcionalidad:

1. **Recopilación de datos:** recopilan datos de múltiples fuentes en la red y sistemas de la organización, incluyendo registros de eventos de sistemas, registros de aplicaciones, registros de dispositivos de seguridad, y registros de redes. También pueden recuperar datos de sucesos como inicios de sesión de usuario, correo electrónico, conexiones VPN, denegaciones de cortafuegos, así como datos de flujo como la información de sesión entre dos servidores en una red. Una vez recopilados los datos se normalizan y estandarizan para que puedan ser procesados y comparados de manera eficiente
2. **Correlación y análisis de eventos:** realizan análisis avanzados para identificar y comprender patrones de datos complejos para poder correlacionar eventos y proporcionar información para localizar y mitigar rápidamente posibles amenazas. Utilizan técnicas de detección de anomalías para identificar comportamientos inusuales que podrían indicar actividad maliciosa o compromiso, incluyendo patrones de acceso, horarios inusuales y cambios de configuración. Mejoran significativamente el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR) de los equipos de seguridad de TI al aliviar los flujos de trabajo manuales asociados con el análisis en profundidad de eventos de seguridad.
3. **Supervisión de incidentes y a alertas de seguridad:** cuando se identifican eventos o comportamientos sospechosos, generan alertas para notificar a los equipos de seguridad. Estas alertas pueden estar basadas en reglas predefinidas o en análisis de comportamiento anómalo. También pueden automatizar respuestas a eventos de seguridad, como el bloqueo automático de dispositivos o la aplicación de políticas de seguridad. Además, incluyen paneles de control y reportes que permiten a los equipos de seguridad visualizar la actividad en la red y los sistemas. Estos informes pueden incluir tendencias, estadísticas, detalles de eventos y más.
4. **Análisis forense:** en caso de incidentes de seguridad, permiten el análisis forense para rastrear el origen y la propagación de las amenazas. Esto es esencial para comprender la magnitud del incidente y tomar medidas adecuadas.

Algunas de las herramientas más utilizadas para la gestión de eventos de seguridad son:

- *Qradar*, es una plataforma de gestión de información y eventos de seguridad que se utiliza para recopilar, procesar, analizar, correlacionar y almacenar datos de seguridad en tiempo real para identificar amenazas y responder a incidentes. Proporciona una arquitectura modular que permite visibilidad en tiempo real de la infraestructura TIC. Esta plataforma de inteligencia de seguridad consta de tres capas (recopilación, proceso y búsqueda de datos) y se aplica a cualquier estructura de despliegue.
- *Splunk*, es una plataforma de análisis de datos en tiempo real que recopila e indexa datos de diversas fuentes, como registros, sensores o métricas. Toda la información recolectada se indexa y almacena en una base de datos optimizada para búsquedas, siendo posteriormente analizada e interpretada para la toma de decisiones. Se puede desplegar en la propia infraestructura o en la nube.

2.3.9 HER.9 – Herramientas de gestión de vulnerabilidades (VM)

Las herramientas de análisis de vulnerabilidades, comúnmente conocidas como VM, son aplicaciones diseñadas para identificar y evaluar posibles vulnerabilidades, y su metodología principal [31] incluye el uso de escáneres o agentes basados en red o desplegados en el propio servidor o estación de trabajo, para descubrir vulnerabilidades de seguridad o configuraciones que puedan ser explotadas. Estos escáneres buscan y descubren dispositivos de manera anónima y tratan de encontrar vulnerabilidades conocidas en sistemas objetivo. Este tipo de plataformas de gestión de vulnerabilidades de dispositivos priorizan los resultados del escaneo (qué activos necesitan atención primero) y el riesgo que representan las vulnerabilidades encontradas para una organización si no se solucionan. La búsqueda de vulnerabilidades también se ha expandido a dispositivos IoT/OT⁴⁴ y a contenedores e infraestructuras en la nube. Algunas de las más importantes del mercado son capaces de trabajar en varios niveles para obtener:

1. **Evaluación básica de activos:** se realiza una evaluación básica de la red para llevar a cabo una detección de vulnerabilidades sobre activos sin credenciales o vista no autorizada (modo caja negra), por lo que los escaneos no son autenticados. Esta vista de hacker simula un posible ataque para ver si un dispositivo puede ser explotado.
2. **Evaluación avanzada de activos:** se realiza una evaluación avanzada ya que la detección de vulnerabilidades se realiza sobre los activos con credenciales usando nombre de usuario y contraseña (modo caja blanca). Gracias a la evaluación con credenciales se puede obtener una gran cantidad de información relacionada con la seguridad sobre el software instalado y sus vulnerabilidades. Además, se puede incluir la detección de malware en los sistemas de archivos, detectando incluso la presencia, estado de actualización y el funcionamiento de ciertos antivirus. Este tipo de evaluación se puede llevar a cabo de dos formas:
 - Con credenciales de acceso al activo. Este tipo de análisis autenticado permite iniciar sesión de forma remota en los dispositivos llevando a cabo el análisis desde dentro hacia fuera.
 - Despliegue de agentes autenticados en cada uno de los activos. Este tipo de análisis se considera con credenciales ya que el software instalado en cada activo permite el inicio de sesión de forma remota en los dispositivos llevando a cabo también el análisis desde dentro hacia fuera. La utilización de agentes resuelve dos problemas comunes de los activos transitorios. En primer lugar, se elimina los puntos ciegos que suponen no evaluar los activos que se desconectan de la red durante los análisis. En segundo lugar, solo informan sobre un activo determinado (y sus vulnerabilidades) una única vez, incluso si su dirección IP cambia con cada reconexión.
3. **Evaluación de las configuraciones y optimización por tipos de activos:** se evalúan los activos de acuerdo a una configuración determinada, con lo que se reduce la superficie de ataque de un activo al deshabilitar servicios innecesarios, como FTP y RDP, y otras configuraciones que dejan caminos de ataques al descubierto. Según el tipo de activo, la configuración seguirá unas pautas determinadas que podrán ser comprobadas durante el proceso de evaluación. Por ejemplo, la evaluación de activo tipo servidor será diferente dependiendo si el servidor es de base de datos, servidor de dominio, servidor web, servidor de aplicaciones u otro.
4. **Evaluación continua de activos:** se agrega la evaluación casi en tiempo real de los nuevos activos. Si el nuevo activo incluye un agente en su imagen de creación, el agente evaluará automáticamente el activo e informará de los resultados.

Algunas de las herramientas más utilizadas para el análisis y gestión de vulnerabilidades son:

⁴⁴ OT, por sus siglas en inglés (*Operational Technology*).

- Tenable Security Center, desplegado en la propia infraestructura, o Tenable Vulnerability Management, desplegado en la nube, lleva a cabo un despliegue para la evaluación de vulnerabilidades basado en la instalación de agentes en servidores y estaciones de trabajo. También puede llevar a cabo evaluaciones de cumplimiento.
- Rapid7 InsihVM, combina análisis de la red y evaluación basada en agentes, llevando a cabo la evaluación tanto en infraestructuras virtuales como en la nube. También puede llevar a cabo evaluaciones de cumplimiento.
- Qualys Vulnerability Management Detection and Response (VMDR), utiliza un motor de escaneo basado en inferencia único para encontrar vulnerabilidades. Cada escaneo comienza con un módulo de preescaneo que identifica de manera precisa un servidor. La identificación se realiza mediante el envío de una serie de paquetes especialmente diseñados y posteriormente se interpretan los resultados.
- Flexera Software Vulnerability Manager, identifica y gestiona vulnerabilidades en sistemas operativos y aplicaciones, priorizando los parches a aplicar teniendo en cuenta las amenazas. Dispone de un repositorio de parches para la aplicación de los mismos, incluso de forma automatizada siguiendo unos criterios establecidos.

2.3.10 HER.10 – Herramientas de gestión TIC y configuración (ITSM y CMDB)

Las herramientas de gestión TIC de configuración están diseñadas para administrar y llevar a cabo la gestión de servicios y cambios, así como la comprobación del estado de configuración de un dispositivo, manteniendo un control preciso sobre la configuración de sus activos. Algunas de las más punteras del mercado proporcionan la siguiente funcionalidad:

1. **Gestión de servicios:** ayudan a operar los servicios, clasificando y priorizándolos. Además, incluyen el registro de incidentes (problemas o interrupciones no planificadas) o solicitudes de servicio (necesidades planificadas).
2. **Gestión de cambios:** gestionan y controlan de manera eficiente los cambios en la infraestructura TIC. Estos cambios pueden incluir actualizaciones de software, modificaciones en la infraestructura de red, cambios en configuraciones, entre otros.
3. **Automatización de la gestión de configuración:** automatizan las tareas de configuración, lo que ayuda a reducir errores humanos, agilizando los procesos de implementación y actualización de cambios. Supervisan la configuración en tiempo real y alertan sobre cambios no autorizados o desviaciones de las políticas establecidas, facilitando la implementación de cambios a gran escala, manteniendo la coherencia y reduciendo el tiempo de inactividad. Además, aseguran que la configuración sea consistente en todos los sistemas, lo que evita problemas de compatibilidad y rendimiento.
4. **Control de versiones:** realizan un seguimiento de versiones de configuración para asegurarse de que las actualizaciones se realizan de manera controlada y se pueden revertir en caso necesario. Además, permiten la generación de registros y auditorías de cambios en la configuración para rastrear quién realizó qué cambios y cuándo.
5. **Cumplimiento normativo:** ayudan a garantizar que las configuraciones cumplan con estándares de seguridad, guías y mejores prácticas. Comprueban que se siguen pautas de seguridad específicas, y configuraciones específicas a través de plantillas de seguridad. Pueden llegar a corregir configuraciones no seguras. Permiten además, generar informes que son enviados a organismos como el CCN para informar del estado de seguridad de la infraestructura.

Algunas de las herramientas más utilizadas para la gestión de la configuración son:

- Clara (CCN-CNI), es una herramienta que se instala en el propio cliente o puede funcionar como agente escuchando a través de un puerto las solicitudes de cliente y remitiendo al

mismo los análisis efectuados, permitiendo analizar las características de seguridad técnica definidas para el Esquema Nacional de Seguridad (ENS). El análisis del cumplimiento está basado en las normas proporcionadas a través de las plantillas de seguridad de las Guías CCN-STIC 850^a, 850B, 851, 851B, 870^a, 870B, 899^a y 899B.

- **Tenable Audit**, es parte de su plataforma de seguridad y se utiliza para evaluar la seguridad de los sistemas y aplicaciones mediante la ejecución de auditorías automatizadas basadas en políticas personalizadas. Estas auditorías ayudan a identificar vulnerabilidades, configuraciones incorrectas y otros problemas de seguridad en los sistemas.
- **Microsoft System Center Configuration Manager**, es un software que administra cambios y configuraciones en servidores, estaciones de trabajo, dispositivos móviles y software desarrollado por Microsoft.
- **BMC Discovery**, es una herramienta diseñada para descubrir y mapear automáticamente todos los activos y relaciones en una infraestructura de tecnología de la información (TI). Además, ayuda en la gestión de configuración al mantener una visión precisa y actualizada de todos los elementos de la infraestructura.
- **IBM Instana**, es una solución que va más allá de una herramienta ITSM, ya que se centra en los aspectos operativos del ciclo de vida de un servicio (ITOM⁴⁵). Proporciona datos continuos de los servicios de una infraestructura gracias al despliegue de agentes en los activos. Además, es capaz de trazar dependencias lógicas y físicas en los activos, incluyendo dispositivos móviles, servicios web, aplicaciones, y la propia infraestructura.
- **Proactivanet**, es una herramienta ITSM que se utiliza para administrar y optimizar procesos relacionados con los servicios de tecnología en una organización. Su funcionalidad puede variar, pero generalmente incluye características como la gestión de incidentes, problemas, cambios, activos, y otros aspectos de la infraestructura tecnológica.

2.3.11 HER.11 – Herramientas de control de acceso a red (NAC)

Las herramientas de control de acceso a red monitorizan continuamente la red y evalúan la configuración, el estado y la seguridad de los dispositivos conectados para determinar sus perfiles de riesgo y si cumplen con las políticas de seguridad y normativa específica. Algunas de las más punteras del mercado proporcionan la siguiente funcionalidad:

1. **Autenticación y autorización:** cuando un dispositivo o usuario intenta acceder a la red, verifican su identidad a través de diversos métodos de autenticación, como credenciales de inicio de sesión, certificados digitales o autenticación de dos factores. Una vez autenticado, verifican si el dispositivo o usuario tiene permiso para acceder a la red.
2. **Descubrimiento de dispositivos:** realizan un descubrimiento continuo de dispositivos en la red, identificando automáticamente todos los dispositivos que se conectan, ya sea por cable o de forma inalámbrica. Esto incluye dispositivos conocidos y desconocidos. Una vez descubiertos, utilizan técnicas de clasificación para identificar el tipo de dispositivo (por ejemplo, estaciones de trabajo, teléfonos, cámaras, impresoras, IoT, etc.) y recopilan información sobre su sistema operativo, dirección IP, puertos abiertos, etc.
3. **Monitorización continua:** Realizan una monitorización continua de los dispositivos a medida que se conectan, desconectan o cambian en la red. También puede detectar actividad anómala o cambios en los dispositivos que puedan indicar una posible amenaza.

⁴⁵ ITOM, por sus siglas en inglés (*IT Operations Management*). ITOM es una subdisciplina de ITSM que se centra en aspectos operacionales del ciclo de vida del servicio. Dentro del modelo de ITSM, ITOM se enfoca en la gestión del servicio entre bastidores que generalmente no es visible para el usuario final.

4. **Evaluación de seguridad y control de acceso a la red:** evalúan la seguridad de los dispositivos en función de políticas predefinidas y recomendaciones de seguridad. Pueden identificar configuraciones inseguras, vulnerabilidades conocidas y si los dispositivos cumplen con los requisitos de seguridad. Permiten la aplicación de políticas de acceso basadas en roles y condiciones. Pueden restringir, limitar o permitir el acceso de los dispositivos a la red según su clasificación, cumplimiento y otros criterios.

Algunas de las herramientas más utilizadas para el control de acceso a la red son:

- NAC Forescout, es una plataforma basada en la visibilidad de los dispositivos de la red en tiempo real, que analiza continuamente la red y monitoriza la actividad de cada dispositivo, aplicando un control de acceso basado en políticas previamente definidas. Es capaz de obtener información de la red sin necesidad de instalar un agente en cada dispositivo y se integra con los switches de la infraestructura, pudiendo asignar cada dispositivo en un segmento concreto de la red de forma dinámica.
- Cisco ISE, es una solución basada en políticas para la red, cuya función principal es autenticar y autorizar dispositivos y usuarios antes de permitirles acceder a la red y a las aplicaciones.
- Aruba ClearPass Policy, es una solución que se basa en la autenticación, autorización y cumplimiento de políticas para garantizar el acceso seguro y adecuado a los recursos de la red.
- FortiNAC, proporciona seguridad en la red mediante la implementación de políticas de acceso, visibilidad y cumplimiento de dispositivos. Su funcionamiento se basa en la autenticación, autorización y cumplimiento de políticas para garantizar un acceso seguro y adecuado a los recursos de la red.

2.4 Tipos de vulnerabilidades en la superficie de exposición

El conjunto de la suma de vulnerabilidades, o vectores de ataque de una infraestructura se considera la superficie de ataque, ya que un atacante los utiliza para obtener acceso no autorizado o llevar a cabo un ciberataque.

A continuación, se describen todos los tipos de vulnerabilidades que constituyen la superficie de ataque y que son identificadas por diferentes proyectos u organismos a través de bases de datos públicas, glosarios, guías y otras publicaciones.

2.4.1 VUL.1 – Vulnerabilidades y Exposiciones Comunes (CVE)⁴⁶

Según el proyecto de MITRE CVE [32] se define una vulnerabilidad como “la lógica computacional (por ejemplo, código) encontrada en componentes de software y hardware que, cuando es explotada, resulta en un impacto negativo en la confidencialidad, integridad o disponibilidad. La mitigación de las vulnerabilidades en este contexto generalmente implica cambios en el código, pero también podría incluir cambios en las especificaciones o incluso la depreciación de especificaciones (por ejemplo, la eliminación de protocolos o funcionalidades afectadas en su totalidad)”.

MITRE define la lista CVE como un glosario de vulnerabilidades y exposiciones disponibles públicamente, debidamente identificadas y categorizadas con el objetivo de intercambiar información sobre vulnerabilidades conocidas. Asimismo, define la gravedad de cada una a través de puntuaciones CVSS⁴⁷ que oscilan entre 0.0 y 10.0 (cuanto mayor será el número, mayor es el grado de gravedad). La

⁴⁶ CVE, por sus siglas en inglés (*Common Vulnerabilities and Exposures*).

⁴⁷ CVSS, por sus siglas en inglés (*Common Vulnerability Scoring System*).

puntuación CVSS sigue una fórmula compuesta por varias métricas de seguridad. Las métricas involucradas en la determinación de la gravedad de una vulnerabilidad incluyen:

- Vector de acceso.
- Complejidad del ataque.
- Confidencialidad de los datos procesados por el sistema que contiene la vulnerabilidad.
- Integridad del sistema explotado.

2.4.2 VUL.2 – Enumeración de Vulnerabilidad Comunes (CWE)⁴⁸

CWE es una lista de tipos de debilidades de software pensada para desarrolladores y expertos en ciberseguridad. Fue creada, al igual que CVE, para unificar la descripción de las debilidades de seguridad de software en cuanto a arquitectura, diseño y código. Es un catálogo de debilidades documentadas que suelen aparecer en el código fuente, y que podría derivar en vulnerabilidades a ser explotadas por un cibertacante. Es muy utilizada por distintas herramientas de seguridad cuyo objetivo es identificar esta debilidades, así como para promover la identificación de vulnerabilidades, mitigación y su prevención

La lista de CWE dispone de tres vistas diferentes:

- Tipo diccionario: incluye las debilidades debidamente enumeradas.
- Vista de árbol: donde se clasifican las debilidades individuales.
- Nueva vista de árbol: permite al usuario ampliar el conocimiento y las relaciones de las debilidades individuales encontradas en la vista anterior.

2.4.3 VUL.3 – Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP)⁴⁹

Según el proyecto de código abierto OWASP [33] para mejorar la seguridad del software, una vulnerabilidad es “una brecha o debilidad en una aplicación, que puede ser un defecto de diseño o un error de implementación, y que permite a un atacante causar daño a las partes interesadas de una aplicación. Las partes interesadas incluyen al propietario de la aplicación, los usuarios de la aplicación y otras entidades que dependen de la aplicación”.

OWASP es una iniciativa de código abierto dedicada a combatir las causas que hacen que el software sea inseguro. De entre los proyectos desarrollados por la comunidad OWASP, destacan los siguientes:

- *OWASP Top 10*: informe que recoge las vulnerabilidades más comunes dentro de las aplicaciones web y cómo prevenirlas.
- *OWASP Proactive Controls*: documento que resume las buenas prácticas que deberían incluirse en cada proyecto de desarrollo de software.
- *OWASP Application Security Verification Standard (ASVS)*: estándar para la realización de comprobaciones de seguridad a nivel de aplicación.
- *OWASP “Cheat Sheet”*: conjunto de guías de buenas prácticas, tanto de prevención como de protección, para tener a mano de forma rápida la información de seguridad necesaria para aplicar las técnicas correctas cuando se está ensamblando y programando las rutinas esenciales de las aplicaciones.

2.4.4 VUL.4 – Configuraciones inseguras

Según el proyecto de código abierto OWASP [33] para mejorar la seguridad del software, una vulnerabilidad es “una brecha o debilidad en una aplicación, que puede ser un defecto de diseño o un

⁴⁸ CWE, por sus siglas en inglés (*Common Weakness Enumeration*).

⁴⁹ OWASP, por sus siglas en inglés (*Open Web Application Security Project*).

error de implementación, y que permite a un atacante causar daño a las partes interesadas de una aplicación. Las partes interesadas incluyen al propietario de la aplicación, los usuarios de la aplicación y otras entidades que dependen de la aplicación”.

Existen herramientas con la capacidad de iniciar sesión en todo tipo de sistemas operativos para realizar análisis de cumplimiento para comprobar la coherencia y conformidad con ciertos estándares, normativas o guías de seguridad. Por ejemplo, existen herramientas que constituyen un mecanismo único para analizar las características de seguridad técnicas definidas en normativa nacional como el ENS y otras guías o configuraciones europeas o internacionales.

2.5 Normativa de ciberseguridad relativa a la superficie de exposición

2.5.1 NOR.1 – Esquema Nacional de Seguridad (ENS)

El Centro Criptológico Nacional (CCN), institución española encargada de garantizar la seguridad de la información y de las comunicaciones del gobierno, las Fuerzas Armadas y otros organismos públicos en España, desarrolla un conjunto de normas [34] que proporcionan los elementos y directrices para aplicar y garantizar la seguridad en sistemas operativos, arquitecturas específicas, servidores web, electrónica de red y otras aplicaciones.

El Esquema Nacional de Seguridad (ENS) [10], de aplicación a todo el sector público, así como a aquellos proveedores que colaboran con la administración, ofrece un marco común de principios básicos, requisitos y medidas de seguridad para una protección adecuada de la información tratada y los servicios prestados, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias [35]. La serie CCN-STIC-800 establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS. Por lo que para el cumplimiento de los controles op.exp.2 y del op.exp.3⁵⁰ del ENS relativos a la configuración segura de los equipos previa a la entrada en operación y a la gestión continuada de la configuración de seguridad respectivamente, se aplican y mantienen las configuraciones de seguridad establecidas en guías 800 del CCN-STIC.

Por otra parte, el control del op.pl.5⁵¹ del ENS [10] establece que se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) [36] del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas del propio ENS. Por lo que, para el cumplimiento con una normativa española de obligado cumplimiento como es el ENS, la arquitectura de seguridad de los sistemas del sector público deberá incluir productos o servicios (prestados por un tercero) contenidos en el catálogo CPSTIC. Además, el sector privado cuando presten servicios o provean soluciones a las entidades del sector público también deberán cumplir con esta normativa.

⁵⁰ Las medidas de seguridad definidas en el ENS referentes a la configuración de seguridad se detallan en la medida [op.exp.2] referente a la configuración de los equipos previamente a su entrada en operación, así como en [op.exp.3] la cual se refiere a la gestión continuada de la configuración de los componentes del sistema.

⁵¹ Las medidas de seguridad definidas en el ENS referentes a los componentes certificados se detallan en la medida [op.pl.5] referente a la utilización del Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas definidas en el real decreto del ENS.

2.5.2 NOR.2 – *Ley de Ciberseguridad de la Unión Europea*

La Ley de Ciberseguridad de la UE [8] establece un sistema de certificación para toda la UE y un mandato nuevo y reforzado de la Agencia de la UE para la Ciberseguridad (ENISA⁵²). Gracias al nuevo marco de certificación de la ciberseguridad de la UE para los productos TIC se establecen un conjunto completo de normas, requisitos técnicos, normas y procedimientos. Por lo que, para el cumplimiento con una normativa europea como es la Ley de Ciberseguridad, la arquitectura de seguridad de los sistemas del sector público deberán incluir productos TIC certificados bajo los esquemas de ciberseguridad europeos, siempre que así lo establezca España (artículo 56.2 de la Ley de Ciberseguridad [8])

Por otra parte, la tarea principal de ENISA es promover la aplicación coherente del marco jurídico pertinente, en particular la aplicación efectiva de la Directiva (UE) 2016/1148 y otros instrumentos jurídicos pertinentes que contienen disposiciones en materia de ciberseguridad, lo que es esencial para aumentar la ciberresiliencia. Según la revisión anual de ENISA referente al Panorama de Amenazas [37], en los últimos años se está incrementando la superficie de ataque debido a la transformación digital, aumento del número de ciberataques dirigidos a organizaciones y empresas a través del teletrabajo.

2.5.3 NOR.3 – *Ley de ciberresiliencia de la Unión Europea*

La regulación desarrollada por la Unión Europea, denominada Ley de ciberresiliencia (CRA)⁵³ [38], establece normas para la comercialización de productos de forma que se garantice su ciberseguridad, definiendo requisitos en su diseño, desarrollo y producción. Esta regulación es de aplicación a todos los productos que estén conectados directa o indirectamente a otro dispositivo o red, existiendo algunas excepciones para productos para los cuales los requisitos de ciberseguridad ya están establecidos en las normas existentes de la UE, por ejemplo, en dispositivos médicos, aviación o automóviles.

Por otra parte, en su Anexo I, se definen requisitos esenciales para los procesos de gestión de vulnerabilidades a implementar por parte de los fabricantes a lo largo de todo el ciclo de vida del producto, de forma que se limite la superficie de ataque. Además, se establecen obligaciones para los operadores económicos, como importadores o distribuidores, en relación con los procesos de gestión de vulnerabilidades.

⁵² La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es una agencia de la Unión Europea encargada de garantizar la ciberseguridad de las comunicaciones y servicios de la administración comunitaria y de los ciudadanos de la Unión.

⁵³ CRA, por sus siglas en inglés (*EU Cyber Resilience Act*), es una propuesta impone un conjunto de requisitos de seguridad de software, ciberseguridad y gestión de vulnerabilidades en productos con elementos digitales (es decir, productos de software o hardware y sus soluciones de procesamiento de datos remotos) que se pongan en el mercado de la UE.

3 ACCIONES DE CIBERRESILIENCIA

3.1 Trazabilidad entre estrategias, objetivos y acciones de ciberresiliencia

Los objetivos definidos anteriormente (i.e. sección 1.3 Objetivos) se llevarán a cabo a través del desarrollo de una serie de acciones de ciberresiliencia que permitan una reducción efectiva de la superficie de exposición y una clara mejora de las capacidades de ciberresiliencia de la organización. En la siguiente tabla, se muestra la trazabilidad entre los objetivos definidos previamente, y las acciones a seguir para alcanzarlos:

Id OBJ	Descripción Objetivo	Id ACC	Descripción Acción
OBJ.1	Definición de acciones de comunicación y coordinación para la reducción de la superficie de exposición	ACC.1.1	Creación de un Grupo de Trabajo para el seguimiento de la reducción de la superficie de exposición
		ACC.1.2	Creación de un Grupo de Trabajo para el seguimiento de las líneas de desarrollo de la plataforma
		ACC.1.3	Creación de un Equipo de Evaluación de Amenazas que evalúe y analice constantemente la superficie de exposición
OBJ.2	Desarrollo de un entorno ciberresiliente que permita reducir la superficie de exposición	ACC.2.1	Identificación de la superficie de exposición
		ACC.2.2	Detección de vulnerabilidades de la superficie de exposición
		ACC.2.3	Priorización de acciones de mitigación en la superficie de exposición
		ACC.2.4	Monitorización de agentes en la infraestructura
		ACC.2.5	Telemetría de seguridad de la infraestructura
		ACC.2.6	Monitorización de la
		ACC.2.7	Evaluación de amenazas
OBJ.3	Cumplimiento con la normativa de ciberseguridad	ACC.3.1	Bastionado de activos según las guías CCN-STIC
		ACC.3.2	Certificación del Esquema Nacional de Seguridad
		ACC.3.3	Actualización de los productos con elementos digitales de acuerdo a la Ley de ciberresiliencia de la UE

Tabla 4 Trazabilidad entre objetivos y acciones [Fuente propia]

Asimismo, estas acciones siguen las estrategias definidas en la sección 1.1 Marco conceptual basadas en los principios estratégicos de Sun Tzu. La Figura 16 resume la trazabilidad entre las

estrategias de ciberresiliencia, los objetivos definidos en este trabajo y las acciones para llevar a cabo la reducción de la superficie de exposición:

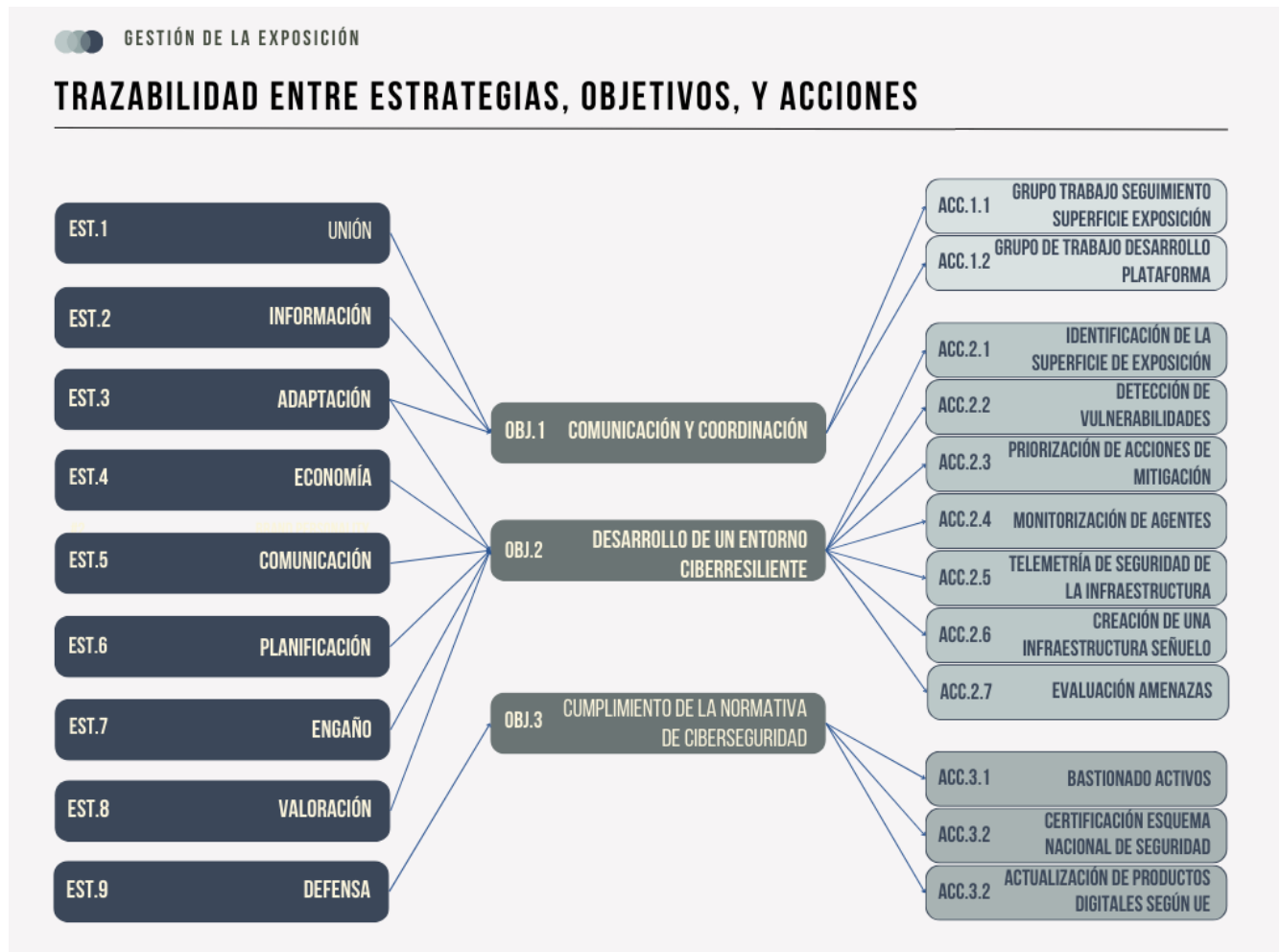


Figura 16 Trazabilidad estrategias, objetivos, y acciones de ciberresiliencia para la reducción de la superficie de exposición [Fuente propia]

3.2 Desarrollo de las acciones de ciberresiliencia

Una vez que se han definido las estrategias de ciberresiliencia como enfoque de alto nivel que adopta la organización (ver Figura 1 Principios estratégicos de Sun Tzu aplicados a la ciberresiliencia [Fuente propia]) para lograr sus objetivos de seguridad (ver sección 1.3 Objetivos) se desarrollan a continuación las medidas prácticas que permiten implementar estos objetivos, y que se definen en función de las estrategias previamente definidas. Las medidas mencionadas engloban una serie de acciones que involucran la realización de tareas, actividades, desarrollo de software, formación de personal, configuración de sistemas, cumplimiento normativo, reuniones de seguimiento, y cualquier otro proceso necesario para la reducción de la superficie de exposición..

Una vez implementadas estas acciones, es crucial monitorizar y evaluar continuamente estas acciones para asegurarse de que estén teniendo el impacto deseado. Esto implica medir el éxito de las acciones en función de los indicadores clave de rendimiento (KPI) y de los propios objetivos definidos en la sección 1.3, los cuales están respaldados por las estrategias definidas anteriormente.

Si las acciones no están logrando los resultados esperados, o si surgen nuevas amenazas o desafíos, se podrían tener que redefinir las estrategias, ajustando los objetivos de forma que se aborden los cambios en el entorno de ciberseguridad.

A continuación, se muestra la Figura 17 que resume las acciones de ciberresiliencia.

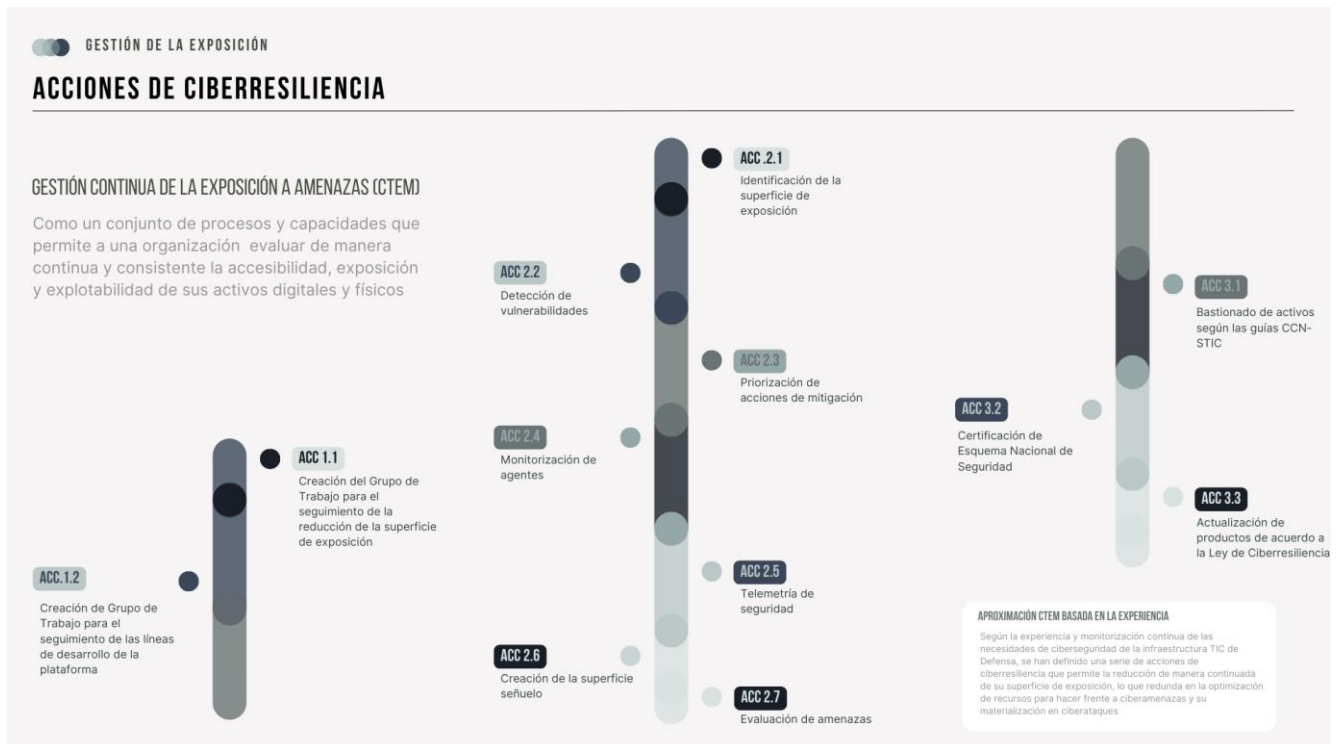


Figura 17 Acciones de ciberresiliencia [Fuente Propia]

En las siguientes secciones, se desarrollan todas las acciones que permiten llevar a cabo la reducción de la superficie de exposición de una infraestructura TIC, y su consiguiente mejora en la ciberresiliencia.

3.2.1 ACC.1.1, 1.2 – Creación de grupos de trabajo (Principio de la unidad – Unir para vencer)

El concepto de “unión para vencer” refleja la idea de que los diferentes componentes de un equipo en una organización deben trabajar juntos de manera armoniosa para alcanzar el éxito. La idea básica de Sun Tzu es que la cooperación y la coordinación estratégica son esenciales para superar desafíos y oponerse eficazmente a un adversario (*el supremo arte de la guerra es someter al enemigo sin luchar. La oportunidad de derrotar al enemigo está en tus manos; no en la oportunidad que el enemigo te brinda*). La cooperación entre los miembros del equipo, la comprensión mutua de roles y responsabilidades, y la coordinación eficiente contribuyen a la eficacia global.

En el desarrollo de una plataforma, que sirva de guía para trazar un camino con hitos que permitan ir mejorando la ciberresiliencia de una infraestructura, se debe contar con todo tipo de compañeros de viaje, que vayan aportando su visión particular de fortalezas y debilidades. Combinando una ejecución hábil y coordinada se puede obtener la victoria.

Por tanto, la creación de grupos de trabajo⁵⁴ es esencial para lograr el éxito, considerando en este caso la creación de dos grupos de trabajo diferenciados y cohesionados para conseguir un objetivo común, la mejora de la ciberresiliencia de la infraestructura TIC:

⁵⁴ En el concepto de grupo de trabajo que se presenta aquí, cada miembro tiene una tarea específica y claramente trazable. Se destaca que el grupo de trabajo no se concibe únicamente como un foro para discusiones y opiniones, sino más bien como un entorno donde el término “trabajo” se traduce concretamente en la asignación y ejecución de tareas específicas.

1. **Grupo de trabajo de usuarios:** este grupo de trabajo tiene como responsabilidad el seguimiento de la reducción de la superficie de exposición. La periodicidad de las reuniones es mensual, y participan todos los usuarios de la organización con algún tipo de responsabilidad en la mitigación de vulnerabilidades de la infraestructura. Se lleva a cabo un repaso de la reducción de la superficie alcanzada por ámbito o áreas, marcando nuevos hitos que lleven a una mejora sostenible en la reducción de la exposición.
2. **Grupo de trabajo de desarrollo:** este grupo se encarga del seguimiento de las líneas de desarrollo marcadas por una especificación clara de requisitos. La periodicidad de las reuniones es semanal y participa el CISO, el Equipo de Seguridad Defensiva⁵⁵, el Equipo de Seguridad Perimetral⁵⁶, COS, desarrolladores, administradores de sistemas y seguridad y desarrolladores. En cada reunión se verifican estos requisitos y se validan las funcionalidades alcanzadas. Además, se marcan nuevos requisitos y se analizan las líneas futuras para la reducción de la exposición.

En resumen, la definición de acciones de comunicación y coordinación para la reducción de la superficie de exposición, persigue el objetivo de superar desafíos y oponerse eficazmente a un adversario a través de la creación de grupos de trabajo que supervisen el desarrollo de acciones de mitigación.

3.2.2 ACC.2.1 – Identificación de la superficie de exposición (Principio del conocimiento – Conocimiento del enemigo y del entorno)

No se puede proteger lo que no se conoce (*conoce al adversario y sobre todo conócete a ti mismo y serás invencible*). Las primeras actividades que se llevan a cabo para la protección de la superficie de exposición es la identificación detallada de cada uno de los elementos que componen esta superficie (*la información es poder*). Esta superficie incluye tanto los elementos estáticos (servidores, estaciones de trabajo, impresoras) como conectores (cortafuegos, enrutadores, *proxies*...), así como la identidad digital de aquellos usuarios que se consideran en riesgo.

Toda la información se obtiene a través de los distintos agentes o sondas proporcionados por los agentes de las herramientas de ciberseguridad desplegados en la infraestructura TIC, así como integrando, correlacionando y cohesionando posteriormente toda esta información.

Se exponen a continuación los distintos tipos de identificación y análisis de activos que se encuentran en los distintos espacios que componen la superficie de exposición de la infraestructura TIC, incluyendo la trazabilidad:

1. **Identificación de activos en la superficie interna:** la superficie interna incluye los activos que no son accesibles desde el exterior ya que están protegidos por uno o más perímetros de seguridad. Los tipos de activos se enumeran gracias a una o más de las herramientas de ciberseguridad previamente desplegadas dentro del perímetro interno de la infraestructura, como son herramientas de análisis de vulnerabilidades, de detección y respuesta ante amenazas y control de acceso a red. Todas estas herramientas, a través del despliegue de agentes o mediante análisis de tráfico, son capaces de llevar a cabo una enumeración de activos conectados a la infraestructura.

Los tipos de activos que se pueden identificar en la superficie interna son:

⁵⁵ El Equipo de Seguridad Defensiva es el encargado de supervisar diariamente la superficie de exposición a través del control y análisis de valores proporcionados por la plataforma CTEM. Tiene además capacidad de notificación con el resto de roles de la plataforma para informar de vulnerabilidades significativas, acciones alternativas para la mitigación de vulnerabilidades y otras comunicaciones de interés.

⁵⁶ El equipo de Seguridad Perimetral es el responsable de proteger los límites externos de la red de una organización. Esta área de seguridad se enfoca en salvaguardar el perímetro de la infraestructura TIC, que es la primera línea de defensa contra amenazas externas, controlando que todos los accesos desde y hacia Internet están debidamente protegidos.

- Servidores (virtualizados, aplicaciones, bases de datos,...).
 - Estaciones de trabajo.
 - OTs/IoTs.
 - Electrónica de red.
 - Impresoras.
 - Móviles.
2. **Identificación de activos en la superficie externa:** la superficie externa incluye los activos que son accesibles desde el exterior, es decir, que quedan expuestos fuera del perímetro exterior (por ejemplo accesibles desde Internet. Los tipos de activos se enumeran gracias a una o más de la herramientas de ciberseguridad especializadas en enumerar e identificar este tipo de activos desde el exterior. Los tipos de activos que se pueden identificar en la superficie externa son:
- Sitios Web.
 - Subdominios y dominios.
 - Direcciones IP públicas y privadas.
 - APIs (Interfaces de Programación de Aplicaciones).
 - Servicios de transferencia de archivos.
 - Servicios de mensajería.
 - Servicios en la nube.
3. **Identificación de activos en la superficie oculta:** para reducir la superficie de exposición es necesario identificar los activos que no son necesarios, que están obsoletos o a aquellos que ni si quiera el Responsable de la Infraestructura conoce de su existencia. Estos activos pueden ser eliminados, desconectados o reconfigurados para que estén actualizados a la versión más reciente de software.
4. **Dependencias entre activos:** existen dependencias entre numerosos activos ya que ejecutan funcionalidad conjunta y por tanto la mitigación de vulnerabilidades se hace también de forma conjunta. Por lo que establecer las dependencias entre todos los activos de la infraestructura es una tarea clave en la intrincada tarea de identificar y etiquetar todos los activos de la superficie de exposición.
5. **Trazabilidad entre los activos de la superficie externa y la interna:** el camino que recorre una petición a un servicio expuesto de la infraestructura se inicia en una petición que solicita acceso a un recurso determinado a través de un Localizador de Recursos Uniforme (URL) y que va pasando por una serie de activos hasta llegar al servidor que pueda dar respuesta a esa solicitud. Uno de los elementos más complicados es conocer, una vez identificada una vulnerabilidad en un activo expuesto, si la mitigación se tiene que llevar a cabo en la propia aplicación o cortafuegos de aplicaciones web (WAF⁵⁷), o en el servidor ubicado en la superficie interna.
6. **Identificación de la lógica de negocio en la superficie exposición:** cada activo tiene una responsabilidad concreta dentro de la infraestructura, pudiendo ser parte de un sistema de información o Servicio que es albergado además en otros activos, e incluso albergar más de un sistema de información. También es importante considerar la dependencia entre estos activos a alto nivel por la necesidad de llevar a cabo acciones de mitigación de vulnerabilidades de forma conjunta para estos Servicios. Se distinguen dos tipos sistemas de información o Servicios:

⁵⁷ WAF, por sus siglas en inglés (*Web Application Firewall*).

- Servicios de Infraestructura: que albergan los servicios esenciales y que dan apoyo al resto de sistemas de información. Este tipo de Servicios son transversales dentro de la infraestructura.
- Servicios de Aplicación: son el resto de Servicios que tienen una función específica y que requieren del apoyo de los Servicios de Infraestructura para su explotación.

3.2.3 ACC.2.2 – Detección de vulnerabilidades de la superficie de exposición (Principio de adaptación – Conocer las debilidades propias)

Una vez que se han enumerado todos y cada uno de los activos de la superficie de exposición, es necesario conocer las debilidades propias para tener claro las acciones defensivas que permitirán adaptarse al enemigo (*sé flexible y reflexiona antes de realizar un movimiento*) gracias a la recopilación y análisis de la información sobre amenazas, la monitorización de los eventos de seguridad, y el conocimiento de las tácticas, técnicas y procedimientos (TTP) utilizados por los ciberatacantes (*no debes depender de las condiciones favorables, ni de las condiciones desfavorables, sino que debes estar preparado para adaptarte a las condiciones*).

La detección de vulnerabilidades implica identificar debilidades y fallos de seguridad en los activos enumerados anteriormente. Esto permite identificar los puntos de debilidad o posibles entradas para atacantes, contribuyendo así a la identificación de la superficie vulnerable (*la invencibilidad está en uno mismo, la vulnerabilidad en el adversario*).

Se presentan a continuación diversos tipos de evaluaciones de seguridad que pueden llevarse a cabo para detectar vulnerabilidades. Estas evaluaciones pueden seguir una periodicidad establecida o realizarse de forma puntual, en respuesta a cambios significativos en los sistemas de información de la infraestructura o para cumplir con normativas específicas:

1. **Análisis de vulnerabilidades:** la evaluación de vulnerabilidades es un proceso que identifica y evalúa las vulnerabilidades de la red mediante la evaluación y monitorización constantes de toda la superficie de ataque en busca de riesgos. Es el primer paso para defender la infraestructura contra las vulnerabilidades que pueden ser un claro camino de ataque.
2. **Evaluación del cumplimiento de la configuración segura:** la evaluación del cumplimiento de la configuración segura con determinados estándares y políticas de seguridad comprueba que el software está configurado de acuerdo a unas pautas de seguridad determinadas. Durante estas evaluaciones de cumplimiento, se verifica que las configuraciones siguen siendo adecuadas y que no se hayan desviado de los estándares establecidos. Es el segundo paso para defender la infraestructura de configuraciones inseguras que pueden constituir un camino de ataque.
3. **Auditorías de seguridad:** las auditorías de seguridad, ya sean internas o de certificación, permiten evaluar el cumplimiento con ciertos estándares, así como la realización de pruebas de penetración en la infraestructura. Pueden ser periódicas, por ejemplo cada dos años, o bien puntuales debido a cambios en los sistemas de información que requieran una recertificación o cumplimiento con normativa de seguridad nacional o internacional. Es el tercer paso para defender la infraestructura como un proceso de mejora continua.
4. **Evaluación de los usuarios en riesgo:** es muy importante conocer las propias debilidades para establecer una buena defensa. Cada usuario dispone en la infraestructura de una identidad digital para acceder al resto de activos, por lo que si un usuario ha puesto en peligro sus credenciales (por ejemplo, utilizándolas en otras infraestructuras más débiles, y que podrían ser robadas por el enemigo) pone en peligro la propia infraestructura. Es esencial localizar estos usuarios y realizar un cambio inmediato de credenciales juntos con acciones de concienciación.

3.2.4 ACC.2.3 – Priorización de acciones de mitigación en la superficie de exposición (Principio de la economía – Priorizar los esfuerzos)

La priorización de las acciones para mitigar vulnerabilidades es un proceso esencial para optimizar los recursos de ciberseguridad de la organización (*si se envían refuerzos a todas partes, se es débil en todas partes*). Siguiendo el principio de Sun Tzu acerca de que dispersar refuerzos en todas direcciones debilita la defensa global, se enfocan los esfuerzos en activos prioritarios y vulnerabilidades críticas. Después de identificar y clasificar las vulnerabilidades (*grandes resultados pueden ser conseguidos con pequeños esfuerzos*), se lleva a cabo la priorización basándose en su gravedad y la evaluación del impacto. Además, se realiza una evaluación de la probabilidad de explotación de cada vulnerabilidad en el contexto específico de la infraestructura.

La priorización de acciones de mitigación comienza con la identificación inicial de activos, seguida por la detección de vulnerabilidades. Un componente clave para esta gestión efectiva es el seguimiento continuo de la superficie de exposición realizado por el Grupo de Trabajo de Usuarios. Este enfoque contribuye significativamente a una gestión de riesgos dinámica, considerando variables como el impacto en la organización, la cantidad de activos afectados y la importancia y tipología específica de cada activo.

Se exponen a continuación los distintos elementos que determinan la priorización de acciones de mitigación de vulnerabilidades mediante el cálculo de diversas variables que determinan el valor total del impacto. Este cálculo se basa en la obtención de tres impactos parciales:

1. **Impacto para la organización:** es el primer paso para el cálculo del impacto y se calcula para cada CVE detectada, pudiendo ser definido manualmente por el Equipo de Seguridad Defensiva, teniendo en cuenta los valores definidos a continuación.
 - a. **Vector de ataque (seguridad perimetral):** es el valor de mitigación determinado por el Equipo de Seguridad Perimetral. La electrónica de red con la que cuenta este equipo aplica una serie de Indicadores de Compromiso (IoCs) que permiten detener ataques en este primer perímetro, específicamente dirigidos a CVEs determinadas. Esto resulta en una disminución de la prioridad de mitigación en los activos para esa CVE en particular, ya que contarían con protección contra esas CVE.
 - b. **Puntuación CVSS:** tiene en cuenta la complejidad del ataque, los privilegios requeridos y la interacción del usuario, a la hora de explotar la vulnerabilidad.
 - c. **Valor de explotación según EPSS⁵⁸:** es la probabilidad de que se explote una vulnerabilidad gracias a los datos permanentemente actualizados sobre amenazas y *exploits* del indicador EPSS.
2. **Impacto genérico:** es el segundo paso para el cálculo del impacto y se basa en el número de activos existentes en la organización que tienen esa CVE asociada, dependiendo del número de servidores, estaciones de trabajo o activos del Equipo de Seguridad Perimetral afectados.
3. **Impacto específico:** es el tercer paso para el cálculo del impacto y se basa en obtener todos los indicadores del activo que tiene esa vulnerabilidad activa, incluyendo el número de servicios implicados, y la catalogación del activo.

⁵⁸ EPSS, por sus siglas en inglés (*Exploit Prediction Score System*).

3.2.5 ACC.2.4 – Monitorización de agentes en la infraestructura (*Principio del terreno – Disponer los mensajeros sobre el terreno*)

Se deben disponer las tropas que actúan como mensajeros, es decir los agentes de las herramientas de ciberseguridad, de una manera organizada y adecuadamente distribuida a lo largo de toda la infraestructura (*la disposición de las tropas es clave para lograr la victoria, ya que una disposición adecuada puede maximizar las fortalezas y minimizar las debilidades de los soldados*). Una vez desplegados todos los agentes, se obtendrá una información muy valiosa que permite obtener información de primera mano de todos los activos existentes y del estado de vulnerabilidad de los mismos (*sólo cuando conoces cada detalle de la condición del terreno puedes maniobrar y luchar*).

Pero de nada sirve tener un ejército de agentes desplegados de manera estratégica por todo el tablero de la infraestructura si éstos agentes no son capaces de hacer llegar la información a los puntos de recogida de datos y finalmente a la plataforma única donde se analiza, procesa y visualiza toda la información recibida (*los que no saben tener mapas, hacer reconocimientos o utilizar guías locales, son incapaces de obtener ventaja del terreno*). Sun Tzu se refiere a la importancia de comprender el entorno o terreno ya que puede tener un impacto significativo en el éxito o fracaso de una estrategia. Por tanto, los agentes están programados para enviar información periódicamente a los puntos de recopilación de datos, y la plataforma CTEM debe monitorizar de forma continua el estado de estos agentes para determinar si es necesario intervenir para "reponer" agentes donde sea necesario.

Se exponen a continuación los distintos tipos de agentes desplegados en la infraestructura que proporcionan información a la plataforma:

1. **Agentes de búsqueda de vulnerabilidades:** este tipo de agentes proporcionados por herramientas VM, se encargan del análisis activo de vulnerabilidades en cada tipo de activo.
2. **Agentes de análisis de comportamiento:** este tipo de agentes recoge información de alertas en servidores de trabajo y estaciones de trabajo, así como telemetría de seguridad para el futuro análisis forense en caso de incidente en un activo en particular.
3. **Agentes de evaluación de configuraciones:** este tipo de agentes realizan un análisis exhaustivo de todos los activos, examinando la dependencia entre ellos (por ejemplo, si están a cargo de la implementación del mismo servicio). Además obtienen información del conjunto de software que ejecuta y de los servicios de infraestructura o negocio que respaldan.

3.2.6 ACC.2.5 – Telemetría de seguridad de la infraestructura (*Principio de la planificación – Planificar y reflexionar*)

Una infraestructura genera una cantidad ingente de datos y métricas que pueden ser utilizados diariamente para estudiar el estado de los activos o los movimientos de un atacante (*reflexionar antes de hacer un movimiento*). Por tanto, se pueden detectar amenazas que incluyan identificación de malware, intentos de intrusión y actividades sospechosas de usuarios, proporcionando visibilidad en tiempo real y datos procesables que permiten una toma de decisiones precisa (*resolver dificultades antes de que surjan*).

La recopilación, análisis y monitorización de datos y métricas relacionadas con la seguridad de la información y el estado de los activos de una infraestructura es fundamental para comprender y mejorar su seguridad (*las tácticas sin estrategia son el ruido antes de la derrota*). Se puede obtener información de todos los activos (de la superficie externa, de la interna, y la señuelo), incluyendo comportamiento de los usuarios, y posteriormente cohesionar y correlacionar la información proporcionada por todas las fuentes.

A continuación, se exponen los tipos de registros que constituyen la telemetría de seguridad de una infraestructura:

1. **Registros de dispositivos de perímetro:** registran información del tráfico malicioso en la red (tráfico entrante y saliente, direcciones IP de los sitios web visitados por los usuarios, e intentos fallidos de sesión), configuraciones de seguridad incorrectas (por ejemplo, cambios no autorizados en la configuración de seguridad), además de detectar ataques a través de patrones de actividad de la red (como la recepción de en un corto periodo de tiempo de gran cantidad de paquetes SYN debido a un ataque de denegación de servicio distribuido DDoS⁵⁹).
2. **Registros de eventos de Windows:** son eventos registrados por las aplicaciones en el sistema operativo Windows, como son registros de seguridad (intentos fallidos de inicio de sesión e instancias de eliminación de archivos), registros del sistema (procesos y drivers cargados con éxito), registros del servicio de directorio (autenticación y modificación de privilegios), registros del servicio de DNS (direcciones IP de cliente, solicitudes de dominio) y registros del controlador de dominio.
3. **Registros de eventos de Linux:** registran información de administración, diagnóstico de problemas, seguimiento de eventos y seguridad. Por ejemplo, `syslog` (mensajes de arranque, registros de seguridad, eventos de red), `auth.log` (eventos de autenticación, inicio de sesión, cambios de contraseña), `messages` (mensajes del *kernel*⁶⁰, información sobre hardware, mensajes de red), `secure` (registros de autenticación y eventos de acceso al sistema), `cron` (información sobre las tareas programadas), `kern.log` (eventos del *kernel* del sistema operativo), `daemon.log` (servicios que se ejecutan en segundo plano), `boot.log` (eventos de arranque del sistema), `xorg.log` (registros relacionados con el servidor gráfico), `audit.log` (eventos de auditoría de seguridad), o bien logs de servidores web (información sobre las solicitudes web entrantes, errores del servidor).
4. **Registros de estaciones de trabajo:** registran actividades en unidades de disco extraíbles, la actividad de usuario para ver si cumple con las políticas internas y normativa de la organización relacionadas con la instalación y el uso de software. Además, monitorizan estas políticas y proporcionan notificaciones en caso de que se produzca una acción no permitida.
5. **Registros de aplicación:** capturan eventos específicos de una aplicación o software en particular. Pueden incluir registros de errores, seguimiento de actividad de usuarios, registros de transacciones y otros eventos relacionados con el funcionamiento de la aplicación. También registran solicitudes y consultas de usuarios (por ejemplo, acceso no autorizado a archivos, o intentos de manipulación de datos de usuarios) y problemas de seguridad en las bases de datos.
6. **Registros de proxies:** registran información importante acerca de estadísticas de uso y comportamiento anómalo de navegación, además de monitorizar la longitud de los paquetes (por ejemplo, un usuario que envía o recibe repetidamente paquetes de la misma longitud en un intervalo de tiempo determinado podría indicar una actualización de software o malware intercambiando señales con servidores de control).
7. **Registros de IoT:** al no tener los dispositivos IoT suficiente memoria para almacenar los registros, envían la información de registro a una solución centralizada de gestión de registros donde puedan almacenarse durante períodos prolongados.

⁵⁹ DDoS, por sus siglas en inglés (*Distributed Denial-of-Service*).

⁶⁰ El *kernel* Linux® es el elemento principal de los sistemas operativos (SO) Linux, y es la interfaz fundamental entre el hardware de una computadora y sus procesos. Los comunica entre sí y gestiona los recursos de la manera más eficiente posible.

3.2.7 ACC2.6 – Creación de una infraestructura señuelo (Principio del engaño – Fingir debilidad)

Tener una perspectiva detallada de cómo un atacante ve la superficie de exposición de una infraestructura TIC permite obtener conocimiento acerca de sus vías de entrada (*conocer al enemigo y utilizar al enemigo para derrotar al enemigo*), por lo que la utilización de una superficie señuelo extendida de la superficie real es ideal para conseguir este propósito [14] (*para conocer a tu enemigo debes convertirte en tu enemigo*).

La creación y monitorización de superficies externas como señuelo es una estrategia de ciberseguridad que implica la implementación de una superficie extendida que simula ser vulnerable y que es atractiva para un ciberatacante (*engaña al enemigo moviendo algo que él está obligado a observar*). El propósito principal de una superficie señuelo es atraer a los atacantes y desviar su atención lejos de los sistemas y datos reales de una organización, permitiendo así monitorizar sus actividades y aprender sobre las tácticas y técnicas que utilizan.

Se expone a continuación algunos componentes clave para construir una infraestructura señuelo, ya que la efectividad de una estructura señuelo depende de la cuidadosa planificación y ejecución de estos elementos. Además, a medida que la situación evoluciona, la adaptabilidad es crucial para mantener la credibilidad del señuelo.

1. **Apariencia auténtica:** la infraestructura creada o “superficie señuelo” debe tener una apariencia auténtica y creíble para el enemigo. Debe mimetizarse con entornos y aplicaciones web similares de la organización para no despertar sospechas. Además, para que sea realmente efectiva debe proporcionar algún servicio que solicite credenciales, y que además puede servir para comprobar si ha habido algún robo de credenciales previo.
2. **Ubicación estratégica:** colocar el señuelo en una ubicación estratégica que sea probable que atraiga al enemigo. Puede ser en una posición de alto valor o en una ruta que el enemigo tienda a utilizar.
3. **Información falsa:** proporcionar documentos o información falsa que refuerce la autenticidad del señuelo. Esto puede incluir registros, datos, o cualquier otro elemento que pueda ser descubierto por el enemigo.
4. **Seguridad aparente:** es importante dotar al señuelo con medidas de seguridad aparentes para que parezca valioso o protegido. Esto puede incluir el despliegue normal de herramientas de ciberseguridad, como por ejemplo un VM o EDR. Por otra parte, es lógico dejar deliberadamente algunas áreas de la estructura señuelo más vulnerables o accesibles. Esto puede motivar al enemigo a acercarse y caer en la trampa.
5. **Señales de actividad:** introducir señales de actividad que indiquen la importancia o el uso reciente de la estructura señuelo. Esto puede incluir logs actualizados diariamente, o cualquier indicio que sugiera actividad reciente.
6. **Coordinación con inteligencia:** alinear la construcción del señuelo con la información de inteligencia disponible sobre las tácticas y comportamientos del enemigo, incluyendo información de las últimas campañas de ataques de amenazas ya conocidas (APT⁶¹). Esto permite personalizar la trampa de manera efectiva.

⁶¹ APT, por sus siglas en inglés (*Advanced Persistent Threat*). Una amenaza avanzada persistente utiliza técnicas de hackeo continuas, clandestinas y avanzadas para acceder a un sistema y permanecer allí durante un tiempo prolongado, con consecuencias potencialmente destructivas.

7. **Respuesta estratégica:** tener una estrategia clara para responder cuando el enemigo caiga en la trampa. Puede incluir emboscadas, contrainteligencia u otras medidas para aprovechar la vulnerabilidad del enemigo.

3.2.8 ACC2.7 – Evaluación de amenazas (Principio de sorpresa – Evaluación constante)

La materialización de amenazas es algo que va a ocurrir seguro, lo que hay que averiguar es cuáles de ellas y cuándo. Sun Tzu enfatiza que para evitar lo que es seguro, es necesario estar en constante guardia y preparado para lo probable (*la manera de evitar lo que es seguro es estar en guardia, lo que es probable es estar preparado, pero lo que es completamente inesperado es ser completamente desconcertante*). Sin embargo, la verdadera ventaja estratégica surge al ser completamente desconcertante, es decir, al realizar acciones que el enemigo no espera en absoluto. La sorpresa estratégica desestabiliza al adversario, crea confusión y a menudo resulta en una ventaja táctica significativa.

La capacidad de ser impredecible y llevar a cabo acciones que van más allá de las expectativas del enemigo es un componente crucial en la estrategia militar según Sun Tzu. Esto se alinea con la noción de que la sorpresa y la imprevisibilidad pueden generar confusión y desorden en las filas enemigas, creando oportunidades estratégicas para aquellos que son capaces de ejecutar movimientos sorprendentes. Por tanto, es necesaria la creación de un equipo de evaluación de amenazas con capacidad para identificar y comprender las amenazas potenciales que pueden afectar a una infraestructura TIC. Su trabajo se traduce en campañas puntuales y en un continuo análisis de amenazas que afectan a otras organizaciones. En resumen, su trabajo ayuda a priorizar las acciones de mitigación.

Se exponen a continuación los elementos imprescindibles para una evaluación constante de amenazas, a través de campañas puntuales o como un proceso programado para ciertos tipos de activos o regiones de la superficie de exposición:

1. **Identificación de amenazas:** el proceso comienza con la identificación de posibles amenazas que podrían afectar la seguridad de los activos de la infraestructura. Esto puede incluir amenazas a la “superficie externa”, a la “superficie interna”, como riesgos operacionales o de falta de configuración segura.
2. **Análisis de vulnerabilidades:** se evalúan las vulnerabilidades existentes en la infraestructura (sistemas, redes y aplicaciones). Esto implica identificar debilidades en el diseño, la configuración o la implementación que podrían ser explotadas por las amenazas. Para ello, se utilizan herramientas automatizadas del tipo ASCA, CAASM, EASM y BAS, así como técnicas manuales para descubrir vulnerabilidades conocidas y desconocidas. Para poder realizar un adecuado de las amenazas, se crean escenarios hipotéticos basados en las amenazas identificadas para simular posibles eventos adversos. Estos escenarios proporcionan información valiosa sobre cómo podrían ocurrir los ataques y cómo mitigarlos.
3. **Valoración del riesgo y análisis de impacto:** se realiza una valoración del riesgo al evaluar la probabilidad de que una amenaza explote una vulnerabilidad específica y el impacto potencial en los activos de información. Esta valoración ayuda a priorizar y abordar los riesgos más críticos. Además, se examina el posible impacto que cada amenaza podría tener para cada uno de los activos. Esta información puede ser incluida asimismo en la plataforma CTEM. Además, se generan recomendaciones para mitigar o reducir los riesgos identificados, lo que puede incluir la implementación de controles de seguridad adicionales, actualizaciones de software, cambios en las políticas de acceso, entre otras medidas.

3.2.9 ACC3.1, 3.2, 3.3 – Bastionado de activos, ENS y Ley de Ciberresiliencia (Principio de defensa – Defender en profundidad)

El bastionado de todos los activos de la infraestructura es parte intrínseca de una estrategia defensiva. Sun Tzu aborda la importancia de la preparación defensiva y la fortificación en algunos de sus principios generales de la guerra (*La defensa es para tiempos de escasez, el ataque para tiempos de abundancia*).

Es necesario construir un sólido “bastionado” de defensas gracias a la securización de los activos desde múltiples capas y en varios niveles. Por ejemplo, mediante el cumplimiento con configuraciones seguras definidas por autoridades o agencias dedicadas a la mejora de la ciberseguridad, como son el NIST⁶², el CCN o ENISA.

Se exponen a continuación los elementos imprescindibles para una adecuada estrategia defensiva:

1. **Bastionado de activos:** el proceso comienza con la identificación de posibles amenazas que podrían afectar la seguridad de los activos de la infraestructura. Esto puede incluir amenazas a la “superficie externa”, a la “superficie interna”, riesgos operacionales o de falta de configuración segura. Algunas de las actividades que se llevan a cabo para obtener un activo securizado son:
 - Ajuste de la configuración del sistema operativo de dispositivos finales o electrónica de red para eliminar servicios o funcionalidades no necesarias, o bien configurarlos de manera segura.
 - Mantenimiento regular de sistemas y aplicaciones mediante la aplicación de actualizaciones de seguridad y parches para corregir vulnerabilidades conocidas.
 - Implementación de políticas de gestión de cuentas de usuario, incluyendo el uso de contraseñas seguras, políticas de caducidad y bloqueo de cuentas tras intentos fallidos.
 - Establecimiento de controles de acceso adecuados, como la aplicación del principio de privilegios mínimos y la implementación de políticas de acceso basadas en roles.
 - Configuración de firewalls para controlar y filtrar el tráfico de red, permitiendo únicamente el tráfico esencial y bloqueando actividades sospechosas.
 - Habilitación de funciones de auditoría y registro para monitorizar y registrar eventos relevantes, facilitando la detección de actividades maliciosas y la investigación forense.
2. **Cumplimiento con normativas de seguridad:** implica seguir y aplicar las directrices y requisitos establecidos por normas y marcos de seguridad para garantizar que los sistemas, redes y activos de una organización estén configurados de manera segura y cumplan con los estándares de seguridad establecidos. En concreto, existen dos entidades de relevancia:
 - A través de normativa nacional, el CCN define normas específicas, a través de sus guías CCN-STIC [34], para configurar de forma segura sistemas operativos, redes inalámbricas, dispositivos de red, dispositivos móviles, aplicaciones... Por lo que los productos que formen parte de la infraestructura TIC deberán estar debidamente configurados de acuerdo a esta guía.
 - La Unión Europea a través de su Ley de Ciberresiliencia (CRA) [38], establece los siguientes requisitos de diseño de seguridad de los productos contra vulnerabilidades conocidas y notificación de vulnerabilidades identificadas. Por lo que los productos incorporados en la infraestructura TIC estarán bajo esta normativa europea.

⁶² NIST, por sus siglas en inglés (*National Institute of Standards and Technology*), tiene como uno de sus objetivos fundamentales desarrollar estándares de ciberseguridad para el sector privado y el público.

4 METODOLOGÍA, IMPLEMENTACIÓN Y VALIDACIÓN

Si bien, los capítulos anteriores han abordado el problema desde un enfoque teórico, esta sección se sumerge en la práctica mediante la implementación de una plataforma real que lleva a cabo el programa de la gestión continua de la superficie de exposición (CTEM). Esto incluye la metodología de desarrollo de la plataforma, la descripción de la propia implementación, la modelización de la superficie anómala (o nivel de riesgo), la verificación de los indicadores de rendimiento, así como la validación de la plataforma como una solución CTEM.

4.1 Metodología de desarrollo

La metodología de desarrollo de la plataforma constituye un enfoque estructurado y organizado para diseñar, construir e implementar una solución CTEM con la capacidad de evolucionar y crear nuevas funcionalidades a través de los criterios definidos por los usuarios y posteriormente verificados por ellos mismos.

A continuación, se detallan los fundamentos seguidos en el desarrollo de la plataforma. Este proceso comienza con una cuidadosa selección de herramientas, evaluándolas a través de pruebas de concepto. Posteriormente, se recopila la información de las herramientas seleccionadas mediante interfaces de programación de aplicaciones (API). Destaca especialmente el ciclo de vida del desarrollo, enfocándose de manera crucial en la participación activa de los usuarios de la plataforma. Este enfoque integral asegura la solidez y la continua adaptabilidad de la plataforma a lo largo de su evolución.

4.1.1 Pruebas de concepto para la selección de herramientas de ciberseguridad

Las pruebas de concepto (PoC⁶³) desempeñan un papel crucial en la selección de nuevas herramientas de seguridad que se integrarán finalmente en el desarrollo de la plataforma como una nueva fuente de información. Facilitan una primera interacción antes de su incorporación efectiva en el desarrollo y constituyen un elemento fundamental en la toma de decisiones, tanto desde una perspectiva funcional como económica. Algunos de los aspectos destacados para llevar a cabo este tipo de pruebas, que implican un coste significativo en términos de tiempo y dedicación de recursos, son:

- **Validación de requisitos específicos:** cada herramienta puede tener características específicas que la hacen adecuada para ciertos casos de uso. Las pruebas de concepto permiten validar si la herramienta cumple con los requisitos específicos y las necesidades de seguridad de la organización. Además, se puede evaluar la compatibilidad y la capacidad de integración de la herramienta con la infraestructura existente. Esto es crucial para garantizar que la nueva herramienta se integre de manera fluida y eficiente con otros componentes de la plataforma.
- **Evaluación de la eficiencia:** permite medir directamente la eficiencia y eficacia de una herramienta en un entorno controlado antes de su implementación a gran escala. Esto ayuda a garantizar que la herramienta cumple con los requisitos y expectativas establecidos. Además, durante las pruebas, se pueden realizar ajustes y optimizaciones para mejorar el rendimiento de la herramienta. Esto asegura que la herramienta funcione de manera eficiente y efectiva en el entorno específico de la organización.
- **Identificación de limitaciones:** brindan la oportunidad de identificar posibles limitaciones o desafíos que pueden surgir al implementar la herramienta en un entorno real. Esto permite abordar problemas antes de que se conviertan en obstáculos significativos. Además, proporciona

⁶³ Una prueba de concepto (PoC), por sus siglas en inglés (*Proof of Concept*), es una implementación práctica y limitada de un concepto o idea para demostrar su viabilidad.

información valiosa sobre el dimensionamiento adecuado, asegurando la adquisición del número preciso de licencias y evitando costes innecesarios.

En resumen, las pruebas de concepto son una fase esencial en el proceso de selección de nuevos silos de información que serán recopilados posteriormente por la plataforma, ya que proporcionan una evaluación crítica que guía la toma de decisiones antes de su incorporación en su ciclo de vida.

4.1.2 Recogida de información a través de APIs

La filosofía de recogida de información se realiza a través de API como un intermediario que permite que dos aplicaciones se comuniquen y compartan datos o funcionalidades sin necesidad de que los desarrolladores tengan acceso al código interno de cada aplicación. La recopilación de información a través de API ofrece varios beneficios clave que permiten la integración eficiente de los datos de las herramientas de ciberseguridad en el centro de control de la plataforma CTEM, como son:

- **Automatización eficiente:** permiten la automatización de la recopilación de datos, lo que ahorra tiempo y reduce errores asociados con la entrada manual de información. Además, las actualizaciones y mejoras en las fuentes de datos se pueden implementar a través de las API sin interrumpir los flujos de trabajo existentes. Cada herramienta de ciberseguridad debe ofrecer una API eficiente y actualizable según las necesidades que requiera la plataforma, por lo que la continua comunicación con el proveedor es esencial para que se disponga de todos los métodos necesarios para disponer de datos actualizados. Gracias al uso de API se facilita por tanto la integración de datos entre las herramientas de ciberseguridad y la plataforma centralizada, lo que permite una interoperabilidad fluida y una visión unificada de la información.
- **Acceso en tiempo real:** la información se puede obtener en tiempo real a través de API, lo que garantiza que los datos estén siempre actualizados y reflejen el estado más reciente de la fuente. Es crucial realizar los procesos de obtención de información de las herramientas de ciberseguridad en momentos que no afecten el rendimiento de los activos de los cuales se están extrayendo datos, como, por ejemplo, durante las horas nocturnas.
- **Escalabilidad:** es posible escalar fácilmente la recopilación de datos para satisfacer las necesidades cambiantes de la organización sin requerir cambios significativos en la infraestructura. Esto se debe a que los sistemas pueden estar compuestos por módulos o componentes independientes que se comunican entre sí a través de interfaces bien definidas, lo que permite que cada componente opere de manera independiente y se pueda escalar de forma aislada sin afectar el resto del sistema. Además, se pueden reutilizar funcionalidades específicas, y cuando un servicio o recurso está encapsulado detrás de una API, otros sistemas pueden acceder y utilizar esa funcionalidad sin necesidad de conocer los detalles internos de implementación.
- **Seguridad:** suelen ofrecer métodos seguros de autenticación y autorización, lo que garantiza que solo las partes autorizadas tengan acceso a los datos, incluso muchas API utilizan tokens de acceso para autenticar solicitudes. Además, la autorización asegura que el usuario tiene los permisos adecuados para acceder a los recursos o realizar determinadas acciones. Por otra parte, las API deben validar y “sanitizar⁶⁴” los datos de entrada para prevenir ataques comunes, como inyecciones SQL o ataques de script entre sitios (XSS⁶⁵). La propia plataforma dispone de una API para proporcionar información a otras soluciones, herramientas o plataformas de la organización que requieran información actualizada de activos, vulnerabilidades, lógica de negocio, conectividad de agentes de ciberseguridad, o bien acciones de mitigación.

⁶⁴ En ciberseguridad, "sanitizar" se refiere al proceso de limpiar, filtrar o desinfectar datos para asegurar que estén libres de cualquier contenido malicioso o peligroso. La sanitización es comúnmente aplicada a datos de entrada, especialmente aquellos provenientes de fuentes externas, como formularios web, para prevenir ataques de inyección de código.

⁶⁵ XSS, por sus siglas en inglés (*Cross-Site Scripting*)

4.1.3 Desarrollo ágil de la plataforma

El desarrollo de la plataforma tal y como se detalla en [18] requiere de la participación activa de los usuarios que hacen uso de ella, lo cual puede incluir tanto el propio responsable de la información (CIO⁶⁶), el CISO, el personal que define las políticas de seguridad, el que opera las herramientas de ciberseguridad (como por ejemplo personal del COS), administradores de seguridad o sistemas, desarrolladores de aplicaciones, encargados de la seguridad perimetral, el responsable del dato (CDO⁶⁷), o cualquier otro miembro de la organización que tenga algo que aportar y que requiera del uso de la plataforma.

El diseño ágil de una plataforma tan compleja, alineada con el enfoque CTEM, requiere la incorporación de principios y prácticas ágiles para asegurar la flexibilidad, fomentar la colaboración y lograr una entrega continua de valor. A continuación, se presenta una visión general del proceso:

- **Definición de objetivos y alcance:** es imprescindible fijar como objetivo líneas de desarrollo relativas a los requisitos CTEM e ir amoldando los objetivos a nuevas herramientas presentes en el mercado. En cualquier caso, se lleva a cabo un seguimiento de las líneas de desarrollo fijadas y se van marcando nuevos hitos cuando se van alcanzado los anteriores.
- **Composición de un equipo multifuncional:** el equipo está formado por los propios desarrolladores, el CISO, expertos en ciberseguridad, administradores de sistemas, administradores de seguridad, consultores, operadores de seguridad, especialistas en seguridad perimetral, y otros roles relevantes de la organización.
- **Planificación ágil y desarrollo iterativo:** se adoptan metodologías ágiles como Scrum⁶⁸ para planificar y organizar el trabajo. Además, se divide el desarrollo en iteraciones cortas llamadas *sprints*⁶⁸ y se crea un *backlog*⁶⁸ de funcionalidades priorizadas según su importancia y valor, lo que permite asegurar la flexibilidad necesaria para ajustar las prioridades según las necesidades cambiantes. Por otra parte, se implementan prácticas de integración continua para fusionar cambios de código de manera regular y se automatiza la entrega continua para desplegar nuevos cambios en producción de forma rápida y segura. Al final de cada *sprint* se realiza una demostración para obtener retroalimentación temprana.
- **Seguimiento continuo del desarrollo:** la colaboración y comunicación continua es esencial para obtener la realimentación de cada una de las iteraciones que permita variar de inmediato el ritmo o funcionalidad de cada desarrollo, identificando áreas de mejora y ajustar el proceso. Además, se mantiene una comunicación constante para abordar problemas, compartir avances y ajustar la dirección según sea necesario a través de los dos siguientes tipos de reuniones de seguimiento:
 - a. Reuniones mensuales con los usuarios que tienen que llevar a cabo la mitigación de vulnerabilidades: durante la revisión mensual, se evalúa el estado de riesgo de la superficie de exposición, se analizan las acciones de mitigación implementadas y se identifican aquellas que presentan mayores desafíos para su resolución. Además, se examinan las nuevas funcionalidades desarrolladas, y se abordan los errores o disfuncionalidades surgidos desde la última reunión.

⁶⁶ CIO, por sus siglas en inglés (*Chief Information Officer*).

⁶⁷ CDO, por sus siglas en inglés (*Chief Data Officer*).

⁶⁸ Scrum es un enfoque ágil para la gestión de proyectos que se centra en la flexibilidad y la colaboración. En Scrum, los equipos trabajan en bloques de tiempo llamados *sprints*, durante los cuales se comprometen a completar ciertas tareas de una lista prioritaria llamada *backlog* del producto. Cada *sprint* tiene una planificación rápida al inicio, seguida de reuniones diarias para mantener al equipo sincronizado. Al final de cada *sprint*, se presenta un "Incremento del Producto" que agrega valor tangible al proyecto.

- b. Reuniones semanales entre el equipo de desarrollo, el CISO, el Equipo de Seguridad Defensiva, el Responsable del Sistema, el Equipo de Seguridad Perimetral, y el COS: se revisan las líneas de desarrollo marcadas y se fijan las nuevas.
- **Seguridad de la propia plataforma:** se lleva a cabo desde el principio un enfoque en la seguridad, incorporando elementos de seguridad en cada etapa del desarrollo, desde el diseño hasta la implementación y las pruebas. Además, se realizan análisis de seguridad, pruebas de penetración y revisión de código para identificar posibles vulnerabilidades en cada iteración.
- **Cumplimiento con normativa:** se garantiza que la plataforma cumple con los requisitos normativos y de cumplimiento relevantes.

Al adoptar un enfoque ágil, el equipo puede adaptarse rápidamente a los cambios, responder a las amenazas de seguridad emergentes y entregar una plataforma CTEM efectiva y resiliente.

4.2 Implementación de una plataforma CTEM

Una plataforma que permita gestionar de forma continua la superficie de exposición a amenazas (CTEM) de una infraestructura TIC compleja y heterogénea como la de Defensa, requiere el cumplimiento de las siguientes características [39]:

1. **Visibilidad completa de la superficie de exposición:** para identificar y gestionar con la mayor rapidez posible el riesgo de ciberseguridad en la superficie de exposición, así como eliminar todos los puntos ciegos, la plataforma debe ofrecer los siguientes elementos.
 - a. Vista unificada de los activos según sus tipologías, vulnerabilidades software y por configuración, y acciones a llevar a cabo para su mitigación.
 - b. Comprobaciones periódicas y exhaustivas para identificar los activos accesibles tanto desde el interior como del exterior, a fin de eliminar las áreas de riesgo para la seguridad.
2. **Predicción de ciberataques y priorización de acciones de mitigación** [16]: para ayudar al Equipo de Seguridad Defensiva de la organización a prevenir ciberataques basados en vulnerabilidades conocidas y configuraciones no deseadas, así como priorizar sus acciones y reducir el riesgo con el mínimo esfuerzo, la plataforma debe proporcionar:
 - a. Contexto sobre los activos, incluyendo tanto las dependencias entre activos, como la agrupación de activos que da lugar a un nuevo tipo de activo que representa una lógica de negocio determinada, y las amenazas a las que se ven sometidos.
 - b. Identificación continua de rutas de ataque que presentan el mayor riesgo de explotación, gracias al análisis de la telemetría de seguridad almacenada y analizada periódicamente.
 - c. Priorización en las acciones de mitigación de vulnerabilidades y propuesta de configuraciones seguras según las normativas aplicables.
3. **Métricas eficaces para informar del riesgo:** para ayudar al Comité de Seguridad acerca del riesgo al que se somete la infraestructura, a través de una herramienta que centralice los datos y que esté alineada con los intereses de la organización mediante KPI claros, así como para permitir la evaluación del riesgo total de exposición en base a situaciones anteriores y datos externos comparados, la plataforma debe ofrecer los siguientes elementos.
 - a. Datos procesables o indicadores específicos sobre el riesgo global y parcial de exposición en la infraestructura, incluido el valor de los esfuerzos diarios para llevar a cabo las acciones de mitigación propuestas por las herramientas de ciberseguridad.
 - b. Permitir a los usuarios de la plataforma analizar los aspectos específicos de su ámbito, o área, así como diferenciar entre el riesgo de los distintos tipos de activo.
 - c. Ayuda en la mejora de comunicación, colaboración y cooperación entre los distintos administradores, gestores y visores de vulnerabilidades de la organización.

- d. Métricas o indicadores procesables que mejoran los tiempos de respuesta, optimizan la toma de decisiones, y respaldan las iniciativas de mejora de ciberseguridad de la infraestructura, reduciendo el riesgo significativamente.

A continuación, se muestra Figura 18 que incluye las capacidades arriba detalladas y que debería incluir una plataforma para la gestión continua de la exposición a amenazas (CTEM) en una infraestructura TIC de forma que combine la gestión de vulnerabilidades basada en el riesgo aprovechando todo el potencial de herramientas desplegadas en esta infraestructura:

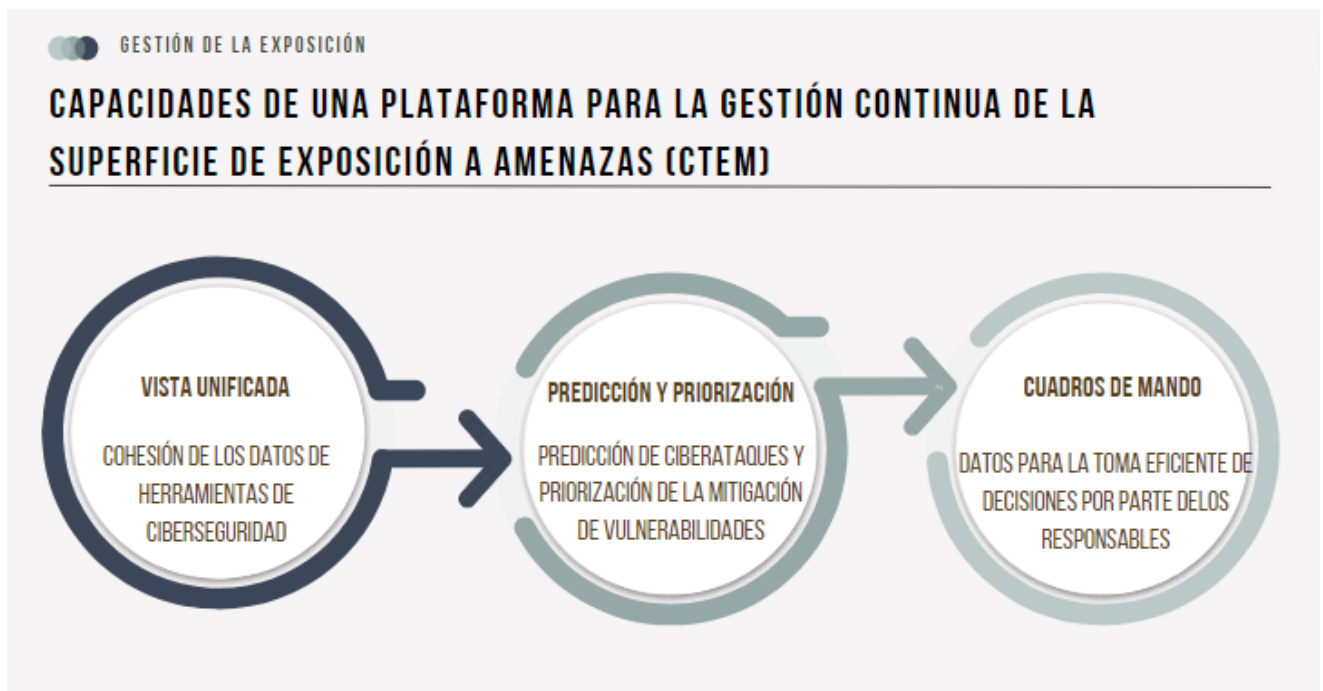


Figura 18 Capacidades necesarias para la gestión de la superficie de exposición a amenazas (CTEM) [39]

Las siguientes secciones definen la funcionalidad proporcionada por la plataforma CTEM desarrollada en Defensa, denominada SUPERFICIE, la cual ha sido diseñada siguiendo la metodología detallada en la sección 4.1 Metodología de desarrollo.

4.2.1 Recopilación nocturna de datos de las herramientas de ciberseguridad

La plataforma CTEM debe contar inicialmente con datos actualizados de la infraestructura TIC, permitiendo así una monitorización continua del estado de todos los activos. El conjunto de datos obtenido proviene de herramientas de ciberseguridad desplegadas previamente en la infraestructura, concretamente de los siguientes tipos:

- (VM) Gestión de vulnerabilidades
- (XDR) Detección y respuesta extendida
- (EASM) Gestión de la superficie externa
- (ASCA) Evaluación automatizada de controles de seguridad
- (BAS) Simulación de amenazas
- (ITSM, CMDB) Gestión de servicios, cambios y configuración
- (NAC) Control de acceso a red

La plataforma actúa como un centro neurálgico que guarda información específica de cada uno de los activos existentes en la plataforma, recopilando toda esta información vía API de cada uno de las herramientas previamente desplegadas en la infraestructura.

Para poder llevar a cabo toda la recogida de datos, se define una API de comunicación en un módulo independiente que recibe, a través de peticiones REST⁶⁹, toda la información necesaria. Además, para automatizar la actualización nocturna de la información se desarrollan una serie de procesos de recopilación de información sin que se necesite la intervención del usuario. Gracias a la ejecución de estos procesos *batch*⁷⁰ (internamente los definimos como procesos CRON⁷¹) se lleva a cabo la regularización de toda la información necesaria en la plataforma.

La Figura 19 muestra el conjunto de herramientas⁷² que alimentan la plataforma CTEM gracias a la recogida de datos de los procesos CRON.

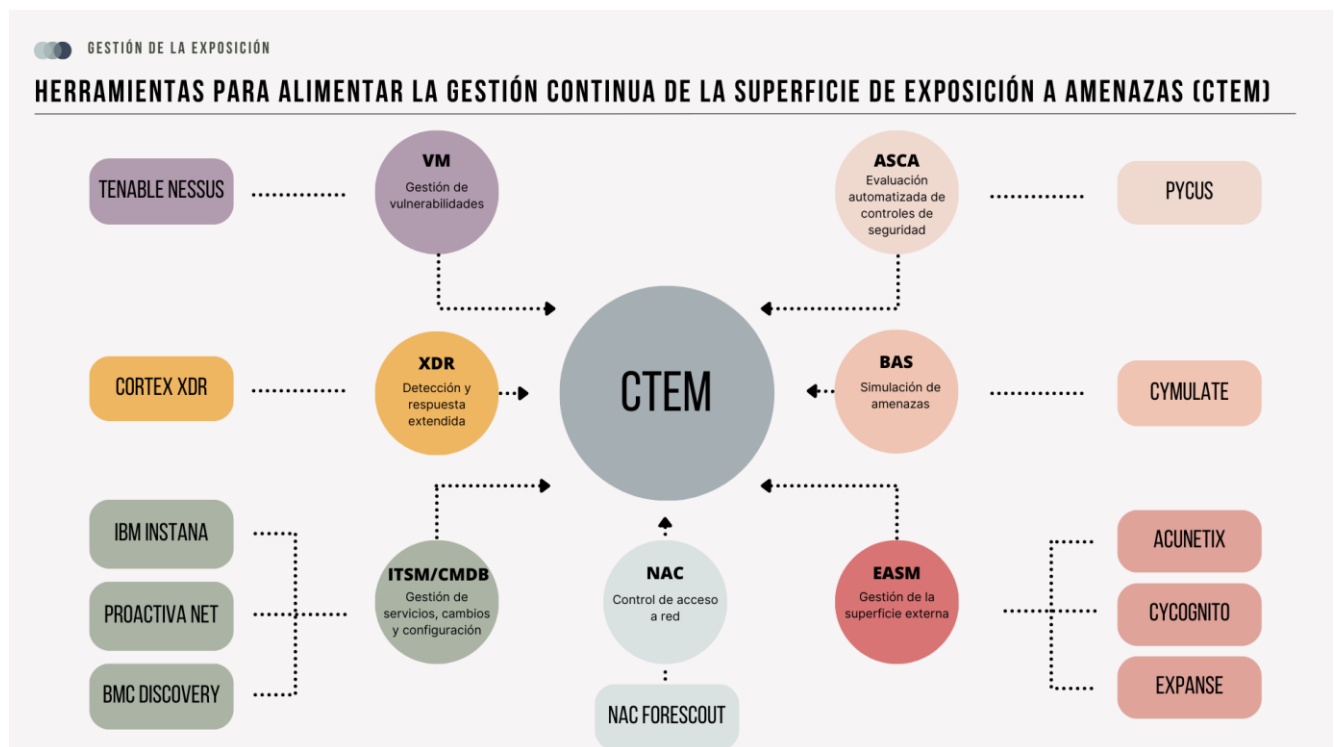


Figura 19 Herramientas para alimentar la gestión de la superficie de exposición a amenazas (CTEM) [Fuente propia]

A continuación, se presenta un flujo de trabajo estándar para la integración de una nueva fuente de información de una herramienta de seguridad en la plataforma CTEM:

- Evaluación de la API del nuevo proveedor.
- Implementación de una nueva funcionalidad, en el módulo de la plataforma encargado de los procesos de recogida automática de datos, para la encapsulación de la información obtenida gracias a las peticiones REST de la API proporcionada por el proveedor.
- Ejecución del proceso *batch* que actualiza la información de la plataforma de manera masiva y nocturna usando la nueva funcionalidad.

⁶⁹ REST, por sus siglas en inglés (*Representational State Transfer*).

⁷⁰ Un proceso *batch*, en informática y programación, se refiere a la ejecución de un conjunto de tareas o trabajos de manera secuencial, sin intervención manual durante la ejecución. Estos trabajos suelen agruparse y ejecutarse en lotes (*batches*) para facilitar la automatización de procesos repetitivos o para gestionar grandes volúmenes de datos de manera eficiente.

⁷¹ CRON, por sus siglas en inglés (*Command Run On Notice*).

⁷² Este conjunto de herramientas puede incluir cualquiera de las existentes en el mercado, mientras que al menos haya una de cada tipo. Incluso es recomendable.

En resumen, esta arquitectura presenta una serie de ventajas ya que encapsula las peticiones al API del fabricante en un módulo propietario. Estas ventajas se resumen a continuación:

- Si cambia el fabricante, el módulo debería devolver los mismos datos aunque los obtenga de manera diferente, no siendo necesario desarrollar nuevo código.
- Se puede desplegar por separado mejorando la seguridad y la fiabilidad.
- Se pueden realizar llamadas controladas a través de roles de usuarios específicos de manera atómica y automatizada.
- Los procesos `batch` no dependen del proveedor si no de elementos propietarios de la organización.

Concluir que, gracias a los procesos CRON, los datos de SUPERFICIE se sincronizan de manera masiva a través de la API definida previamente que encapsula las peticiones de consulta a los proveedores de servicios.

4.2.2 Descubrimiento de activos (superficie interna)

El proceso de descubrimiento y enumeración de activos de la superficie interna consiste en identificar y clasificar todos los activos presentes en la infraestructura TIC, gracias a la información proporcionada por herramientas XDR y NAC. La Figura 20 ilustra un ejemplo de enumeración de activos en la plataforma SUPERFICIE, donde se puede apreciar la clasificación de un activo tipo servidor. La información incluye detalles sobre el ámbito, el nombre, los servicios asociados, el área, la dirección IP, entre otros.

Ámbito	Hostname	IP	Servicios	Área	Entorno	Dominio	SO	Vulnerabilidades	Criticidad	Pr.
USINCLAS DIVERPER (DIL...)	USINCLAS DIVERPER (DIL...)	10.10.10.10	(0) Sin servicio	USINCLAS DIVERPER (DIL...)	Produccion	Uso Oficial	RHEL	110 CVEs activos	Critico	3
USINCLAS DIVERPER (DIL...)	USINCLAS DIVERPER (DIL...)	10.10.10.10	(0) Sin servicio	USINCLAS DIVERPER (DIL...)	Produccion	Gestion-Uso Oficial	RHEL	109 CVEs activos	Critico	3
USINCLAS DIVERPER (DIL...)	USINCLAS DIVERPER (DIL...)	10.10.10.10	(0) Sin servicio	USINCLAS DIVERPER (DIL...)	-	-	Windows Server	481 CVEs activos	Critico	3
EA-ABA (EA)	EA-ABA (EA)	10.10.10.10	(0) Sin servicio	EA-ABA (EA)	-	WAN-PG	Windows Server	11 CVEs activos	Critico	3
EA-BOBADILLA (EA)	EA-BOBADILLA (EA)	10.10.10.10	(0) Sin servicio	EA-BOBADILLA (EA)	-	-	Windows Server	11 CVEs activos	Critico	3
EA-ACARGETAFE (EA)	EA-ACARGETAFE (EA)	10.10.10.10	(0) Sin servicio	EA-ACARGETAFE (EA)	-	-	Windows Server	10 CVEs activos	Critico	3
EA-AR-HISTORICO (EA)	EA-AR-HISTORICO (EA)	10.10.10.10	(0) Sin servicio	EA-AR-HISTORICO (EA)	-	-	Windows Server	1662 CVEs activos	Critico	3
USINCLAS DIVERPER (DIL...)	USINCLAS DIVERPER (DIL...)	10.10.10.10	(0) Sin servicio	USINCLAS DIVERPER (DIL...)	Produccion	-	Windows Server	1730 CVEs activos	Critico	3
EA-TABLADA (EA)	EA-TABLADA (EA)	10.10.10.10	(0) Sin servicio	EA-TABLADA (EA)	-	-	Windows Server	10 CVEs activos	Critico	3
ET-T4110 (ET)	ET-T4110 (ET)	10.10.10.10	(0) Sin servicio	ET-T4110 (ET)	-	-	Windows Server	2056 CVEs activos	Critico	3
EA-CUATROVIENTOS (EA)	EA-CUATROVIENTOS (EA)	10.10.10.10	(0) Sin servicio	EA-CUATROVIENTOS (EA)	-	-	Windows Server	434 CVEs activos	Critico	3
EA-CGEA (EA)	EA-CGEA (EA)	10.10.10.10	(0) Sin servicio	EA-CGEA (EA)	-	-	Windows Server	1422 CVEs activos	Critico	3

Figura 20 SUPERFICIE – Enumeración de activos internos (servidores) [Fuente SUPERFICIE]

A su vez, la Figura 21 muestra el estado de exposición de un servidor, con las vulnerabilidades identificadas, y las acciones asociadas a cada vulnerabilidad.

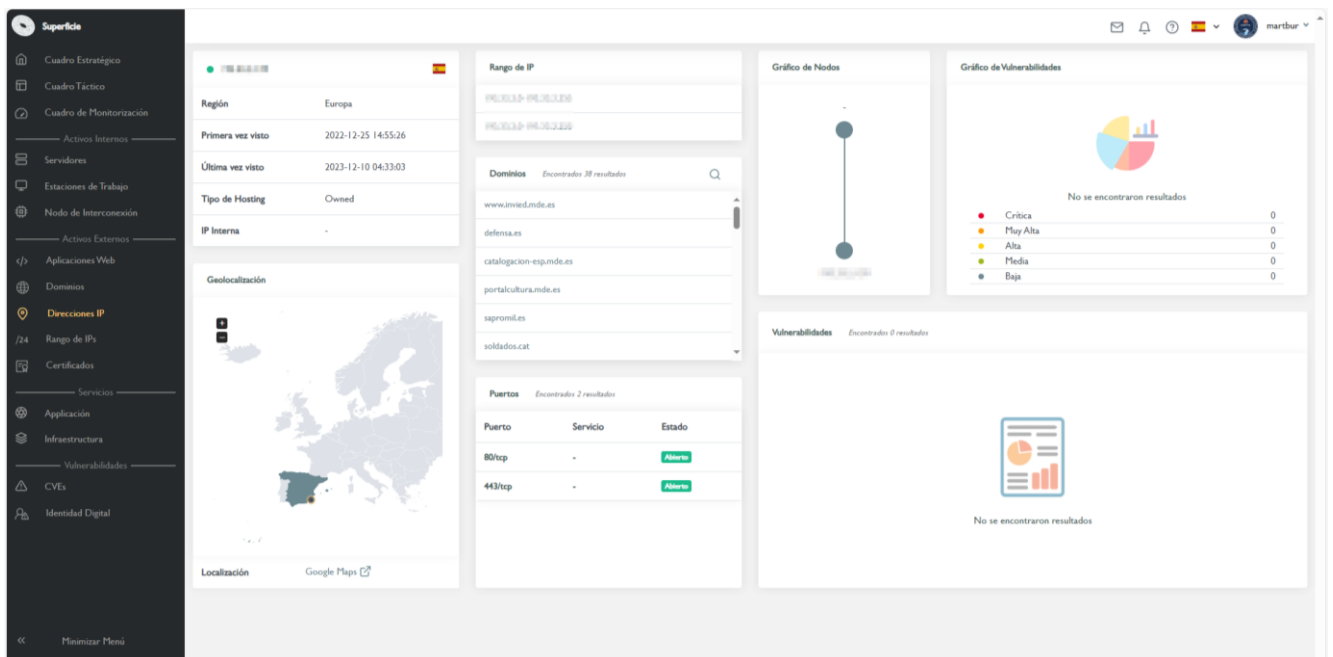


Figura 23 SUPERFICIE – Información de activos externos (direcciones IP) [Fuente SUPERFICIE]

Finalmente, la Figura 24 muestra la enumeración de activos de la superficie externa del tipo certificados, donde puede observarse información como la IP, el nombre, el dominio, la caducidad del certificado, los puertos abiertos, el número de vulnerabilidades, el último análisis y el estado en el que se encuentra.

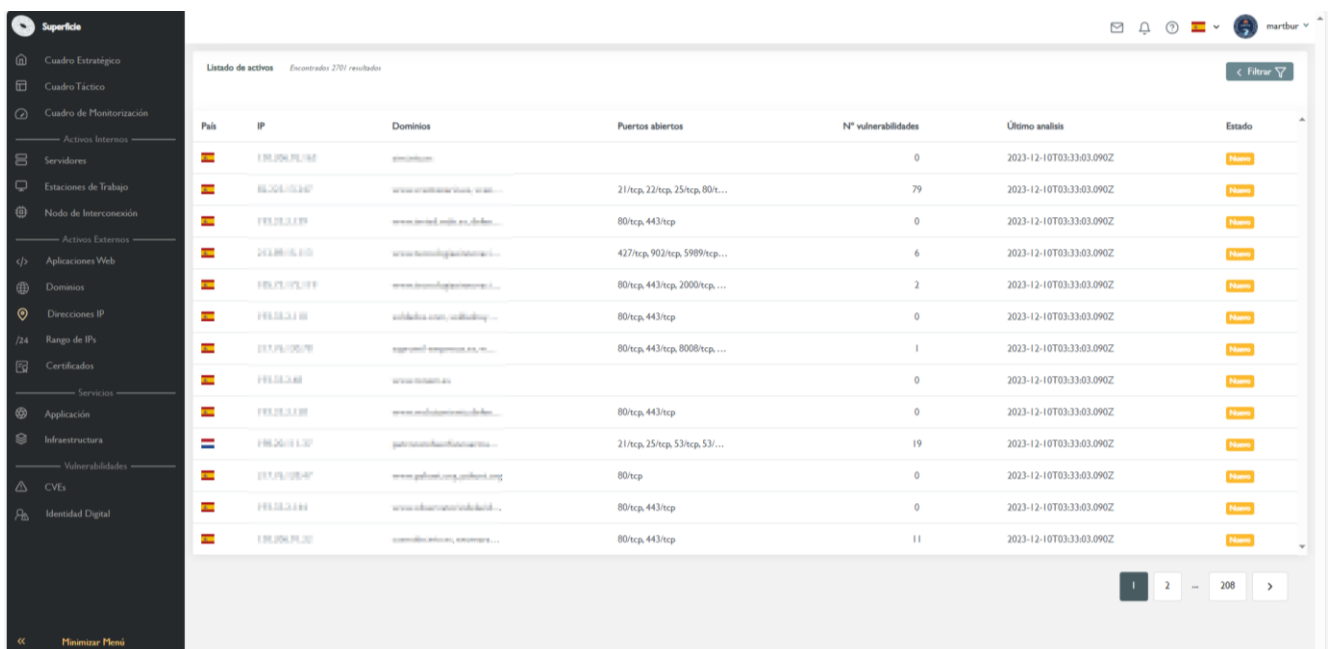


Figura 24 SUPERFICIE – Enumeración de activos externos (certificados) [Fuente SUPERFICIE]

4.2.4 Trazabilidad superficie interna-externa

En términos generales, los activos de la superficie interna que ofrecen servicios web no suelen estar relacionados directamente a la superficie externa. En las organizaciones, es común contar con diversas capas y niveles de red por motivos de seguridad (segmentación) y la implementación de diversos dispositivos de red. Debido a esta configuración, identificar fácilmente a qué dirección IP interna

(superficie interna) se vincula una dirección IP pública (superficie externa) resulta complicado, ya que no se establece una traslación directa. Además, conceder acceso a todos los dispositivos de red por los que pasa un paquete, para correlacionar la información, no es práctico en términos de velocidad y logística. Por lo tanto, la mejor manera de realizar un seguimiento es mediante el uso de una "miguita de pan" que se pueda lanzar desde el principio y se sepa que llegará hasta el final.

La "miguita de pan" en este contexto se refiere a una cabecera establecida en el protocolo HTTP, la cual queda registrada en los registros (logs) del servidor. Esta cabecera puede contener datos como el dominio solicitado o la dirección IP externa de entrada. Cuando un paquete llega al nivel final, los datos de las cabeceras HTTP se registran en el servidor web. Es esencial configurar el servidor para que registre estas cabeceras HTTP, ya que no se guardan de forma predeterminada. Una vez que estos registros están en el servidor web dentro de la superficie interna, si se envían a un dispositivo centralizador de registros, como una herramienta SIEM, sólo es necesario consultar los datos para obtener información sobre la entrada y hasta dónde ha llegado.

4.2.5 Listado de Vulnerabilidades

Se muestra a continuación, la Figura 25 que incluye el listado de las vulnerabilidades identificadas en la superficie de exposición, junto con las acciones de mitigación (propuestas por las herramientas VM y EASM). En caso de no poder llevar a cabo la acción de mitigación propuesta, podría proponer una acción manual. También se puede observar el número total de dispositivos afectados y los que en algún momento han sido vulnerables.

ID CVE	Tipología	Total Hosts Afectados	Hosts Vulnerables	Fecha de Publicación	Peligrosidad	CVSS
CVE-2015-0301	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before ...	19	19	13-01-2015 23:59	Crítico	10
CVE-2015-0306	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before ...	19	19	13-01-2015 23:59	Crítico	10
CVE-2015-0315	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 ...	16	16	06-02-2015 00:59	Crítico	10
CVE-2015-0310	Adobe Flash Player before 13.0.0.262 and 14.x through 16.x before ...	15	15	23-01-2015 21:59	Crítico	10
CVE-2015-0308	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.260 ...	19	19	13-01-2015 23:59	Crítico	10
CVE-2015-0316	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before ...	16	16	06-02-2015 00:59	Crítico	10
CVE-2015-0325	Heap-based buffer overflow in the __ms_hostname_digits_dots fun...	2	2	28-01-2015 19:59	Crítico	10
CVE-2015-0314	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before ...	16	16	06-02-2015 00:59	Crítico	10
CVE-2015-0303	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before ...	19	19	13-01-2015 23:59	Crítico	10
CVE-2015-0313	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 ...	16	16	02-02-2015 19:59	Crítico	10
CVE-2015-0304	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.260...	19	19	13-01-2015 23:59	Crítico	10
CVE-2015-0311	Unspecified vulnerability in Adobe Flash Player through 13.0.0.262 a...	16	16	23-01-2015 21:59	Crítico	10
CVE-2015-0309	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.260...	19	19	13-01-2015 23:59	Crítico	10

Figura 25 SUPERFICIE – Listado de vulnerabilidades [Fuente SUPERFICIE]

La Figura 26 muestra los activos internos afectados por una vulnerabilidad en concreto, incluyendo la descripción y el estado de mitigación por activo. También se incluye información del sistema operativo, el área asignada, la fecha de la detección, la fecha de mitigación, y el sistema de puntuación de vulnerabilidades CVSS.



Supercide 📧 🔔 ⓘ 🇪🇸 martbur



A continuación, se muestra la Figura 28 que muestra el panel estratégico, que muestra los indicadores estratégicos para medir la superficie de exposición (i.e., Estado de la superficie de exposición, número de activos, número de servicios, número de vulnerabilidades, gráfico de servidores vulnerables vs no vulnerables, evolución de estado de acciones completadas y pendientes, tiempo medio de mitigación de una vulnerabilidad, distribución de servidores prioritarios por ámbitos, geolocalización de los servidores y el número de vulnerabilidades en los activos servidor según su criticidad).



Figura 28 SUPERFICIE – Panel estratégico [Fuente SUPERFICIE]

4.2.8 Comunicación del Equipo de Seguridad Defensiva con el resto de gestores de vulnerabilidades

El Equipo de Seguridad Defensiva dispone de un panel propio (ver Figura 29) para obtener una idea del estado de mitigación de vulnerabilidades llevado a cabo por los Ámbitos. Además, cuenta con la posibilidad de notificar incidencias o comunicar información a los gestores de vulnerabilidades. Finalmente, también puede generar informes del estado de seguridad con un formato previamente definido.

La Figura 29 contiene el panel táctico que ilustra los indicadores específicos para el Equipo de Seguridad Defensiva y que permite obtener vistas específicas para los Ámbitos. El riesgo global mostrado es específico para el Ámbito sobre el que se hace el filtrado, siendo solamente accesible para aquellos usuarios que pertenezcan a ese Ámbito.

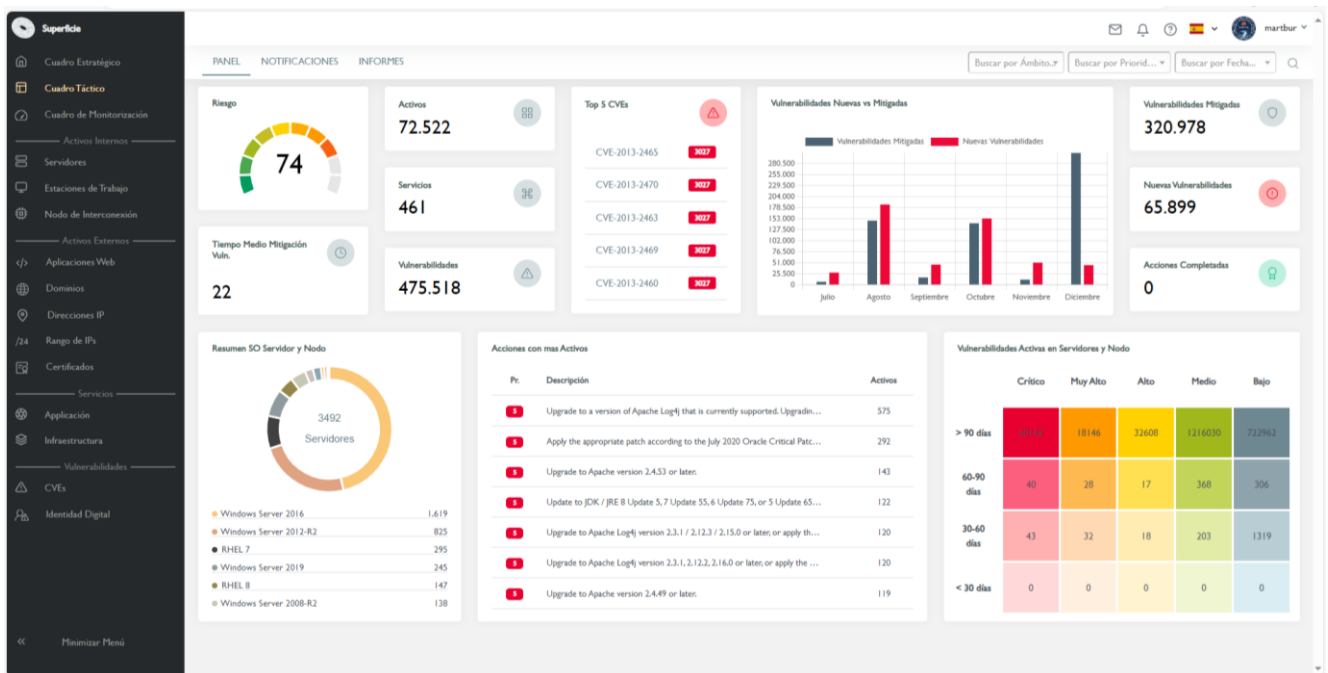


Figura 29 SUPERFICIE – Panel táctico-operativo [Fuente SUPERFICIE]

La Figura 30 ilustra la comunicación del Equipo de Seguridad Defensiva con los gestores de vulnerabilidades a través de la funcionalidad de emisión de notificaciones.

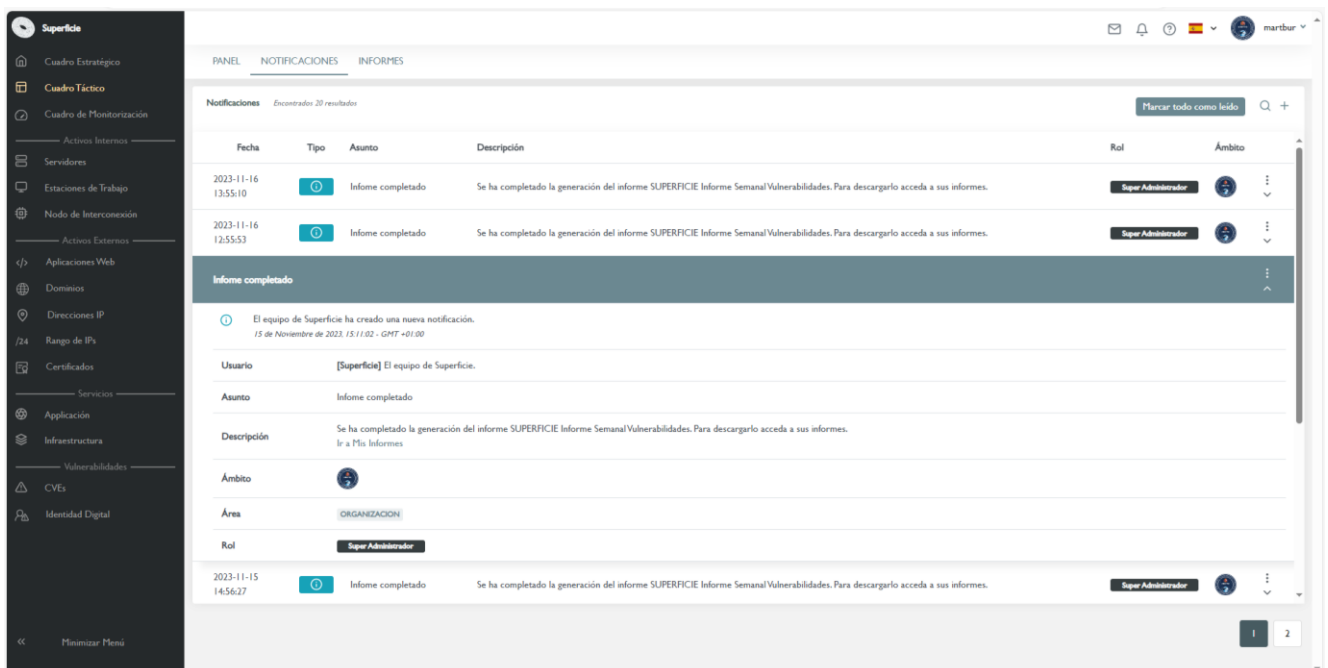


Figura 30 SUPERFICIE – Panel táctico y operativo con notificaciones a los gestores de vulnerabilidades [Fuente SUPERFICIE]

4.2.9 Conectividad de los agentes

A continuación, se presenta la Figura 31 que incluye el panel de monitorización indicando el estado de conectividad de los agentes desplegados en la infraestructura. Este panel es esencial para supervisar los activos de la superficie oculta.

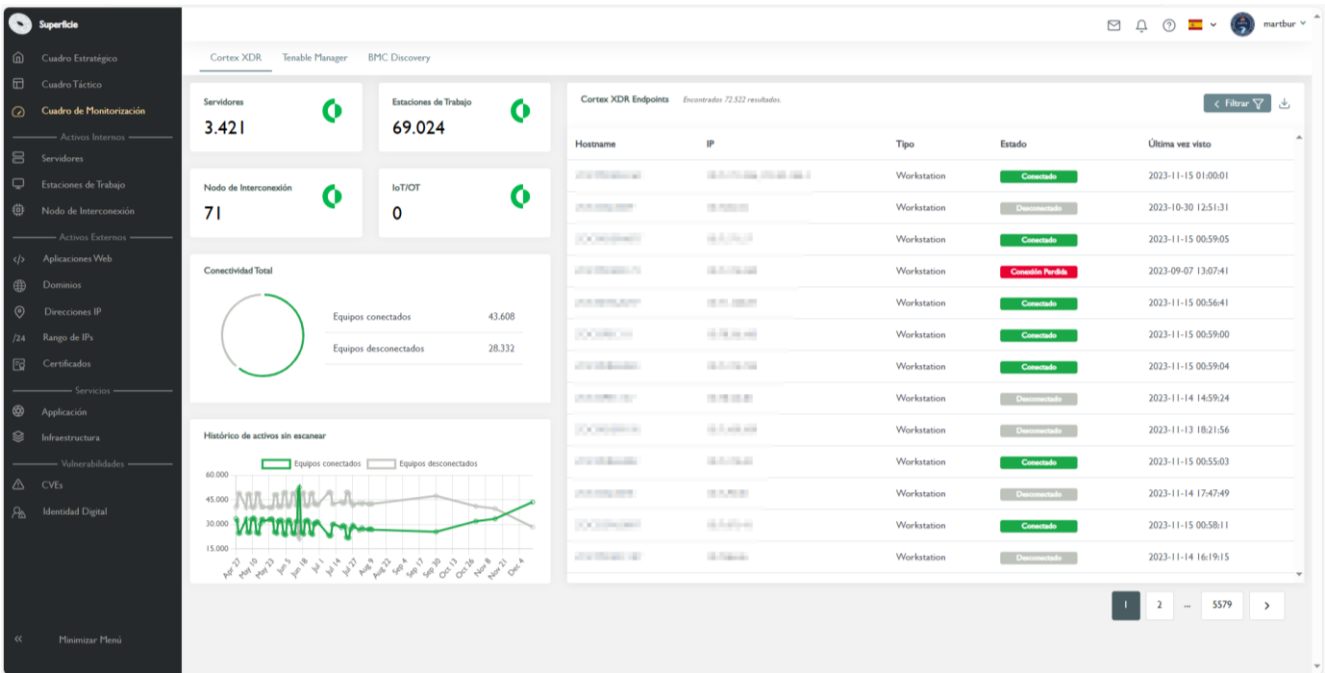


Figura 31 SUPERFICIE – Panel de monitorización [Fuente SUPERFICIE]

4.2.10 Gestión de usuarios

En la figura siguiente se ilustra la gestión de usuarios a través de la Figura 32 que muestra distintos tipos de usuarios con su rol, incluyendo si pertenecen a la Organización, a un Ámbito, o bien a un Área.

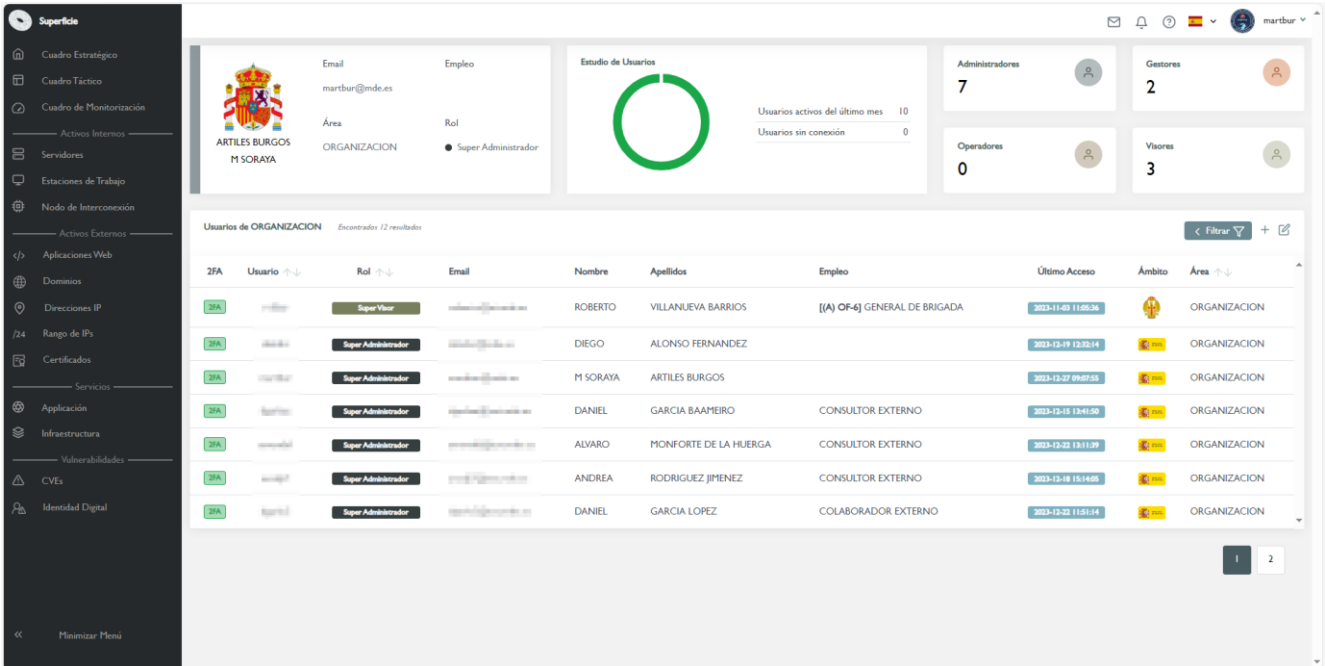


Figura 32 SUPERFICIE – Roles y privilegios [Fuente SUPERFICIE]

4.2.11 Seguridad de la plataforma CTEM

Como no podía ser de otra forma, la propia plataforma CTEM debe contar con medidas de seguridad elevadas que cumplan con las normativas de seguridad, como es el propio ENS. Se exponen a continuación el cumplimiento de las medidas de seguridad de esta normativa para ciertos controles en los que se ha llevado a un cumplimiento de nivel ALTO:

- [op.acc.5⁷³] Uso de un segundo factor de autenticación e información a través de correo electrónico de los accesos a la plataforma (la gestión de la identidad digital de los usuarios está separada de la gestión del correo electrónico).
- [op.exp.8]⁷⁴ Registro de la actividad con revisión automática, correlación de eventos y respuesta automática ante los mismos con la propia herramienta XDR.
- [op.mon.1⁷⁵] Se ejecutan automáticamente acciones predeterminadas de respuesta para alertas generadas.
- [mp.com.4⁷⁶] Se lleva a cabo el control de entrada de los usuarios que llegan a cada segmento y control de entrada y salida de la información disponible en cada segmento.

4.3 Cuantificación de la superficie anómala

La cuantificación de la superficie anómala incluye el análisis de aquellas partes de la superficie que constituyen una vía de entrada. Tal métrica se evalúa como el promedio ponderado de las puntuaciones de riesgo para todas las vulnerabilidades reconocidas en la superficie de exposición, dando un peso sustancialmente mayor a aquellas vulnerabilidades que se saben explotables. Este método de cálculo del estado de riesgo de la superficie permite comparar estados de seguridad con otras infraestructuras TIC. Esta métrica se ha seleccionado para que varíe en un rango de [0,100], siendo una puntuación más baja indicativa de una superficie de ataque más segura. Dicha métrica se actualiza diariamente para tener en cuenta las vulnerabilidades mitigadas y los nuevos riesgos identificados en su superficie de ataque. Al centrar sus esfuerzos de remediación en vulnerabilidades de alto riesgo basadas en sus puntuaciones de riesgo y otros factores de criticidad, se puede reducir el riesgo global en la superficie de ataque e intentar su puntuación de seguridad con el tiempo.

Se ha diseñado un algoritmo de aprendizaje automático para el reconocimiento del estado de riesgo de la superficie, que permita al CISO poder llevar a cabo una adecuada y precisa toma de decisiones basada en un dato simple y entendible: el estado de riesgo de la superficie de la infraestructura TIC. A continuación, se detallan los elementos necesarios que se han tenido en cuenta para el diseño del algoritmo de forma que sea capaz de extrapolar el dato del riesgo de la superficie de exposición, dados una serie de valores.

1. **Recopilación de datos:** se reúnen las siguientes variables de entrada para llevar a cabo el objetivo de la identificación de la superficie vulnerable, distinguiendo entre aquellos intrínsecos del activos y aquellos de carácter estadístico.
 - Número de vulnerabilidades por activo servidor (diaria).
 - Número de servidores conectados (existe un al menos un agente desplegado que proporciona información de forma diaria).
 - Riesgo global (diario)⁷⁷.

⁷³ Las medidas de seguridad definidas en el ENS referentes a los mecanismos de autenticación (usuarios de la organización) se detallan en [op.acc.6].

⁷⁴ Las medidas de seguridad definidas en el ENS referentes al registro de la actividad se detallan en [op.exp.8].

⁷⁵ Las medidas de seguridad definidas en el ENS referentes a la monitorización del sistema se detallan en [op.mon.1].

⁷⁶ Las medidas de seguridad definidas en el ENS referentes a la separación de flujos de información en la red se detallan en [mp.com.4].

⁷⁷ El riesgo global se ha calculado teniendo en cuenta el número total de vulnerabilidades, el valor CVSS y el de EPSS de cada CVE detectada en un activo servidor, y si los IoCs de Seguridad Perimetral son capaces de bloquear esa CVE.

2. **Procesamiento de datos:** se han realizado los siguientes pasos para procesar previamente los datos⁷⁸.
 - Eliminación de datos anómalos o duplicados (i.e. no existían datos duplicados).
 - Normalización de datos con la técnica de escalado⁷⁹, no teniendo éste ajuste apenas repercusión en la precisión del modelo.
3. **Selección de características:** se seleccionan las características más relevantes para la evaluación de la superficie vulnerable, sobre datos recopilados en los últimos cuatro meses.
 - Media de vulnerabilidades por activo servidor (sumatorio del mes) es igual al número de vulnerabilidades por activo servidor (sumatorio del mes) dividido entre el número de servidores conectados (sumatorio del mes), por ámbito.
 - Número de servidores conectados (sumatorio del mes).
 - Riesgo global (sumatorio del mes).
4. **Diseño del modelo de IA:** el modelo de inteligencia artificial escogido es el de aprendizaje supervisado mediante un modelo de regresión lineal múltiple⁸⁰. Este enfoque de aprendizaje automático permite identificar el estado de vulnerabilidad potencial de la superficie de exposición en función de las características seleccionadas (i.e. media de vulnerabilidades identificadas por activo en función del número de servidores conectados). La regresión lineal múltiple es la seleccionada ya que se sospecha que múltiples variables están relacionadas con el valor del estado de riesgo de la superficie de exposición en una infraestructura y se desea comprender la naturaleza de esas relaciones. La interpretación de los coeficientes permite entender la magnitud y dirección de la influencia de cada variable independiente (i.e. media de vulnerabilidades por servidor, y el número de servidores conectados) sobre la variable dependiente (i.e. riesgo global mensual).
5. **Entrenamiento del modelo:** se utilizan los datos recopilados para enseñar al algoritmo a hacer predicciones. La división en el conjuntos de datos (*data set*⁸¹) se ha llevado a cabo de la siguiente forma: asignando el 85% de los el conjunto de datos de entrenamiento (*training data*⁸²) y el 15% restante para datos de prueba (*test data*⁸³), siendo éstos datos que el modelo no ha visto anteriormente. Se observa en el conjunto de datos generados que la relación entre la media de vulnerabilidades por servidor y el riesgo global no es lineal (por ejemplo, a más vulnerabilidades no existe mayor riesgo global). Se expone a continuación la Figura 33 de que muestra la distribución de datos con los que el modelo ha entrenado⁸⁴.

⁷⁸ Se ha utilizado la librería Pandas de Python especializada en el manejo y análisis de estructuras de datos, en este caso para el tratamiento de los datos, eliminación de duplicados y anómalos.

⁷⁹ La normalización de datos con escalado es una técnica utilizada en el procesamiento de datos para ajustar las características numéricas de un conjunto de datos a una escala común. Este proceso es especialmente útil cuando las características del conjunto de datos tienen rangos muy diferentes, lo que puede afectar el rendimiento de ciertos algoritmos de aprendizaje automático.

⁸⁰ La regresión lineal múltiple es una técnica estadística que se utiliza para modelar la relación entre una variable dependiente (o de respuesta) y dos o más variables independientes (o predictoras). A diferencia de la regresión lineal simple, que involucra solo dos variables (una variable predictora y una variable de respuesta), la regresión lineal múltiple permite analizar cómo múltiples variables independientes están relacionadas con la variable de respuesta.

⁸¹ El conjunto de datos (*data set* en inglés) se utiliza en un análisis específico o en un experimento. Puede incluir datos de entrenamiento, datos de prueba y, en algunos casos, datos de validación.

⁸² Los datos de entrenamiento (*training data* en inglés) son conjuntos de datos que se utilizan para el análisis.

⁸³ Los datos de prueba (*test data* en inglés) son conjuntos de datos que no se utilizan durante el entrenamiento del modelo, pero se emplean para evaluar su rendimiento una vez que ha sido entrenado.

⁸⁴ Se ha utilizado la librería de visualización de datos Seaborn de Python.

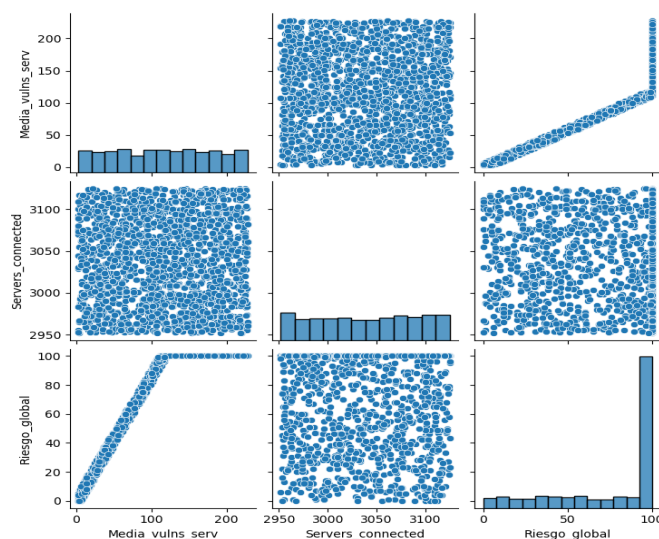


Figura 33 Algoritmo de regresión lineal múltiple – Valores de entrenamiento [Fuente propia]

6. **Evaluación del modelo:** la evaluación del modelo se basa, primero en el cálculo del riesgo global mensual con los datos de prueba (*test data*), que son el 15%⁸⁵. A continuación, se compara el resultado obtenido por el modelo con los resultados reales. Se constata que el modelo, después de haber completado la fase de entrenamiento, es capaz de acertar un 80% en la fase de prueba, donde el modelo se enfrenta a datos que no ha visto antes⁸⁶. La Figura 34 muestra los resultados que predice el modelo en comparación con los resultados reales.

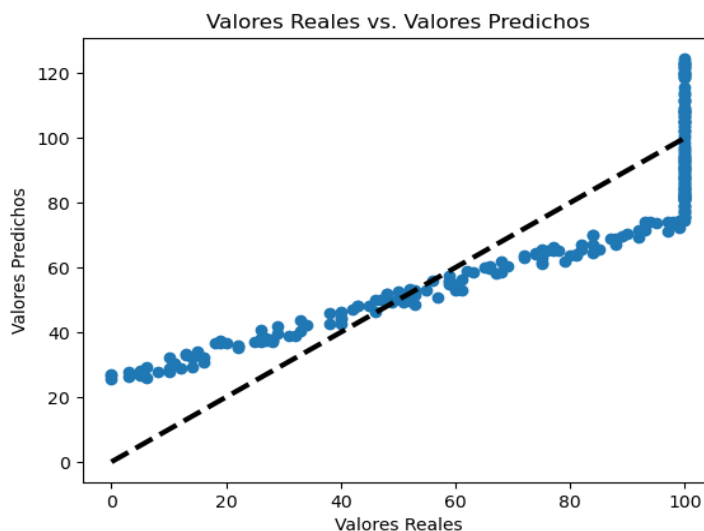


Figura 34 Algoritmo de regresión lineal múltiple – Valores reales vs. reales predichos [Fuente propia]

7. **Interpretación de los resultados:** se observa que el coeficiente de determinación⁸⁷, que indica la viabilidad de la regresión del modelo, tiene un valor relativamente alto (i.e. cercana

⁸⁵ Se ha utilizado la librería Scikit-learn para Python, para la realización de la regresión, los cálculos del modelo, las fases de entrenamiento, la fase de test y la de normalización.

⁸⁶ La métrica utilizada para evaluar el modelo ha sido el coeficiente de determinación o R^2 . Aunque el modelo no sea de clasificación ni de *clustering*, se eligió esta métrica debido a que el valor del error cuadrático medio era considerablemente alto.

⁸⁷ El coeficiente de determinación indica qué tan bien los valores observados se ajustan al modelo propuesto. Su valor varía de 0 a 1, donde 1 indica una perfecta concordancia entre el modelo y los datos, mientras que 0 indica que el modelo no explica ninguna variabilidad.

al 80%) pero no es óptimo para el objetivo esencial de cuantificar la superficie anómala. Se concluye, por tanto, que debería emplearse un modelo diferente, dado que los datos sugieren una relación no lineal entre sus variables.

8. **Acciones derivadas:** al concluir que debería utilizarse un modelo diferente, éste debería considerar además otros valores, como por ejemplo el valor de criticidad de cada vulnerabilidad, e incluso otros valores de entrenamiento como la criticidad del servicio, o ciberincidentes ocurridos. El fenómeno de cuantificación de la superficie anómala es complejo, y se ha evidenciado que no puede simplificarse con una relación lineal. Un ejemplo que podría mejorar el resultado sería el empleo de una red neuronal con al menos una capa oculta.

4.4 Verificación de los KPI con la plataforma CTEM

En la siguiente lista se enumeran los indicadores de rendimiento contrastados en la operación diaria de la propia plataforma CTEM, lo que permite comparar los valores de partida, tal y como se expresan en las tablas de la sección 1.3 Objetivos, con los objetivos alcanzados.

Id KPI	Descripción	Actual	Meta	Comentarios (Actual)	Comentarios (Meta)
KPI.1.1	Número de actuaciones de seguimiento de la superficie de exposición	Anual	Mensual	Se convoca una reunión anual de seguimiento de la Política de Seguridad de la Información	Se convoca una reunión mensual para el seguimiento de la superficie de exposición
KPI.1.2	Número de actuaciones de seguimiento de desarrollo de la plataforma de ciberseguridad	Ninguna	Semanal	No existen reuniones periódica para el seguimiento de desarrollos de ciberseguridad	Se convoca una reunión semanal para el seguimiento del desarrollo de la plataforma CTEM
KPI.2.1	Estado de la superficie de exposición	Sin visibilidad	Visibilidad completa	El valor de medición corresponde al riesgo global	Se puede comprobar diariamente la evolución del riesgo global en la plataforma CTEM
KPI.2.2	Porcentaje de activos identificados y controlados	30%	99.9%	Se lleva un control manual (i.e., hoja Excel) de los activos	Se realiza un seguimiento del porcentaje de activos identificados por herramientas XDR e ITSM/CMDB y EASM.

KPI.2.3	Porcentaje de activos parcheados	30%	99.9%	Principalmente a través de actualizaciones de seguridad de grandes fabricantes	Se realiza un seguimiento en la plataforma CTEM del porcentaje de activos parcheados.
KPI.2.4	Método de descubrimiento de activos TIC	Manual	Automático	Actualmente se descubren de forma manual	El descubrimiento de activos en automático gracias a herramientas EASM, XDR, y ITSM/CMDB
KPI.2.5	Método de comprobación del cumplimiento de configuración segura de los activos TIC	Local	Distribuido	Actualmente se comprueba la configuración mediante el despliegue de la herramienta CLARA [9] de forma local	Se realiza la comprobación de la configuración segura con herramientas EASM y VM.
KPI.2.6	Priorización de las acciones de mitigación de vulnerabilidades en los activos TIC	No existe	Automatizada	Se mitigan vulnerabilidades en base a actualizaciones proporcionadas por los fabricantes	Se priorizan las acciones de mitigación en base a su criticidad, capacidad de explotación, protección perimetral y criticidad del activo/servicio.
KPI.2.7	Tiempo medio de mitigación de una vulnerabilidad (MTTC ⁸⁸)	No se controla	Control diario	No se contempla el seguimiento de la tasa de corrección de cada vulnerabilidad.	Se realiza el seguimiento del tiempo de mitigación de cada vulnerabilidad.

⁸⁸ También se denomina tiempo media de corrección (MTTC, por sus siglas en inglés, *Mean Time to Contain*), en este caso de vulnerabilidades, siendo una métrica que se utiliza en ciberseguridad para medir el tiempo promedio de mitigación de una amenaza una vez ha sido detectada.

KPI.2.8	Número de tecnologías integradas para obtener información de la superficie expuesta	+5 ⁸⁹	1 ⁹⁰	Las herramientas no tienen comunicación entre sí, por lo que se pretenda integrar y centralizar la información proporcionada por cada herramienta	Se dispone de una única plataforma (i.e. CTEM) que cohesiona y correlaciona la información proporcionada por el resto de herramientas de ciberseguridad.
KPI.2.9	Monitorización de la conectividad de los distintos agentes de seguridad desplegados en la Organización	Mala	Muy buena	No se conoce el estado de despliegue de los agentes	Se dispone de un panel de monitorización en la plataforma para el seguimiento de la conectividad de los agentes desplegados en la plataforma.
KPI.2.10	Control de la telemetría de seguridad	Dispersa	Centralizada	Si bien se mandan logs a la plataforma de gestión de incidentes, existen logs de aplicaciones que se pierden	Se prevé centralización de los registros de seguridad en un único repositorio para su explotación en distintos casos de uso.
KPI.2.11	Número de servicios utilizados para obtener ciberinteligencia que permita una adecuada predicción de las ciberamenazas	+20 ⁹¹	-3 ⁹²	No existe un equipo de evaluación de amenazas	Existe un Equipo de Evaluación de Amenazas que realiza una constante evaluación de la superficie.

⁸⁹ Existen más de 5 herramientas de ciberseguridad desplegadas en la infraestructura, no siendo cohesionados ni correlacionados los datos obtenidos.

⁹⁰ El objetivo ha sido integrar los datos de todas la herramientas de ciberseguridad desplegadas en la infraestructura en una única plataforma.

⁹¹ Existen más de 20 servicios de ciberinteligencia, proporcionados por el CCN o Incibe.

⁹² El objetivo es disponer de fuentes centralizadas, menos de 3, que proporcionen datos de inteligencia de forma integrada.

KPI.3.1	Porcentaje de activos bastionados (cumplen configuración segura según guías CCN ⁹³ -STIC)	60%	99.9%	Se lleva a cabo la configuración segura de forma manual	Se realiza una comprobación periódica de forma automatizada del cumplimiento con guías de seguridad para cada activo.
KPI.3.2	Tasa de cumplimiento del Esquema Nacional de Seguridad (ENS)	1%	99.9%	Existen servicios en proceso de certificación del ENS	Se ha desarrollado toda la documentación la certificación de ENS del sistema de información vertebral de la infraestructura.
KPI.3.3	Tasa de cumplimiento con regulación europea	30%	99.9%	Se están empezando a incluir cláusulas en las licitaciones contemplando regulaciones de certificación y cualificación de productos	Se hace un seguimiento por parte del Equipo de Seguridad para el cumplimiento de certificación de seguridad de productos digitales.

Tabla 5 Indicadores clave de rendimiento para medir la superficie de exposición [Fuente Propia]

Dada la información recopilada en la lista de indicadores de rendimiento, para el cumplimiento de los objetivos fijados inicialmente, se considera que se ha alcanzado un nivel de cumplimiento cercano al 100% de los criterios establecidos en el proceso de verificación de KPI. Algunos elementos de cumplimiento adicional se integrarán en un futuro próximo para lograr la totalidad del cumplimiento de los objetivos.

4.5 Validación de la plataforma SUPERFICIE como enfoque CTEM

Para poder validar si la plataforma SUPERFICIE proporciona realmente las funcionalidades atribuidas a la tecnología CTEM [41] se ha llevado a cabo una prueba de valor (PoV⁹⁴) que conlleva la comprobación de una serie de pasos de la siguiente lista de verificación [17]:

⁹³ El CCN es el organismo responsable de garantizar la seguridad de los servicios de tecnologías de la información y comunicaciones en las diferentes entidades de la Administración Pública, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.

⁹⁴ Una prueba de valor (PoV) se refiere en este contexto a una evaluación o demostración que tiene como objetivo demostrar la eficacia de la plataforma desarrolla contra los requisitos definidos para el enfoque CTEM.

Cumple	Requisito	Directrices	Observaciones
ALCANCE			
(Esta fase consiste en la clasificación de las vulnerabilidades según la información de riesgo y activos)			
Sí	Construye un modelo de las relaciones organizativas en relación con la entidad matriz, incluyendo entidades subsidiarias u otras entidades asociadas.	<i>Asegurar que la herramienta proporcione reconocimiento totalmente automatizado de la estructura organizativa a nivel global, con recopilación de evidencia para cada decisión.</i>	A través de la estructura de roles y privilegios en función de su posición dentro de la organización (Organización, Ámbito, Área).
Sí	Descubre automáticamente nuevas organizaciones y cambios en las organizaciones existentes.	<i>Las herramientas que requieren entrada manual para mantenerse al tanto de los cambios no tienen el nivel de sofisticación necesario para CTEM.</i>	A través de herramientas EASM, ITSM/CMDB y XDR.
Sí	Proporciona un camino de descubrimiento claramente definido para todas las organizaciones descubiertas.		A través de herramientas EASM, ITSM/CMDB y XDR.
Sí	No requiere información de entrada o datos iniciales para descubrir organizaciones.		Requiere indicar al menos la denominación de la organización o rango de IP (opcional) a la herramienta EASM.
DESCUBRIMIENTO			
(Esta fase consiste en el descubrimiento y prueba de los activos de la superficie externa)			
DESCUBRIMIENTO DE ACTIVOS			
Sí	Descubre automáticamente activos expuestos en rangos de IP conocidos y nuevos (aquellos descubiertos durante el reconocimiento organizacional).	<i>Asegurar que la herramienta proporcione descubrimiento automático de activos en toda la organización. La evidencia de descubrimiento y la puntuación de confianza son fundamentales para esta fase de CTEM.</i>	A través de herramientas EASM.
Sí	Descubre automáticamente activos internos previamente identificados y nuevos (aquellos descubiertos durante el reconocimiento organizacional).		A través de herramientas XDR, VM, ITSM/CMDB y NAC.

Sí	Muestra la relación de activos relacionados entre sí.	<i>Las herramientas que solo buscan activos dentro de rangos de IP preconfigurados no pueden escalar para satisfacer los requisitos de la organización.</i>	A través de herramientas ITSM/CMDB.
Sí	Proporciona un camino de descubrimiento claramente definido para todos los activos descubiertos.		A través de agentes desplegados en los activos de la organización y herramientas ITSM/CMDB sin agente.
Sí	Ofrece opciones de descubrimiento de activos de alta frecuencia (diaria/semanal/bisemanal/mensual).		El descubrimiento de servidores es diario, el de estaciones de trabajo y activos externos semanal.

ATRIBUCIÓN DE ACTIVOS

Sí	Tecnologías más vulnerables (incluidos Sistemas Operativos)	<i>Asegurar que la herramienta proporcione contexto de atribución automatizado para acelerar la reparación y permitir mensajes de CTEM dirigidos.</i> <i>La automatización es clave. Realizar la atribución manualmente puede llevar de 5 a 10 horas por activo.</i>	Detecta las vulnerabilidades en todos los activos, incluyendo el software desplegado en estos activos a través de herramientas XDR, VM, y NAC.
----	---	---	--

CLASIFICACIÓN DE ACTIVOS

Sí	Clasifica los activos según el contexto	<i>Asegurar que la herramienta proporcione contexto organizacional junto con el propósito del activo y los servicios en ejecución para permitir una priorización precisa en el proceso de mitigación.</i>	Clasifica los activos y los atribuye al Ámbito y Área correspondiente. Incluye demás información del servicio(s) que despliega. Se realiza a través de la clasificación previa de los activos según su nomenclatura, junto con herramientas ITSM/CMDB.
Sí	Determina de la criticidad del activo para la organización	<i>Las herramientas que se centran solo en los servicios en ejecución carecen de la información necesaria</i>	A través de herramientas EASM para activos de la superficie externa, y manualmente cuando se despliega un activo en la superficie interna (la actualización posterior es en parte automática).

Sí	Identifica de las aplicaciones y sus elementos claves	<i>para tomar decisiones efectivas.</i>	Identifica todo el software de cada uno de los activos con herramientas XDR, VM, ITSM/CMDB y NAC.
NS/NC	Identifica activos en la nube y sus componentes clave		No se han considerado activos en la nube.
DETECCIÓN DE RIEGOS			
Sí	Identifica las vulnerabilidades para cada activo	<i>Asegurarse de realizar pruebas activas completas en todos los activos externos de forma continua para obtener una visibilidad integral del riesgo externo.</i>	Identifica las vulnerabilidades con herramientas EASM para los activos de la superficie externa, y con herramientas VM para activos de la superficie interna.
Sí	Busca vulnerabilidades en todos los activos	<i>Las herramientas que se centran en los resultados del escaneo pasivo (también conocido como banner grabbing) tanto para el descubrimiento de activos como para la detección de riesgos generan numerosos falsos positivos y carecen de riesgos verificados. El escaneo pasivo tampoco es capaz de identificar riesgos complejos ni de verificar el éxito de los esfuerzos de mitigación de vulnerabilidades.</i>	Busca las vulnerabilidades con herramientas EASM para los activos de la superficie externa, y con herramientas VM para activos de la superficie interna.
Sí	Busca vulnerabilidades CVE de todos los activos internos.		Busca las vulnerabilidades con herramientas VM para activos de la superficie interna.
Sí	Busca vulnerabilidades OWASP Top 10 en las aplicaciones web		Identifica las vulnerabilidades OWASP Top 10 con herramientas EASM para los activos de la superficie externa.
Sí	Busca debilidades o credenciales por defecto en servicios con autenticación		Busca credenciales por defecto en servicios con autenticación a través de herramienta EASM en activos de la superficie externa.
Sí	Detecta datos expuestos y clasifica los datos según su sensibilidad		Detecta datos expuestos y clasifica los datos según su sensibilidad a través de herramienta EASM en activos de la superficie externa.
Sí	Proporciona detección de riesgos de forma periódica (diaria/semanal/bimensual/mensual).		Proporciona detección de riesgos diariamente para servidores y semanalmente estaciones de trabajo de la superficie interna con herramientas VM. Para los activos de la superficie externa la detección es semanal con herramientas EASM.
Sí	Proporciona actualización de riesgos de forma		Proporciona actualización de riesgos diariamente para

	periódica (diaria/semanal/bimensual/ mensual).		servidores y semanalmente estaciones de trabajo de la superficie interna con herramientas VM. Para los activos de la superficie externa la detección es semanal con herramientas EASM.
Sí	Proporciona pruebas de seguridad activa de forma periódica (diaria/semanal/bimensual/ mensual).		Proporciona pruebas de seguridad activa diariamente para servidores y semanalmente estaciones de trabajo de la superficie interna con herramientas VM. Para los activos de la superficie externa la detección es semanal con herramientas EASM.
Sí	Valida los esfuerzos de mitigación mediante pruebas activas		Valida los esfuerzos de mitigación con cada análisis realizado de las herramientas VM y EASM.
Sí	Documenta la evidencia de riesgo por activo		Todas las evidencias de riesgo proporcionadas por cada activo se muestra en la plataforma a través de la información proporcionada por las herramientas VM y EASM.

PRIORIZACIÓN

(Esta fase consiste en la clasificación de las vulnerabilidades según la información de riesgo y la del propio activo)

Si	Clasifica las vulnerabilidades según la disponibilidad del <i>exploit</i> (gracias al conocimiento de inteligencia de amenazas)	<i>Asegurarse de que los datos de priorización incluyan inteligencia de amenazas actualizada y contexto empresarial para comprender el verdadero riesgo para tu organización.</i>	Clasifica las vulnerabilidades según el valor EPSS.
Sí	Realiza la búsqueda de vulnerabilidades propietarias para mejorar la priorización	<i>Las herramientas que dependen únicamente de la información CVSS para la priorización de riesgos no se alinean con los requisitos comerciales de la organización.</i>	Busca vulnerabilidades propietarias para mejorar la priorización de los activos de la superficie externa.
Sí	Clasifica la exposición según el nivel de riesgo		Clasifica la criticidad de las vulnerabilidades según el valor CVSS, EPSS y la protección del Equipo de Seguridad Perimetral para los activos de la superficie interna.

Sí	Clasifica la vulnerabilidades según la severidad	Clasifica la criticidad de las vulnerabilidades según el valor CVSS, EPSS y la protección del Equipo de Seguridad Perimetral para los activos de la superficie interna.
----	--	---

VALIDACIÓN

(Esta fase consiste en la evaluación de la probabilidad de éxito del atacante y la estimación del impacto)

Sí	Clasifica las vulnerabilidades en base al descubrimiento del activo	<i>Asegurar que la herramienta asigne automáticamente una clasificación de priorización de problemas basada en pruebas activas validadas e información de inteligencia de amenazas.</i>	Clasifica las vulnerabilidades en función de la posibilidad de explotación con herramientas EASM para los activos de la superficie externa y VM para los activos de la superficie interna.
Sí	Clasifica las vulnerabilidades en base a la criticidad del activo	<i>Las herramientas que no realizan pruebas activas de vulnerabilidades generarán muchos falsos positivos y esfuerzos desperdiciados.</i>	Clasifica las vulnerabilidades en función de la criticidad con herramientas EASM para la superficie externa y VM para la superficie interna.
Sí	Prioriza los principales vectores críticos de ataque		Prioriza los vectores de ataque con herramientas EASM para la superficie externa. Pendiente de integración de herramientas BAS para la superficie interna junto con la trazabilidad del vector entre el activo externo y el interno.
Sí	Recopila evidencias para todos los resultados de escaneo y pone a disposición la evidencia a través de la consola y la interfaz de programación de aplicaciones (API).		Recopila las evidencias de los resultados de los escaneos y se visualizan en la plataforma CTEM. La información se obtiene de herramientas EASM para los activos de la superficie externa y VM para los activos de la superficie interna.

MOBILIZACIÓN

(Esta fase consiste en informar de las vulnerabilidades a los responsables de la mitigación)

Sí	Proporciona instrucciones de prueba para simplificar la validación	<i>Asegurar que la herramienta proporcione un contexto preciso del problema que incluya la disponibilidad de exploits, el interés del</i>	Proporciona instrucciones de prueba para comprobar la existencia de vulnerabilidades con información propuesta por herramientas VM para la superficie interna y EASM para la superficie externa.
----	--	---	--

Sí	Proporciona una planificación de mitigación trazable tanto dentro de la organización como en cada ámbito o área.	<i>atacante, las herramientas de explotación, el esfuerzo de remediación y las instrucciones de remediación.</i> <i>Las herramientas que requieren una investigación adicional para obtener orientación sobre la remediación no pueden adaptarse a los requisitos empresariales a gran escala.</i>	Proporciona instrucciones para mitigar las vulnerabilidades propuestas por herramientas VM para la superficie interna y EASM para la superficie externa. Además el Equipo de Seguridad defensiva puede proponer acciones de mitigación alternativas.
Sí	Proporciona métricas para mostrar la mejora en la postura de riesgo con el tiempo y para visualizar las tendencias de remediación a lo largo del tiempo		Proporciona cálculos automatizados del riesgo global con información proporcionada por herramientas EASM y VM. También se han incorporado cálculos con modelos de aprendizaje automático.
Sí	Proporciona métricas para mostrar las acciones de mitigación a lo largo del tiempo		Proporciona un histórico de resolución de vulnerabilidades y KPI para ver su evolución según Ámbitos.
Sí	Incluye automatización de flujo de trabajo e integración de comunicación a través de API para proporcionar información sobre vulnerabilidades		Proporciona automatización de flujos de trabajo de mitigación de vulnerabilidades. El Equipo de Seguridad Defensiva puede notificar acciones de seguimiento de vulnerabilidades a través de la plataforma CTEM.

Tabla 6 Validación de la plataforma SUPERFICIE como CTEM [17]

Dada la información recopilada en la lista de verificación para la validación de la plataforma SUPERFICIE como CTEM, se ha alcanzado un grado de realización cercano al 100% de los criterios establecidos en el proceso de validación. Algunos elementos adicionales se integrarán en un futuro próximo para lograr la totalidad de los objetivos.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

Tradicionalmente, la mejora en la seguridad de una infraestructura ha consistido en ir incorporando cada vez más herramientas de ciberseguridad que, de forma automatizada, detecten vulnerabilidades, y vayan limitando el potencial de un ataque. Por otra parte, se han ido consolidando figuras con roles relevantes en seguridad, contando casi cualquier organización con la figura de un CISO y un departamento de ciberseguridad. Pero si realmente una organización quiere mejorar la seguridad de sus infraestructuras TIC, necesita reducir sus debilidades, con una priorización adecuada y una movilización de sus tropas inmediata, una vez que sepa dónde está situado el enemigo y cuál es la configuración del terreno. Sin olvidar que todos los roles de la organización requieren un trabajo conjunto en el día a día para estar siempre por delante del enemigo. Para ello, cada rol contribuirá con su conocimiento intrínseco, y aportará su capacidad para fortalecer la infraestructura y hacerla inexpugnable.

Por otra parte, gracias a la definición de indicadores de rendimiento que se pueden verificar en la operación diaria de la propia plataforma CTEM (tal y como se ha comprobado en 4.4 Verificación de los KPI con la plataforma CTEM), se posibilita el seguimiento de los valores de partida y la medición periódica del progreso de la plataforma hacia los objetivos establecidos. Este trabajo ha expuesto con precisión la medición de los valores iniciales y su consecución, alcanzando un grado de realización cercano al 100% de los criterios previamente establecidos.

El siguiente modelo mostrado en la Figura 35, y propuesto por Gartner, puede ayudar a una organización a priorizar sus acciones para la mejora de la ciberresiliencia y muestra cómo la madurez de los pasos individuales del programa CTEM puede diferir y evolucionar a diferentes velocidades. Como es bastante habitual, el camino rápido (adquisición compulsiva de las herramientas más punteras en el mercado de la ciberseguridad) ayuda a los equipos de seguridad a ganar batallas. Sin embargo, un progreso desequilibrado podría limitar seriamente ganar la guerra, especialmente cuando se tarda demasiado tiempo en mitigar una vulnerabilidad una vez que se ha establecido previamente su existencia (demasiado tiempo entre el paso de descubrimiento y el de movilización).

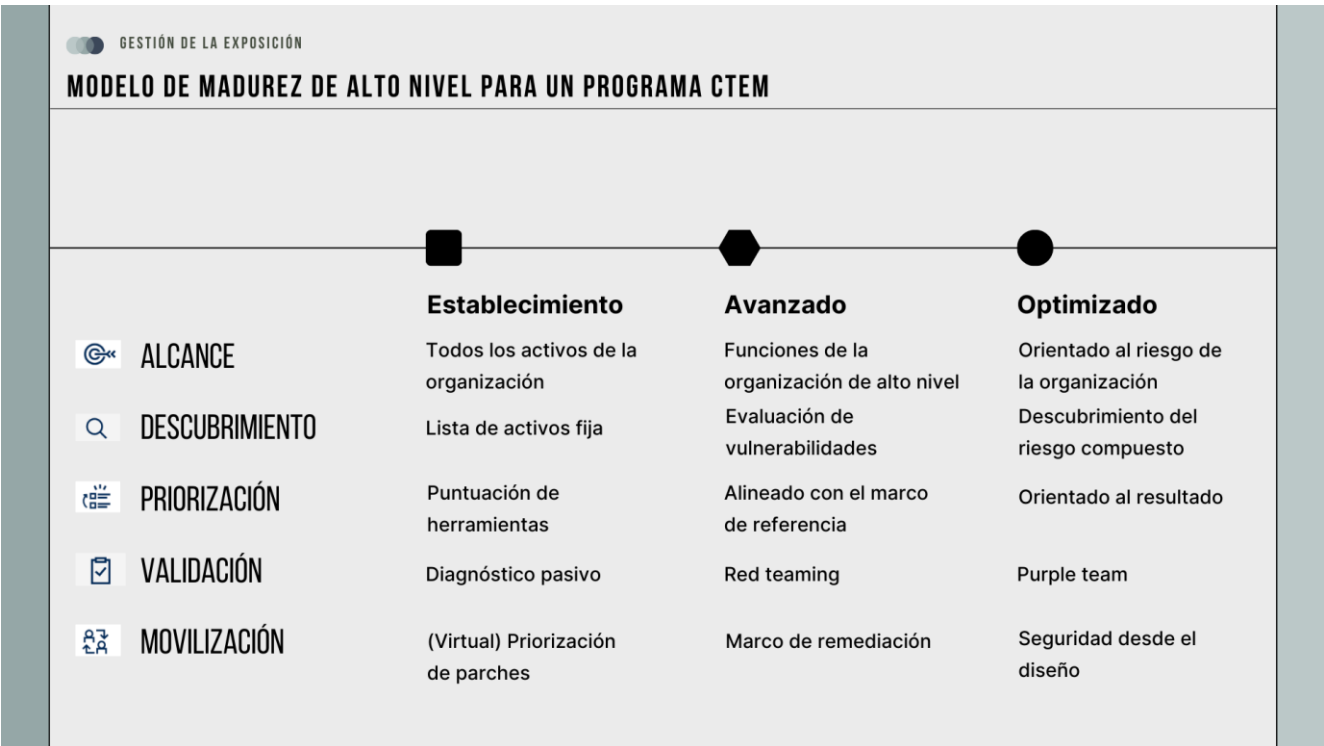


Figura 35 Modelo de madurez de alto nivel para un programa CTEM [16]

En conclusión, para lograr un nivel avanzado de madurez siguiendo el programa CTEM y alcanzar una optimización máxima, es esencial seguir una serie de pasos clave. Éstos incluyen la medición sistemática del nivel de riesgo de la organización, la identificación proactiva de riesgos a través del aprendizaje y la predicción de amenazas futuras, la priorización de acciones de mitigación basadas en evaluaciones previas de amenazas, la integración de las capacidades del Equipo de Evaluación de Amenazas con las del Equipo de Seguridad Defensiva, y la incorporación de nuevos desarrollos diseñados con enfoque en la seguridad. Al implementar de manera óptima estas etapas, se logrará una infraestructura resiliente y mejor preparada para resistir los embates del enemigo.

5.2 Líneas futuras

Las líneas futuras que van a marcar los siguientes pasos en ciberresiliencia, y que concretamente marcarán el desarrollo de plataformas que sigan el programa CTEM, están vinculadas con las herramientas e iniciativas que se incluyen en la etapa de “desencadenante de la innovación” según Gartner [16]. Además, se contempla la integración estratégica y coordinación del Equipo de Evaluación de Amenazas con su némesis, el Equipo de Seguridad Defensiva.

Se ilustra a continuación en la Figura 36 un resumen de las líneas futuras que se seguirán para mejorarla ciberresiliencia en una infraestructura TIC.



Figura 36 Líneas futura para la reducción de la superficie de exposición – Mejora de la ciberresiliencia

6 BIBLIOGRAFÍA

- [1] J. M. Millán Martínez, «Operaciones en el ciberespacio: ¿esas desconocidas?,» *Revista Ejército*, nº 972, 2022.
- [2] S. Tzu, *El arte de la guerra*, Siglo V AC.
- [3] J. López de Turiso y Sánchez, «La evaluación del conflicto hacia un nuevo escenario bélico,» *Monografías del CESEDEN*, nº 126, 2012.
- [4] M. De Álvaro Mizzian, «El ciberespacio en tiempos de guerra: la IT Army ucraniana,» *Instituto Español de Estudios Estratégicos - Documento Opinión*, 2023.
- [5] S. Freedberg JR, «Russian phishing attacks flooded Ukraine, tripled against NATO nations in 2022: Report,» 16 February 2023. [En línea]. Available: <https://breakingdefense.com/2023/02/russian-phishing-attacks-flooded-ukraine-tripled-against-nato-nations-in-2022-report/>.
- [6] RedHat, «Standardize to improve IT efficiency,» 2021. [En línea]. Available: <https://www.redhat.com/en/resources/standardize-to-improve-efficiency-e-book>.
- [7] ACPV, «NATO Communications and Information Agency,» 2022. [En línea]. Available: <https://www.ncia.nato.int/business/current-opportunities/ifb/115699-ACPV.html>.
- [8] «REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la,» *Diario Oficial de la Unión Europea*, nº L 151/15, 2019.
- [9] CCN-CERT, «CLARA (Soluciones de Seguridad),» [En línea]. Available: <https://www.ccn-cert.cni.es/es/soluciones-seguridad/clara.html>.
- [10] Ministerio de Asuntos Económicos y Transformación , «Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad,» *Boletín Oficial del Estado*, nº BOE-A-2022-7191, 2022.
- [11] «DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y,» *Diario Oficial de la Unión Europea*, nº L 194/1.
- [12] M. Hubbard, «What is Attack Surface Management and What Role Does CAASM Play?,» 10 Abril 2023. [En línea]. Available: <https://www.armis.com/blog/what-is-attack-surface-management-and-what-role-does-caasm-play/>.
- [13] C. Crandall, «TechTarget - IoT Agenda - Emerging IoT attack surfaces present attackers with tempting new targets,» 8 Oct 2019. [En línea]. Available: <https://www.techtarget.com/iotagenda/blog/IoT-Agenda/Emerging-attack-surfaces-present-attackers-with-tempting-new-targets>.
- [14] X. E. Shen, S. L. Liu y C. H. Fan, «Preprints.org - Honeypots for Internet of Things Research: An Effective Mitigation Tool,» 2021. [En línea]. Available: <https://www.preprints.org/manuscript/202109.0461/v1>.
- [15] K. T. Hanna, «TechTarget - Whatis - Attack surface,» 2023. [En línea]. Available: <https://www.techtarget.com/whatis/definition/attack->

surface#:~:text=An%20attack%20surface%20is%20defined,carry%20out%20a%20security%20attack..

- [16] J. D'Hoine, P. Shoard y M. Schneider, «Implement Continuous Threat Exposure Management (CTEM) Program,» 21 July 2022. [En línea]. Available: <https://www.gartner.com/doc/reprints?id=1-2APCAC3H&ct=220729&st=sb>.
- [17] Cycognito, «Demystifying Continuous Threat Exposure Management (CTEM),» 2023. [En línea]. Available: <https://www.cycognito.com/resources/solution-brief/demystifying-continuous-threat-exposure-management-ctem>.
- [18] Cymulate, «Implementing CTEM with Cymulate,» 2022. [En línea]. Available: [https://4347852.fs1.hubspotusercontent-na1.net/hubfs/4347852/eBook/Implementing%20Continuous%20Threat%20Exposure%20Management%20\(CTEM\)%20-%20August%202022.pdf](https://4347852.fs1.hubspotusercontent-na1.net/hubfs/4347852/eBook/Implementing%20Continuous%20Threat%20Exposure%20Management%20(CTEM)%20-%20August%202022.pdf)2022.
- [19] MITRE, «MITRE | ATT&CK,» [En línea]. Available: <https://attack.mitre.org/>.
- [20] Cycognito, «Discovery and Contextualization,» 2023. [En línea]. Available: <https://www.cycognito.com/resources/data-sheet/discovery-and-contextualization>.
- [21] N. Wenzler, «Tenable Blog - Exposure Management: Reducing Risk in the Modern Attack Surface,» 4 Oct 2022. [En línea]. Available: <https://www.tenable.com/blog/exposure-management-reducing-risk-in-the-modern-attack-surface>.
- [22] J. D'Hoine, P. Shoard y J. W. Schneider, «Predicts 2023: Enterprises Must Expand From,» 1 December 2022. [En línea]. Available: <https://www.gartner.com/en/documents/4021605>.
- [23] P. L. «What Is Cyber Asset Attack Surface Management (CAASM)?,» 31 Mayo 2023. [En línea]. Available: <https://www.picussecurity.com/resource/glossary/what-is-cyber-asset-attack-surface-management-caasm>.
- [24] Á. San José Arranz, La ciberseguridad y sus herramientas, Universidad de Vigo, 2022.
- [25] J. Nunez y A. Davies, «Hype Cycle for Security Operations, 2023,» Gartner, 2023.
- [26] P. L. «What Is Automated Security Control Assessment (ASCA)?,» 7 septiembre 2023. [En línea]. Available: <https://www.picussecurity.com/resource/glossary/what-is-automated-security-controls-assessment>.
- [27] runZero, «runZero,» [En línea]. Available: <https://www.runzero.com/>.
- [28] S. Kaelble, R. Gurzeev y D. Potekhin, External Exposure & Attack Surface Management For Dummies, 111 River St. Hoboken NJ 07030-5774: John Wiley & Sons, Inc., 2023.
- [29] SafeBreach - GUIDE, «What is breach and attack simulation (BAS)?,» [En línea]. Available: <https://www.safebreach.com/breach-and-attack-simulation/>.
- [30] A. S. «Online brand protection: a guide busy person's guide,» 2023. [En línea]. Available: <https://alluresecurity.com/online-brand-protection/>.
- [31] M. Abraham, «IDC - Market Share - Worldwide Device Vulnerability Management Market Shares,» 2022. [En línea]. Available: https://static.tenable.com/marketing/research-reports/AnalystReport-IDC_Worldwide_Device_Vulnerability_Management_Market_Shares_Report_2021.pdf.

- [32] National Cyber Security Division, «MITRE CVE List,» Estados Unidos, [En línea]. Available: <https://cve.mitre.org/index.html>.
- [33] M. Curphey y D. Groves, «Open Web Application Security Project (OWASP),» 2023. [En línea]. Available: <https://owasp.org/>.
- [34] CCN-CERT, «Índice de guías,» [En línea]. Available: <https://www.ccn-cert.cni.es/guias/indice-de-guias.html>.
- [35] CCN-CNI, «Esquema Nacional de Seguridad (ENS),» 3 mayo 2022. [En línea]. Available: <https://www.boe.es/eli/es/rd/2022/05/03/311>.
- [36] CCN-CNI, «CPSTIC,» 2023. [En línea]. Available: <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html>.
- [37] Agencia de la Unión Europea para la Ciberseguridad, «INFORME «PANORAMA DE AMENAZAS» DE ENISA DE 2019, 2021,» 2021-222. [En línea]. Available: https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_es.pdf.
- [38] «Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020,» EUR-Lex, nº Document 52022PC0454, 2022.
- [39] «Tenable - 3 Real-world challenges facing cybersecurity organizations, How and exposure management platform can hel,» 2022. [En línea]. Available: <https://www.tenable.com/whitepapers/3-real-world-challenges-facing-cybersecurity-organizations-how-an-exposure-management>.
- [40] CCN-CERT, «REYES (Soluciones de Seguridad),» [En línea]. Available: <https://www.ccn-cert.cni.es/es/soluciones-seguridad/reyes.html>.
- [41] P. L. «What Is Continuous Threat Exposure Management (CTEM)?,» 03 july 2023. [En línea]. Available: <https://www.picussecurity.com/resource/glossary/what-is-continuous-threat-exposure-management-ctem>.
- [42] R. Circus, «ISACA Journal - Indicadores de exposición y visualización de superficie de ataque,» 20 Feb 2017. [En línea]. Available: <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/sponsored-feature-indicators-of-exposure-and-attack-surface-visualization>.
- [43] A. Bhardwaj y S. Goundar, «ScienceDirect - Reducing the threat surface to minimise the impact of cyber-attacks,» Abr 2018. [En línea]. Available: <https://www.sciencedirect.com/science/article/abs/pii/S1353485818300345>.
- [44] J. D'Hoine y P. Shoard, «Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management,» 16 october 2023. [En línea]. Available: https://www.gartner.com/doc/reprints?__hstc=7655085.8be9c75ddff66e41435b3a5b38981419.1703156306240.1703156306240.1703156306240.1&__hssc=7655085.1.1703156306240&__hsfp=2009540761&id=1-2FEADHJZ&ct=231023&st=sb&submissionGuid=07d07a0f-88ef-4a55-9ac7-cb7f166e.

ANEXO I: ACRÓNIMOS

ACPV	Activos, configuración, parches y vulnerabilidad, por sus siglas en inglés
API	Interfaz de programación de aplicaciones, por sus siglas en inglés
APT	Amenaza persistente avanzada, por sus siglas en inglés
ASCA	Evaluación automatizada de controles de seguridad, por sus siglas en inglés
BAS	Simulación de ataques, por sus siglas en inglés
CAASM	Gestión de la superficie de ataque de ciberactivos, por sus siglas en inglés
CCN	Centro Criptológico Nacional
CDO	Responsable del dato, por sus siglas en inglés
CIO	Responsable de la información, por sus siglas en inglés
CISO	Responsable de seguridad de la información, por sus siglas en inglés
CMDB	Base de datos de la configuración del sistema, por sus siglas en inglés
CPSTI	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación
CRA	Ley de Ciberresiliencia europea
CRON	Comando que se ejecuta previo aviso, por sus siglas en inglés
CTEM	Gestión continua de la superficie de exposición a amenazas, por sus siglas en inglés
CVE	Enumeración común de vulnerabilidades y exposiciones, por sus siglas en inglés
CVSS	Sistema de Puntuación de Vulnerabilidad Común, por sus siglas en inglés
CWE	Enumeración común de debilidades, por sus siglas en inglés
DAST	Pruebas de seguridad de aplicaciones dinámicas, por sus siglas en inglés
DDoS	Ataque de denegación de servicio, por sus siglas en inglés
DLP	Prevención de pérdida de datos, por sus siglas en inglés
DRPS	Servicios de protección de riesgos digitales, por sus siglas en inglés
EASM	Gestión de la superficie de exposición externa, por sus siglas en inglés
ENISA	Agencia Europea para la Ciberseguridad
ENS	Esquema Nacional de Seguridad
EPSS	Sistema de evaluación de predicción de la explotación, por sus siglas en inglés
KPI	Indicador de rendimiento, por sus siglas en inglés
IoC	Indicador de compromiso, por sus siglas en inglés
IoT	Internet de las cosas, por sus siglas en inglés
IP	Protocolo de Internet, por sus siglas en inglés
ITOM	Gestión de operaciones de tecnologías de la información, por sus siglas en inglés
ITSM	Gestión de servicios de tecnologías de la información, por sus siglas en inglés

MFA	Autenticación multifactor, por sus siglas en inglés
MTTC	Tiempo medio de corrección, por sus siglas en inglés
MTTD	Tiempo medio de detección, por sus siglas en inglés
MTTI	Tiempo medio de identificación, por sus siglas en inglés
MTTR	Tiempo medio de respuesta, por sus siglas en inglés
NAC	Control de acceso a red, por sus siglas en inglés
NCIA	<i>NATO Communication and Information Agency</i>
NDR	Detección y respuesta de red, por sus siglas en inglés
NIST	Instituto Nacional de Estándares y Tecnologías, por sus siglas en inglés
OT	Tecnología de operación, por sus siglas en inglés
OTAN	Organización del Tratado del Atlántico Norte
OWASP	Proyecto de aplicaciones web abierto, por sus siglas en inglés
PoC	Prueba de concepto, por sus siglas en inglés
PoV	Prueba de valor, por sus siglas en inglés
REST	Transferencia de estado representacional, por sus siglas en inglés
ROI	Retorno de inversión, por sus siglas en inglés
SIEM	Gestión de eventos e información de seguridad, por sus siglas en inglés
SO	Sistema Operativo, , por sus siglas en inglés
SOC	Centro de operaciones de seguridad, por sus siglas en inglés
TIC	Tecnologías de la información y la comunicación
TTP	Tácticas, técnicas y procedimientos, por sus siglas en inglés
VM	Gestión de vulnerabilidades, por sus siglas en inglés
WAF	Cortafuegos de aplicaciones web, por sus siglas en inglés
XDR	Detección y respuesta extendida, por sus siglas en inglés
XSS	Secuencia de comandos en sitios cruzados, por sus siglas en inglés