Universitat Oberta de Catalunya

uoc.edu

Caso práctico de una prueba de concepto de tres herramientas de gestión y análisis de vulnerabilidades

Beatriz Cortés Santamaría

Máster Universitario en Ciberseguridad y Privacidad

Seguridad empresarial

María Francisca Hinarejos Campos

Junio - 2021

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Caso práctico de una prueba de concepto de tres herramientas de gestión y análisis de vulnerabilidades*
Nombre del autor:	*Beatriz Cortés Santamaría*
Nombre del consultor/a:	*María Francisca Hinarejos Campos*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2021
Titulación:	*Máster Universitario en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*Seguridad empresarial*
Idioma del trabajo:	*Español*
Palabras clave	*Ciberseguridad, Detección de vulnerabilidades, Herramientas de gestión, Análisis comparativo*

Resumen del Trabajo:

El objetivo de este trabajo es la realización de una prueba de concepto para la elección de una herramienta de gestión de vulnerabilidades en una empresa real. Para ello, se ha realizado el estado del arte sobre el proceso de gestión de vulnerabilidades y se han estudiado diferentes trabajos de comparaciones entre herramientas de gestión de vulnerabilidades, con el objetivo de identificar los criterios utilizados para compararlas. Una vez realizada esta investigación y definida la base teórica, se ha identificado la necesidad de implantación de este tipo de herramienta en la empresa, analizando el contexto de la compañía

Para realizar la selección de la herramienta, se ha definido un procedimiento de evaluación, el cual consiste en definir unos criterios generales, basándose en la base teórica definida, y en unos criterios específicos basados en la necesidad de la empresa. Estos criterios se han ponderado con porcentajes para establecer cuánto peso tendrán sobre la calificación final. Finalmente, se han probado las tres herramientas líderes en el mercado para evaluar cada uno de los criterios. Como resultado, se obtiene una calificación final de las tres herramientas, siendo la herramienta con mejor puntuación la herramienta seleccionada por la compañía para implementar en su proceso de gestión de vulnerabilidades.

Abstract in English:

The purpose of this work is the performance of a proof of concept for the choice of a vulnerability management tool in a real company. For this purpose, the state of the art in vulnerability management process and different comparisons between vulnerability management tools have been studied in order to identify the criteria used to compare them. Once this research has been made and theoretical basis has been defined, the need to implement this kind of tool in the company has been identified, analyzing the company's context.

To select the vulnerability management tool, an evaluation procedure has been defined. This procedure consists of defining general criteria, based on the defined theoretical basis, and specific criteria based on the need of the company. These criteria have been weighted with percentages to establish how much weight they will have on the final score. Finally, the three leading tools in the market have been tested to evaluate each of the criteria. As a result, a final rating of the three tools has been calculated, being the tool with the best score the tool selected by the company to implement in the vulnerability management process.

Índice

Lista de tablas

Lista de figuras

1 Introducción

1.1 Contexto y justificación del Trabajo

Hoy en día, las empresas se enfrentan cada vez más a cambios y desafíos respecto a la seguridad en Internet, debido al continuo cambio en las tecnologías. Estos cambios en las tecnologías y el aumento de su utilización, hace que cada año se encuentren cada vez más vulnerabilidades en los sistemas. En un informe de Redscan, donde se realiza un análisis de vulnerabilidades identificadas en 2020 ((NIST National Vulnerability Database Analysis 2021), indica que es el año que más vulnerabilidades se han identificado y, de estas vulnerabilidades, el 57% son clasificadas como críticas o altas. Además, las vulnerabilidades que no requieren interacción del usuario han aumentado un 68% con respecto al año anterior. Debido a este aumento, las compañías ven cada vez más la necesidad de implicarse en la gestión y el análisis de vulnerabilidades de los sistemas.

Este aumento de vulnerabilidades es un punto que preocupa bastante a las empresas, no sólo por las vulnerabilidades que puedan tener sus propios activos sino también los activos de otras empresas con las que trabajan. Por esta razón, las empresas cada vez más se sienten más cómodas trabajando con otras empresas que demuestren su gestión en la seguridad y en las vulnerabilidades de sus activos.

Una de las certificaciones en seguridad cada vez más demandada es la ISO27001. Esta norma proporciona unos requisitos para la implementación de un sistema de gestión de la seguridad de la información (UNE-EN ISO/IEC 27001 2017) y, con la certificación, la empresa demuestra que estos se cumplen. Y en su anexo, donde se incluyen una serie de controles que debe tener en cuenta la empresa para implementar, incluye un apartado donde indica que las empresas deben disponer de un procedimiento gestión de vulnerabilidades de sus activos. Por tanto, con esta certificación la empresa puede demostrar que dispone de una correcta gestión de seguridad, incluyendo la gestión de vulnerabilidades.

Otra forma de demostrar las compañías que tienen un nivel alto en seguridad es contratando los servicios de empresas externas expertas en ciberseguridad que revisen sus activos publicados en internet y evalúen su nivel en ciberseguridad con una puntuación que será pública para sus clientes y/o proveedores. Una de las empresas líder en realizar este tipo de evaluaciones es Bitsight, la cual analiza y clasifica periódicamente su nivel en ciberseguridad en base a las vulnerabilidades identificadas en los activos publicados en Internet que la empresa tiene en dominio (BitSight Technologies s. f.) y permite comparar este nivel con otras compañías. De esta forma, la empresa puede destacar respecto a sus competidores a nivel de seguridad y dar mayor confort al cliente.

Dentro de esta preocupación de demostrar un alto nivel en la gestión de la seguridad, entra una empresa distribuidora de material farmacéutico. En esta empresa, están cada vez más preocupados con respecto a la seguridad y quieren dar mayor tranquilidad a sus clientes demostrando su correcta gestión

en seguridad. Por tanto, deciden certificarse en la ISO27001 y contratar a Bitsight para que puntúe su nivel de seguridad en sus activos publicados.

Debido a estas dos decisiones, surge la necesidad de implementar un proceso de gestión de vulnerabilidades y, por tanto, seleccionar una herramienta que les ayuda a identificarlas, analizarse y remediarlas. Esta necesidad surge debido a que, como se comentaba anteriormente, la certificación ISO27001 establece que la gestión de vulnerabilidades debe ser un control para tener en cuenta en el sistema de gestión de la seguridad, y además, debido a que Bitsight establece una puntuación en base a las vulnerabilidades detectadas, la empresa quiere anticiparse antes de ser puntuados y resolver las vulnerabilidades que pueda identificar para que su puntuación no descienda.

En este trabajo, se ayudó a la empresa realizar la selección de esta herramienta. Para ello, se seleccionaron las tres herramientas mejor valoradas y extendidas en el mercado según Gartner (Gartner Inc. s. f.): Qualys, Rapid7 y Tenable. Se definieron unos criterios de evaluación para poder comparar las tres herramientas y se establecieron unos porcentajes sobre la nota final a cada uno de estos criterios en base a las necesidades del cliente. Se realizó una prueba de concepto, probando las herramientas y evaluando los criterios definidos. Una vez evaluados, se dio una nota final de cada herramienta, siendo seleccionada la que mayor nota obtuvo de las tres.

1.2 Objetivos del Trabajo

El objetivo principal de este trabajo es la realización de una prueba de concepto para la elección de una herramienta de gestión de vulnerabilidades en una empresa real. Para alcanzar este objetivo, se definen los subobjetivos descritos a continuación:

- Explicar el concepto de vulnerabilidad, así como el proceso de gestión de vulnerabilidades y normativas que las recomiendan.
- Identificar las características que debe tener un sistema de gestión de vulnerabilidades e identificar criterios utilizados en otros trabajos que se hayan hecho de comparativas sobre las herramientas de gestión de vulnerabilidades.
- Identificar la necesidad de la empresa para la elección de esta herramienta.
- Identificar las tres herramientas para realizar la prueba de concepto
- Identificar y describir los criterios y el sistema de evaluación de cada uno de ellos para evaluar las herramientas.
- Aplicar y evaluar estos criterios en una prueba de concepto para la selección de herramienta de vulnerabilidades de una empresa real.
- Presentar los resultados de esta evaluación entre las diferentes herramientas.

1.3 Enfoque y método seguido

Para alcanzar el objetivo de este TFM, inicialmente se realizará un estado del arte para obtener una base sobre las herramientas de gestión de vulnerabilidades y comparativas entre herramientas para ver los criterios utilizados. Una vez realizado este estudio, se seleccionarán tres herramientas de análisis de vulnerabilidades a ser evaluadas y se definirá un proceso de selección de la herramienta para unos criterios cualitativos agrupados por categorías y que estarán formados por unos elementos de evaluación que serán utilizados para evaluar el criterio. Estos elementos de evaluación tendrán una valoración numérica (del 1 al 5) y tendrán un porcentaje sobre la valoración total del criterio.

Antes de empezar las pruebas con las herramientas, se deben establecer los porcentajes de los elementos de evaluación sobre la nota total de los criterios, los porcentajes de los criterios sobre la nota total de la categoría y los porcentajes de las categorías sobre la nota final de la herramienta. Una vez establecidos los porcentajes, se realizará una segunda evaluación donde serán ponderados para determinar a qué criterios dar mayor valor. Una vez probadas las herramientas y establecidas las puntuaciones sobre los elementos de evaluación, se calculará la nota de cada uno de los criterios y categorías en base a los porcentajes definidos anteriormente. Finalmente, se calculará la nota final con las categorías.

En resumen, la metodología que se llevará a cabo será en cascada y secuencial y se seguirán las fases de la Ilustración 1:

Ilustración 1. Fases de la metodología

- Identificar tres herramientas a evaluar: analizar las herramientas mejor valoradas en el mercado y seleccionar las tres mejores.
- Definir e identificar criterios: una vez realizado el estado del arte, se identificarán los criterios a utilizar para la evaluación de la herramienta.
- Ponderar los criterios: establecer las ponderaciones de los criterios en base a las valoraciones de la empresa
- Recopilar información de las herramientas: probar las herramientas y calificar los criterios
- Evaluar las herramientas en base a los criterios: una vez los criterios calificados, calcular la nota final con las ponderaciones y calcular la nota final.

1.4 Tareas

Para alcanzar los diferentes objetivos de este trabajo, se deben llevar a cabo las siguientes tareas:

- Estado del arte sobre definiciones de vulnerabilidad y procesos de gestión de vulnerabilidades.
- Estado del arte sobre la gestión de vulnerabilidades, así como normativas que recomiendan y/o obligan a esta gestión de vulnerabilidades.
- Estado de arte sobre comparativas de herramientas de gestión de vulnerabilidades.
- Realizar una breve contextualización de la empresa donde se realizará esta prueba de concepto, sus objetivos y necesidades de esta prueba.
- Seleccionar las tres herramientas mejor valoradas en el mercado
- Ponderar los criterios en base a las necesidades presentadas por la empresa.
- Presentar los procesos llevados a cabo para evaluar los diferentes criterios: alcance de servidores para realizar las pruebas, funcionalidades y uso de la herramienta, análisis de los resultados de la evaluación.
- Una vez realizada la evaluación, calcular la valoración final y presentar los resultados finales de esta valoración.
- Presentación de las conclusiones del trabajo realizado.

1.5 Planificación del Trabajo

En la Ilustración 2, se puede observar el cronograma de planificación del trabajo. En algunas tareas, están intercaladas en caso de que acabe alguna tarea antes de que acabe la semana y así empezar la siguiente:

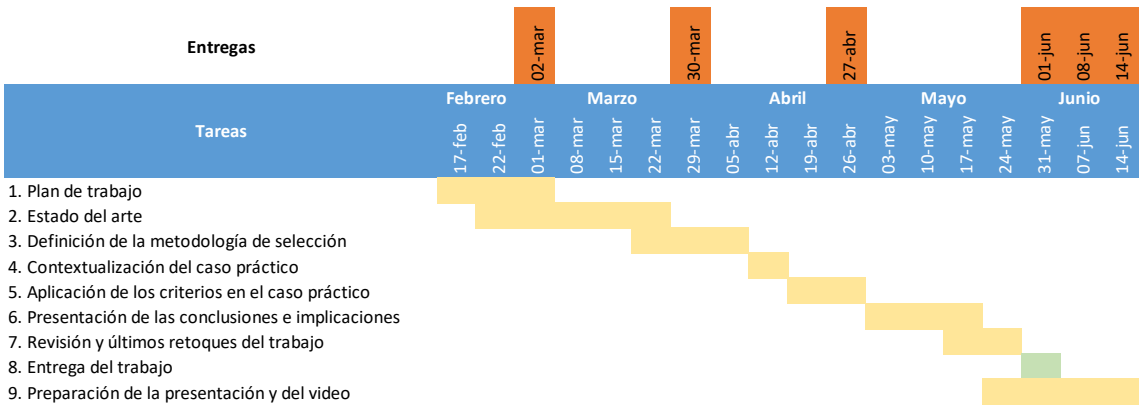

Ilustración 2. Planificación del trabajo

1.6 Riesgos

En este apartado, se definen los riesgos que pueden surgir durante la elaboración del proyecto:

- Problemas en la instalación de las aplicaciones. Las aplicaciones requieren una puesta en marcha que podría complicarse debido a que los servidores no estén correctamente preparados para la instalación.
- Limitación de los periodos de pruebas. Las herramientas de vulnerabilidades tienen un tiempo de periodo de prueba de 30 días que puede no ser suficiente para la evaluación completa de estas.
- Problemas en la definición de criterios. A pesar de realizar un estudio previo de los criterios, podrían definirse criterios complicados de evaluar o que no son relevantes para la evaluación de las herramientas en el caso práctico.

2 Estado del arte

2.1 Vulnerabilidades

Según (NIST 2012), “una vulnerabilidad es una debilidad en un sistema de información, en los procedimientos de seguridad del sistema, en los controles internos o en la implementación que podría ser explotada por una fuente de amenaza.”

También es definida por (Shirey 2000) como “un defecto o debilidad en el diseño, la implementación o el funcionamiento y la gestión de un sistema que podría ser explotado para violar la política de seguridad del sistema”.

En otras palabras, la seguridad de la información del sistema puede verse comprometida si se explota una vulnerabilidad.

Debido a que el concepto de vulnerabilidad es muy amplio, se pueden encontrar diferentes enfoques para clasificar estas vulnerabilidades, pero ninguno de ellos está generalmente aceptado. (Jin et al. 2009) realizan un estudio de 25 clasificaciones extendidas en el cual indican que ninguno cumple con los principios de clasificación definidos por (Amoroso 1994), que son: aceptación del público, comprensibilidad, integridad, determinismo, exclusión mutua, repetibilidad y terminología.

Sin embargo, algunas organizaciones han intervenido para desarrollar un etiquetado común de todas las vulnerabilidades identificadas a nivel internacional, llamado CVE (Common Vulnerabilities and Exposures). Este estándar está gestionado por The MITRE Coorporation y ha permitido crear una base de datos de vulnerabilidades de seguridad conocidas. Este listado puede descargarse desde (https://cve.mitre.org/ s. f.)

Pero, además del etiquetado para poder identificar las vulnerabilidades, un estándar muy extendido es el CVSS (Common Vulnerability Scoring System) , un marco abierto para transmitir determinadas características y gravedad de vulnerabilidades del software (Common Vulnerability Scoring System SIG s. f.). El CVSS consta de tres grupos de métricas: Base, Temporal y Ambiental. A partir de estas métricas, el estándar permite calcular una puntuación numérica la cual puede traducirse en una representación cualitativa de la gravedad de la vulnerabilidad (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidades.

2.2 Gestión de vulnerabilidades

2.2.1 Evaluación de vulnerabilidades

La evaluación de vulnerabilidades es el proceso de identificación de activos vulnerables. El equipo de evaluación de vulnerabilidades funciona como un hacker "ético" e intenta encontrar y corregir las vulnerabilidades antes de que lo haga un hacker malicioso (Brackin 2003).

Para que esta evaluación sea efectiva y se puedan observar resultados reales en seguridad, la empresa debe llevar a cabo regularmente evaluaciones de vulnerabilidades y actuar sobre los resultados de esas evaluaciones. Un sistema de gestión de la vulnerabilidades puede facilitar la identificación, el análisis y la corrección de los problemas y, por lo tanto, ayudar a las empresas a darse cuenta del valor de la propia evaluación de la vulnerabilidad (ISACA 2017).

La gestión de vulnerabilidades, por tanto, es un subproceso dentro de la evaluación de vulnerabilidades y consiste en identificar las vulnerabilidades técnicas y en evaluar los riesgos de estas vulnerabilidades. Esta evaluación puede llevar a la corrección de las vulnerabilidades y eliminar el riesgo o aceptar el riesgo (Palmaers 2013).

2.2.2 Proceso de gestión de vulnerabilidades

En (Palmaers 2013), se define un proceso de gestión de vulnerabilidades basado en 5 fases:

1. **Preparación:** En esta primera fase, se deben identificar los activos a escanear. Se debe empezar con un número limitado de activos, por ejemplo, por los considerados más críticos, o por un número limitado de vulnerabilidades. Posteriormente, se deben definir los escáneres a realizar. Estos escáneres pueden ser internos, desde dentro de la red de la compañía, o externos. A pesar de que los escaneos internos pueden identificar más vulnerabilidades, los externos muestran las vulnerabilidades visibles fuera de la red y, por tanto, con mayor alcance para ser explotado. Para esto, se debe considerar si los activos son externos o internos de la compañía.
2. **Escaneo de vulnerabilidades:** Una vez definido el alcance, se realizan los escaneos a los activos. En caso de problemas al lanzarlos, se deben registrar por si surgen los mismos problemas a futuro. Es importante en esta etapa seleccionar el informe con el cual se quiere reportar las vulnerabilidades al equipo.
3. **Definir acciones de remediación**: En esta fase, los propietarios de los activos, junto con el equipo de seguridad, definirán las acciones correctivas para resolver estas vulnerabilidades, así como las fechas en las que deberían estar resueltas. Estas fechas deben establecerse según la criticidad de la actividad. En caso de aceptar el riesgo, esto debe quedar documentado.
4. **Implementar las acciones correctivas:** Una vez planificadas las acciones, se deben ir ejecutando intentado seguir las fechas definidas. El responsable de seguridad debe ir haciendo un seguimiento de estas.
5. **Re-escanear:** Una vez remediada una vulnerabilidad, se debe volver a lanzar el escáner para validar que la vulnerabilidad ha quedado resuelta. Por último, se debe establecer cada cuánto tiempo se deben lanzar estos escáneres. Cuanto más frecuentes sean, antes serán identificadas las vulnerabilidades, pero también se debe considerar

cuál es el tiempo de respuesta de la empresa para remediar las vulnerabilidades identificadas.

2.2.3 Componentes de la gestión de vulnerabilidades

Dentro del proceso de gestión de vulnerabilidades, se debe disponer de unos determinados componentes para implementar correctamente el proceso de gestión de vulnerabilidades. De acuerdo con (Shanks 2015), los componentes principales que deben estar en todo proceso de gestión de vulnerabilidades son:

- **Elaboración de un inventario de activos:** Sin un inventario actualizado de activos, es difícil abordar adecuadamente el riesgo asociado a las vulnerabilidades identificadas. En este paso, la herramienta de evaluación de vulnerabilidades escanea las redes especificadas en busca de activos, y los sistemas descubiertos durante el escaneo se añaden al inventario de activos. Este proceso ayuda a garantizar que todos los sistemas sean identificados y parcheados adecuadamente.
- **Clasificación de los activos:** Las categorías o grupos de activos se crean a partir del inventario de activos. Los grupos de activos se utilizan para escanear activos específicos (en lugar de toda la red). Estas categorías también permiten la personalización del escaneo de vulnerabilidades, atendiendo a los requisitos de los activos o del negocio, y ayuda a asignar clasificaciones de riesgo.
- **Opciones de escaneo e informe de vulnerabilidades**: El escaneo de vulnerabilidades está diseñado para probar y analizar sistemas y servicios en busca de vulnerabilidades conocidas. El escaneo comprende una lista de opciones de escaneo (puertos, protocolos y características de comportamiento de los paquetes de red utilizados para el escaneo) y activos. El informe resultante de este escaneo debe contener la lista priorizada de vulnerabilidades, la descripción de la vulnerabilidad, el riesgo calculado y las actividades de corrección.
- **Clasificación de los riesgos**: Los riesgos se priorizan según el riesgo empresarial calculado. A los activos y grupos de activos se les asigna una calificación de criticidad empresarial. Cuando se descubre una vulnerabilidad, la herramienta de evaluación de vulnerabilidades calcula el riesgo empresarial de un activo. El esfuerzo de remediación se prioriza posteriormente en función del riesgo. Por ejemplo, un servidor web susceptible de sufrir una vulnerabilidad que permita el acceso con permisos de administración debería ser reparado antes que una aplicación interna que requiera un parche de seguridad de severidad baja.
- **Gestión de parches:** Los parches se prueban en un entorno de no producción para determinar si hay problemas de compatibilidad con el sistema. Los parches probados se trasladan a producción y se aprueban para su publicación.

2.2.4 Estándares y normativas

La gestión de vulnerabilidades es un proceso imprescindible en la mayoría de las normativas, estándares y regulaciones. Podemos encontrar este proceso en los siguientes mandatos (ISACA 2017):

- **Payment Card Industry Data Security Standard (PCI-DSS)**: establece controles de seguridad para los comercios electrónicos que aceptan pagos de tarjetas de crédito y proveedores de servicios. La versión 3.2 de la PCI DSS exige que las vulnerabilidades de la red externa (es decir, la conexión a Internet) y vulnerabilidades de la red interna (requisito 11.2) sean escaneadas.
- **NIST Cybersecurity Framework**: Este Marco es el resultado de una normativa, cuyo objetivo es proporcionar a las empresas una guía de mejores prácticas para su gestión de ciberseguridad. Dentro del núcleo del marco NIST CSF, se incluye la exploración de la vulnerabilidad (control DE.CM-8).
- **Norma ISO/IEC 27002:2013**: La norma ISO/IEC 27002:2013, "Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información" es un sistema para la normalización a nivel mundial de los requisitos de un sistema de gestión de seguridad de la información (UNE-EN ISO/IEC 27001 2017, 27001). En su anexo, uno de los puntos que incluye es la gestión de las vulnerabilidades (control 12.6.1).
- **COBIT®:** En este marco de gestión para el gobierno y la gestión de las TI en la empresa publicado por ISACA(COBIT 5 s. f., 5), la evaluación de la vulnerabilidad se encuentra en el dominio Servicio y Soporte (DS5) bajo el objetivo de control DS5.5 Pruebas de Seguridad, Vigilancia y Monitoreo. Específicamente, en COBIT® 5 para la Seguridad de la Información, donde se presenta este marco de gestión desde el punto de la seguridad, la gestión de las vulnerabilidades reside, en parte, dentro del dominio Build, Acquire and Implement (BAI).

2.3 Herramientas de gestión de vulnerabilidades

Basándose en lo indicado por (Shanks 2015), una herramienta de gestión de vulnerabilidades permite a las empresas automatizar las tareas de:

- Recoger información sobre el inventario de activos
- Categorizar los activos
- Escanear las vulnerabilidades
- Valorar los riesgos descubiertos

Además, según (Scarfone et al. 2008), los escáneres de vulnerabilidades no solo realizan un seguimiento de los hosts y sus respectivas características, sino que también ayudan a "identificar versiones de software obsoletas, parches faltantes y configuraciones incorrectas, y validar el cumplimiento o las desviaciones de la política de seguridad de una organización.

(Manzuik, Pfeil, y Gold 2006) presenta las capacidades que debería cumplir una herramienta de gestión de vulnerabilidades perfecta, debiendo todas ellas funcionar bien en conjunto, además de integrarse bien con tecnologías de terceros. Las capacidades que presenta son:

- La gestión de activos: Sin un inventario de activos completo y actualizado, el programa de gestión de vulnerabilidades será sólo parcialmente efectivo. Por lo tanto, es crítico que las herramientas aprovechen este repositorio para la lista de activos representados en su entorno.
- Evaluación de vulnerabilidades y monitorización: la herramienta debe evaluar las vulnerabilidades para determinar su criticidad, y monitorizar si han sido remediadas o si vuelven a aparecer.
- Integración de tecnologías con terceros: las herramientas de gestión de vulnerabilidades y herramientas auxiliares deberían comunicarse entre sí para facilitar su detección o remediación.
- Gestión de la configuración, gestión de parches e informes de remediación o resolución: son elementos que pueden ser de ayuda para la fase de implementación de acción correctivas.

2.3.1 Criterios utilizados para comparar herramientas

En la literatura, encontramos diferentes trabajos de comparaciones entre herramientas, o metodologías para compararlas, que han utilizado diferentes criterios.

(Holm et al. 2011) realiza un pequeño estado del arte donde compara diferentes trabajos que han realizado comparaciones entre los sistemas de gestión de vulnerabilidades que hay en el mercado y los criterios utilizados para compararlas. Indica que la mayoría de estos trabajos se basan en criterios cualitativos en lugar de cuantitativos, y destaca los siguientes:

- (Welberg 2008): en su trabajo, describe cualitativamente una gran variedad de herramientas de evaluación de la seguridad, incluyendo escáneres de vulnerabilidad. Como primera clasificación, utiliza una taxonomía que consta de alcance y análisis. El alcance describe qué datos pueden evaluar las herramientas y cómo se ajustan a diferentes normas. Este criterio se basa en las plataformas de software, el número de activos, las normas utilizadas para etiquetar las vulnerabilidades y el tipo de vulnerabilidades. Por otra parte, el criterio de análisis se define por el tipo de escaneo utilizado, la representación de los resultados y la información disponible para realizar la comparación.
- (Wang, Balaouras, y Coit 2010): evalúa las herramientas de gestión de vulnerabilidades en base a tres dimensiones de manera cualitativa: Demanda actual, Estrategia y Presencia en el mercado. La demanda actual analiza la capacidad de la herramienta en la evaluación de la vulnerabilidad, la evaluación del cumplimiento de la configuración, cualquier capacidad de soporte para la remediación, la elaboración de informes, el rendimiento y el soporte que da para la gestión de riesgos.

En cuanto a la estrategia de la empresa, los autores examinaron la visión del proveedor y su propuesta para dar valor a su herramienta, el grado de ejecución de esta visión y la entrega de la propuesta de valor, y si la estrategia está enfocada al liderazgo del sector. La última dimensión incluye unas métricas tradicionales, como los ingresos del vendedor y el número de clientes. Este trabajo está más enfocado al mercado de este tipo de herramientas que en las propias capacidades de las herramientas.

- (Andress 2004) y (Forristal y Shipley 2001) ambos trabajos realizan una comparación cuantitativa utilizando como criterio la tasa de detección de vulnerabilidades de los escáneres.

Adicional a estos tres trabajos, (Villora Divino 2018), realizó un análisis de mercado entre diferentes herramientas de análisis de vulnerabilidades basándose también en sus características. Para realizar este análisis de mercado, tuvo en cuenta los siguientes criterios:

- Gestión de los activos de la empresa.
- Calidad de la enumeración de vulnerabilidades, uso de escaneo activo/pasivo, autenticado/no autenticado y si tiene agentes de sistema.
- Rapidez y calidad de las actualizaciones de la base de datos de vulnerabilidades y/o amenazas usadas.
- Soporte para la evaluación de servicios en la nube y contenedores.
- Compatibilidad con diferentes sistemas operativos e integración con terceros.
- Algoritmo de priorización de amenazas.
- Evaluación de conformidad respecto de estándares y normativas.
- Calidad de los informes generados.
- Usabilidad ofrecida por la solución.
- Soporte proporcionado por el vendedor.

Adicional a las comparativas realizadas, (Bhajanka, Schneider, y Lawson 2019) en su artículo plantea diferentes criterios a tener en cuenta a la hora de elegir una herramienta de escaneo de vulnerabilidades. Los principales criterios de evaluación son:

- Arquitectura: en este criterio, se revisa lo relacionado con la arquitectura del programa, como el despliegue de la herramienta, la configuración de los escáneres (internos, externos, basados en agentes, etc.) y la escalabilidad que tiene.
- Evaluación: en este punto se evalúa la función de descubrimiento de activos, si las vulnerabilidades que detecta son a nivel de cumplimiento, de configuración o de red, si dispone de escaneo con autenticación, si permite escaneos de entornos virtuales o en la nube y si el escaneo puede ser continuo o monitorizado en tiempo real.
- Priorización: este criterio evalúa principalmente si es posible asignar criticidad en base al negocio y si la puntuación de las vulnerabilidades está basada en riesgo.

- Informes: si los informes que genera la herramienta pueden ser unificados, si dispone de recomendaciones para resolver las vulnerabilidades, si representa evaluación de medición del rendimiento, las alertas de vulnerabilidades y la personalización del panel de control y de los informes generados.
- Tratamiento: en este criterio, se revisa hasta qué punto es posible automatizar la recuperación, si se recomiendan formas de mitigar la vulnerabilidad y si es posible realizar un re-escaneo para validar el tratamiento.
- Administración: este criterio hace referencia más a la propia aplicación en sí, que incluiría como evaluación si es posible gestionar los accesos por roles, la gestión de actualizaciones de la propia herramienta y los agentes y las medidas para asegurar la privacidad de los datos de la herramienta.

2.4 Conclusiones del estado del arte

En este apartado, se ha presentado la definición de vulnerabilidades y las diferentes formas de identificación de estas. También se ha presentado el proceso de gestión de vulnerabilidades, identificando las fases y los elementos necesarios para su implantación, así como las normativas que recomiendan la implantación de este proceso.

Otro punto que se ha presentado es la definición de herramienta de gestión de vulnerabilidades y sus características. Finalmente, se han presentado diferentes comparativas de herramientas de gestión de vulnerabilidades y se han identificado los criterios utilizados para compararlas.

Este estado del arte se ha realizado para que la definición de los criterios de evaluación de las herramientas contemple todos los puntos clave en el proceso de gestión de vulnerabilidades. Además, los criterios utilizados en las comparativas nos sirven de base para definir cómo evaluar y como estructurar los criterios a utilizar.

3 Contextualización del caso práctico

3.1 Descripción de la empresa

El caso práctico se ha realizado en una empresa de distribución de material farmacéutico y de diagnóstico clínico. La empresa tiene más de 5000 empleados y está presente en más de 30 países y sirviendo en más de 100 territorios a través de distribuidores. La misión de la empresa es mejorar la calidad de los laboratorios y hospitales donde distribuyen para mejorar el cuidado del paciente y mejorar la eficiencia del cuidado de la salud.

La empresa tiene formado un departamento de Tecnologías de la Información (TI) que es responsable de gestionar todos los sistemas de información internos de la compañía. Este departamento está segregado en 6 áreas:

- Sistemas: es el área encargada de mantener los sistemas e infraestructuras que dan servicios a los sistemas de información y de dar soporte al usuario.
- Desarrollo SAP: es el área encargada del desarrollo de nuevos programas y funcionalidades para el negocio dentro del sistema SAP, el software de gestión de la compañía.
- Desarrollo web: es el área encargada del desarrollo de nuevas aplicaciones web personalizadas para la empresa
- Organización: es el área que hace de intermediario entre el desarrollador y el personal de negocio, para recoger las necesidades del negocio y transmitirlas al área de desarrollo.
- Calidad: Es el área responsable de dar los accesos a los usuarios a los diferentes sistemas, así como de asegurar la calidad en los procesos de TI.
- Seguridad: es el área responsable de la gestión de la seguridad en los procesos de TI y de asegurar que se mantengan unos requisitos de seguridad en los sistemas de información de la compañía. E

En la Ilustración 3, se muestra el organigrama del departamento de TI. El CIO es el máximo responsable del departamento y el CIO Deputy le ayuda en determinadas responsabilidades. Los directores de cada área reportan al CIO sobre sus proyectos:

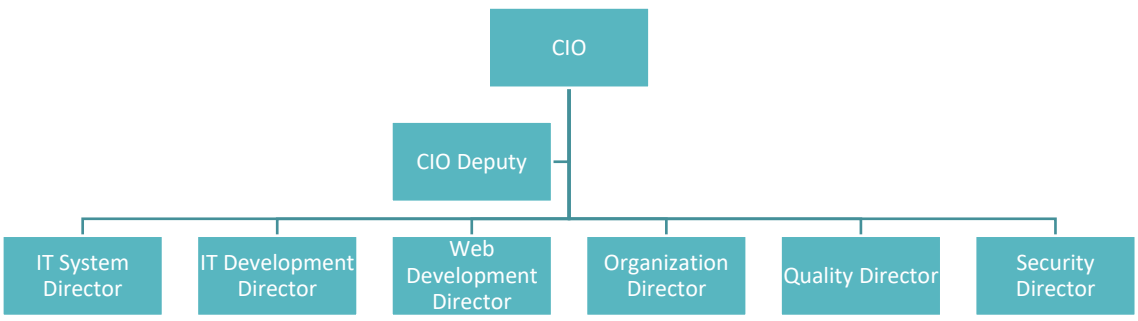

Ilustración 3. Organigrama del departamento de TI

3.2 Necesidad del trabajo

Debido a que la empresa distribuye material sanitario y de diagnóstico, la mayoría de sus contratos de venta se consiguen mediante licitaciones. Estas licitaciones, cada vez más solicitan mayor calidad y seguridad entre sus clientes y, por tanto, exigen que estén certificadas en la ISO9001 y cada vez más, dispongan de la certificación en la ISO27001. Debido a esta exigencia, la empresa decidió obtener la certificación ISO27001, para poder dar tranquilidad al cliente con respecto a la gestión de seguridad de la información tratada en la compañía. Para obtener esta certificación, contrataron a un proveedor externo para revisar su sistema de gestión de seguridad y analizar si necesitaban implementar algún procedimiento más para poder obtenerla. De esta revisión, uno de los puntos que salió fue la necesidad de implementar un procedimiento de gestión de vulnerabilidades, ya que es uno de los puntos del Anexo de la norma ISO27001.

Además de las exigencias en las licitaciones, determinados clientes, también preocupados por la seguridad, solicitan que sus proveedores sean auditados o analizados por empresas que califican la seguridad en los activos del dominio. Este es el caso de la empresa donde realizaremos el caso práctico. Para poder dar tranquilidad al cliente respecto a la gestión de la seguridad, la empresa contrata a Bitsight, la cual realiza un escaneo de vulnerabilidades de todos los activos bajo el dominio de la empresa publicados en Internet, y, en base al escaneo, les asigna una puntuación que mide su nivel de seguridad (BitSight Technologies s. f.). Bitsight, además, no sólo revisa vulnerabilidades externas de red, sino también de las propias aplicaciones web. Debido a que esta puntuación de seguridad es visible por sus clientes y puede ser comparadas con otras empresas del mismo sector, la empresa también ve la necesidad de poder anticiparse a estas revisiones con alguna herramienta de gestión de vulnerabilidades y así resolver las vulnerabilidades identificadas en sus activos antes de ser analizados por Bitsight.

Por tanto, la empresa decide implementar un proceso de gestión de vulnerabilidades. Para poder implementar este proceso, el primer paso es la selección y contratación de una herramienta que les permite identificar y analizar vulnerabilidades. Debido a que los escaneos de Bitsight no son sólo de los servidores, sino que también realiza escaneos de las aplicaciones web dentro del dominio de la empresa, se debe contratar una herramienta que también permita realizar escaneos de vulnerabilidades de aplicaciones web.

Para realizar este proceso de selección, al área de Seguridad será la responsable de realizar un estudio de las herramientas a evaluar y finalmente seleccionar una de ellas, ya que el área de Seguridad será la responsable de llevar la gestión de vulnerabilidades y, por tanto, de gestionar la herramienta.

Debido a que el área de Seguridad será la responsable de llevar la gestión de vulnerabilidades y, por tanto, de gestionar la herramienta, será la responsable de seleccionar tres herramientas, realizar un estudio de las herramientas a evaluar y finalmente seleccionar una de ellas.

3.3 Selección de herramientas a evaluar

Según (Lawson, et al. 2019), no se recomiendan herramientas de análisis de vulnerabilidades de código abierto para casos de uso empresarial debido a que estas versiones no serán adecuadas para la mayoría de las organizaciones, porque las capacidades de investigación y generación de informes no son tan completas como las soluciones empresariales. Además, no hay garantía de que una entidad responsable mantenga continuamente un producto de código abierto.

Por tanto, se decidió tomar 3 herramientas bajo licencia y se eligieron las herramientas líderes de la industria. Según el informe de (The Forrester WaveTM: Vulnerability Risk Management, Q4 2019 s. f.) y el Gartner Peer Insight (Gartner Inc. s. f.), donde los clientes valoran diferentes herramientas que hay en el mercado, los proveedores líderes y mejor valorados internacionalmente para herramientas de gestión de vulnerabilidades son Qualys con la herramienta VMDR, Tenable con Nessus y Rapid7 con InsigtVM.

3.3.1 Qualys

Qualys (Information Security and Compliance | Qualys, Inc. s. f.)fue fundada en 1999 como una de las primeras empresas de seguridad SaaS. Desde entonces ha establecido alianzas estratégicas con varios proveedores en la nube y proveedores de servicios gestionados. Actualmente, dispone de más de 19.000 clientes de diferentes sectores.

Dispone de una plataforma en la nube formada por aplicaciones integradas, clasificadas en gestión de activos, seguridad IT, seguridad en la nube/Contenedor, seguridad de aplicaciones web y cumplimiento:

- **Gestión de activos**: dispone de herramientas para monitorizar los activos dentro de la red de la compañía, con opciones para categorizarlos mediante etiquetas, además de permitir sincronizarlo con un CMDB (Configuration Management DataBase), es decir, una herramienta interna de la compañía para la gestión de inventario físico. También dispone de herramientas para realizar inventarios de certificados TLS/SSL de manera global. Las aplicaciones son:
    - Global IT Asset Inventory
    - CMDB Sync
    - Certificate Inventory
- **Seguridad de las tecnologías de la información**: en esta categoría, dispone de muchas aplicaciones, de las cuales en este trabajo se destacan:
    - Vulnerability Management, Detection and Response (VMDR): es la herramienta principal de gestión de vulnerabilidades para identificarlas y priorizarlas.
    - Threat Protection: Permite notificar las últimas vulnerabilidades identificadas globalmente, identificándolas en los activos de la compañía.

    - Continuous Monitoring: Permite crear alertas para identificar amenazas y monitorear cambios en la red.
    - Patch Management: con esta herramienta es posible remediar vulnerabilidades desde la propia aplicación, ya que se instala un agente en el activo y permite realizar la actualización o instalar el parche pertinente para remediar la vulnerabilidad.
- **Seguridad en la nube**: la aplicación permite tener controlados los servidores ubicados en la nube y los contenedores de código, revisando configuración de seguridad, usuarios, etc.
- **Aplicaciones web**: en esta categoría, dispone de la aplicación "Web Application Scanning", para realizar escaneos sobre las webs de la compañía y gestionar las vulnerabilidades identificadas. También disponen de la aplicación "Web Application Firewall", para bloquear ataques y parchear vulnerabilidades directamente en las aplicaciones web.
- **Compliance**: en estas últimas categorías, se encuentran todas las aplicaciones que permiten ayudar a la compañía con el cumplimiento de determinadas legislaciones o políticas de seguridad de la compañía, realizando auditorías técnicas sobre servidores, ayudando a gestionar el riesgo con los proveedores o registrando cambios sobre determinados ficheros. Las aplicaciones que se incluyen son:
    - Policy Compliance
    - Security Configuration Assessment
    - PCI Compliance
    - File Integrity Monitoring
    - Security Assessment Questionnaire
    - Out-of-Band Configuration Assessment

3.3.2 Rapid 7

Rapid7 (Rapid7 | Cybersecurity & Compliance Solutions & Services s. f., 7) es una empresa fundada en el año 2000 que provee soluciones para gestionar la seguridad de la información a más de 9.100 clientes por todo el mundo. Este proveedor también dispone de una herramienta en la nube que permite el acceso a sus diversas aplicaciones, para poder tener centralizada la gestión. El núcleo de esta herramienta en la nube dispone de 5 módulos:

- **InsightVM**: desde este módulo, se realizar la administración de vulnerabilidades en vivo y análisis de terminales para ver el riesgo en tiempo real. Los escáneres, gestión de activos, etc. se gestionan de manera local y se comunican con la herramienta en la nube para comunicar los resultados y gestionar la priorización de resolución de las vulnerabilidades.
- **InsightAppSec**: el objetivo de este módulo es aplicar y gestionar la seguridad en todo ciclo de vida del desarrollo de las páginas webs (SDLC), proporcionando pruebas de seguridad de aplicaciones

dinámicas. Permite rastrear y evaluar automáticamente aplicaciones web para identificar vulnerabilidades como SQL Injection, XSS y CSRF.

- **InsightIDR:** es un centro de seguridad que unifica diferentes tecnologías de monitorización y rastreo para detección y respuesta a incidentes, monitoreo de autenticación y visibilidad de terminales. Este módulo identifica el acceso no autorizado de amenazas externas e internas y destaca la actividad sospechosa para que no tenga que eliminar miles de flujos de datos.
- **InsightConnect:** es una herramienta de automatización de procesos, la cual consiste en conectar las herramientas de la empresa, crear flujos de trabajo y toma de decisiones automatizadas entre estas herramientas para así mejorar la eficiencia operativa.
- **DivvyCloud:** esta herramienta proporciona visibilidad unificada de todos los entornos disponibles en la nube, incluidos AWS, Azure y Google Cloud Platform, proporcionando seguridad y cumplimiento continuo.

3.3.3 Tenable

Tenable (Tenable® s. f.) es un proveedor de soluciones de ciberseguridad, el cual trabaja con más de 30 000 organizaciones de todo el mundo para ayudarles a gestionar y medir el riesgo para la ciberseguridad.

La plataforma de Tenable es una herramienta en la nube que proporciona amplitud de visibilidad hacia el riesgo cibernético a lo largo de los entornos de TI, IoT, TO y la nube, y análisis más profundos para medir y comunicar el riesgo cibernético en términos de negocios, a fin de tomar mejores decisiones estratégicas. Esta plataforma incluye las siguientes aplicaciones:

- **Nessus:** es la herramienta de evaluación de vulnerabilidades, que permite:
  - Detectar activos a través del escaneo activo, agentes, monitoreo pasivo, conectores en la nube e integraciones con bases de datos de gestión de configuraciones.
  - Evaluar la seguridad de los activos con los escaneos
  - Asignar puntuaciones de riesgo a las vulnerabilidades para conocer cuáles son prioritarias
- **Tenable.sc y tenable.io**: estas herramientas, adicional a la evaluación de vulnerabilidades que realiza Nessus, permiten identificar y priorizar las vulnerabilidades de forma precisa. La diferencia entre las dos es simplemente su forma de despliegue: Tenable.sc es gestionado de forma local y Tenable.io es gestionado en la nube.
- **Tenable.ot**: está enfocado a la seguridad en el Internet de las cosas, escaneando y analizando las redes industriales contra las amenazas cibernéticas, los agentes maliciosos que tienen acceso a información privilegiada y los errores humanos.

- **Tenable Lumin**: Permite medir de manera sencilla el nivel de ciberseguridad de la empresa y compararla con la de la competencia.

3.3.4 Ventajas e inconvenientes de cada una de ellas

Las tres herramientas disponen de las características indicadas por (Manzuik, Pfeil, y Gold 2006) sobre una herramienta de gestión de vulnerabilidades que son: capacidades de gestión de activos, evaluación de vulnerabilidades, gestión de la configuración, gestión de parches, informes de remediación y/o resolución y monitorización.

Pero, a pesar de disponer estas características básicas de cualquier herramienta de escaneo de vulnerabilidades, cada una de ellas dispone de alguna característica diferencial añadida:

- Qualys: dispone de una herramienta de priorización de vulnerabilidades y de gestión de parches para remediarlas.
- Tenable: dispone de una herramienta que realiza una comparación del nivel de seguridad con empresas de diferentes sectores en base a puntuación
- Rapid 7: dispone de una herramienta de gestión de proyectos para planificar la remediación de las vulnerabilidades.

Pero, a pesar de disponer de las características básicas, cada una de estas herramientas presenta ventajas e inconvenientes, descritos por (Yair Regev 2020) en un artículo donde realiza una pequeña descripción de cada una de las herramienta y presenta sus ventajas e inconvenientes basándose en el informe de (Wang, Balaouras, y Coit 2010). En la Tabla 1, se han reflejado estas ventajas e inconvenientes para cada una de las herramientas:

Proveedores	Ventajas	Inconvenientes
VMDR (Qualys)	• Pionero en la gestión de vulnerabilidades • Pantallas de datos personalizables • Gran amplitud de protección • Fuertes funciones de automatización con mínima intervención del usuario	• Curva de aprendizaje pronunciada • Tiende a ofrecer más falsos positivos • Aumento del coste de los análisis a través de red frente a los análisis de los agentes • No es tan competitivo en precio
Nessus (Tenable)	• Estrategia de análisis centrada en amenazas y basada en agentes • Buena fuente de información • Solución flexible con una buena y completa formación sobre el producto	• Interfaz de usuario más anticuada y menos atractiva • Requiere experiencia especializada • Requiere comprobación manual y verificación de resultados

	• Precio competitivo	• Conjunto confuso de opciones en la nube frente a las locales
InsightVM (Rapid7)	• Configuración e implementación simple • Se integra fácilmente con la propia plataforma Metasploit de Rapid7 para probar exploits • Aceleración rápida, curva de aprendizaje fácil • Priorización clara de vulnerabilidades para ayudar en la remediación	• Los paneles no siempre proporcionan una interfaz fácil de usar • Tiende a ofrecer más falsos positivos • Consultas y filtros a menudo inflexibles y complejos • Funciones faltantes para los informes, como, por ejemplo, la personalización

Tabla 1. Ventajas e inconvenientes de las herramientas

3.4 Alcance para evaluar las herramientas

La empresa dispone del sistema de gestión SAP, el cual sirve de soporte para todos los procesos de negocio de la compañía. Este sistema se comunica con la mayoría de las aplicaciones de la compañía y con servidores que sirven de intermediarios para comunicaciones con aplicaciones externas. Adicional a esta estructura relacionada con el sistema de gestión, la compañía dispone de múltiples servidores para diferentes aplicaciones web o para dar soporte a otros departamentos. Esto hace que la compañía disponga de más de 200 servidores virtuales.

Para poder evaluar las herramientas correctamente, se decidió seleccionar unos pocos servidores y aplicaciones web a incluir para poder analizar mejor los resultados. Esta selección se realizó en base a las necesidades por las cuales se decidió implementar un sistema de gestión de vulnerabilidades.

Debido a que una de las razones fue por la certificación de la ISO27001, se decidió seleccionar los activos que estaban incluidos dentro del alcance de la certificación. El alcance de la certificación se centró en la gestión de los sistemas de información que daban soporte al proceso de ventas de la compañía. Estos sistemas son el servidor donde se encuentra SAP y servidores intermediarios con información de ventas que envían la información a servidores de otras herramientas.

Otra de las razones por las cuales se decidió implantar una herramienta de gestión de vulnerabilidades fue por las revisiones de Bitsight. Como comentábamos anteriormente, Bitsight identifica los activos que están dentro del dominio de la compañía y los analiza, incluyendo las páginas web. Por tanto, se decidió incluir dos aplicaciones web que estaban siendo analizadas por Bitsight, para así poder comparar los resultados de las herramientas con los resultados proporcionados por Bitsight. Adicional a estas dos páginas web, se incluyó una página web relevante para compañía.

4 Proceso de selección de la herramienta de gestión de vulnerabilidades

Tal como indica (Palmaers 2013), se recomienda que una organización pruebe a fondo los productos de escaneo de vulnerabilidades antes de decidir cuál es la solución que mejor se ajusta a los requisitos de la organización.

Para ello, una vez elegidas las tres herramientas a evaluar, se ha llevado a cabo un proceso de selección que consta de las siguientes fases:

1) **Definición de criterios iniciales a evaluar**: en esta fase, se definirán los criterios en base al estado del arte realizado y los elementos de evaluación a considerar para puntuar cada uno de los criterios definidos.
2) **Criterios evaluación para el caso práctico**: debido a las necesidades de la empresa, pueden surgir nuevos criterios específicos para el caso práctico. En esta fase, se identificarán estos criterios.
3) **Cálculo de la puntuación final**: en esta fase, se definirán los valores con los que se evaluarán los criterios y cómo se calculará la puntuación final con estos valores
4) **Ponderación de criterios:** se establecerán unos porcentajes base a los criterios en base a las necesidades del equipo de Seguridad IT de la compañía y luego recibirán una ponderación por parte de los responsables de IT que participarán en el proceso de gestión de vulnerabilidades.
5) **Evaluación de los criterios:** se realizarán unas pruebas y se evaluarán los elementos de evaluación de cada uno de los criterios.
6) **Evaluación final:** una vez todos los criterios evaluados, se obtendrá la nota final de las herramientas, siendo la mejor valorada como la herramienta a implementar.

4.1 Definición de criterios iniciales a evaluar

En base al estado del arte realizado previamente, se han definido 11 criterios, los cuales se han agrupado en 5 categorías:

1. Detección de vulnerabilidades internas
2. Detección de vulnerabilidades externas
3. Funcionalidades
4. Operativa
5. Proveedores

Las categorías 1 y 2 están relacionadas con la capacidad de detectar aplicaciones web y amenazas del sistema interno. Esta parte de la evaluación se basará en los resultados de los escaneos de vulnerabilidades, por tanto, son unas categorías más objetivas de evaluar, ya que se basará en la cantidad de vulnerabilidades identificadas y en la forma de ser detectadas. Las categorías 3 y 4 son más subjetivas porque se centran en la funcionalidad y la operatividad

de la herramienta, ya que incluyen la evaluación de las capacidades de inventario, gestión de vulnerabilidades, gestión de amenazas y la inteligencia de la herramienta y, por tanto, se evaluarán de una forma más subjetiva. Por último, la quinta categoría está relacionada con la evaluación de los proveedores (madurez, tamaño de la empresa, referencias, presencia, modelos de licencia, etc.).

A continuación, se explican y detallan las 5 categorías y los criterios seleccionados dentro de cada una de ellas. Para cada uno de estos criterios, se han definido unos elementos de evaluación que serán los evaluados cuando se realicen las pruebas con las herramientas.

Las dos primeras se han unido en un solo apartado, ya que los criterios son los mismos, pero a la hora de evaluarse se diferencian entre las vulnerabilidades encontradas en los escáneres realizados desde dentro de la red de los activos y por otro lado las encontradas desde los escáneres de vulnerabilidades de aplicación web.

4.1.1 Detección de vulnerabilidades internas y externas

Uno de los criterios principales son las vulnerabilidades detectadas por los escáneres de las herramientas, ya que es el criterio visto en todos los trabajos anteriormente tanto de manera cualitativa (Villora Divino 2018; Wang, Balaouras, y Coit 2010; Welberg 2008) como cuantitativa (Andress 2004; Forristal y Shipley 2001). En este punto, se deben realizar escáneres de alto alcance e identificar las vulnerabilidades críticas que se han detectado en cada uno de los aplicativos. Las vulnerabilidades críticas y altas serán los elementos de evaluación de este criterio. Una vez identificadas, se debe revisar y comparar si todas las aplicaciones han encontrado estas vulnerabilidades o hay alguna que no la ha identificado. Para las vulnerabilidades internas, se realizan escáneres internos de los servidores que están dentro de la red de la compañía. Y para las vulnerabilidades externas, se realizan escáneres externos de las aplicaciones web desde fuera de la red de la compañía.

Otro criterio a evaluar es la capacidad tecnológica de las vulnerabilidades, donde se incluyen los elementos de evaluación revisados por (Bhajanka, Schneider, y Lawson 2019; Villora Divino 2018, 2018) sobre cómo las vulnerabilidades son etiquetadas e identificadas, cómo se realiza la evaluación de la criticidad y con qué frecuencia se actualizan las base de datos de vulnerabilidades.

En resumen, los criterios y los elementos de evaluación incluidos dentro de esta categoría son:

- **Vulnerabilidades detectadas**:
  - Vulnerabilidades críticas y altas
- **Capacidad tecnológica**:
  - Etiquetado e identificación de vulnerabilidades
  - Evaluación de la criticidad
  - Actualización de la base de datos de las vulnerabilidades

4.1.2 Funcionalidades

Como hemos visto anteriormente en el apartado *2.2 Gestión de vulnerabilidades*, en la primera fase se incluía la identificación de los activos a evaluar y las vulnerabilidades que deben priorizarse. En esta categoría, se han incluido los criterios basándose en estos aspectos del proceso de gestión de vulnerabilidades:

- **Gestión de inventario**. Tanto (Villora Divino 2018) como (Bhajanka, Schneider, y Lawson 2019) incluyen este criterio de comparación entre herramientas, donde se evalúa cómo son gestionados los activos dentro de la herramienta. Los 5 elementos de evaluación dentro de estos criterios serían:
    - Clasificación del inventario: cómo son agrupados y clasificados los activos dentro de la aplicación, si es por sistema operativo, por segmento de red, etc.
    - Representación gráfica de los activos: si visualmente son fácilmente identificables
    - Identificación: los activos deben utilizar una identificación única en la aplicación
    - Informes: qué tipo de información se puede extraer de los activos incluidos en la aplicación y si son visualmente fáciles de entender.
    - Escáneres: si es posible realizar escáneres pasivos y/o activos para identificar nuevos activos
- **Gestión de vulnerabilidades**. En este criterio, se evalúa las características o las herramientas de gestión para el proceso de gestión de vulnerabilidades:
    - Priorización: si la priorización es basada en la criticidad del activo o si dispone de algoritmos de priorización específicos.
    - Escáneres: la tipología de escáneres que es posible realizar. Por ejemplo, si son escáneres de red, de configuración, por cumplimiento, etc.
    - Integración: la posibilidad de integrar la herramienta con otro tipo de aplicaciones como SIEM o firewalls.
    - Monitorización de la evolución: cómo son identificadas la vulnerabilidades resueltas o aceptadas.
    - Completitud de la información: qué tipo de información es mostrada por cada vulnerabilidad. Por ejemplo, si hay una descripción detallada de las vulnerabilidades, si presenta formas de explotarlas o si describe la remediación.
    - Exportación de los datos: hasta qué punto facilita la exportación de la información, permitiendo seleccionar el formato de exportación o la información a extraer.

4.1.3 Operativa

(Welberg 2008) en su trabajo, uno de los criterios estaba relacionado con el alcance de la aplicación: cuántos activos están permitidos, el tipo de plataforma del software, etc. Además, (Bhajanka, Schneider, y Lawson 2019) también incluye criterios relacionados con la gestión de usuarios y la personalización de los informes. Por último, (Villora Divino 2018) incluye como criterio el soporte a los usuarios, que en esta categoría se ha definido como la documentación de ayuda de la herramienta. En esta categoría, se han incluido todos estos criterios que están relacionados con la operativa de la aplicación en sí. A continuación, se presentan estos criterios y los elementos de evaluación de estos:

- **Escalabilidad**: en este criterio, se revisa el rendimiento de la aplicación y la personalización de esta:
    - Despliegue: identificar la complejidad de la infraestructura de la aplicación, si es en local, cloud o mixto.
    - Número de activos: valorar el máximo de activos a escanear
    - Requerimientos para instalar el servidor y los agentes que realizarán los escáneres internos
    - Gestión de usuarios: posibilidad de crear perfiles, de trabajar varios usuarios simultáneamente, etc.
    - Personalización: hasta qué punto pueden ser personalizados los dashboards con los resultados de las vulnerabilidades
- **Herramienta de ayuda**: cómo es la información de soporte del usuario, si es completa, fácil de entender, etc. En este caso, sólo hay un criterio de evaluación:
    - Herramientas de ayuda: cómo de completa y sencilla es la información de ayuda disponible en la herramienta.

4.1.4 Proveedores

Como decíamos previamente, (Wang, Balaouras, y Coit 2010) evaluaba las aplicaciones en base a su posición en el mercado actual, por tanto, en esta categoría se incluye esta evaluación de los proveedores. Como decíamos en la categoría anterior, (Villora Divino 2018) incluye como criterio el soporte a los usuarios y, en esta categoría, se ha incluido este criterio referente al servicio y soporte del propio proveedor. Por tanto, los criterios y elementos de evaluación quedarían como se indican a continuación:

- **Tamaño y presencia en mercado**:
    - Años de experiencia: años que lleva el proveedor de la herramienta ofreciendo el servicio
    - Número de empleados del proveedor
    - Número de oficinas del proveedor
    - Localización de las oficinas: si el proveedor está distribuido por todo el mundo
    - Ventas: la cantidad de facturación total del proveedor

- **Servicio y soporte**
    - Disponibilidad: diferentes herramientas para solicitar soporte técnico
    - Referencias: opiniones de otras empresas
    - Atención personal: la disponibilidad de los comerciales para resolver dudas sobre la aplicación
    - Tiempos de servicio: si han demorado mucho la resolución cuando ha surgido algún problema y se ha necesitado ayuda del proveedor

4.2 Criterios de evaluación para el caso práctico

Adicional a estos criterios iniciales definidos en base al estado del arte, se han añadido algunos criterios más en algunas categorías, ya que la empresa tiene unos criterios adicionales que quiere también considerar para su evaluación:

- **Detección en Bitsight**: debido a que los activos dentro del dominio de la compañía están siendo revisados por esta empresa, también se ha decidido incluirse como criterio la detección de vulnerabilidades que son detectadas por Bitsight. En este caso, sería un criterio parecido a *Vulnerabilidades detectadas*, pero en este caso se compararán los resultados del escaneo de vulnerabilidades externas de las herramientas con las vulnerabilidades detectadas por Bitsight. Por tanto, este criterio será incluido en la categoría de *Vulnerabilidades externas* y, como elementos de evaluación, se han tomado 5 vulnerabilidades de las dos aplicaciones web que estaban siendo analizadas por Bitsight
- **Licencias y precio**: un criterio importante a considerar también para la compañía es el precio de adquisición de la herramienta. Este criterio se ha incluido en la categoría de *Proveedores,* ya que tiene relación con la evaluación de proveedores y no con las funcionalidades de la herramienta en sí. Para este criterio, se han incluido 3 elementos de evaluación que son:
    - Precio fijo: se evalúa el precio inicial de contratación y las licencias incluidas dentro de este precio
    - Precio recurrente: se evalúa el precio por licencia incluida
    - Descuento: se evalúa si el proveedor realiza algún tipo de descuento inicial

Por tanto, las categorías, los criterios y los elementos de evaluación que se utilizarán en este caso práctico son los indicados a continuación en la Tabla 2:

Categorías	Criterios	Elementos de evaluación
1. Detección de vulnerabilidades internas	Vulnerabilidades detectadas	Vulnerabilidades críticas y altas
	Capacidad tecnológica	Etiquetado e identificación de vulnerabilidades

		Evaluación de la criticidad de los activos
		Actualización de la base de datos de las vulnerabilidades
2. Detección de vulnerabilidades externas	Vulnerabilidades detectadas	Vulnerabilidades críticas y altas
	Capacidad tecnológica	Etiquetado e identificación de vulnerabilidades
		Evaluación de la criticidad de los activos
		Actualización de la base de datos de las vulnerabilidades
	Detección en Bitsight	Vulnerabilidades detectadas por Bitsight
3. Funcionalidades	Gestión de inventario	Clasificación del inventario
		Representación gráfica de los activos
		Identificación
		Informes
		Escáneres
	Gestión de vulnerabilidades	Priorización
		Escáneres
		Integración
		Monitorización
		Completitud de la información
		Exportación de los datos
4. Operativa	Escalabilidad	Despliegue
		Número de activos
		Requerimientos
		Gestión de usuarios
		Personalización
	Herramienta de ayuda	Herramienta de ayuda
5. Proveedores	Tamaño y presencia en el mercado	Años de experiencia
		Número de empleados
		Número de oficinas
		Localización de las oficinas
		Ventas
	Servicio y soporte	Disponibilidad
		Referencias
		Atención personal
		Tiempos de servicio
	Licencias y precio	Precio fijo
		Precio recurrente
		Descuento

Tabla 2. Listado de categorías, criterios y elemento de evaluación

4.3 Cálculo de la puntuación final

Antes de evaluar los criterios, se debe definir con qué valores serán puntuados los elementos de evaluación, cómo se calcularán las ponderaciones y finalmente, cómo se calcula la puntuación final de la herramienta.

El cálculo de la puntuación está basado en porcentajes. Lo primero será establecer cuánto porcentaje de la calificación final puntuará de cada uno de los criterios definidos anteriormente. Para establecer estos porcentajes, se realiza la asignación por niveles: se establece el porcentaje del elemento de evaluación sobre la valoración final del criterio, luego se establece el porcentaje del criterio sobre la valoración final de la categoría y, por último, el porcentaje de la categoría sobre la valoración final de la herramienta.

Una vez definidos los porcentajes iniciales, se ponderan cada uno de los niveles para tener en cuenta si algún criterio debiera tener mayor o menor porcentaje sobre la valoración final en base a otras necesidades. Para ello, se realiza una ponderación por niveles:

- Se ponderan los elementos de evaluación para que se tengan más o menos en cuenta a la hora de calcular la puntuación del criterio.
- Se ponderan los criterios para que tengan mayor o menor valor en la puntuación final de la categoría.
- Se ponderan las categorías para que puntúen más o menos a la hora de realizar el cálculo de evaluación final de la herramienta.

La ponderación se realiza de manera cualitativa, por niveles, estableciendo un nivel de interés por cada elemento, desde Nada interesado hasta Extremadamente interesado. Para ello, se han definido 5 niveles de interés y cada uno de estos niveles tiene asignado un valor numérico para calcular el porcentaje final de la puntuación. En la Tabla 3, se muestran los niveles de ponderación cualitativos, su descripción y su valor cuantitativo a multiplicar por el porcentaje:

Niveles		**Descripción**	**Valor**
Nivel 4	**Extremadamente interesado**	Corresponde a los campos en los que los responsables consideran que la función, subcategoría o categoría es crítica y desea aumentar la importancia.	1,5
Nivel 3	**Muy interesado**	Esta puntuación refleja un interés por parte de los responsables en la función, subcategoría o categoría en la que se aplica.	1,25
Nivel 2	**Algo interesado**	Se refiere a las funciones, subcategorías y categorías en las que los responsables están de acuerdo con la importancia que le han dado el departamento de Seguridad	1

Nivel 1	**Poco interesado**	Se aplica a campos en los que los responsables consideran poco relevantes o críticos	0,5
Nivel 0	**Nada interesado**	Este valor se otorgará en aquellos campos en los que los responsables consideren que no es aplicable, es decir, que por el nivel de madurez de su empresa o su situación, no necesita la función, subcategoría o categoría.	0

Tabla 3. Niveles de ponderación

Una vez indicados los niveles de ponderación para todos los elementos de evaluación, criterios y categorías, se multiplica el porcentaje base definido previamente por el valor numérico del nivel de ponderación asignado, dando como resultado el porcentaje medio, tal como se muestra en la fórmula siguiente:

$$Porcentaje\ medio = Porcentaje\ base * Valor\ ponderación$$

Debido a que el porcentaje medio puede ser superior o inferior al inicial, se debe calcular el porcentaje proporcional para que el total no exceda el 100%. Para ello, se calcula el porcentaje final dividiendo el porcentaje medio del elemento por la suma de todos los porcentajes medio de los elementos del criterio, tal como se muestra en la siguiente fórmula:

$$Porcentaje\ final_{elemento} = \frac{Porcentaje\ medio_{elemento}}{\sum_{\substack{elementos \\ del\ criterio}} Porcentaje\ medio_{elemento}}$$

Para las ponderaciones de los criterios y las categorías se realiza de igual manera, pero sumando todos los porcentajes de su mismo nivel. Es decir, para calcular el porcentaje final del criterio, se divide su porcentaje medio por la suma del porcentaje medio de todos los criterios de su misma categoría, tal como se muestra en la formula siguiente:

$$Porcentaje\ final_{criterio} = \frac{Porcentaje\ medio_{criterio}}{\sum_{\substack{criterios\ de \\ la\ categoria}} Porcentaje\ medio_{criterio}}$$

Igualmente, para calcular el porcentaje final de la categoría, se divide su porcentaje medio por la suma del porcentaje medio de todas las categorías:

$$Porcentaje\ final_{categoria} = \frac{Porcentaje\ medio_{categoria}}{\sum_{categorias} Porcentaje\ medio_{categoria}}$$

Una vez los criterios ponderados y calculado el porcentaje final de la nota, se prueban las herramientas seleccionadas y se califican cada uno de los elementos de evaluación cualitativamente por niveles: Insatisfactorio, No funcional,

Funcional, Altamente Funcional y Excepcional. Cada uno de estos niveles, tendrá un valor de calificación tal como se muestra en la Tabla 4:

Niveles		Descripción	Valor calificación
Nivel 5	**Excepcional**	Que permiten el correcto funcionamiento de la función evaluada y añaden aspectos diferenciales que facilitan y completan las demás funciones.	1
Nivel 4	**Altamente funcional**	Presentan algunas cualidades que facilitan la realización de la actividad evaluada.	0,75
Nivel 3	**Funcional**	Presentan las cualidades necesarias para realizar la función evaluada.	0,50
Nivel 2	**No funcional**	No tienen las cualidades necesarias para realizar la función evaluada.	0,25
Nivel 1	**Insatisfactorio**	Tienen características que impiden el correcto funcionamiento de la función evaluada.	0

Tabla 4. Niveles de evaluación

Estos niveles se utilizarán para todos los elementos de evaluación, excepto los elementos de los criterios Vulnerabilidades detectadas de la categoría Detección de vulnerabilidades internas y Vulnerabilidades detectadas y Bitsight detection de la categoría Vulnerabilidades externas. Esto se debe a que los elementos de evaluación son las vulnerabilidades detectadas de nivel alto y crítico y sólo se indicará si ha sido detectadas la vulnerabilidad por la herramienta o no. Por tanto, los niveles de evaluación sólo son dos, que sería Detectado o No detectado, donde los valores de calificación sería 1 y 0 respectivamente.

Una vez evaluados los elementos de evaluación, se multiplica el porcentaje final del elemento calculado anteriormente por el valor de calificación del nivel de evaluación asignado y se suman todos estos valores para obtener la valoración final del criterio. Por tanto, la valoración del criterio se calcula tal como se presenta en la siguiente fórmula:

$$Valoración_{criterio} = \sum_{\substack{elementos \\ del\ criterio}} Porcentaje\ final_{elemento} * Valor\ calificación_{elemento}$$

Una vez calculadas las valoraciones de los criterios, se multiplica la valoración del criterio por el porcentaje final calculado anteriormente y se suman para obtener la valoración de la categoría, tal como se muestra en la siguiente fórmula:

$$Valoración_{categoría} = \sum_{\substack{criterios\ de \\ la\ categoría}} Porcentaje\ final_{criterio} * Valoración_{criterio}$$

Finalmente, para obtener la valoración final de la herramienta, se multiplica la valoración de la categoría por el porcentaje final de esta, y se suma el resultado de esta multiplicación de todas las categorías. En la siguiente fórmula, se muestra la fórmula de este cálculo:

$$Valoración_{herramienta} = \sum_{categorías} Porcentaje\ final_{categoría} * Valoración_{categoría}$$

Esta nota final será una nota sobre 100, representada como porcentaje y la herramienta con la valoración más alta será la seleccionada finalmente.

4.4 Ponderación de los criterios

Para saber cuánto van a puntuar cada uno de los elementos sobre la evaluación final, se deben definir los porcentajes de cada uno de los criterios y los elementos de evaluación. Primero, el equipo de Seguridad IT, formado por IT Security Director y por mí, definiremos los porcentajes iniciales para cada uno de los elementos de evaluación, criterios y categorías. Una vez definidos, debido a que el director de Sistemas va a participar en la remediación de las vulnerabilidades y el CIO y el CIO Deputy serán quienes supervisarán el proceso de gestión de vulnerabilidades, establecerán una ponderación por si quieren dar mayor importancia a algún elemento a la hora de valorar la herramienta.

Antes de establecer los porcentajes, debemos realizar escáneres de vulnerabilidades tanto internos como externos sobre los respectivos activos para poder extraer los elementos de evaluación de los criterios de Vulnerabilidades Detectadas. Por un lado, las vulnerabilidades detectadas en los escáneres internos serán los elementos de evaluación del criterio de Vulnerabilidades detectadas en la categoría de Detección de vulnerabilidades internas. Por otro lado, las vulnerabilidades detectadas en los escáneres externos serán los elementos de evaluación del criterio de Vulnerabilidades detectadas en la categoría de Detección de vulnerabilidades externas. Una vez realizados estos escáneres, se han obtenido 22 vulnerabilidades de los escáneres internos con severidad crítica y alta y 16 vulnerabilidades de la misma criticidad de los escáneres externos.

Una vez que ya tenemos todos los elementos de evaluación identificados, pasamos a definir los porcentajes de la nota de cada uno de los elementos sobre la nota final. Los porcentajes de las categorías se han definido en base a la criticidad o a la importancia que se le da en los trabajos vistos previamente en el estado del arte, dando mayor porcentaje a las categorías de Detección de vulnerabilidades internas y externas, ya que es un criterio evaluado en todos los trabajos vistos previamente, y menor peso a la categoría de Proveedores, ya que los criterios *Tamaño y presencia en mercado* y *Servicio y soporte* sólo aparecen en un trabajo respectivamente.

En las categorías de Detección de vulnerabilidades internas, se ha dado mayor porcentaje a la detección de vulnerabilidades que a la capacidad tecnológica ya que para el equipo de seguridad es más relevante la cantidad de vulnerabilidades a detectar que la capacidad tecnológica de la herramienta sobre las vulnerabilidades. Dentro de la capacidad tecnológica, se le ha dado mayor valor

al elemento de evaluación de Etiquetado e identificación de vulnerabilidades ya que deben estar correctamente identificadas y clasificadas para poder buscar información sobre las vulnerabilidades.

Dentro de la categoría de Detección de vulnerabilidades externas, se ha dado mayor porcentaje a la categoría de Bitsight, ya que es una de las necesidades por las que surge la elección de la herramienta. Los otros criterios se han evaluado con las mismas razones que en la categoría *Detección de vulnerabilidades internas.*

En la categoría de Funcionalidades, se ha dado mayor porcentaje a la gestión de vulnerabilidades que a la gestión de activos, ya que es la función principal de esta herramienta. Dentro de la gestión de inventario, se ha dado mayor valor a la clasificación de inventario ya que se ha considerado que es un punto importante a la hora de poder gestionar los activos y priorizar las vulnerabilidades. Otro elemento de evaluación importante tanto en el criterio de Gestión de inventario como en el criterio de Gestión de vulnerabilidades es el de Escáneres, ya que la configuración de los escáneres es la que te va a permitir identificar más o menos vulnerabilidades y activos.

Dentro de la categoría de Operativa, ambos criterios se establecieron con el mismo porcentaje. Dentro del criterio de escalabilidad, se le dio mayor importancia al elemento de Despliegue, debido a que el equipo de Seguridad es pequeño y es importante que la infraestructura tecnológica sea sencilla para poder gestionarse correctamente.

Por último, en la categoría de Proveedores, el porcentaje es mayor en el criterio de Servicio y Soporte, concretamente los criterios de Atención personal y Tiempos de servicio, ya que se consideró más relevante que el proveedor reaccionara con calidad y con tiempo a posibles problemas. También se dio mayor porcentaje a las licencias y al precio, ya que fue un criterio específico para la empresa y es importante tener en cuenta si la herramienta está dentro del presupuesto y lo que supondría ampliar activos a futuro.

Una vez identificados estos porcentajes iniciales, se indica el valor de ponderación en cada uno de los criterios. En este caso, el CIO, el CIO Deputy y el director de Sistemas han querido dar mayor importancia a los siguientes aspectos:

- Las vulnerabilidades con un CVSS elevado. A pesar de que las herramientas han clasificado con niveles la criticidad de las vulnerabilidades, se ha decidido dar mayor valor a las vulnerabilidades con un CVSS alto, ya que según el estándar tienen mayor riesgo.
- Las categorías de amenazas externas. Además, de que este tipo de vulnerabilidades son más críticas debido a que son activos publicados en internet, se ha decido que tengan un valor mayor en la puntuación final debido a que son las vulnerabilidades detectadas por Bitsight y, como se comentaba previamente, es un punto importante para dirección mejorar la puntuación de ciberseguridad dad por esta empresa.

- El criterio de licencias y precio. La compañía dispone de un presupuesto para esta herramienta y este es un punto importante a la hora de evaluarla.

Una vez revisados todos los criterios y teniendo en cuenta estos puntos, los porcentajes base, ponderaciones y porcentaje final ha sido evaluado tal como se presenta en la Tabla 5:

Categorías	Criterios de evaluación	Elementos de evaluación	Porcentaje Base	Valor ponderación	Porcentaje medio	Porcentaje final
Vulnerabilidades internas			25,00%	2	25,00%	22,22%
	Vulnerabilidades detectadas		75,00%	2	75,00%	75,00%
		Critical Vulnerability	4,55%	4	6,82%	5,83%
		Critical Vulnerability	4,55%	3	5,68%	4,85%
		Critical Vulnerability	4,55%	3	5,68%	4,85%
		Critical Vulnerability	4,55%	4	6,82%	5,83%
		Critical Vulnerability	4,55%	4	6,82%	5,83%
		Critical Vulnerability	4,55%	4	6,82%	5,83%
		Critical Vulnerability	4,55%	3	5,68%	4,85%
		Critical Vulnerability	4,55%	3	5,68%	4,85%
		High Vulnerability	4,55%	2	4,55%	3,88%
		High Vulnerability	4,55%	3	5,68%	4,85%
		High Vulnerability	4,55%	2	4,55%	3,88%
		High Vulnerability	4,55%	2	4,55%	3,88%
		High Vulnerability	4,55%	2	4,55%	3,88%
		High Vulnerability	4,55%	2	4,55%	3,88%
		High Vulnerability	4,55%	2	4,55%	3,88%
		High Vulnerability	4,55%	2	4,55%	3,88%
		High Vulnerability	4,55%	3	5,68%	4,85%
		High Vulnerability	4,55%	2	4,55%	3,88%
		High Vulnerability	4,55%	2	4,55%	3,88%
		High Vulnerability	4,55%	2	4,55%	3,88%
		High Vulnerability	4,55%	2	4,55%	3,88%
		High Vulnerability	4,55%	3	5,68%	4,85%
	Capacidad tecnológica		25,00%	2	25,00%	25,00%
		Etiquetado e identificación de vulnerabilidades	40,00%	2	40,00%	40,00%
		Evaluación de la criticidad de los activos	30,00%	2	30,00%	30,00%
		Actualización de la base de datos de las vulnerabilidades	30,00%	2	30,00%	30,00%
Vulnerabilidades externas			25,00%	4	37,50%	33,33%
	Vulnerabilidades detectadas		25,00%	2	25,00%	25,00%
		Critical Vulnerability	9,09%	2	9,09%	9,09%
		Critical Vulnerability	9,09%	2	9,09%	9,09%
		Critical Vulnerability	9,09%	2	9,09%	9,09%
		High Vulnerability	9,09%	2	9,09%	9,09%
		High Vulnerability	9,09%	2	9,09%	9,09%
		High Vulnerability	9,09%	2	9,09%	9,09%

		High Vulnerability	9,09%	2	9,09%	9,09%
		High Vulnerability	9,09%	2	9,09%	9,09%
		High Vulnerability	9,09%	2	9,09%	9,09%
		High Vulnerability	9,09%	2	9,09%	9,09%
		High Vulnerability	9,09%	2	9,09%	9,09%
	Capacidad tecnológica		20,00%	2	20,00%	20,00%
		Etiquetado e identificación de vulnerabilidades	40,00%	2	40,00%	40,00%
		Evaluación de la criticidad de los activos	30,00%	2	30,00%	30,00%
		Actualización de la base de datos de las vulnerabilidades	30,00%	2	30,00%	30,00%
	BitSight detection		55,00%	2	55,00%	55,00%
		Medium Vulnerability	20,00%	2	20,00%	20,00%
		Medium Vulnerability	20,00%	2	20,00%	20,00%
		High Vulnerability	20,00%	2	20,00%	20,00%
		Medium Vulnerability	20,00%	2	20,00%	20,00%
		Medium Vulnerability	20,00%	2	20,00%	20,00%
Funcionalidades			20,00%	2	20,00%	17,78%
	Gestión del inventario		20,00%	2	20,00%	20,00%
		Clasificación del inventario	40,00%	2	40,00%	40,00%
		Representación gráfica de los activos	10,00%	2	10,00%	10,00%
		Identificación	30,00%	2	30,00%	30,00%
		Informes	10,00%	2	10,00%	10,00%
		Escáneres	10,00%	2	10,00%	10,00%
	Gestión de vulnerabilidades		80,00%	2	80,00%	80,00%
		Priorización	20,00%	2	20,00%	20,00%
		Escáneres	12,50%	2	12,50%	12,50%
		Integración	30,00%	2	30,00%	30,00%
		Monitorización	12,50%	2	12,50%	12,50%
		Completitud de la información	12,50%	2	12,50%	12,50%
		Exportación de los datos	12,50%	2	12,50%	12,50%
Operativa			15,00%	2	15,00%	13,33%
	Escalabilidad		50,00%	2	50,00%	50,00%
		Despliegue	40,00%	2	40,00%	40,00%
		Número de activos	15,00%	2	15,00%	15,00%
		Requerimientos	15,00%	2	15,00%	15,00%
		Gestión de usuarios	0,00%	2	15,00%	15,00%
		Personalización	15,00%	2	15,00%	15,00%
	Herramienta de ayuda		50,00%	2	50,00%	50,00%
		Herramienta de ayuda	100,00%	2	100,00%	100,00%
Vendors			15,00%	2	15,00%	13,33%
	Tamaño y presencia en el mercado		15,00%	2	15,00%	14,48%
		Años de experiencia	20,00%	2	20,00%	20,00%
		Número de empleados	20,00%	2	20,00%	20,00%
		Número de oficinas	20,00%	2	20,00%	20,00%
		Localización de las oficinas	20,00%	2	20,00%	20,00%
		Ventas	20,00%	2	20,00%	20,00%
	Servicio y soporte		45,00%	2	45,00%	43,44%

		Disponibilidad	10,00%	2	10,00%	10,00%
		Referencias	10,00%	2	10,00%	10,00%
		Atención personal	40,00%	2	40,00%	40,00%
		Tiempos de servicio	40,00%	2	40,00%	40,00%
	Licencias y precio		40,00%	3	50,00%	48,27%
		Precio fijo	33,33%	3	41,67%	33,33%
		Precio recurrente	33,33%	4	50,00%	40,00%
		Descuento	33,33%	2	33,33%	26,67%

Tabla 5. Porcentajes de los elementos de evaluación, criterios y categorías

4.5 Evaluación de los criterios

Para el proceso de evaluación de los criterios, se han llevado a cabo de unas pruebas para evaluar los criterios definidos. Para las primeras 4 categorías, se ha decidido seguir las siguientes fases: puesta en marcha y preparación de las herramientas, escaneo de vulnerabilidades, revisión de vulnerabilidades y remediación. Estas fases se han definido basándose en el proceso la gestión de vulnerabilidades visto previamente de (Palmaers 2013)

En la primera fase, se solicitará a los proveedores una licencia de periodo de prueba de las herramientas para darnos acceso a la plataforma *cloud*. Una vez con el usuario de acceso, se revisarán los requerimientos de las tres herramientas y se realizará la instalación de estas. Una vez instaladas, se crearán los usuarios que deben acceder a la herramienta para realizar las pruebas para así poder tener un primer contacto con la herramienta y estudiar las funcionalidades que pueden hacer y cómo pueden hacerlas. También se deben introducir los activos del alcance en la herramienta.

En la fase de escaneo de vulnerabilidades, se empezarán a realizar los escáneres de los activos. Primero, se debe empezar realizando un escáner de descubrimiento. Esto quiere decir realizar un escáner que revise los puertos comunes que tienen abiertos los activos y obtiene información del servidor, como los servicios que corren por estos puertos, el sistema operativo, etc.

Una vez realizado este escáner, se pasa a realizar un escáner de nivel intermedio que revise las vulnerabilidades de los puertos comunes que tiene abiertos. Por último, se realiza un escáner de alto alcance para que escanee todos los puertos del servidor y todas las vulnerabilidades incluidas en la base de datos de la herramienta. Hay dos tipos de escáneres para detectar las vulnerabilidades: por un lado, los escáneres de vulnerabilidades de red y que se realizarán desde dentro de la red de la compañía sobre los activos internos, y por otro lado, los escáneres de vulnerabilidades web, que se realizará desde la red pública sobre las aplicaciones web seleccionadas.

Una vez realizados los escáneres y detectadas las vulnerabilidades, pasamos a la fase de revisión de vulnerabilidades, donde se revisará la información disponible de cada una de las vulnerabilidades y se extraerán diferentes informes para observar cómo de personalizables son, qué tipo de información permite extraer y cómo representa dicha información.

Con los informes ya generados, se pasa a la fase de Remediación. En este punto, se observarán las diferentes medidas que tiene la herramienta para

gestionar las vulnerabilidades abiertas, las funcionalidades que dispone para priorizarlas y la información disponible sobre su remediación.

Para evaluar la última categoría, la categoría de Proveedores, se debe realizar una búsqueda de la información de los proveedores, solicitar el presupuesto a cada uno de ellos y se debe ir observando su atención al cliente y los tiempos de respuesta para los diferentes problemas que surjan durante el proceso de evaluación.

4.5.1 Vulnerabilidades internas

Este criterio ha sido evaluado en la fase de revisión de las vulnerabilidades, donde se han analizado las vulnerabilidades detectadas por cada uno de los activos internos. Para poder compararlas, se han listado y agrupado las vulnerabilidades críticas y altas detectadas en los activos que se han escaneado internamente. Una vez las vulnerabilidades agrupadas, se ha ido indicando en cada una de ellas qué herramientas las ha detectado. En este análisis de vulnerabilidades internas, cómo se ha indicado anteriormente, se han detectado 8 vulnerabilidades críticas y 14 vulnerabilidades altas, de las cuales, hay 4 vulnerabilidades altas que sólo ha identificado Rapid7, 1 que sólo ha identificado Qualys y 1 que sólo ha identificado Tenable. En la tabla, se muestra más detalle de las vulnerabilidades detectadas por cada una de las herramientas.

Al realizar esta comparación entre las vulnerabilidades detectadas por cada uno de los activos, se ha revisado también el elemento de evaluación de la identificación y etiquetado. Las tres herramientas disponen del identificador CVE de la vulnerabilidad e incluso identificadores de otras bases de datos. También las tres herramientas etiquetan o agrupan las vulnerabilidades por diferentes campos el tipo de impacto o amenaza de la vulnerabilidad. Sin embargo, debido a que Qualys y Rapid7 disponen de más campos que Tenable, proporcionando así más información sobre la vulnerabilidad, facilitan más la identificación de la vulnerabilidad y sus características, por tanto, han tenido una calificación superior a Tenable, siendo igualmente bien calificada esta última.

Para evaluar el elemento de Evaluación de la criticidad, se ha revisado si todas las herramientas han clasificado con los mismos niveles las vulnerabilidades críticas y altas. Debido a que todas las vulnerabilidades han sido igual valoradas, se han valorado con el mismo nivel.

Respecto al elemento de evaluación de Actualización de la base de datos, todas las herramientas tardan 1 o 2 días en añadir la detección de una nueva vulnerabilidad, por tanto, han sido calificadas todas al mismo nivel.

En la Tabla 6, se muestran las valoraciones para cada uno de los elementos de evaluación:

Criterio	Elemento de evaluación	Porcentaje final	Valor calificación		
			Tenable	Qualys	Rapid7
Vulnerabilidades detectadas		**75,00%**	**66,99%**	**80,58%**	**82,52%**
	Critical Vulnerability	*5,83%*	yes	yes	yes
	Critical Vulnerability	*4,85%*	yes	yes	no
	Critical Vulnerability	*4,85%*	no	yes	yes

	Critical Vulnerability	*5,83%*	yes	yes	yes
	Critical Vulnerability	*5,83%*	yes	yes	yes
	Critical Vulnerability	*5,83%*	yes	yes	yes
	Critical Vulnerability	*4,85%*	yes	yes	yes
	Critical Vulnerability	*4,85%*	yes	yes	no
	High Vulnerability	*3,88%*	no	yes	yes
	High Vulnerability	*4,85%*	no	yes	yes
	High Vulnerability	*3,88%*	no	yes	no
	High Vulnerability	*3,88%*	no	no	yes
	High Vulnerability	*3,88%*	no	no	yes
	High Vulnerability	*3,88%*	no	no	yes
	High Vulnerability	*3,88%*	yes	yes	yes
	High Vulnerability	*3,88%*	yes	yes	yes
	High Vulnerability	*4,85%*	yes	yes	yes
	High Vulnerability	*3,88%*	yes	no	no
	High Vulnerability	*3,88%*	yes	yes	yes
	High Vulnerability	*3,88%*	no	no	yes
	High Vulnerability	*3,88%*	yes	yes	yes
	High Vulnerability	*4,85%*	yes	yes	yes
Capacidad tecnológica		**25,00%**	**75,00%**	**85,00%**	**85,00%**
	Etiquetado e identificación de vulnerabilidades	40,00%	4	5	5
	Evaluación de la criticidad de los activos	30,00%	4	4	4
	Actualización de la base de datos de las vulnerabilidades	30,00%	4	4	4

Tabla 6. Evaluación de la categoría Vulnerabilidades Internas

4.5.2 Vulnerabilidades externas

Al igual que en la categoría anterior, se han agrupado las vulnerabilidades de aplicación críticas y altas detectadas para los activos publicados en Internet y se ha indicado con sí o no cada una de las vulnerabilidades, para así indicar si la herramienta la ha detectado o no. En esta categoría, se han detectado 3 vulnerabilidades críticas y 8 vulnerabilidades altas, de las cuales 1 ha sido identificada únicamente por Qualys.

Respecto al criterio de capacidad tecnológica, se han evaluado las herramientas igual que en la categoría de Vulnerabilidades internas. Con respecto al elemento de Identificación y etiquetación, al igual que en la anterior categoría, las tres tienen informados para cada vulnerabilidad identificadores estándar y otras características para calificarlas. Sin embargo, la herramienta que más campos dispone para clasificar o etiquetar las vulnerabilidades en base a sus características es Qualys, por tanto, ha obtenido mejor calificación con respecto a Rapid7 y Tenable.

Respecto a los elementos de Evaluación de la criticidad y Actualización de la base de datos de las vulnerabilidades se han calificado al mismo nivel ya que todas las vulnerabilidades han sido identificadas con la misma criticidad en las tres herramientas y la actualización de la base de datos de vulnerabilidades de aplicaciones web es igual que para la base de datos de vulnerabilidades de red.

Por último, se ha evaluado el criterio de Bitsight, indicando con sí o no cada una de las vulnerabilidades de Bitsight que han detectado cada una de las herramientas. En este caso, todas han identificado estas vulnerabilidades, por tanto, todas tienen una puntuación de 100% en este criterio.

En la Tabla 7, se observan las valoraciones de todos los elementos de evaluación para la categoría de Vulnerabilidades externas:

Criterio	Elemento de evaluación	Porcentaje final	Valor calificación		
			Tenable	Qualys	Rapid 7
Vulnerabilidades detectadas		**25,00**	**72,73%**	**90,91%**	**90,91%**
	Critical Vulnerability	9,09%	yes	yes	yes
	Critical Vulnerability	9,09%	yes	yes	yes
	Critical Vulnerability	9,09%	no	yes	yes
	High Vulnerability	9,09%	yes	yes	yes
	High Vulnerability	9,09%	yes	yes	yes
	High Vulnerability	9,09%	yes	yes	yes
	High Vulnerability	9,09%	no	yes	no
	High Vulnerability	9,09%	yes	no	yes
	High Vulnerability	9,09%	no	yes	yes
	High Vulnerability	9,09%	yes	yes	yes
	High Vulnerability	9,09%	yes	yes	yes
Capacidad tecnológica		**20,00%**	***75,00%***	***85,00%***	***75,00%***
	Etiquetado e identificación de vulnerabilidades	*40,00%*	4	5	4
	Evaluación de la criticidad de los activos	*30,00%*	4	4	4
	Actualización de la base de datos de las vulnerabilidades	*30,00%*	4	4	4
Bitsight detection		**55,00%**	**100,00%**	**100,00%**	**100,00%**
	Medium Vulnerability	*20,00%*	yes	yes	yes
	Medium Vulnerability	*20,00%*	yes	yes	yes
	High Vulnerability	*20,00%*	yes	yes	yes
	Medium Vulnerability	*20,00%*	yes	yes	yes
	Medium Vulnerability	*20,00%*	yes	yes	yes

Tabla 7. Evaluación de la categoría Vulnerabilidades Externas

4.5.3 Funcionalidades

En esta categoría, se ha evaluado el criterio de gestión de activos por un lado y el criterio de gestión de vulnerabilidades por otro, revisando las funcionalidades que tienen las herramientas para cada uno de los criterios.

De los elementos de evaluación del Criterio de activos, la mejor puntuación la tiene la herramienta de Qualys debido a que tiene la mejor puntuación en los elementos de representación gráfica y en escaneos. Para probar evaluar estos dos criterios, se configuraron escáneres de descubrimiento y se observaron los cuadros de mando de gestión de inventario y el listado de los activos para ver a la representación gráfica después de los descubrimientos.

En el caso de los escáneres, todas las herramientas disponen de plantillas para realizar escaneos de descubrimiento, pero a la hora de modificar la configuración de este escáner, Qualys fue considerado el más intuitivo. Además, esta herramienta dispone de un tipo de escaneos de descubrimiento llamado mapas, los cuales te permiten descubrir dispositivos de red y una vez finalizado, muestra un listado de los activos identificados y puedes seleccionar los activos que se quieran añadir al análisis de vulnerabilidades. Rapid7 ha tenido una puntuación más baja ya que, a pesar de ser muy completos, estos son complejos de configurar y deben realizarse desde el servidor local, es decir, no es posible crear o modificar ningún escaneo desde la aplicación de la nube.

En el caso de la representación gráfica, los listados de activos se mostraban bastante similares en todas las herramientas, pero Qualys destaca gracias a los mapas, ya que, una vez finalizado este tipo de escáneres, además de poder visualizar una lista, te muestra los activos en modo gráfico para que puedas ver desde que dispositivos de red ha encontrado cada uno de los servidores. En la Ilustración 4, se muestra un ejemplo del resultado de un mapa en Qualys, donde se puede observar las relaciones entre los diferentes servidores y los routers:

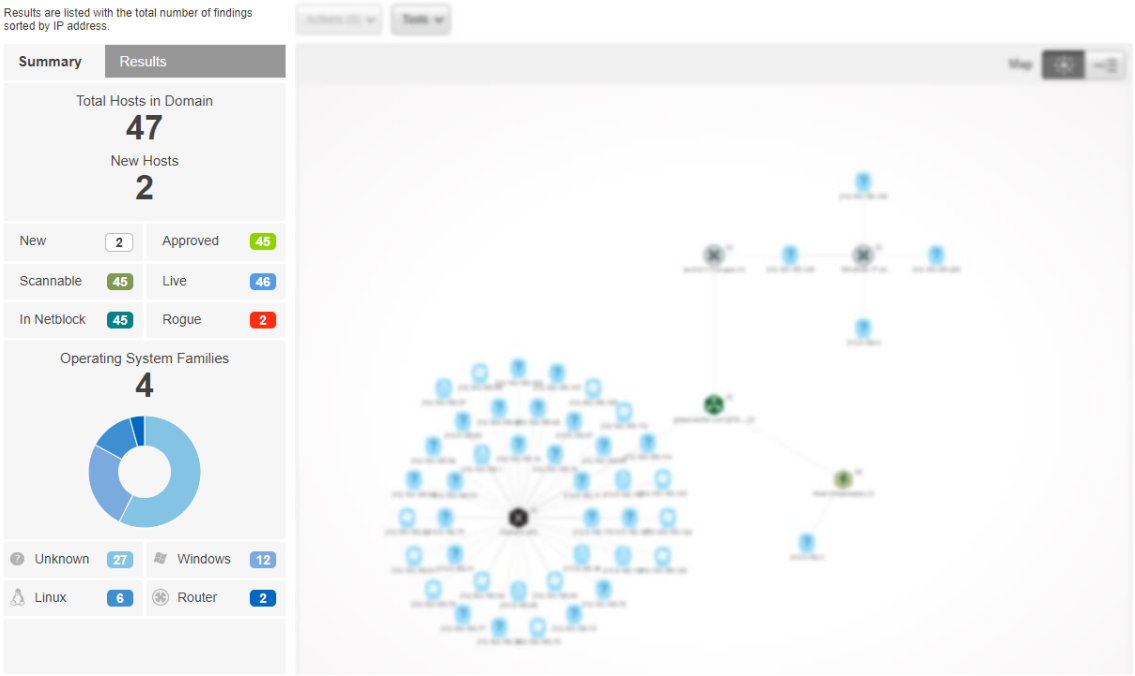

Ilustración 4. Ejemplo de la representación gráfica de un mapa en Qualys

En el elemento de clasificación de inventario, queda al mismo nivel de Rapid7, ya que ambas disponen de similares características para clasificar los activos por criticidad. En ambas herramientas, la clasificación se realiza creando grupos de activos y asignándoles una criticidad, a diferencia de Tenable, donde se debe asignar la criticidad individualmente por cada uno de los activos.

Rapid7 se ha calificado con mayor puntuación en los informes de los activos, ya que dispone de información más completa y detallada de los activos. Tenable tiene una puntuación más baja en este punto debido a que los reports no son personalizables, sólo permite generar reports con las plantillas que dispone. En el elemento de identificación, se han puntuado todos con el mismo valor, ya que

en las tres herramientas se utiliza el nombre del dominio del servidor o, en el caso de que no disponga de este, la dirección IP.

Respecto a los elementos de evaluación para el criterio de gestión de vulnerabilidades, también tiene la mayor valoración Qualys. Esta herramienta destaca en la priorización, ya que dispone de un módulo específico para priorizar las vulnerabilidades y agrupar las soluciones para eliminarlas, incluso indicando si dispone de parche o no para su resolución. En la Ilustración 5, se puede observar el módulo de priorización, donde puedes seleccionar los activos a analizar y te muestra los activos que deben priorizarse en base a los filtros seleccionados. También te muestra las vulnerabilidades a priorizar (Instancias) en base al filtro y el número de resoluciones para remediar las vulnerabilidades a priorizar (Unique), así como si hay parches disponibles para remediarlas. Por ejemplo, de una versión no actualizada del sistema operativo, pueden aparecer varias vulnerabilidades, pero sólo es necesario una acción para resolverla que sería la instalación del parche, es decir, la actualización del sistema operativo.

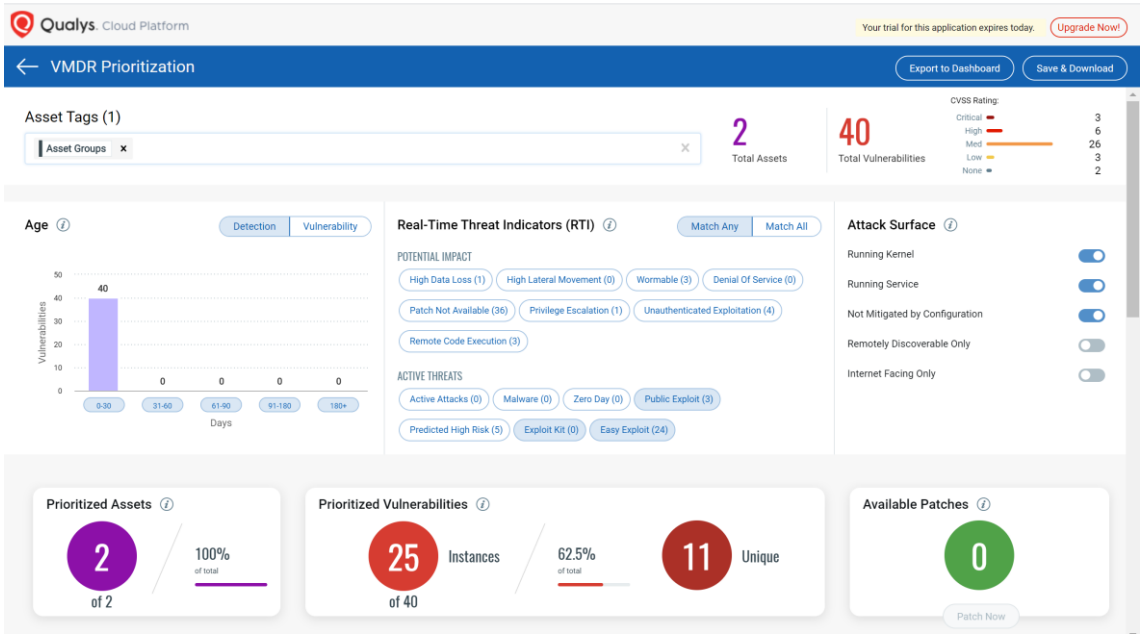

Ilustración 5. Módulo de priorización de Qualys

Respecto a los elementos de integración con otras herramientas y exportación de los datos, las tres han sido calificadas con buena puntuación, ya que permiten sincronizarse con cualquier tipo de herramienta (SIEM, firewalls, etc.) mediante el uso de APIs, y la información de las vulnerabilidades puede exportarse en diferentes formatos (csv, pdf, html, etc.) en las tres herramientas.

Al igual que en el elemento de evaluación de Escáneres en el criterio de gestión de activos, Qualys ha sido calificado con una puntuación alta debido a que los escáneres son muy intuitivos. Tenable se ha calificado también con una nota elevada en los escaneos ya que son fáciles de configurar y dispone de varias tipologías de escáneres ya preconfigurados para determinadas certificaciones. En la Ilustración 6, se pueden ver todas las plantillas de las que dispone Tenable y se puede observar que es bastante intuitivo visualmente:

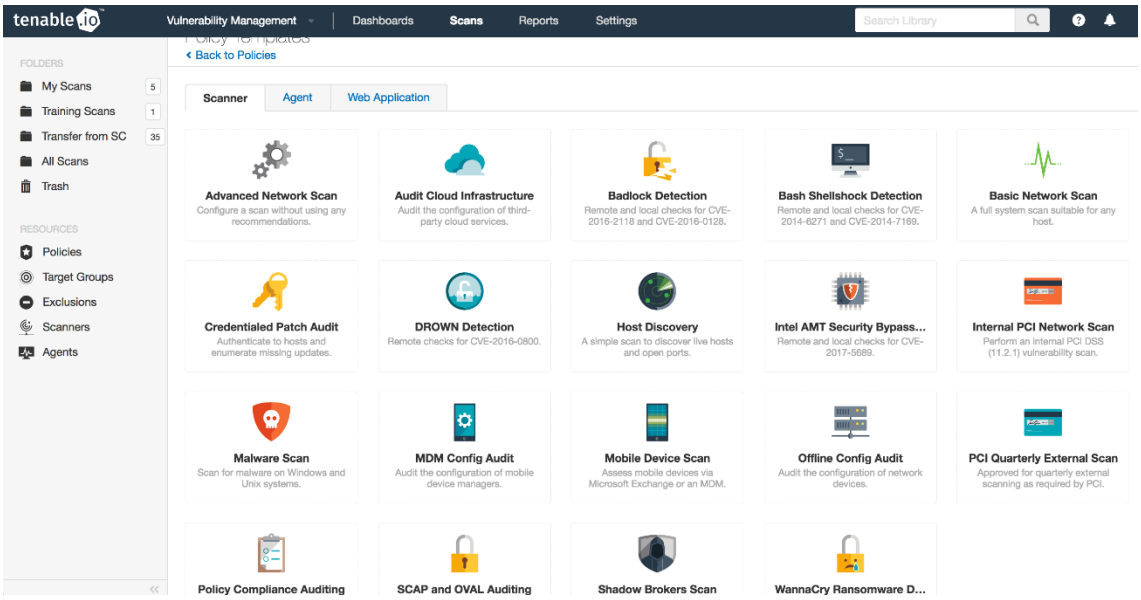

Ilustración 6. Plantillas de escáner en Tenable

Rapid7 dispone también de un alto catálogo de escáneres, pero es más complejo de lanzar, ya que siempre debes enlazarlo a un grupo de activos (llamados Sites) y asociar la plantilla de escaneo que necesites lanzar. Además, debe ser configurado en local, al igual que los escáneres de inventario de activos. En la Ilustración 7, se puede ver la configuración de un Site, es decir, un grupo de activos, desde el cual se configuran la plantilla de escaneo que se van a lanzar para los activos pertenecientes a este grupo:

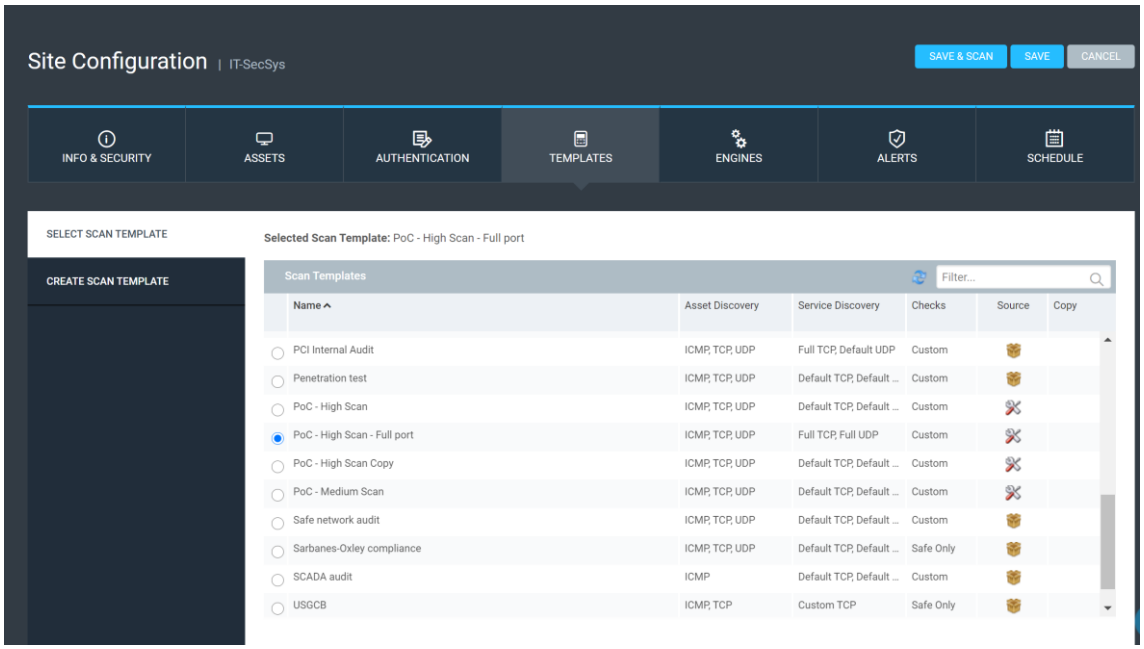

Ilustración 7. Configuración de un Site en Rapid7

Sin embargo, Tenable se ha penalizado bastante en el elemento de Completitud de la información, ya que mientras las otras herramientas ofrecen bastante información sobre la vulnerabilidad cómo detalle de la vulnerabilidad, información sobre la explotación o sobre cómo remediarla, Tenable sólo proporciona una descripción de la vulnerabilidad y ofrece un link externo de la aplicación a la base

de datos global de vulnerabilidades de Tenable para más información sobre esta. Rapid 7 tiene mayor puntuación ya que sus soluciones de remediación eran técnicamente mucho más completas que las de Qualys.

Rapid7 también destaca en la monitorización de la evaluación, ya que dispone de un módulo que permite agrupar las vulnerabilidades a ser resueltas y ser gestionadas como un proyecto, permitiendo indicar comentarios en cada una de ellas, si está resuelta o no, reescanear el activo de nuevo para ver si ha sido remediada o no, asignar la remediación a usuarios, etc. En la Ilustración 8, se muestra un ejemplo de un proyecto de remediación, en el cual se incluyeron todas las vulnerabilidades relacionadas con versiones de certificados SSL obsoletos:

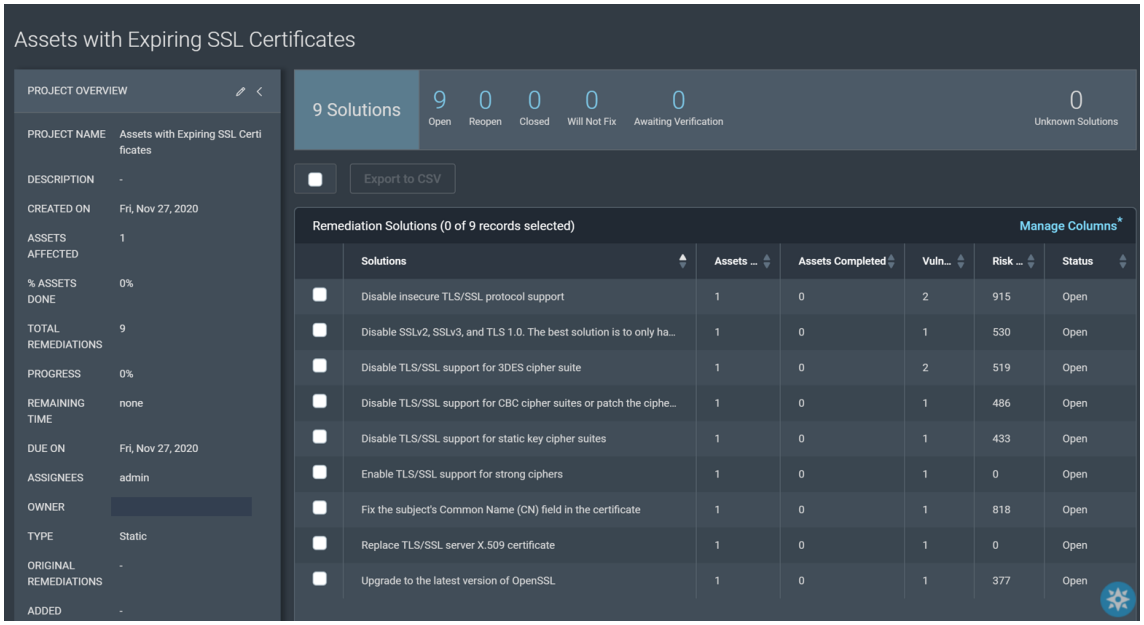

Ilustración 8. Ejemplo de proyecto de remediación de Rapid7

Qualys dispone de un módulo de remediación que permite crear tickets por vulnerabilidades, ya sea de forma manual o de forma automática mediante reglas configurables por el usuario, y asignarlos al responsable que deba solucionarlas. Sin embargo, Tenable sólo dispone de informes de seguimiento y comentarios en la propia vulnerabilidad.

En la tabla 8, se muestra el resumen de la calificación de los diferentes elementos de evaluación para los criterios de Inventario y gestión de vulnerabilidades:

Criterio	Elemento de evaluación	Porcentaje final	Valor calificación		
			Tenable	Qualys	Rapid 7
Gestión de inventario		**20,00%**	**72,50%**	**95,00%**	**72,50%**
	Clasificación del inventario	40,00%	4	5	5
	Representación gráfica de los activos	10,00%	4	5	4
	Identificación	30,00%	4	5	2
	Informes	10,00%	4	4	4
	Escáneres	10,00%	3	4	5

Gestión de vulnerabilidades		**80,00%**	**82,50%**	**93,75%**	**80,00%**
	Priorización	20,00%	4	5	4
	Escáneres	12,50%	5	5	5
	Integración	30,00%	5	5	3
	Monitorización	12,50%	3	4	5
	Completitud de la información	12,50%	3	4	5
	Exportación de los datos	12,50%	5	5	5

Tabla 8. Evaluación de la categoría Funcionalidades

4.5.4 Operativa

En el criterios de escalabilidad, las herramientas han sido calificadas bastante equitativamente, a excepción de algunos elementos de evaluación. En el caso del elemento de Máximo y mínimo de activos, las aplicaciones no disponen de máximo o mínimo de activos a incluir en la herramienta, pero las licencias si tienen un mínimo de activos a contratar. En el caso de Rapid7 y Qualys el mínimo de licencia a contratar es de 128 y en el caso de Tenable es 60 activos, por eso su puntuación es un superior a la demás herramientas.

En las especificaciones para los servidores, Rapid7 ha tenido peor valoración y Tenable la mejor, ya que el dispositivo local que se debe instalar para realizar los escáneres internos requería muchos espacio de disco (100 GB) y memoria RAM (8 gigabytes). Esto se debe a que toda la información es almacenada en local y luego enviada al cloud. El dispositivo de Qualys es un servidor virtual que también ocupa bastante de disco duro (unos 50GB), pero de memoria RAM requiere muy poco (2 gigabytes). Tenable es más ligero y por eso ha sido el mejor valorado: sólo memoria RAM de 1GB y 2 GB de disco duro.

Respecto a los elementos de Despliegue de la aplicación y Simultaniedad, las tres tuvieron una complejidad similar para instalarlas, ya que para las tres se requería de un servidor virtual para instalar los dispositivos de escaneo y en las tres herramientas pueden trabajar varios usuarios de manera simultanea sin afectar las acciones que estén realizando.

Respeto a la personalización, Qualys se ha calificado mejor que las demás herramientas, ya que, a pesar de que los cuadros de mando eran personalizables en las tres herramientas, en Qualys te permite configurar tus propios gráficos además de los gráficos predeterminados de la herramienta. En la Ilustración 9, se pueden observar la configuración de un gráfico nuevo, donde se observan las diferentes opciones de personalización, como filtros, elección del tipo de gráfico (tabla, gráfico de barras, etc.) e incluso colores:

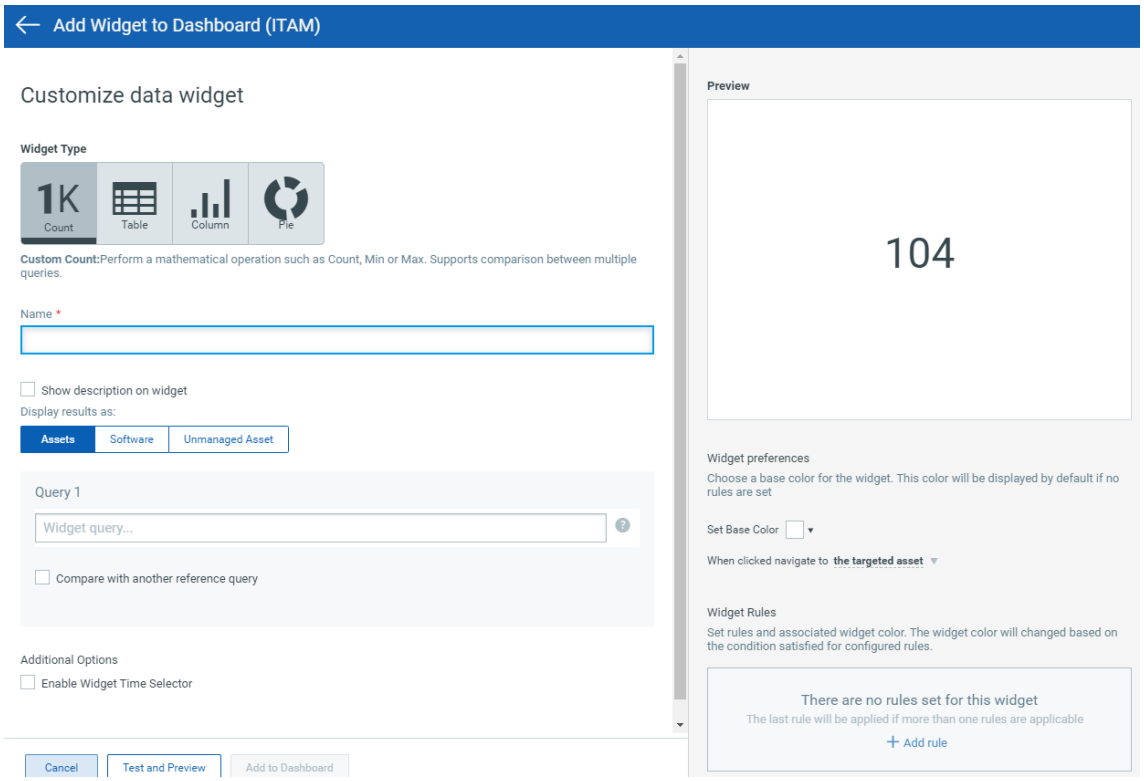

Ilustración 9. Configuración de un gráfico en Qualys

Por último, con respecto al criterio de Herramienta de ayuda, se han calificado las tres herramientas con la misma puntuación, ya que a la hora de probar las herramientas y buscar información sobre cómo hacer las diferentes tareas, la información era muy completa, facilmente accesible desde cualquier ventana de la herramienta, además de estar bien estructurada para poder buscar fácilmente la información necesaria.

En la Tabla 9, se pueden observar los valores de calificación indicados para cada uno de los elementos:

Criterio	Elemento de evaluación	Porcentaje final	Valor calificación		
			Tenable	Qualys	Rapid 7
Escalabilidad		**50,00%**	**82,50%**	**78,75%**	**71,25%**
	Despliegue	40,00%	4	4	4
	Número de activos	15,00%	5	4	4
	Requerimientos	15,00%	5	4	3
	Gestión de usuarios	15,00%	5	5	5
	Personalización	15,00%	4	4	4
Herramienta de ayuda		**50,00%**	**75,00%**	**75,00%**	**75,00%**
	Herramienta de ayuda	*100,00%*	4	4	4

Tabla 9. Evaluación de la categoría Operativa

4.5.5 Proveedores

En el criterio de tamaño y presencias, las tres herramientas quedan igualadas, ya que las tres son las herramientas líderes en su sector y, por tanto, los proveedores de estas tres herramientas disponen de muchos años de

experiencia, alto número de empleados y de oficinas distribuidas por todo el mundo, además de ofrecer servicio en todas a ellas a un elevado número de clientes.

Respecto al criterio de Servicio y Soporte, concretamente en los elementos de Disponibilidad del proveedor y Referencias de otras compañías, todas han estado disponibles en caso de cualquier duda o necesidad de renovación y sus referencias de otras empresas han sido buenas. Sin embargo, en los elementos de Atención personal y Rapidez de resolución, Tenable ha obtenido menor puntuación respecto a las otras. Esto fue debido a que hubo que renovar el periodo de prueba en las tres herramientas y en el caso de Tenable, tardó más de una semana en realizar la renovación, a pesar de realizar varias comunicaciones con ellos e indicar que lo harían ese mismo día, cuando las otras herramientas realización la renovación el mismo día de la solicitud.

Por último, en el criterio de Precios y licencias, se tomaron en cuenta las licencias para el escaneo de vulnerabilidades de red en servidores como las licencias para escaneos de vulnerabilidades de aplicaciones web. Todas las herramientas entraban dentro del presupuesto previsto para la implementación de esta herramienta, por tanto, se compararon los precios de las tres y en base a los precios, se calificaron con una puntuación u otra. Debido a que cada una de las herramientas ofrecía un número diferente de licencias de inicio para la implementación, se calculó el precio unitario por licencia y se compararon para calificar el elemento de evaluación de Precio Fijo. Para el elemento de evaluación de precio recurrente, se compararon los precios por licencia por ampliación una vez implementada la herramienta.

Para el escaneo de vulnerabilidades de red en servidores, todas las licencias tienen un coste similar, tanto para la contratación inicial, como para la recurrente, siendo Rapid7 el más económico, aunque por poca diferencia. Sin embargo, los precios para el escaneo de vulnerabilidades de aplicaciones web era mucho más elevado en Rapid7 frente a las otras dos herramientas, ya que costaba más del doble por licencia. Respecto al descuento, todos los comerciales ofrecían el mismo descuento para contratar la herramienta que ofrecían.

En la Tabla 10, se resumen los valores de calificación asignados a cada uno de los elementos de evaluación de esta categoría:

Criterio	Elemento de evaluación	Porcentaje final	Valor calificación		
			Tenable	Qualys	Rapid 7
Tamaño y presencia en el mercado		**13,64%**	**75,00%**	**75,00%**	**75,00%**
	Años de experiencia	20,00%	4	4	4
	Número de empleados	20,00%	4	4	4
	Número de oficinas	20,00%	4	4	4
	Localización de las oficinas	20,00%	4	4	4
	Ventas	20,00%	4	4	4
Servicio y soporte		**40,91%**	**65,00%**	**95,00%**	**95,00%**
	Disponibilidad	10,00%	4	4	4
	Referencias	10,00%	4	4	4
	Atención personal	40,00%	4	5	5
	Tiempos de servicio	40,00%	3	5	5

Licencias y precio		**45,45%**	**93,33%**	**93,33%**	**75,00%**
	Precio fijo	33,33%	5	5	4
	Precio recurrente	40,00%	5	5	4
	Descuento	26,67%	4	4	4

Tabla 10. Evaluación de la categoría Proveedores

4.6 Evaluación final

Una vez evaluadas las tres herramientas y puntuados los criterios, podemos ver en Tabla 11, el resumen de las valoraciones de todos los criterios:

Categorías	Criterios	Porcentaje final	Valoración		
			Tenable	Qualys	Rapid7
1. Detección de vulnerabilidades internas		**22,22%**	68,99%	81,69%	**83,14%**
	Vulnerabilidades detectadas	75,00%	66,99%	80,58%	82,52%
	Capacidad tecnológica	25,00%	75,00%	85,00%	85,00%
2. Detección de vulnerabilidades externas		**33,33%**	88,18%	**94,73%**	92,73%
	Vulnerabilidades detectadas	25,00%	72,73%	90,91%	90,91%
	Capacidad tecnológica	20,00%	75,00%	85,00%	75,00%
	BitSight detection	55,00%	100,00%	100,00%	100,00%
3. Funcionalidades		**17,78%**	80,50%	**94,00%**	78,50%
	Gestión de inventario	20,00%	72,50%	95,00%	72,50%
	Gestión de vulnerabilidades	80,00%	82,50%	93,75%	80,00%
4. Operativa		**13,33%**	**78,75%**	76,88%	73,13%
	Escalabilidad	50,00%	82,50%	78,75%	71,25%
	Herramienta de ayuda	50,00%	75,00%	75,00%	75,00%
5. Proveedores		**13,33%**	79,24%	**91,52%**	83,18%
	Tamaño y presencia en el mercado	13,64%	75,00%	75,00%	75,00%
	Servicio y soporte	40,91%	65,00%	95,00%	95,00%
	Licencias y precio	45,45%	93,33%	93,33%	75,00%

Tabla 11. Valoración de los criterios y categorías

De estas valoraciones, se han extraído las valoraciones por categorías y se han representado a modo de gráfico, que puede verse en la Ilustración 10:

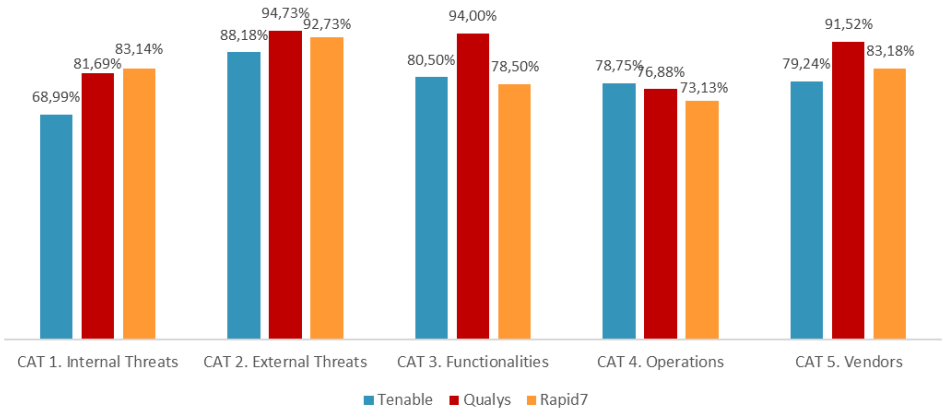

Ilustración 10. Comparativa de puntuaciones por categorías

Rapid7 es la herramienta con mejor valoración para la categoría de vulnerabilidades internas. Esto se debe a que ha sido la herramienta que más vulnerabilidades ha encontrado, además de tener una capacidad tecnológica para la detección de vulnerabilidades muy elevada.

Tenable tiene mejor valoración respecto a las otras dos herramientas en la categoría de Operativa, ya que es la que tiene mejores requerimientos de instalación, ocupando muy poco espacio, además de tener un mínimo de activos inferior respecto a las otras herramientas. Estas características ha hecho que el criterio de Escalabilidad des esta categoría tenga la mejor valoración.

Por último, Qualys es la que ha obtenido la mejor valoración en 3 categorías: Vulnerabilidades externas, Funcionalidades y Proveedores. En la categoría de Vulnerabilidades externas, es la que ha detectado mayor número de vulnerabilidades, además de tener también una valoración alta en capacidad tecnológica. En el caso de los criterios de la categoría Funcionalidades, tiene la puntuación más alta tanto para Gestión de activos como para Gestión de vulnerabilidades. Esto se debe a que la herramienta dispone de funcionabilidades muy bien calificadas para clasificar el inventario, priorizar las vulnerabilidades y realizar escaneos tanto de descubrimiento como de vulnerabilidades, así como representar los resultados y activos de una manera muy intuitiva y disponer de funcionalidades muy completas para esta gestión. Por último, en la categoría de Proveedores, a pesar de estar bastante igualadas las calificaciones de los criterios de esta categoría, ha mantenido las evaluaciones más altas en los criterios de Servicio y Soporte y Licencias y precio.

Por tanto, la evaluación final queda como se presenta en el siguiente gráfico (Ilustración 11), donde se observan los porcentajes ponderados para cada una de las categorías y el porcentaje final, dando como resultado unas puntuaciones muy altas para las tres herramientas:

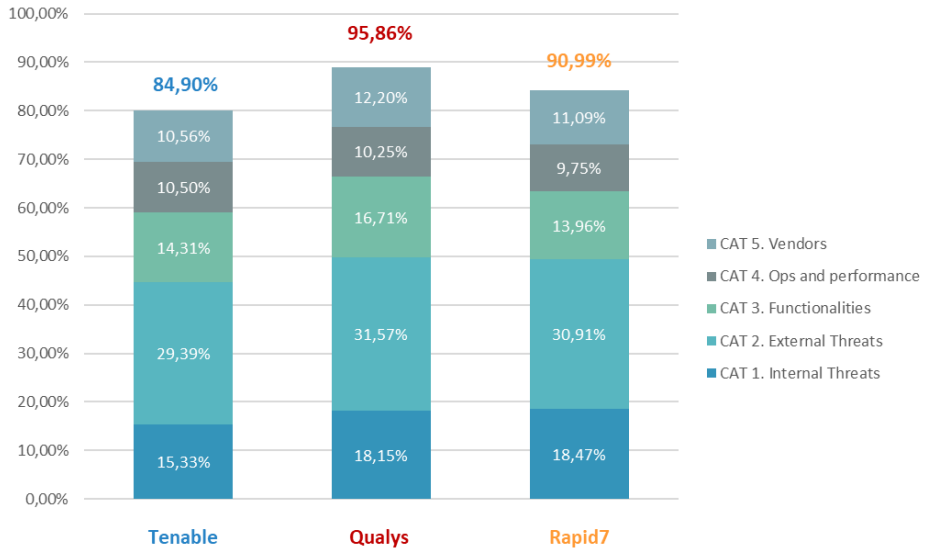

Ilustración 11. Valoraciones ponderadas y comparativas de la evaluación final

Finalmente, para este caso práctico, la herramienta mejor valorada ha sido Qualys, seguido de Rapid7 y, por último, Tenable. Por tanto, la herramienta elegida para implementar en la empresa es Qualys.

5 Conclusiones

En este último capítulo, se describen los objetivos cumplidos tras el desarrollo del trabajo, las lecciones aprendidas y, por último, el posible trabajo futuro que podría realizarse a partir de este trabajo.

5.1 Objetivos alcanzados

El objetivo principal de este trabajo era la realización de una prueba de concepto para la elección de una herramienta de gestión de vulnerabilidades en una empresa real. Una vez finalizado el trabajo, se puede concluir que se ha conseguido alcanzar este objetivo principal. Esto también ha sido gracias a que también se ha conseguido alcanzar los subobjetivos planteados:

- Se ha conseguido explicar el concepto de vulnerabilidad, así como el proceso de gestión de vulnerabilidades, identificando las fases del proceso y los componentes principales para esta gestión. También se ha podido identificar las normativas que recomiendan esta gestión.
- Se han podido describir las características que debe tener un sistema de gestión de vulnerabilidades y se han conseguido identificar los criterios utilizados en diferentes trabajos para realizar comparativas de herramientas de gestión de vulnerabilidades.
- Ha sido posible identificar correctamente la necesidad de la empresa para la elección de esta herramienta.
- Se han identificado las tres herramientas mejor valoradas y utilizadas en el mercado para realizar la prueba de concepto, así como realizar una descripción sobre sus funcionalidades.
- Ha sido posible definir los criterios tanto globales, en base a los criterios revisados en otros trabajos, como específicos, en base a la necesidad de la compañía. También se ha diseñado un sistema de evaluación utilizando estos criterios para evaluar las herramientas.
- Se han conseguido aplicar el sistema de evaluación y evaluar estos criterios en las tres herramientas seleccionadas y así realizar la prueba de concepto para la selección de herramienta de vulnerabilidades de una empresa real.
- Se han presentado los resultados de la evaluación final de las tres herramientas, mostrando los puntos fuertes de cada una de ellas e indicando la mejor valorada finalmente en este trabajo.

5.2 Lecciones aprendidas

Al realizar este trabajo, se ha mostrado que los resultados de las evaluaciones de las herramientas de vulnerabilidades dependen mucho de los criterios escogidos y de las necesidades de la empresa. Al presentar el resultado final, se ha podido observar que, en algunas categorías y criterios, la herramienta con

mejor valoración final en este proyecto no siempre ha sido la mejor calificada. A pesar de tener en algunos criterios la calificación más baja, estas calificaciones no han afectado a su nota final debido a que estos criterios tenían muy poco peso sobre la nota final. Y, por el contrario, herramientas que tenían puntuaciones muy altas en algunos criterios, con funcionalidades muy interesantes, no han destacado tanto debido a que estos criterios tenían una ponderación baja sobre la nota final.

Por tanto, con este trabajo, se puede demostrar que:

- No se puede seleccionar una herramienta en base a una comparativa externa o global, ya que debe tenerse muy en cuenta las necesidades de la empresa para su implementación.
- Con esta comparativa realizada, no se puede concluir qué herramienta es mejor o peor a nivel global, sino cuál ha sido la mejor elección para esta empresa y concretamente para su necesidad.

5.3 Problemas encontrados

Los problemas que han aparecido en el trabajo han sido debidos a que este trabajo describe un proyecto realizado con la empresa con anterioridad a la redacción del trabajo, es decir, que no se ha redactado paralelamente con la realización del trabajo. Esto ha ocasionado obtener los siguientes problemas:

- No seguir con la planificación, debido a que se generó poca documentación del proyecto con la empresa y ha dificultado sintetizar y plasmar toda la información en este trabajo, haciendo que los tiempos fueran más extensos que los planificados.
- No disponer de las herramientas evaluadas. A pesar de que se tomaron algunas capturas de pantalla de las diferentes herramientas, en algunos puntos de la evaluación del trabajo, no se ha podido evidenciar con capturas de pantalla de las herramientas debido a que ya no se disponía de ellas.

5.4 Trabajo futuro

Debido a que este trabajo ha sido enfocado a una empresa y una necesidad en concreto, se proponen algunas líneas de trabajo futuro para mejorar el proyecto o ampliarlo en otras empresas que necesiten realizar una prueba de concepto para seleccionar una herramienta de gestión de vulnerabilidades:

- Definir para cada uno de los criterios o elementos de evaluación, una serie de pasos o de pruebas a realizar para evaluarlos. En este trabajo, se han definido unas pautas para realizar las pruebas, pero no se ha llegado a detallar las pruebas que se debían realizar para cada uno de los criterios.
- Diseñar un cuestionario para evaluar los elementos de evaluación, de forma que el resultado final de evaluación del elemento sea en base a las respuestas indicadas.

- Búsqueda de nuevos criterios para empresas con activos en la cadena de suministro. Hoy en día, con el crecimiento del Internet de las cosas, cada vez existen más activos vulnerables en las cadenas de producción o en almacenes y se deben analizar también este tipo de activos. Por tanto, incluir criterios relacionados con este punto puede ser una línea interesante futura de trabajo.

6 Bibliografía

Amoroso, Edward G. 1994. *Fundamentals of computer security technology*. USA: Prentice-Hall, Inc.

Andress, Mandy. 2004. «Network Vulnerability Assessment Management». *Network World*. https://www.networkworld.com/article/2326811/network-vulnerability-assessment-management.html (24 de abril de 2021).

Bhajanka, Prateek, Mitchell Schneider, y Craig Lawson. 2019. «Gartner: A Guide to Choosing a Vulnerability Assessment Solution, 2019». https://www.gartner.com/en/documents/3906374/a-guide-to-choosing-a-vulnerability-assessment-solution (30 de marzo de 2021).

BitSight Technologies. «BitSight: Security Ratings Leader - Cyber Risk Management Solutions». *BitSight*. https://www.bitsight.com (30 de marzo de 2021).

Brackin, Cathleen. 2003. «Vulnerability Management: Tools, Challenges and Best Practices». : 18.

«COBIT 5». *ISACA*. https://www.isaca.org/bookstore/cobit-5/wcb5 (14 de mayo de 2021).

«Common Vulnerability Scoring System SIG». *FIRST — Forum of Incident Response and Security Teams*. https://www.first.org/cvss (26 de marzo de 2021).

Forristal, J., y G. Shipley. 2001. «Vulnerability Assessment Scanners». *Network World*.

Gartner Inc. «Vulnerability Management Tools Reviews 2021 | Gartner Peer Insights». *Gartner*. https://www.gartner.com/market/vulnerability-assessment (26 de marzo de 2021).

Holm, Hannes, Teodor Sommestad, Jonas Almroth, y Mats Persson. 2011. «A quantitative evaluation of vulnerability scanning». *Information Management & Computer Security* 19(4): 231-47.

«https://cve.mitre.org/». https://cve.mitre.org/ (26 de marzo de 2021).

«Information Security and Compliance | Qualys, Inc.» https://www.qualys.com/ (1 de junio de 2021).

ISACA. 2017. «Vulnerability Assessment». *ISACA*. https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpva (16 de marzo de 2021).

Jin, S., Y. Wang, X. Cui, y X. Yun. 2009. «A review of classification methods for network vulnerability». En *2009 IEEE International Conference on Systems, Man and Cybernetics*, , 1171-75.

Manzuik, Steve, Ken Pfeil, y Andrew Gold. 2006. *Network Security Assessment: from Vulnerability to Patch*. Rockland, MA.

NIST. 2012. *Guide for Conducting Risk Assessments*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (16 de marzo de 2021).

«NIST National Vulnerability Database Analysis». 2021. *Redscan*. https://www.redscan.com/news/nist-nvd-analysis/ (9 de mayo de 2021).

Palmaers, Tom. 2013. «Implementing a Vulnerability Management Process». : 23.

«Rapid7 | Cybersecurity & Compliance Solutions & Services». https://www.rapid7.com/ (1 de junio de 2021).

Scarfone, K A, M P Souppaya, A Cody, y A D Orebaugh. 2008. *Technical Guide to Information Security Testing and Assessment.* 0 ed. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (26 de marzo de 2021).

Shanks, Wylie. 2015. «Building a Vulnerability Management Program - A Project Management Approach». : 22.

Shirey, R. 2000. *RFC2828: Internet Security Glossary*. USA: RFC Editor.

«Tenable®». *Tenable*®. https://es-la.tenable.com/homepage-rotator (1 de junio de 2021).

UNE-EN ISO/IEC 27001. 2017. «UNE-EN ISO/IEC 27001:2017 Tecnología de la información. Técnic...» https://www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0058428 (26 de marzo de 2021).

Villora Divino, Borja. 2018. «Evaluación y gestión de vulnerabilidades: Cómo sobrevivir en el mundo de los ciberataques». Proyecto/Trabajo fin de carrera/grado. Universitat Politècnica de València. https://riunet.upv.es/handle/10251/106947 (30 de marzo de 2021).

Wang, Chenxi, Stephanie Balaouras, y Lindsey Coit. 2010. «The Forrester Wave™: Vulnerability Management, Q2 2010». https://www.forrester.com/report/The+Forrester+Wave+Vulnerability+Management+Q2+2010/-/E-RES56932 (30 de marzo de 2021).

Welberg, S. M. 2008. «Vulnerability management tools for COTS software - A comparison». https://research.utwente.nl/en/publications/vulnerability-

management-tools-for-cots-software-a-comparison (30 de marzo de 2021).

Yair Regev. 2020. «Qualys vs. Tenable vs. Rapid7...and the Remediation “Missing Link”». *JetPatch - Intelligent Vulnerability Remediation*. https://jetpatch.com/blog/patch-management/comparing-qualys-tenable-rapid7-and-the-remediation-missing-link/ (14 de abril de 2021).