| PROGRAMA DE FORMACIÓN | Seguridad de aplicaciones web |
| --- | --- |

| COMPETENCIA | 220501108. Diagnosticar la seguridad de la información de acuerdo con métodos de análisis y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501108-01. Aplicar métodos de análisis y valoración de riesgos de seguridad digital para aplicaciones web, de acuerdo con estándares y normativa. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 001 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Metodologías, normas y estándares de seguridad orientada a aplicaciones web |
| BREVE DESCRIPCIÓN | En este componente se presentan los fundamentos necesarios para el desarrollo de una auditoría de la seguridad en aplicaciones web, mediante el reconocimiento de estándares, metodologías, técnicas y herramientas necesarias para la evaluación de la seguridad. |
| PALABRAS CLAVE | Auditoría, *pentesting*, prueba, riesgo, vulnerabilidad |

| ÁREA OCUPACIONAL | Servicios |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS:**

**Introducción**

1. **Fundamentos de seguridad en aplicaciones web**
   1. Conceptos
   2. Infraestructura de aplicaciones web
   3. Normatividad y estándares para la gestión de la seguridad
   4. Metodologías para la gestión de la seguridad en aplicaciones web
2. **Vulnerabilidades en aplicaciones web**
   1. Metodologías para la gestión de vulnerabilidades
   2. Fundamentos de *pentesting*
   3. Owasp: *top* 10 de vulnerabilidades
   4. Herramientas especializadas
   5. Análisis de resultados

**Síntesis**

1. **DESARROLLO DE CONTENIDOS:**

**INTRODUCCIÓN**

Le damos la bienvenida al componente formativo denominado **Metodologías, normas y estándares de seguridad orientada a aplicaciones web**, el cual hace parte del programa de formación técnico en “Seguridad en aplicaciones web”, para lo cual se invita a observar el siguiente video:



1. **Fundamentos de seguridad en aplicaciones web**

La seguridad de la información en las organizaciones presenta una responsabilidad compartida dada por algunas normas, estándares, implementaciones de cumplimiento legal y algunas iniciativas de buenas prácticas que conllevan a generar una cultura de seguridad en los datos gestionados.

Ahora bien, existe un gran número de este tipo de iniciativas enfocadas a la seguridad perimetral, de procesos, de infraestructura, y no se le da la correspondiente importancia al desarrollo de aplicaciones las cuales son la ventana o interfaz que los usuarios o clientes van a utilizar para acceder y gestionar la información.

De acuerdo con lo anterior, a continuación, se reconocerán algunas iniciativas que han surgido y que son muy utilizadas dentro de la seguridad de aplicaciones web.

* 1. **Conceptos**

Dentro del ejercicio de la gestión de las vulnerabilidades en aplicaciones web se hará uso de metodologías, técnicas y herramientas especializadas, las cuales presentan términos que no son muy comunes y que es necesario reconocer para dar una adecuada interpretación de la información, así como transmitir los resultados obtenidos.

Se invita a conocer cuáles son los principales conceptos de vulnerabilidades en aplicaciones web:



Los anteriores conceptos deben ser comprendidos adecuadamente, pues la presencia de una vulnerabilidad no significa que esté afectando la información, como se observa en la siguiente figura, el riesgo resulta del aprovechamiento de una vulnerabilidad y una amenaza materializada

En el siguiente recurso, se ofrece información en detalle de la relación de otros conceptos, se invita a consultarlo:



A continuación, se podrán conocer otros conceptos importantes:



| Figura 1  *Uso de las medidas, métricas y KPI* | Estos conceptos permiten comprender mejor el ejercicio realizado, interpretar algunos resultados obtenidos, así como generar informes técnicos con datos coherentes y que pueden demostrar el estado actual de la seguridad de una aplicación web. |
| --- | --- |

* 1. **Infraestructura de aplicaciones web**

Las aplicaciones web han ganado terreno en la adopción e implementación de soluciones para las organizaciones, dada su flexibilidad, compatibilidad, capacidades de gestionar información y sobre todo su rapidez para la implementación dado que requiere de una infraestructura centralizada, esto conlleva a facilitar también su mantenimiento; y, por otra parte, a los usuarios finales les significa accederlas desde cualquier dispositivo haciendo uso de un navegador web y estar conectados a una red local o internet.

En el siguiente recurso se presentan algunos de los componentes que integran una infraestructura de aplicaciones web, lo cual servirá para comprender mejor su funcionamiento:



Todos estos componentes se interrelacionan para conformar las arquitecturas técnicas de aplicaciones web, en la siguiente figura, se aprecia su interrelación y flujo de información ante una solicitud de un recurso web.

| Figura 2  *Arquitectura de una aplicación web* | * El usuario realiza la solicitud de un recurso web a través de un navegador. * El navegador realiza la petición del recurso web a través del protocolo http. * El servidor web recibe la petición y procesa la respuesta:   + Procesa lógica de negocio.   + Procesa información desde bases de datos.   + Conforma la respuesta. * El servidor devuelve la respuesta hacia el navegador. * Navegador despliega resultado al usuario. |
| --- | --- |

Actualmente existen diferentes tipos de aplicaciones web, entre las más comunes se resaltan:



Comprender la arquitectura técnica que sirven las aplicaciones web, así como sus tipos, permitirá comprender el funcionamiento y determinar un ejercicio que facilite el aseguramiento de las aplicaciones web.

* 1. **Normatividad y estándares para la gestión de la seguridad**

La gestión de la seguridad en las aplicaciones web es una tarea que actualmente no se le presta la debida atención, y esta no depende únicamente de las buenas prácticas de programación de *software*, en su lugar es importante tener presente que la responsabilidad de poseer una aplicación web pública, que gestione información importante para la organización o maneje información confidencial, y ello obliga a contar con ciertos controles de seguridad que garantice los pilares de la seguridad de la información, a saber:



Ahora bien, para cumplir con estos tres pilares se hace necesario de acciones, y aquí es donde han surgido algunas buenas iniciativas como normatividad, estándares y buenas prácticas para una adecuada gestión de la información, entre las cuales poder revisar:

* **Norma ISO/IEC 27001:2013**: esta norma nos brinda los lineamientos para la adopción de Sistemas de Gestión de la Seguridad de la Información SGSI, que buscan consolidarse como estrategias corporativas para la seguridad de la información a partir de los siguientes principios.
  + Concientización de la necesidad de adoptar una cultura de seguridad.
  + Delegación de responsabilidades sobre la seguridad de la información.
  + Involucrar la alta dirección en la estrategia de seguridad.
  + Seleccionar los controles adecuados para garantizar la seguridad de la información.
  + Adoptar la seguridad como elemento esencial de los sistemas de información.
  + Adoptar estrategias activas para la prevención de incidentes de seguridad activa.
  + Adoptar la mejora continua en la evaluación de la seguridad.



Ahora bien, este estándar es base para la adopción de un SGSI, lo que conlleva a que, si una organización esta certificada o está pensando en certificar sus procesos bajo esta norma, debe tener presente la seguridad de la información que se gestiona a través de aplicaciones web, de acuerdo con las siguientes recomendaciones:

* + - Los elementos y componentes de las aplicaciones web deberán ser objeto de análisis, planificación y evaluación para que sean cubiertos por el SGSI, esto involucra que también se le haga un análisis de riesgos.
    - Dado el cambio continuo tecnológico, se requiere que las aplicaciones web sean evaluadas permanentemente según los nuevos retos, tecnologías y amenazas.
* **Norma ISO/IEC 27002:2013**: este estándar establece una guía para la implementación de controles de seguridad en una organización, a partir de sus objetivos, controles y estrategias de implementación.

Este estándar está compuesto por 14 dominios, 35 objetivos de control y 114 controles, con los cuales se busca adoptar medidas de seguridad en una organización.

A continuación, se exponen algunos de los controles asociados directamente con la seguridad de la información en aplicaciones web:

* Documento con política de seguridad de la información.
* Asignación de responsabilidades relativas a la seguridad.
* Formación y concienciación sobre la seguridad de la información.
* Notificación de los eventos de seguridad de la información.
* Gestión de los derechos de propiedad intelectual.
* Protección de activos de documentación de la organización.
* Protección de datos y privacidad de la información de carácter sensible de índole personal.

Desde el punto de vista de aporte de este estándar en la seguridad web, se pueden referenciar algunas medidas importantes que ayudan a gestionar la seguridad de los datos en las aplicaciones web, así:



* **Norma ISO/IEC 25010:2013**: este estándar aplica para la industria del desarrollo de *software*, así como para las organizaciones que realizan desarrollos propios para gestionar su información, es así como esta norma busca mejorar la calidad en los productos de desarrollo de *software* a partir de las siguientes características:



Esto fortalece los procesos de desarrollo de *software* dentro las organizaciones y en los procesos de desarrollo en sitio en las organizaciones, que buscan mejorar los niveles de seguridad.

Para reforzar esta temática, se sugiere observar el siguiente video.



* 1. **Metodologías para la gestión de la seguridad en aplicaciones web**

Existen normas y estándares que orientan en la adopción de iniciativas de seguridad en las organizaciones y que impactan directamente en la seguridad de las aplicaciones web y en la información gestionada a través de ellos, ahora bien, desde el punto de vista práctico existen iniciativas metodológicas para la gestión de las vulnerabilidades en aplicaciones web específicamente, una de ellas es Owasp.

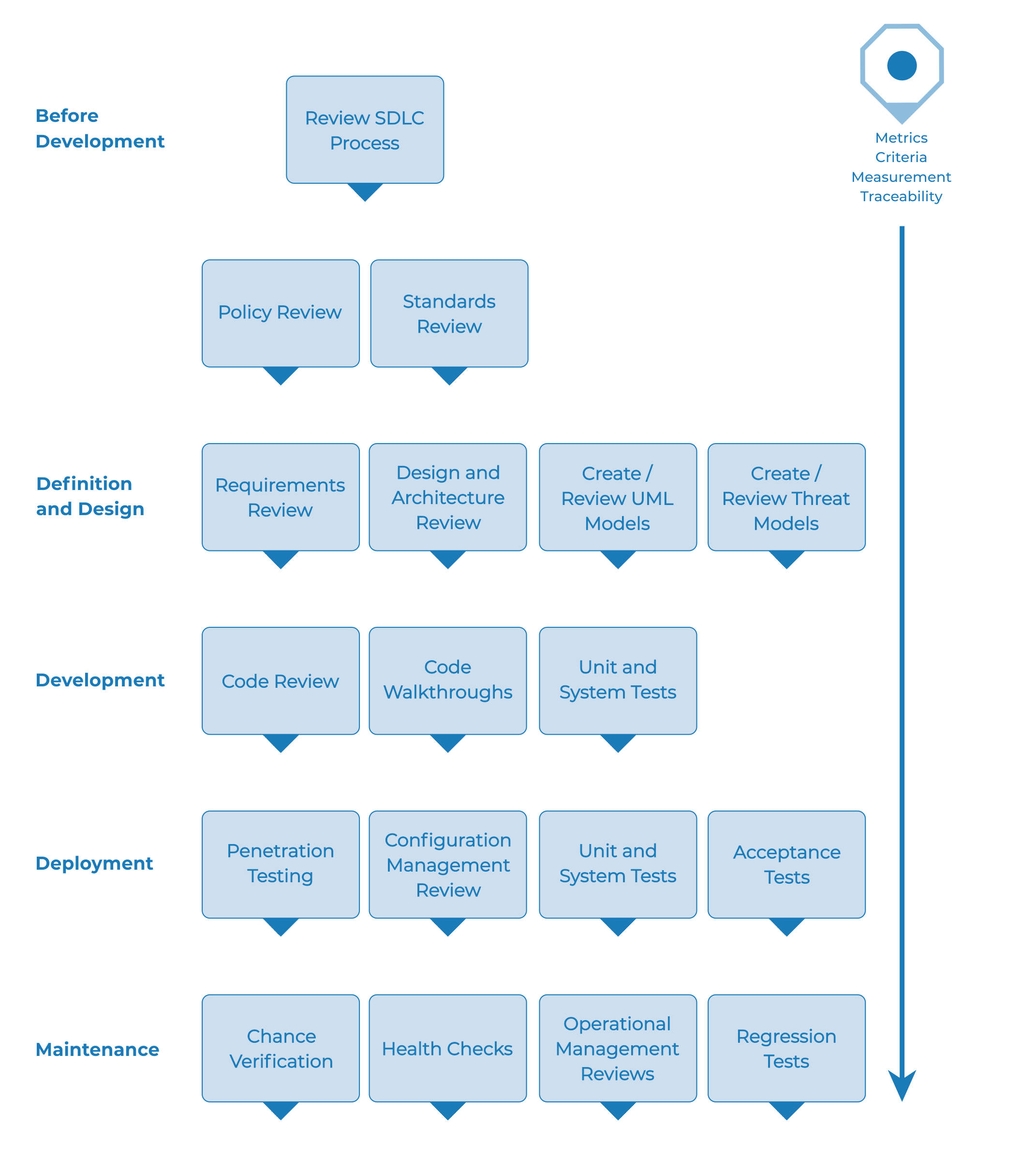
Owasp (*Open Web Application Security Project*) es una metodología de seguridad para la auditoría web, orientada al análisis de seguridad de estas aplicaciones. Esta metodología está siendo utilizada en la mayoría de los trabajos de auditoría de seguridad, ya que permite a partir de la auditoría realizar una evaluación de riesgos.

Parte de la revisión de los controles definidos por la metodología, la cual permite al auditor garantizar que una revisión de la plataforma se realiza de forma adecuada, garantizando que todos los vectores de ataque han sido analizados y que los fallos de seguridad han sido detectados.

Este proceso ayuda a mejorar la seguridad y la protección de los sistemas informáticos en las organizaciones.

**Figura 4**

*Flujo de trabajo de prueba SDLC genérico*



Actualmente la mayoría de los desarrolladores de *software* no realizan la validación de vulnerabilidades en sus productos si no hasta que este ya es funcional, pero esto no es tan eficiente, por ello se sugiere la adopción de un Ciclo de Vida de Desarrollo de *Software* (SDLC), el cual lleva a tener presente el factor de seguridad en cada una de las fases del desarrollo, así:





1. **Vulnerabilidades en aplicaciones web**

| Actualmente se cuenta con una amplia gama de recursos normativos y estándares para la gestión de vulnerabilidades, algunas de ellas con un nivel de cobertura más amplio dado su capacidad de aplicación dentro de las necesidades de una organización. Cada una de estas normas tiene como talante la gestión proactiva de las vulnerabilidades antes de una ocurrencia de un incidente que ponga en riesgo la información administrada | Confirmado, usar 2FA es la mejor protección en Internet. – Blog EHCGroup |
| --- | --- |

* 1. **Metodologías para la gestión de vulnerabilidades**

Owasp propone una metodología para la identificación de vulnerabilidades basada en pruebas de seguridad sobre las aplicaciones web, con el cual se busca encontrar las debilidades presentes en un sistema.

Este modelo de pruebas está conformado por:

* **Probador/Auditor**: quien realiza las pruebas y validaciones.
* **Herramientas y metodología**: guía de pruebas de Owasp.
* **Aplicación**: objeto que se desea probar.

A su vez, las pruebas se pueden clasificar así:



* 1. **Fundamentos de *pentesting***

Dentro del ejercicio de la gestión de vulnerabilidades, cobran vital importancia las metodologías para el descubrimiento e identificación de estas, ya que orientan y dan un mapa de ruta de cómo se debe realizar el ejercicio, uno de estos es el *pentesting* o prueba de penetración, que no es más que un ejercicio de descubrimiento apoyado en técnicas y herramientas especializadas para la validación y búsqueda de vulnerabilidades en un sistema o aplicación.

Existen los siguientes tipos de *pentesting*:



Para cualquiera de los tipos de *pentesting*, se sugiere un ciclo de vida como se muestra en la siguiente figura, en donde se resalta:



Ahora bien, este ejercicio se puede realizar de manera exploratoria sin conocimiento del escenario e información de acceso, y dependiendo de esto, las pruebas se pueden clasificar en:

* **Caja negra**: aquí los auditores no cuentan con información previa sobre el escenario en el cual se va a trabajar, se desarrollan ejercicios de exploración e intrusión, este tipo de pruebas por lo general son realizadas por personas externas a la organización.
* **Caja blanca**: los auditores cuentan con datos del escenario e incluso credenciales de acceso a los sistemas de información, este tipo de pruebas lo realizan principalmente personal interno de la organización.
* **Caja gris**: se cuenta con parte de la información, pero se requiere detallar ciertos aspectos técnicos.

El *pentesting* se considera uno de los ejercicios más importantes para la identificación de vulnerabilidades necesarias para el fortalecimiento de los recursos de tecnologías de la información.

* 1. **Owasp: *top* 10 de vulnerabilidades**

De acuerdo con la comunidad de Owasp, este genera reportes sobre las vulnerabilidades que más se encuentran en las aplicaciones web y en su último reporte se puede observar el siguiente comportamiento del *top* 10 de las vulnerabilidades identificadas.



* 1. **Herramientas especializadas**

Estas son un elemento fundamental en el ejercicio de la búsqueda y gestión de vulnerabilidades, dado que permiten agilizar, automatizar y realizar cientos de validaciones en segundos, y generando informes muy completos sobre los hallazgos encontrados.

A continuación, se exponen algunas de las herramientas más comunes, aunque más adelante se profundizará sobre su utilidad y manejo en el ejercicio de la auditoría.

Dentro del universo de herramientas a utilizar, están las siguientes categorías:

* Herramientas de pruebas de seguridad de aplicaciones estáticas (SAST).
* Herramientas de pruebas dinámicas de seguridad de aplicaciones (DAST), principalmente para aplicaciones web.
* Herramientas interactivas de pruebas de seguridad de aplicaciones (IAST), principalmente para aplicaciones web y API web
* Mantener actualizadas las bibliotecas de código abierto, para evitar el uso de componentes con vulnerabilidades conocidas (Owasp Top 10-2017 A9)
* Herramientas de calidad de código estático.

**Herramientas SAST**

En el siguiente recurso podrá conocer las herramientas más importantes SAST.



**Herramientas DAST**

Si un proyecto tiene un componente de aplicación web, se recomienda ejecutar análisis automatizados contra él para establecer las vulnerabilidades.



**Herramientas IAST**

Estas herramientas suelen estar orientadas a analizar aplicaciones web y API web, pero eso es específico del proveedor. Puede haber productos IAST que también realicen un buen análisis de seguridad en aplicaciones que no sean web.

| * Contrast Community Edition (CE) * Versión con todas las funciones para 1 aplicación y hasta 5 usuarios (algunas funciones Enterprise deshabilitadas). Contrast CE solo admite Java y .NET. | Figura 6  *Contrast Community Edition (CE)* |
| --- | --- |

A continuación podrá conocer algunas de las herramientas disponibles para la auditoría de aplicaciones web y para proyectos de desarrollo de aplicaciones web, y vale la pena aclarar que algunas de ellas son *open source*, o tienen una posibilidad de ser utilizados cuando son proyectos abiertos, pero para proyectos comerciales o de gran tamaño requieren de una licencia o contrato de uso.



* 1. **Análisis de resultados**

Una vez realizado el plan de pruebas programado con las herramientas y técnicas seleccionadas, se deben documentar los hallazgos encontrados en el ejercicio, para ello se emplean instrumentos que permitan registrar, analizar y evaluar el estado actual de la seguridad de las aplicaciones web.

Desde el proyecto Owasp, se han propuesto varios instrumentos para registrar la información a manera de *checklist*, a saber:

| Instrumento *checklist* para registro de la evaluación  Este permite obtener un informe del riesgo que pueden llegar a presentar una determinada aplicación web, registrando cada una de las aplicaciones web que se desea evaluar, y registrar el resultado de las pruebas practicadas, esta información será útil para generar un informe final del nivel del riesgo presente en las aplicaciones.  Se encuentra disponible en la url: <https://github.com/OWASP/wstg/tree/master/checklist> , | Figura 7  *Instrumento checklist para registro de la evaluación* |
| --- | --- |
| Instrument OWASP Risk Assessment Calculator Esta herramienta es una calculadora de evaluación de riesgos OWAS y se puede encontrar un instrumento de evaluación en línea, disponible en <https://javierolmedo.github.io/OWASP-Calculator/> | Figura 8  *OWASP Risk Assessment Calculator* |

Es importante resaltar que el ejercicio de pruebas y la obtención del indicador de riesgo es un producto importante, pero ante la organización o los propietarios de la información se deben presentar reportes técnicos, con evidencias, detalles de las pruebas realizadas y resultados obtenidos, así como una serie de recomendaciones para subsanar dichas vulnerabilidades.





1. **Síntesis**

En el siguiente recurso se podrá evidenciar un resumen de este componente formativo.



1. **ACTIVIDADES DIDÁCTICAS**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la Actividad | Conceptos sobre seguridad en aplicaciones web |
| Objetivo de la actividad | Reconocer los conceptos relevantes asociados a los fundamentos de la seguridad en aplicaciones web |
| Tipo de actividad sugerida | Crucigrama |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo5\_ActividadDidactica1 |

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la Actividad | Interpretación del resultado de una prueba bajo Owasp |
| Objetivo de la actividad | Reconocer los resultados de una prueba que permita determinar el nivel de riesgo en una aplicación web |
| Tipo de actividad sugerida | falso o verdadero |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo6\_ActividadDidactica2 |

1. **MATERIAL COMPLEMENTARIO:**

| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del Recurso o  Archivo del documento o material |
| --- | --- | --- | --- |
| * 1. Análisis de resultados | Owasp. (2022). *Web Security Testing Guide 4.2.* Owasp. [https://github.com/owasp/wstg/releases/download/v4.2/wstg-v4.2.pdf](https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf) | Página Web | <https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf> |
| * 1. Análisis de resultados | Owasp. (2022). *Web Security Testing Guide Checklist.* Owasp. [https://github.com/owasp/wstg/tree/master/checklist](https://github.com/OWASP/wstg/tree/master/checklist) | Página Web | <https://github.com/OWASP/wstg/tree/master/checklist> |
| * 1. Análisis de resultados | Olmedo, J. (2021). *Owasp risk assessment calculator.* <https://javierolmedo.github.io/OWASP-Calculator/> | Página Web | <https://javierolmedo.github.io/OWASP-Calculator/> |

1. **GLOSARIO:**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| 2FA | término que representa doble factor de autenticación, solución que agrega una capa de seguridad en sistemas d autenticación basados en componentes externos a un sistema, por ejemplo, un *token*, una aplicación, tarjeta inteligente, etc. |
| *Checklist* | lista de chequeo que sirve para registrar un proceso de auditoría. |
| GUI | interfaz gráfica de usuario, por ejemplo, una aplicación, o aplicación móvil. |
| KPI | *Key Performance Indicator* o indicador clave de desempeño, que representa las métricas de eficacia de las acciones adoptadas y así determinar si son efectivas o no. |
| URL | *Uniform Resource Locator* (localizador de recursos uniforme), representa una dirección que apunta hacia un recurso único en la web. |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

Guijarro, O., J., Caparrós, R., J., & Cubero, L., L. (2019). *DevOps y seguridad cloud.* Editorial UOC. <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/128889>

Incibe. (2022). *Top 10 vulnerabilidades web de 2021*. Incibe. <https://www.incibe.es/protege-tu-empresa/blog/top-10-vulnerabilidades-web-2021>

MinTIC. (2016). *Guía de gestión de riesgos.* MinTIC. <https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf>

MinTIC. (2016). *Guía para la gestión y clasificación de activos de información.* MinTIC. MinTIC.<https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf>

MinTIC. (2016). *Guía para la implementación de seguridad de la información en una mipyme.* MinTIC. <https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf>

MinTIC. (2020) Anexo 3 - Resolución MinTIC 1519 del 2020, Condiciones mínimas técnicas y de seguridad digital. <https://gobiernodigital.mintic.gov.co/692/articles-160770_Condiciones_minimas.pdf>

Ortega, C., J. M. (2018). *Seguridad en aplicaciones web Java.* RA-MA Editorial. <https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/106511>

Owasp. (2022). *Owasp Top 10:2021*. <https://owasp.org/Top10/>

Owasp. (2022). *Owasp web Security Testing Guide.* <https://owasp.org/www-project-web-security-testing-guide/latest/>

1. **CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Hernando José Peña Hidalgo | Experto Temático | Regional Cauca, Centro de teleinformática y producción industrial | Mayo de 2022 |
| Paula Andrea Taborda Ortiz | Diseñadora Instruccional | Regional Norte de Santander, Centro de la Industria, la Empresa y Los Servicios CIES | Mayo de 2022 |
| Carolina Coca Salazar | Asesora Metodológica | Regional Distrito Capital- Centro de Diseño y Metrología | Mayo de 2022 |
| José Gabriel Ortiz Abella | Corrector de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Julio del 2022. |

1. **CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| --- | --- | --- | --- | --- | --- |
| Autor (es) |  |  |  |  |  |