Monitoreo de la Seguridad Web

Breve descripción:

En la construcción de un sistema de información por procesamiento electrónico de datos orientado a la web, se deben implementar los mecanismos que permiten medir el comportamiento de la seguridad, como monitoreo, metodologías, indicadores y métricas, unido a las herramientas de “software”.

Septiembre 2023

Tabla de contenido

Introducción

La seguridad web está relacionada directamente con la vigilancia en todos los aspectos del diseño y uso de un sitio web, es decir, es aquella actividad encargada de proteger sitios web del acceso, uso, modificación, destrucción o interrupción, no autorizados.

Es importante tener en cuenta existen muchos riesgos que se pueden presentar, por solo el hecho de que el sistema de información se encuentre desprotegido y se presenten situaciones como, robo de información, explotación de datos, redireccionamiento a páginas web maliciosas, mostrar anuncios no deseados, entre otros.

Teniendo en cuenta lo anterior, el aprendiz en el presente componente formativo, conocerá sobre las diferentes estrategias para monitorear la seguridad web, para lo cual se invita a observar el siguiente video:

Video 1. Monitoreo de la Seguridad Web

Enlace de reproducción del video

Síntesis del video: Monitoreo de la Seguridad Web

El presente componente formativo se denomina 'Monitorear las aplicaciones web'. En este componente, vamos a verificar cuáles son los conceptos fundamentales que debemos tener para realizar el proceso de monitoreo de una aplicación web en su parte de seguridad, siguiendo el estándar OWASP. Básicamente, un monitoreo significa que vamos a estar revisando periódicamente cuáles son las posibles vulnerabilidades que se puedan presentar, con el objetivo de detectar de manera temprana posibles amenazas.

Unido a la metodología OWASP, dentro de este componente, también vamos a revisar en la parte OWASP 10, que corresponde a las diez vulnerabilidades que recomienda el estándar que deben ser abordadas. Para ello, el proceso de monitoreo implica recoger un tipo de información. Normalmente, el tipo de información tiene que ver con eventos que se presentan dentro de nuestra aplicación web. Un tipo de evento puede ser, por ejemplo, un inicio de sesión, para el cual se recomienda recoger información por medio de las herramientas que nos permiten hacer el monitoreo, que ya vamos a ver cuáles pueden ser, y colocarlas en formato de fácil manejo con una codificación también de fácil manejo.

Unido a la metodología OWASP, también vamos a mirar cuál es el concepto de las normas ISO 27000, que es la norma que nos da las mejores prácticas para realizar la revisión de seguridad. La norma ISO 27000 nos da las mejores prácticas en tres puntos fundamentales: confidencialidad, integridad y disponibilidad.

Unido a estas dos normas anteriores, es importante también tener en cuenta dentro del componente el marco normativo general de la seguridad de la protección de

datos en nuestro país, en Colombia, que es la Ley 1581 de 2012. Entonces, este es el conjunto de normas que nos debemos conocer y debemos saber para aplicar y utilizarlas en nuestras organizaciones.

También, dentro de una organización, es importante definir las políticas de seguridad y, para ello, se recomienda hacer una combinación del estándar COBIT más la ISO 17799, o en su defecto, la utilización de solo el estándar COBIT o solo la ISO 17799. Normalmente, las organizaciones utilizan una combinación de las dos.

Después de la definición de las políticas de la organización, es importante también definir los indicadores de gestión. Entonces, en esos indicadores de gestión, vamos a evaluar la eficiencia, vamos a evaluar la efectividad, vamos a promover datos de seguridad y vamos a comunicar valores. Entonces, es importante tener en cuenta estos indicadores de gestión.

Dentro del componente, vamos a ver que están definidos diferentes indicadores de gestión con su respectivo formato y estándar. Unido a los indicadores, vienen las métricas para el proceso de seguridad, y para estas métricas, vamos a tener en cuenta tres aspectos fundamentales: métricas de red de tráfico, métricas de "software" y métricas de calidad.

Unido a las métricas y a los indicadores de gestión, finalmente, vienen las herramientas de monitoreo, que para nuestro caso, vamos a tener en cuenta la herramienta Monster High, el mismo OWASP, en ZAP y herramientas elásticas como Elasticsearch. Para finalmente, con esta información recopilada y con un análisis que se hace de la información recopilada, poder generar el respectivo informe de monitoreo y presentarlo de acuerdo a nuestras necesidades.

1. Monitorear la seguridad web

Las empresas y organizaciones deben cuidar muy bien sus sistemas y equipos informáticos, dado que en la actualidad existen muchos tipos de ataques que podrían afectar la seguridad de la información y de los datos y no solo basta con tener un antivirus instalado a pesar de que sea de pago, este de igual manera está propenso a recibir ataques y a generar bloqueos que afecten todo el sistema operativo, provocando pérdida de la información.

Por tanto, se hace necesario realizar monitoreo activo y permanente de amenazas, donde se lleven a cabo pruebas de verificación del correcto funcionamiento y de la no existencia de brechas de seguridad, amenazas en el sistema o programas obsoletos que se puedan convertir en la entrada de piratas informáticos y finalmente, revisar periódicamente el cumplimiento de las medidas de seguridad, acatando las normas, metodologías y estándares.

El monitoreo activo de amenazas es un factor muy importante y que debemos tener muy en cuenta y que se debe aplicar sin importar si somos usuarios domésticos o una gran empresa, porque es esencial detectar lo antes posible las amenazas.

2. Metodologías, normas y estándares

En el mundo de la seguridad en las aplicaciones web, se han implementado metodologías, normas y estándares importantes para la detección y prevención de riesgos informáticos, a continuación se describirán los más comunes:

Metodologías

El concepto de metodología en el mundo de la informática, se refiere a la acción de detallar, observar y evaluar las páginas web, cumpliendo con una serie de normas diseñadas para esa área específicamente; la metodología OWASP es la más requerida en la actualidad.

Metodologías OWASP

Según esta metodología, comprende el OWASP Top 10 que corresponde a un documento de los diez riesgos de seguridad más importantes en aplicaciones web y por otra parte se deben tratar OWASP con (ASVS).

Dentro del OWASP Top 10 se encuentra el ítem 09 que trata del registro y monitoreo, en donde estos pueden ser desafiantes para ser testeados, implicando la realización de entrevistas o preguntando si los ataques fueron detectados durante las pruebas de penetración. No hay muchos datos de CVE/CVSS para esta categoría, pero realizar detecciones y responder a las brechas es crítico. Aun así, puede tener un gran impacto para la auditabilidad, visibilidad, alertas de incidentes y análisis forense. Esta categoría se expande más allá de CWE-117 Neutralización de salida incorrecta de registros, CWE-223 Omisión de información relevante para la seguridad, y CWE-532 Inserción de información sensible en archivo de registro.

En registros y monitoreo, las brechas no pueden ser detectadas. Registros, detecciones, monitoreo y respuestas activas insuficientes pueden ocurrir en cualquier momento; por lo tanto se recomienda recoger información sobre los siguientes eventos, que se presentan a continuación:

- Registros en aplicaciones y API no son monitoreados para detectar actividades sospechosas.
- Advertencias y errores generan registros poco claros, inadecuados y en algunos casos ni se generan.
- Eventos auditables, tales como los inicios de sesión, fallas en el inicio de sesión y transacciones de alto valor no son registradas.
- Los registros son únicamente almacenados en forma local.
- Las pruebas de penetración y los escaneos utilizando herramientas de pruebas dinámicas de seguridad en aplicaciones (como OWASP ZAP) no generan alertas.
- Las aplicaciones no logran detectar, escalar, o alertar sobre ataques activos en tiempo real ni cercanos al tiempo real.
- Los umbrales de alerta y procesos de escalamiento no están correctamente implementados o no son efectivos.

Para prevenir a los desarrolladores, se deberían implementar algunos o todos los siguientes controles, dependiendo del riesgo de la aplicación:

- **PASO 1. Identificar errores.** Asegúrese que todos los errores de inicio de sesión, de control de acceso y de validación de entradas de datos del lado del servidor se pueden registrar con suficiente contexto como para

identificar cuentas sospechosas o maliciosas y mantenerlo durante el tiempo suficiente para permitir un posterior análisis forense.

- **PASO 2. Gestión de riesgos**. Verifique que los registros se generan en un formato fácil de procesar por las herramientas de gestión de registros.
- **PASO 3. Verificación de datos**. Revise que los datos de registros estén correctamente codificados para prevenir inyecciones o ataques en el sistema de monitoreo o registros.
- **PASO 4. Realizar auditoría.** Asegúrese que las transacciones de alto valor poseen una traza de auditoría con controles de integridad para evitar la modificación o el borrado, tales como permitir únicamente la inserción en las tablas de base de datos o similares.
- **PASO 5. Establecer alertas.** Los equipos de DevSecOps deben establecer alertas y monitoreo efectivo tal, que se detecten actividades sospechosas y responder rápidamente.
- **PASO 6. Adoptar plan de respuesta y recuperación**. Establezca o adopte un plan de respuesta y recuperación, tal como NIST 800-61r2 o posterior.

Normas

Las normas son documentos que contienen directrices, características o en su defecto requisitos, que se deben tener en cuenta en la elaboración, diseño o utilización de productos, procesos y servicios, de modo que garantice la calidad del mismo. Con relación a esta finalidad, existen las normas ISO, las cuales son estándares internacionales que ayudan a las empresas a establecer criterios de homogeneidad frente a la gestión, prestación de servicios y desarrollo de productos en la industria.

La familia de normas ISO/IEC 27000 hacen parte del conjunto de estándares de seguridad (desarrollados o en fase de desarrollo) que proporcionan un marco para la gestión de la seguridad.

Contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La seguridad de la información, según la ISO 27001, se basa en la preservación de los siguientes conceptos:

- **Confidencialidad.** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad.** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad**. Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requieran.

En la tabla que se presenta a continuación, se encuentra un resumen de las Normas ISO 27000, con su respectiva descripción:

Tabla 1. Resumen de Normas ISO 27000

Norma	Descripción
ISO/IEC 27000	Vocabulario estándar para el SGSI para todas las normas de la familia. Se encuentra en desarrollo actualmente.
ISO/IEC 27001	Certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación de SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.
ISO/IEC 27002	"Information technology- Security techniques-Code of practice for information security management". Previamente BS 7799 parte 1 y la norma ISO/IEC 17799. Es un código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2002 el 01 de julio de 2007.
ISO/IEC 27003	Directrices para la implementación de un SGSI, es el soporte de la norma ISO/IEC 27001, publicada el 1 de febrero del 2010, no está certificada actualmente.
ISO/IEC 27004	Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.
ISO/IEC 27005	Normativa dedicada exclusivamente a la gestión de riesgos de seguridad de la información, proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos en seguridad de la información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual "British Standard" BS 7799 parte 3. Publicada en junio de 2008.
ISO/IEC 27006	Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de seguridad de la información. Esta norma específica de requisitos para la

Norma	Descripción
	certificación del SGSI es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
ISO/IEC 27007	Guía para auditar al SGSI. Se encuentra en preparación.
ISO/IEC 27709:2008	Guía para implementar ISO/IEC 27002 en la industria de la salud.

A continuación, podrá ampliar la información sobre la Ley 1581 de 2012, la cual se constituye en el marco general de la norma de protección de los datos personales en Colombia:

Ley 1581 de 2012

En el siguiente enlace de la página web de Función Pública, podrá ampliar la información sobre la Ley 1581 de 2012, la cual se constituye en el marco general de la norma de protección de los datos personales en Colombia.
https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Estándares

Continuando con la temática de metodologías, normas y estándares, en este punto se hablará sobre este último, pero haciendo especial énfasis en el estándar OWASP top 10 en conjunto con el estándar (ASVS) de OWASP. El Proyecto del Estándar de Verificación de Seguridad de Aplicaciones (ASVS) de OWASP proporciona una base para probar los controles técnicos de seguridad de las aplicaciones web y también proporciona a los desarrolladores una lista de requisitos para un desarrollo seguro.

El objetivo principal del Proyecto del Estándar de Verificación de Seguridad de Aplicaciones (ASVS) de OWASP es normalizar el rango en la cobertura y el nivel de rigor disponible en el mercado cuando se trata de realizar la verificación de seguridad de aplicaciones web utilizando un estándar abierto comercialmente viable. El estándar proporciona una base para probar los controles de seguridad técnica de la aplicación, así como cualquier control de seguridad técnica en el entorno, en los que se confía para proteger contra vulnerabilidades como Cross-Site Scripting (XSS) e inyección de SQL. Este estándar se puede utilizar para establecer un nivel de confianza en la seguridad de las aplicaciones web.

La siguiente tabla muestra cuándo es apropiado utilizar el OWASP top 10 unido al (ASVS) de OWASP.

Tabla 2. Otros estándares COBIT e ISO 17799

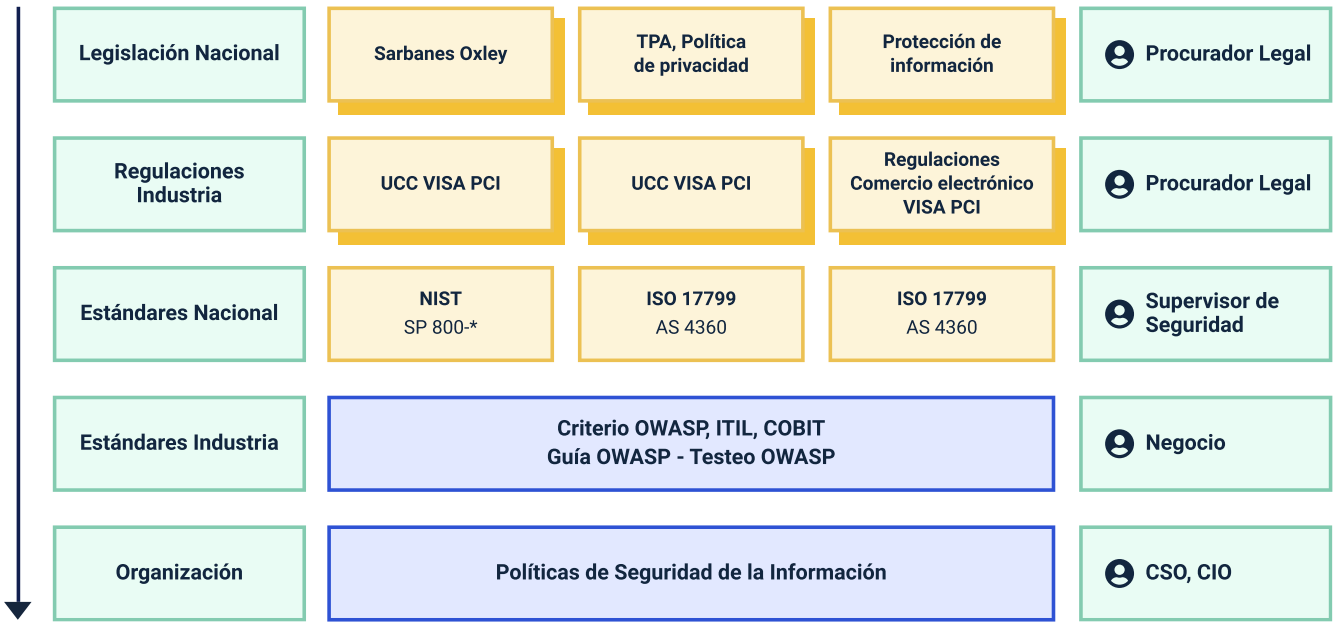
Finalmente, en la siguiente figura se resume la aplicación de normas y estándares de una organización:

Caso Uso	OWASP Top 10 2021	Estándar de verificación en seguridad aplicaciones de OWASP (ASVS)
Concientización	Sí	
Capacitación	Nivel de introductorio	Completo
Diseño y arquitectura	Ocasionalmente	Sí
Estándar de codificación	Apenas mínimo	Sí
Revisión de código seguro	Apenas mínimo	Sí
Lista de verificación para la revisión por pares	Apenas mínimo	Sí

Caso Uso	OWASP Top 10 2021	Estándar de verificación en seguridad aplicaciones de OWASP (ASVS)
Pruebas unitarias	Ocasionalmente	Sí
Pruebas de integración	Ocasionalmente	Sí
Pruebas de penetración	Apenas mínimo	Sí
Soporte de herramientas	Apenas mínimo	Sí
Cadena de suministro de agua	Ocasionalmente	Sí

Finalmente, en la siguiente figura se resume la aplicación de normas y estándares de una organización:

Figura 1. Aplicación de normas y estándares de una organización



3. Políticas internas de una organización

Aquellas organizaciones donde la seguridad cuenta con el soporte de la alta gerencia, generalmente desarrollarán y adquirirán aplicaciones que cumplen con principios básicos de seguridad. En cambio, es muy poco probable que organizaciones que no cuentan con el soporte de la gerencia, o que simplemente no se preocupan por la seguridad, desarrollen aplicaciones seguras. Cada organización segura documenta su apetito por el riesgo en su política de seguridad de la información, haciendo de esa manera que sea fácil determinar que riesgos serán aceptados, mitigados o asignados.

Las organizaciones inseguras simplemente no conocen donde se encuentra este límite, por lo tanto es probable que cuando se van a ejecutar proyectos dirigidos por este tipo de organizaciones y seleccionan los controles a implementar, estos terminan siendo inadecuados o insuficientes. La mayoría de las organizaciones produce políticas de seguridad de la información derivadas de la ISO 17799 o del marco de trabajo COBIT, u ocasionalmente los dos o uno de los estándares. No hay una regla infalible o rápida que dicte cómo crear políticas de seguridad de la información, pero en general se debe tener en cuenta los siguientes aspectos:

- Si la organización cotiza en bolsa en la mayoría de los países, debe tener una política de seguridad de la información.
- Si la organización es propia pero posee cierto número de empleados y desarrolladores, probablemente necesite una política.

Es perfectamente correcto mezclar y combinar controles de COBIT y de ISO 17799 y casi cualquier otro estándar de seguridad de la información; rara vez se

encuentran en desacuerdo en los detalles. El método de producción puede ser a veces difícil – en el caso de requerir una política certificada, se necesitará involucrar a firmas calificadas para que ayuden a la organización.

4. Indicadores

La creación de indicadores de gestión está orientada principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora.

Los objetivos de estos procesos de medición en seguridad de la información son:

a) Evaluar la efectividad de la implementación de los controles de seguridad.
b) Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
c) Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
d) Comunicar valores de seguridad al interior de la entidad.
e) Servir como insumos al plan de análisis y tratamiento de riesgos.

A continuación se profundizará sobre la temática de indicadores:

- **Indicador 01. Organización de la seguridad de la información.** Determina y hace seguimiento al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad.
- **Indicador 02. Cubrimiento del SGSI en activos de información.** Determina y hace seguimiento al cubrimiento que se realiza a nivel de activos críticos de información de una entidad y los controles aplicados.
- **Indicador 03. Tratamientos de eventos relacionados en marco de seguridad y privacidad de la información**. Determina la eficiencia en el tratamiento de eventos relacionados con la seguridad de la información; los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.
- **Indicador 04. Implementación de los procesos de registro y auditoría.** Grado de existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.
- **Indicador 05. Prevención de código malicioso.** Mide el nivel de efectividad del proceso de prevención de código malicioso.

5. Métricas

Las métricas se encuentran divididas en seguridad, red, "software" y calidad, los cuales se describen a continuación:

- **Métricas en procesos de seguridad.**
    - Métricas en procesos de seguridad
        - Medición de los procesos y procedimientos Implica alta utilidad de la seguridad, políticas y procesos.
        - La relación entre indicadores y nivel de seguridad no está claramente definida.
        - Cumplimiento / Gobierno impulsado generalmente apoya una mayor seguridad.
        - Impacto real difícil de definir.
- Métricas de red.
    - Impulsado por productos ("firewalls", IDS, etc.).
    - Disponible.
    - Ampliamente utilizado.
    - Brinda una sensación de control.
    - Gráficos agradables.
    - Puede ser engañoso.
- **Métricas de "software".**
    - Medidas de "software" están problemáticas (LOC, FPS, Complejidad, etc.).
    - Dependen del contexto y son sensibles al entorno.
    - Dependiente de arquitectura.

- **Métricas de calidad.**
    - Correctitud (Grado de operación del programa respecto a los requerimientos).
    - Mantenibilidad (Grado en el que un programa puede cambiar).
    - Integridad (Grado de resistencia ante pérdida de información).
    - Usabilidad (Grado de facilidad de uso).

6. Herramientas de “software”

Las herramientas de “software” tienen el objetivo de facilitar, optimizar y mejorar el desempeño del trabajo realizado; estas herramientas ofrecen soluciones, las cuales se aplica en diferentes áreas de una empresa y por tanto ayudan en el desarrollo de tareas desde las más complejas hasta las más simples.

El video a continuación habla de algunas herramientas, que le serán de utilidad en la implementación de aplicaciones web:

- **Elasticsearch.** Es un motor de búsqueda que se basa en Lucene, el cual permite realizar búsquedas de texto, autocompletado, soporte de geolocalización entre otros.

  Se puede definir a Elasticsearch como un base de datos NoSQL orientada a documentos JSON, los cuales pueden ser consultados, creados, actualizados o borrados mediante un sencillo API Rest.
- **Logstash.** Es una herramienta desarrollada por Elastic y que funciona bajo la JVM de Java, la cual permite administrar los logs de nuestras aplicaciones, de manera que se puede usar para recolectar, “parsear” y guardar los logs para búsquedas posteriores.
- **Kibana.** Es un “dashboard” de recopilación de gráficos, grafos, métricas, búsquedas y mapas que se recopilaron en un solo panel. Los “dashboards” permiten obtener información de un vistazo sobre datos desde varias perspectivas y permiten a los usuarios explorar los detalles.

7. Informe de monitoreo

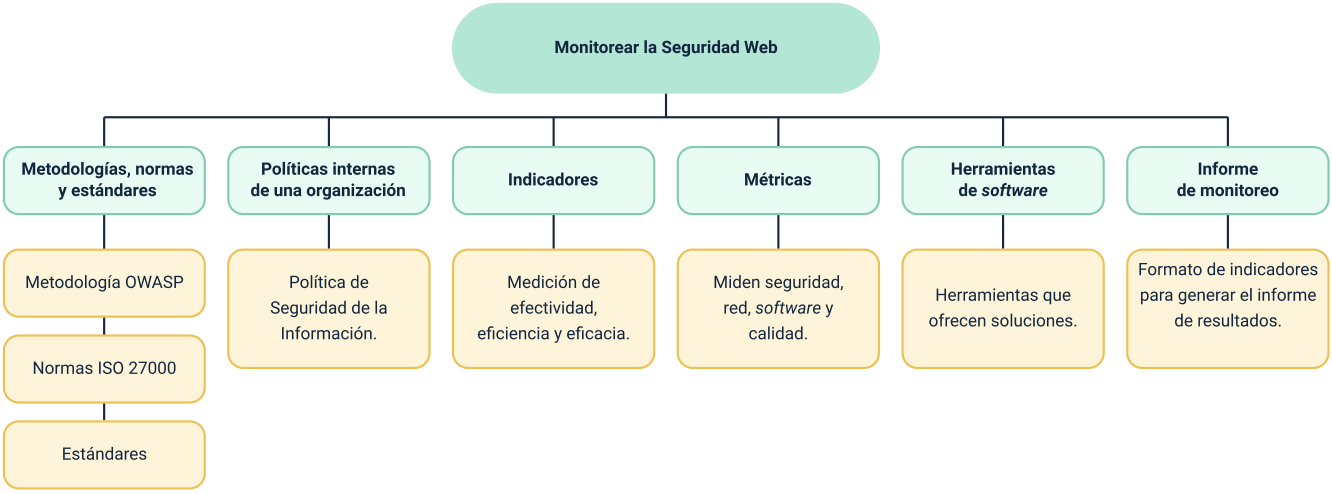
Con base en las métricas antes descritas, se deben generar los formatos de indicadores para generar el informe de resultados; a continuación se ilustra un formato de presentación de indicador unido a los reportes generados desde las herramientas de "software".

Figura 2. Ejemplo de informe de monitoreo

INDICADOR 01-ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN					
Identificador	SGIN01				
DEFINICIÓN					
El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad.					
OBJETIVO					
Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección.					
TIPO DE INDICADOR **INDICADOR DE GESTIÓN**					
DESCRIPCIÓN DE VARIABLES		**FÓRMULA**		**FUENTE DE INFORMACIÓN**	
VISI01: Número de personas con su respectivo rol definió según el modelo de operación. Capítulo 2.		(VISI01/VSI02)*100		Capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información.	
VISI02: Número de personas con su respectivo rol definido después de un año.				Actas de asignación de personal	
METAS					
Mínima	75-80%	**Satisfactoria**	80-90%	**Sobresaliente**	100%
OBSERVACIONES					
De acuerdo a lo establecido en el capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información, es necesario crear nuevos cargos y asignar responsabilidades en los actuales, por lo tanto, el indicador está enfocado, no solo a la contratación de nuevas personas, sino a la asignación de responsabilidades					

Síntesis

En el siguiente mapa conceptual se resumen los conceptos vistos en este componente formativo:



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Metodologías, normas y estándares	Caballero, A. [Alonso Caballero]. (2019, 31 de enero). Webinar Gratuito: Guía de Pruebas de OWASP.	Video	https://www.youtube.com/watch?v=kXfZqQY0rcg&ab_channel=AlonsoCaballer

Glosario

ASVS: estándar de verificación de seguridad de aplicaciones.

“Checklist”: lista de chequeo qué sirve para registrar un proceso de auditoría.

CVE/CVSS: vulnerabilidades y exposiciones comunes.

OWASP: Open Web Application Security Project.

“Pentesting”: proceso que imita posibles ataques a una red informática e intenta robar datos.

Referencias bibliográficas

Cec, N. (2020). *ISO/IEC 27034: Estándar Internacional para la seguridad de las aplicaciones* | noticias.cec.es. https://www.cec.es/isoiec-27034-estandar-internacional-para-la-seguridad-de-las-aplicaciones/

Negocio, IPT. (2018). *Indicadores de riesgo en la seguridad de datos.* https://www.informaticaparatunegocio.com/blog/indicadores-riesgo-la-seguridad-datos/

Normas ISO. (2018). *Normas ISO sobre gestión de seguridad de la información* | Seguridad Informática. http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

OWASP Top 10. (2021). *A09 Fallas en el Registro y Monitoreo* - OWASP Top 10:2021. https://owasp.org/Top10/es/A09_2021-Security_Logging_and_Monitoring_Failures/

Créditos

Nombre	Cargo	Centro de Formación y Regional
Claudia Patricia Aristizábal	Líder del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carlos Muñoz	Experto temático	Centro de teleinformática y producción industrial - Regional Cauca
Paula Andrea Taborda Ortiz	Diseñadora instruccional	Centro de la Industria, la Empresa y Los Servicios CIES - Regional Norte de Santander
Ana Catalina Córdoba Sus	Asesora metodológica	Centro de Diseño y Metrología - Regional Distrito Capital
Sandra Patricia Hoyos Sepúlveda	Corrección de estilo	Centro de Diseño y Metrología - Regional Distrito Capital
Juan Daniel Polanco Muñoz	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Edward Leonardo Pico Cabra	Desarrollador Fullstack	Centro Industrial del Diseño y la Manufactura - Regional Santander
Maria Natalia Maldonado	Diseño web	Centro Industrial del Diseño y la Manufactura - Regional Santander
Luis Jesús Pérez Madariaga	Desarrollo front-end	Centro Industrial del Diseño y la Manufactura - Regional Santander
Gilberto Junior Rodríguez Rodríguez	Validación audiovisual	Centro Industrial del Diseño y la Manufactura - Regional Santander
John Jairo Arciniegas González	Producción audiovisual	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Centro de Formación y Regional
María Carolina Tamayo López	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Wilson Andrés Arenales Cáceres	Validación Ilustración	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruíz Torres	Revisión de guion audiovisual	Centro de Comercio y Servicios - Regional Tolima
Yuli Marcela Gómez Tarazona	Validación de contenido	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruiz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Luis Gabriel Urueta Alvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis Gómez	Evaluador para contenidos inclusivos y accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander