**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Técnico en tratamiento de riesgos de ciberseguridad en la micro, pequeña y mediana empresa (MiPyME) |
| --- | --- |

| COMPETENCIA | 220501111 -  Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501111-01-Establecer indicadores, métricas y alcance de seguimiento de la seguridad digital.  220501111-02-Realizar seguimiento de la seguridad digital de acuerdo con los indicadores y métricas establecidos. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF05 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Evaluación de la ciberseguridad en la organización. |
| BREVE DESCRIPCIÓN | El componente aborda conceptos clave para la generación de métricas de seguridad: el Testing, y su propósito en la seguridad de la información, el SIEM, una forma de hacer gestión para prevenir problemas de seguridad, el SOC, sitio para centralizar la operación de seguridad de los sistemas computacionales, y por último el concepto de recopilación de información para el entorno de seguridad informática. |
| PALABRAS CLAVE | Métricas, recopilación de información, SIEM, SOC, testing, monitoreo. |

| ÁREA OCUPACIONAL | 2 - CIENCIAS NATURALES, APLICADAS Y RELACIONADAS |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS**

1. Métodos de métricas e indicadores de monitoreo

1.1. Características

1.2. Tipos.

2. Testing y monitoreo de la seguridad digital

2.1. Tipos

2.2. Características

2.3. Software.

3. Fundamentos de SIEM - Security Information and Event Management

3.1. Tipos

3.2. Características

3.3. Aplicación

4. Fundamentos de SOC - Security operation Center

4.1. Objetivos

4.2. Alcance

5. Técnicas de recopilación de información (Information gathering)

5.1. Tipos

5.2. Características

5.3. Aplicación

1. **INTRODUCCIÓN**

En los últimos años se ha producido un creciente interés por las métricas de seguridad, varios libros, numerosos artículos e informes se han dedicado a demostrar las ventajas de medir la seguridad de computación. Las métricas de seguridad se han convertido en un tema candente tan rápidamente que algunos podrían suponer que se acaba de descubrir la posibilidad de medir lo que se hace. Pero esto no es exacto, métricas de seguridad como la esperanza de pérdida anualizada (ALE), el coste total de propiedad (TCO) y la evaluación de riesgos cuantitativa y cualitativa, han sido utilizadas por los profesionales de la seguridad durante años.

Lo que es nuevo en las métricas de seguridad es la creciente comprensión de que muchos de los esfuerzos tradicionales de medición son insatisfactorios, dado que no ofrecen la información que realmente se necesita para apoyar las decisiones y articular el valor de las actividades de seguridad. Tampoco son adecuados para el cambiante panorama de la seguridad, con amenazas más sutiles y una mayor responsabilidad y escrutinio. El consenso creciente es que se debe medir mejor y considerar formas nuevas e innovadoras de analizar los datos métricos que ya se tienen.

El presente componente formativo analiza algunos conceptos clave para la generación de métricas de seguridad desde la lógica del proceso de evaluación a la ciberseguridad de las organizaciones. Se puede revisar el siguiente video de introducción a la temática:



1. **DESARROLLO DE CONTENIDOS**

**1. Métodos de métricas e indicadores de monitoreo**

Se mide la seguridad fundamentalmente, para entenderla. Lo ideal es establecer programas de métricas de seguridad que vayan más allá de la recopilación de datos y estén orientados realmente a la medición.

La recopilación de datos de seguridad es fundamental para cualquier programa de métricas eficaz, pero sin un contexto para esos datos y una idea de por qué se recopilan y qué se pretende hacer con ellos, podría verse limitado a describir la medición sólo en términos de terabytes de datos de registro y el volumen de estanterías que ocupan los informes de los auditores.

A continuación se pueden observar algunas consideraciones a la hora de emprender un programa de métricas de seguridad:



* 1. **Características**

Dadas sus limitaciones, algunas métricas pueden convertirse en indicadores engañosos de la eficacia de la seguridad. Hay muchos argumentos sobre lo que hace que una métrica sea buena o mala:

* Cualquier medida empírica que ayude a una organización a reducir la incertidumbre es una buena métrica.
* Una métrica que deba descartarse simplemente porque no sea cuantitativa o específica.
* Una métrica es buena simplemente porque sea fácil e inequívoca.

Cualquier medición se vuelve problemática cuando se realiza de forma deficiente y cuando quienes miden no son suficientemente críticos con sus propios métodos. Los problemas que pueden surgir de los intentos poco sofisticados de medir la seguridad pueden incluir cuestiones de calidad de los datos, rigor empírico o el hecho de que las métricas se utilicen de forma inmadura o engañosa.

De todos los fenómenos que preocupan en el ámbito de la seguridad informática, el riesgo parece ser el primero de la lista. Pero, pese a su importancia, a menudo es uno de los conceptos menos comprendidos. Una matriz de riesgos de seguridad basada en juicios de expertos puede ser una estimación útil, pero sigue siendo un conjunto de opiniones sobre el riesgo. Los mayores problemas de seguridad identificados en la matriz no son necesariamente los mayores problemas de seguridad a los que se enfrenta la empresa. La esperanza es que los verdaderos riesgos de seguridad se correlacionen de alguna manera con las opiniones de los expertos responsables de la seguridad. 

El punto no es que la matriz de riesgos de seguridad sea un mal método de medición, sino pretender que la matriz mida el riesgo real. Desgraciadamente, la mayoría de los usuarios de la matriz en la seguridad informática la utilizan para tomar decisiones "basadas en el riesgo".

La matriz de riesgos se ha convertido en el motor de algunas de las metodologías de evaluación de riesgos de seguridad más comunes hoy en día, utilizadas como metodología formal de evaluación y gestión de riesgos de la organización, como exigen algunos marcos de cumplimiento. En estos casos, la matriz no actúa como un prototipo inicial de medición de riesgos que conduce a más preguntas y métricas, sino como el resultado final del proceso de evaluación de riesgos. El asunto no es abandonar la matriz de riesgos como medio de apoyo a las decisiones de seguridad, pero sí utilizarla para fines diferentes a los acostumbrados, como se puede ver a continuación:



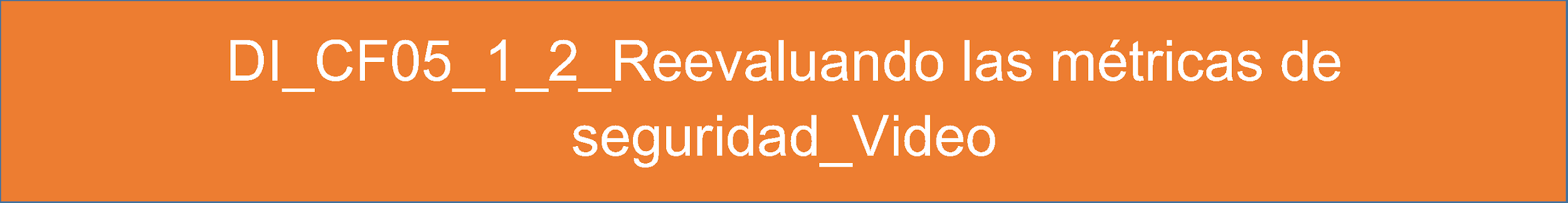
**1.2 Tipos**

Los datos que se recogen con más frecuencia para entender la seguridad de la información tienen que ver con las vulnerabilidades del sistema y los esfuerzos para comprometerlas.

Las estadísticas de vulnerabilidad del sistema se producen cuando una organización ejecuta un escáner de seguridad en su red, se identifican nuevos exploits y se dan a conocer a los proveedores y al público, y cuando las organizaciones publican los informes resultantes de las encuestas de la industria que han realizado o los análisis de los datos de seguridad que han recogido.

Las estadísticas de incidentes proceden de los registros del sistema, de los sistemas de detección y prevención de intrusiones y de las encuestas y análisis del sector. Estas cifras suelen utilizarse como indicadores generales del estado actual de la seguridad informática.

Las métricas de seguridad que se utilizan hoy en día son insuficientes para el futuro de la seguridad de la información. Es preciso desarrollar enfoques más sofisticados de los procesos de seguridad en general y de la medición y evaluación de esos procesos en particular. Las experiencias de otros sectores como los seguros, la fabricación y el diseño, que se han enfrentado a los mismos retos, ofrecen valiosas lecciones sobre cómo pensar los datos, los procesos y las personas a la hora de abordar la generación de métricas de seguridad. Observe el siguiente video e identifique aspectos clave en la definición de un programa de métricas de seguridad:



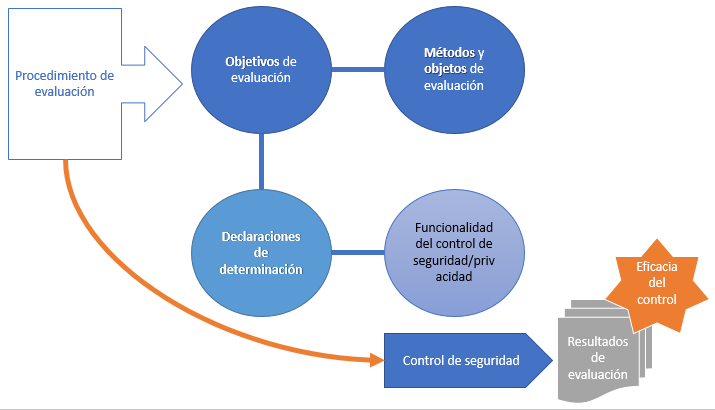
**2 Testing y monitoreo de la seguridad digital**

La evaluación de un sistema o aplicación es el proceso de revisar, probar y evaluar los componentes, la documentación y todos los parámetros de este sistema o aplicación con el fin de garantizar que sea lo más seguro posible, dentro de la tolerancia al riesgo de una organización, mientras está operativo y se utiliza para su propósito.

De acuerdo con la Guía para la evaluación de controles de seguridad (National Institute of Standards and Technology.[NIST], 2010, p. 9) un procedimiento de evaluación consiste en un conjunto de objetivos de evaluación, cada uno con un conjunto asociado de posibles métodos y objetos de evaluación, en donde cada objetivo de evaluación incluye un conjunto de declaraciones de determinación relacionadas con el control de seguridad o privacidad particular que se está evaluando. Las declaraciones de determinación están vinculadas al contenido del control de seguridad o privacidad para garantizar la trazabilidad de los resultados de la evaluación hasta los requisitos fundamentales del control. La aplicación de un procedimiento de evaluación a un control de seguridad o privacidad produce resultados de evaluación, que se reflejan en la eficacia general del control de seguridad o privacidad, determinando si el control se ha implementado correctamente, funciona según lo previsto y produce el resultado deseado en relación con los requisitos de seguridad del sistema o aplicación en cuestión (Ver figura a continuación):

**Figura 1**

*Evaluación de controles de seguridad*



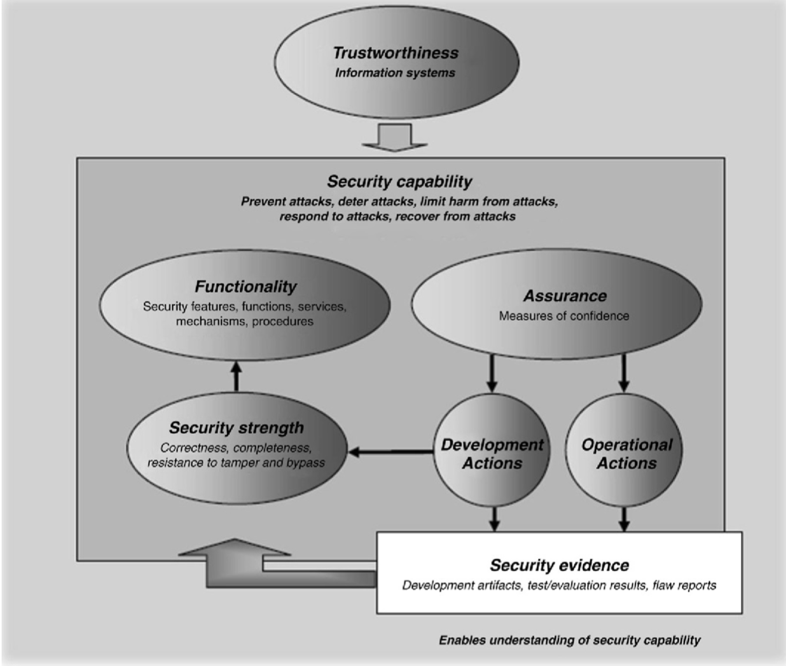
Los objetos de evaluación identifican los elementos específicos que se evalúan e incluyen especificaciones, mecanismos, actividades e individuos, a continuación se puede ver en qué consisten:



El objetivo de estas distintas áreas de evaluación y su cobertura del sistema y la red en cuestión, es proporcionar pruebas de evaluación que los responsables puedan utilizar para tomar decisiones operativas desde el punto de vista de la fiabilidad, tal y como se muestra en la siguiente figura.

**Figura 2**

*Sistemas de información de confiabilidad*



Nota. *Security controls evaluation, testing, and asssment handbook*. J. Leighton (2019).

**2.1 Tipos**

A partir de las experiencias y buenas prácticas desarrolladas por expertos en el proceso de evaluación, validación y auditoría y lo contemplado en la Guía para la evaluación de controles de seguridad (NIST, 2010), es posible determinar una secuencia de pasos a realizar durante el proceso de evaluación, como se puede observar a continuación:



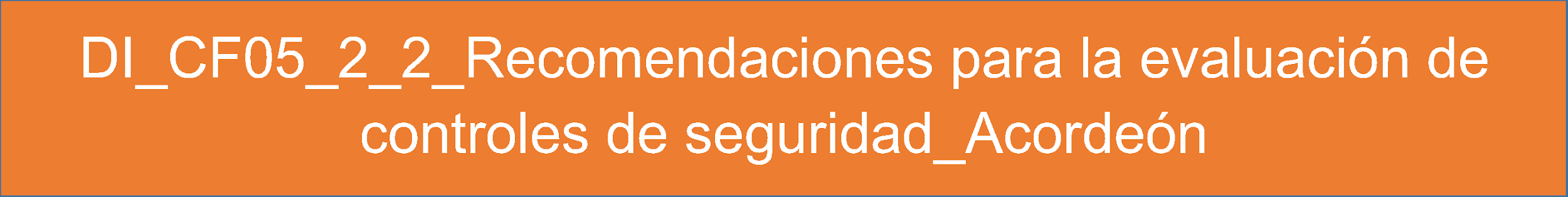
**2.2. Características**

Para llevar a cabo la evaluación de un sistema o aplicación, hay que centrarse inicialmente en las áreas de mayor impacto, mayor valor y mayor volatilidad. Una vez determinado esto, el enfoque se desplaza al resto del sistema o aplicación para cubrir todas las posibles áreas de impacto, ya que, en el ámbito de la seguridad, hoy en día es posible cualquier método de ataque o entrada en el sistema.

Según la SP 800-115, algunas evaluaciones se centran en verificar que un control de seguridad concreto (o un conjunto de controles) cumple los requisitos, mientras que otras evaluaciones pretenden identificar, validar y valorar los puntos débiles de seguridad explotables de un sistema. Las evaluaciones también se realizan para aumentar la capacidad de una organización para mantener una defensa proactiva de la red informática. En todo caso, las evaluaciones no pretenden sustituir la implementación de controles de seguridad y el mantenimiento de la seguridad del sistema.

El enfoque especializado de un evaluador es necesario cuando el sistema bajo prueba o la aplicación en cuestión se encuentra en un entorno de alta volatilidad, acaba de remediar problemas de seguridad que se han reparado, o requiere una revisión de verificación y validación independiente para futuras operaciones en una red federal.

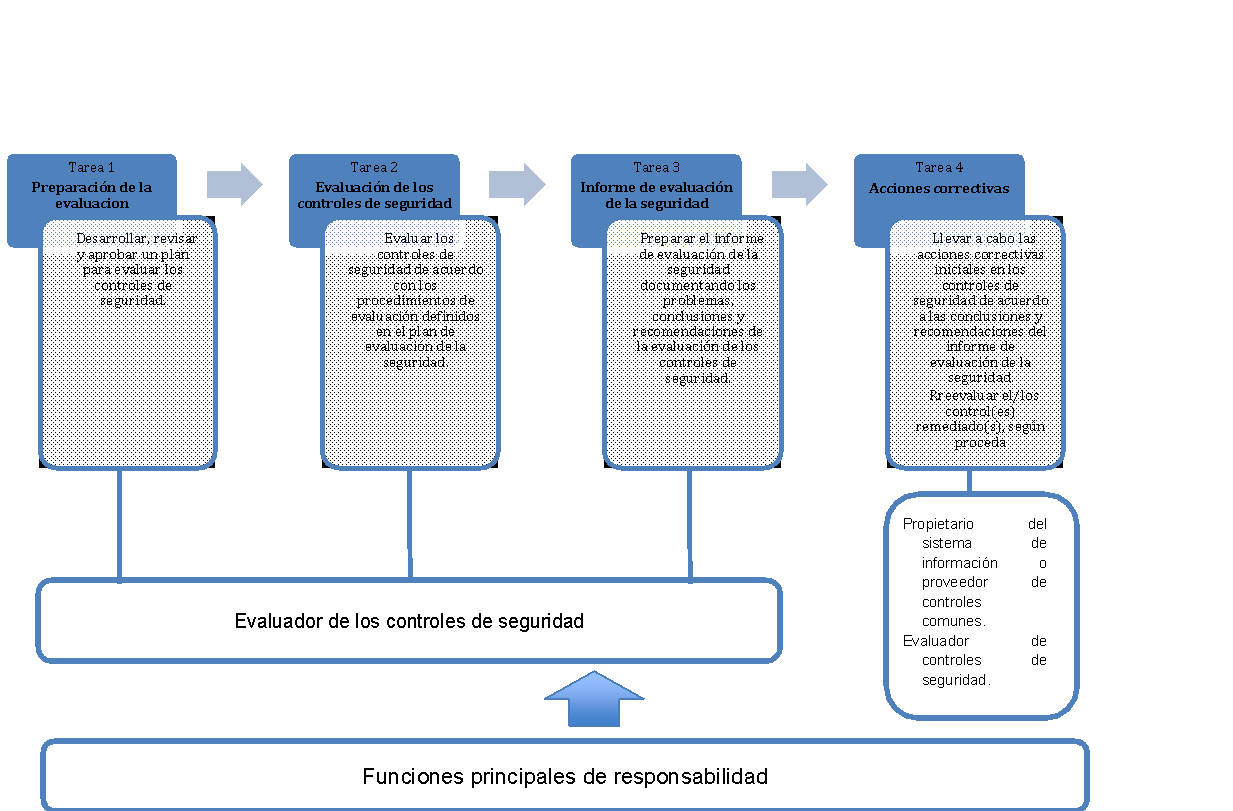
El NIST en la Guía para la evaluación de controles de seguridad (2010), hace las siguientes recomendaciones a las organizaciones interesadas en llevar a cabo evaluaciones técnicas de seguridad y garantizar que las pruebas y exámenes técnicos de seguridad proporcionen el máximo valor:



Dentro del marco del proceso RMF, el SP 800-53A proporciona la guía especializada y el flujo del proceso para llevar a cabo las pruebas reales y los eventos de evaluación en cada control de seguridad implementado en el sistema o aplicación bajo evaluación. El paso 4 del RMF - evaluación - es el paso dirigido dentro del RMF (SP 800-37, rev. 1) que proporciona la guía general para llevarlo a cabo (ver figura).

**Figura 3**

*RMF Paso 4 - Evaluar los controles de seguridad*



**Métodos de evaluación**

Los métodos y procedimientos de evaluación se utilizan para determinar si los controles de seguridad se aplican correctamente, funcionan como se pretende y producen el resultado deseado con respecto al cumplimiento de los requisitos de seguridad de la organización. Las organizaciones utilizan los procedimientos de evaluación recomendados en el SP 800-53A como punto de partida para desarrollar procedimientos de evaluación más específicos, que pueden, en ciertos casos, ser necesarios debido a las dependencias de la plataforma u otras consideraciones relacionadas con la implementación. El empleo de procedimientos de evaluación estandarizados promueve evaluaciones de seguridad más consistentes, comparables y repetibles de los sistemas de información.

A continuación se pueden revisar los tipos de métodos de evaluación que se pueden utilizar:



**Testing**

Las pruebas implican un trabajo práctico con sistemas y redes para identificar las vulnerabilidades de seguridad, y pueden ejecutarse en toda una empresa o en sistemas seleccionados. El uso de técnicas de escaneo y penetración puede proporcionar información valiosa sobre posibles vulnerabilidades y predecir la probabilidad de que un adversario o intruso sea capaz de explotarlas. Las pruebas también permiten a las organizaciones medir los niveles de cumplimiento en áreas como la gestión de parches, la política de contraseñas y la gestión de la configuración.

Aunque las pruebas pueden proporcionar una imagen más precisa de la postura de seguridad de una organización que la que se obtiene a través de los exámenes, son más intrusivas y pueden afectar a los sistemas o redes del entorno objetivo. El nivel de impacto potencial depende de los tipos específicos de técnicas de prueba utilizados, que pueden interactuar con los sistemas y redes de destino de varias maneras, como el envío de paquetes de red normales para determinar los puertos abiertos y cerrados, o el envío de paquetes especialmente diseñados para probar las vulnerabilidades. Cada vez que una prueba o probador interactúa directamente con un sistema o red, existe la posibilidad de que se produzcan paradas inesperadas del sistema y otras condiciones de denegación de servicio. Las organizaciones deben determinar sus niveles aceptables de intrusión cuando decidan qué técnicas utilizar. Excluir las pruebas conocidas por crear condiciones de denegación de servicio y otras interrupciones puede ayudar a reducir estos impactos negativos.

**2.3. Software**

Se debe revisar cada detalle en la siguiente infografía, sobre los métodos de evaluación y lineamientos establecidos en relación al software:



**3. Fundamentos de SIEM - Security Information and Event Management**

El sistema de gestión de información y eventos de seguridad (SIEM) consiste en una compleja colección de tecnologías diseñadas para proporcionar visión y claridad sobre el sistema de tecnología de la información (TI) corporativo en su conjunto, beneficiando también a los analistas de seguridad y administradores de TI. 

Observar en el siguiente video algunas de las ventajas ofrecidas por el sistema de gestión de información y eventos de seguridad (SIEM).



**3.1. Tipos**

Ahora se debe revisar algunas consideraciones relacionadas con la tipología del sistema SIEM, partiendo de la gestión de registros, que implica las acciones descritas a continuación:



**3.2. Características**

Implementar un sistema SIEM no es un asunto de poca monta económicamente hablando, por lo que es necesario justificar adecuadamente la propuesta. Al proporcionar una visión más completa de las operaciones de TI y sobre la seguridad y protección de los activos valiosos de información dentro de organización, se espera que con un sistema SIEM en funcionamiento, la empresa experimente menos pérdidas, que, llevadas a costos, compensan el precio del SIEM:

* En primer lugar, con un SIEM se automatizan muchas funciones de supervisión, alerta, análisis, correlación y elaboración de informes, de manera más eficiente que los sistemas propios, que se realizan muchas veces de forma manual.
* En segundo lugar, el sistema SIEM ayuda a la organización a cumplir las directrices legales exigidas en materia de TI y seguridad, permitiendo identificar y corregir los sistemas y procesos que no cumplen la normativa y protegiéndola de multas relacionadas con el cumplimiento.
* Por último, y quizás lo más importante, de contar con el sistema SIEM es poder reducir drásticamente la superficie de ataque de una organización, lo que, combinado con las capacidades de reconocimiento, alerta y respuesta más rápidas proporcionadas por el SIEM, traerá beneficios al reducir la probabilidad de una violación de la seguridad y minimizar las pérdidas potenciales ocurridas durante una violación de la seguridad u otro tipo de evento de pérdida.

**3.3. Aplicación**

Ante el aumento de sucesos de ciberdelincuencia, incidentes de robo de identidad y de propiedad intelectual y ciberataques, los profesionales de la seguridad deben velar por asegurar cada vez mejor su entorno, utilizando toda la información a disposición para determinar cómo desplegar los recursos de que dispone.

Al abordar un nuevo entorno o reevaluar el actual, es primordial determinar la mejor estrategia de seguridad que dependerá en gran medida del modelo de negocio de la organización. Pero ¿Qué son los modelos de negocio de TI? Aproxímese al concepto a través de la revisión de la siguiente infografía:



**4. Fundamentos de SOC - Security Operation Center**

El centro de operaciones de seguridad, más comúnmente llamado "el SOC", es una unidad centralizada que se ocupa de los problemas de seguridad tanto a nivel organizativo como técnico. Esto ocurre mediante el uso de personas, procesos y capacidades para prestar servicios que pueden incluir:

* Identificación y la reducción de riesgos.
* Tratamiento de vulnerabilidades.
* Adhesión a los requisitos de cumplimiento.
* Respuesta a los incidentes.
* Recogida de pruebas forenses.

A continuación, se detallan algunos conceptos y elementos generales de las etapas de operación de un SOC, que favorecen un correcto funcionamiento:

**4.1 Objetivos**

El objetivo de un SOC es detectar, analizar y corregir incidentes de ciberseguridad utilizando soluciones tecnológicas y enfoques diferentes. Estos supervisan y analizan la actividad en redes, servidores, terminales, bases de datos, aplicaciones, sitios web y otros sistemas, en busca de señales débiles o comportamientos anormales que puedan indicar un incidente de seguridad o un compromiso (Oracle.com, 2021).

Los objetivos de un centro de operaciones de seguridad (SOC), deben enfocarse en:

* Reducir riesgos y tiempo de indisponibilidad de aplicaciones y servicios.
* Control y prevención de amenazas.
* Disminuir la carga de trabajo administrativa del personal de seguridad.
* Establecer el personal de seguridad y definir responsabilidades.
* Indicar los tiempos de soporte y escalamiento de eventos.
* Definir los procesos de auditoría y soportes de cumplimiento.
* Responder a incidentes y recuperación.

**4.2. Alcance**

Los SOC maduros de todo el mundo suelen tener en común un conjunto básico de servicios de seguridad que pueden ser internos, subcontratados o incluso bajo demanda, lo que permite al SOC disponer de los servicios deseados cuando los necesite. Independientemente del enfoque de prestación, hay servicios que todo SOC debe ofrecer. Para resumir esos servicios comunes del SOC, se pueden definir las siguientes ofertas:



**5. Técnicas de recopilación de información (Information gathering)**

Cuando se lleva a cabo la vigilancia y el reconocimiento digital, una de las prioridades es reunir información sobre un objetivo o un grupo de objetivos. Con los progresos del ámbito digital, se puede estar en un terminal de ordenador o en un dispositivo móvil en cualquier parte del mundo, conectarse a la Internet pública y reunir gran cantidad de información sobre variedad de objetivos en cuestión de minutos, todo ello sin ser detectado.

Esto tiene gran importancia en primer lugar, porque para poder atacar, hay que encontrar vectores en los que se pueda vulnerar el objetivo. Hoy día, con la tecnología digital es evidente el creciente vector de ataque. Una conversación telefónica, por ejemplo, puede ser almacenada digitalmente dentro de un dispositivo de cambio de rama privada, de forma local en el teléfono o capturada en la transmisión y colocar aplicaciones en el dispositivo receptor para escuchar la conversación. Hay más puntos en la transmisión para capturar datos y más lugares en los que se almacenan.

Asumida la posibilidad de recopilar información de forma rápida y fácil, es necesario considerar todos los puntos en los que se puede recopilar. Así entendido el vector de ataque, considerar si la información es realmente privada y para adelantar entonces medidas de protección y mitigar los ataques.

**5.1. Tipos**

A medida que se centralizan más y más datos, y las herramientas evolucionan para hacer un mejor trabajo de extracción de información clave, la capacidad de utilizar esto para el espionaje crece exponencialmente. Los big data y la informática/analítica son las principales áreas de crecimiento tecnológico en la actualidad, respondiendo a la necesidad de las organizaciones de aprovechar los datos almacenados para obtener resultados específicos

Existen muchas herramientas de vigilancia, las que realizan tareas específicas de recopilación de información y otras en las que se puede recopilar y correlacionar información, algunas de ellas se destacan en la siguiente imagen:



**5.2. Características**

A continuación se ven las características de las principales técnicas de recopilación de información, determinando su alcance y relevancia:



**5.3. Aplicación**

Las técnicas de recolección de información pueden ser aplicadas a través de varias formas o tácticas que se detallan a continuación:



Implica engañar a alguien a través de una conversación para obtener las respuestas requeridas. Por ejemplo, llamar desde un número de teléfono falsificado que parece que proviene de una fuente de confianza, contar cosas de interés particular para ganar confianza y a través de preguntas específicas, obtener información para entrar en un sitio web personal o una cuenta bancaria.

1. **SÍNTESIS**

Revise el siguiente esquema que a manera de síntesis articula los elementos principales abordados en el desarrollo del componente formativo.

1. **ACTIVIDADES DIDÁCTICAS**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la actividad | Conceptos básicos para la evaluación de la ciberseguridad. |
| Objetivo de la actividad | Identificar conceptos básicos de evaluación de la ciberseguridad aplicables a la generación de controles de seguridad de los sistemas computacionales. |
| Tipo de actividad sugerida | Cuestionario |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | DI\_CF05\_Actividad didáctica\_1  (Carpeta formatos de diseño) |

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la actividad | Técnicas de recopilación de información |
| Objetivo de la actividad | Identificar las principales técnicas de recopilación de información aplicables a la generación de controles de ciberseguridad en las organizaciones. |
| Tipo de actividad sugerida | Relación de términos |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | DI\_CF01\_Actividad didáctica\_2  (Carpeta formatos de diseño) |

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 |
| --- | --- | --- | --- |
| Testing y monitoreo de la seguridad digital | Mo, Y. Hyun-Jin, T., Brancik, K., Dickinson, D., Lee, H., Perrig, A. and Sinopoli, B. Cyber–Physical Security of a  Smart Grid Infrastructure. *Proceedings of the IEEE*, *100* (1), 195-209. <https://www.researchgate.net/profile/Yilin-Mo/publication/224257991_Cyber-Physical_Security_of_a_Smart_Grid_Infrastructure/links/004635395d2f66a584000000/Cyber-Physical-Security-of-a-Smart-Grid-Infrastructure.pdf> | Artículo | <https://www.researchgate.net/profile/Yilin-Mo/publication/224257991_Cyber-Physical_Security_of_a_Smart_Grid_Infrastructure/links/004635395d2f66a584000000/Cyber-Physical-Security-of-a-Smart-Grid-Infrastructure.pdf> |
| Técnicas de recopilación de información | Owasp Foundation. (2021). *Vulnerability scanning tools.* Owasp.<https://owasp.org/www-community/Vulnerability_Scanning_Tools> | Página Web | <https://owasp.org/www-community/Vulnerability_Scanning_Tools> |

1. **GLOSARIO**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| AWS | Nube de Amazon. |
| AZURE | Nube de Microsoft. |
| DOS | Ataque de negación de servicio. |
| SCI | Sistema de control interno. |
| SCD | Sistema de control distribuido. |
| ACL | Listas de control de acceso. |
| AAA | Autenticación, autorización y contabilidad. |
| IDS | Sistemas de detección de intrusos. |
| Sistemas ERP | Estaciones de trabajo de usuarios finales. |
| PLC | Controlador lógico programable. |
| DNS | Protocolo de sistema de nombres de dominio. |
| DHCP | Protocolo de configuración dinámica de host. |
| UI | Interfaz de usuario. |
| Dockerfile | Archivo para configurar contenedores de Docker. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

Johnson, L. (2019). *Security controls evaluation, testing, and assessment handbook*. Academic Press.

National Institute of Standards and Technology. (2010). *Guide for assessing the security controls in federal information systems and organizations* U.S. Department of Commerce.

Oracle. (2021). *¿Qué es un SOC?* Oracle. <https://www.oracle.com/es/database/security/que-es-un-soc.html>

1. **CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Joaquín Fernando Sánchez | Experto temático | Regional Norte de Santander | Octubre de 2022 |
| Maribel Avellaneda Nieves | Diseñadora instruccional | Regional Norte de Santander - Centro de la Industria, la Empresa y los Servicios | Octubre de 2022 |
| Silvia Milena Sequeda Cárdenas | Asesora metodológica y pedagógica | Regional Distrito Capital - Centro de Diseño y Metrología. | Octubre de 2022 |
| Rafael Neftalí Lizcano Reyes | Responsable Equipo desarrollo curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Octubre de 2022 |
|  | Jhon Jairo Rodríguez Pérez | Corrector de estilo | Regional Distrito Capital - Centro de Diseño y Metrología | Noviembre de 2022 |

1. **CONTROL DE CAMBIOS**

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

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