

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.

**Junio 2023**

Tabla de contenido

[Introducción 1](#_Toc141015236)

[1. Métodos de métricas e indicadores de monitoreo 4](#_Toc141015237)

[1.1. Características 5](#_Toc141015238)

[1.2. Tipos 7](#_Toc141015241)

[2. “Testing” y monitoreo de la seguridad digital 12](#_Toc141015242)

[2.1. Tipos 15](#_Toc141015243)

[2.2. Características 19](#_Toc141015244)

[2.3. “Software” 24](#_Toc141015247)

[3. Fundamentos de SIEM – “Security Information and Event Management” 25](#_Toc141015248)

[3.1. Tipos 27](#_Toc141015249)

[3.2. Características 29](#_Toc141015250)

[3.3. Aplicación 30](#_Toc141015251)

[4. Fundamentos de *SOC* – “Security Operation Center*”* 31](#_Toc141015252)

[4.1. Objetivos 32](#_Toc141015253)

[4.2. Alcance 33](#_Toc141015254)

[5. Técnicas de recopilación de información (“Information gathering”) 35](#_Toc141015255)

[5.1. Tipos 35](#_Toc141015256)

[5.2. Características 37](#_Toc141015257)

[5.3. Aplicación 40](#_Toc141015258)

[Síntesis 41](#_Toc141015259)

[Material complementario 42](#_Toc141015260)

[Glosario 43](#_Toc141015261)

[Referencias bibliográficas 44](#_Toc141015262)

[Créditos 45](#_Toc141015263)

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. Evaluación de la ciberseguridad en la organización



[Enlace de reproducción del video](https://youtu.be/NGJBT7D2hpQ)

|  |
| --- |
| **Síntesis del video: Evaluación de la ciberseguridad en la organización** |
| Cuando se informa a los clientes sobre cómo desarrollar un programa eficaz de métricas de seguridad, se suele enfrentar a varios retos.  Si bien la gente entiende la relevancia de las métricas, tiende a medirse sólo aquello con lo que se trata regularmente.  Por ejemplo, todas las mañanas cuando se prepara el café, midiendo cuidadosamente las cucharadas de café y las tazas de agua.  Estas medidas importan porque afectan directamente el desayuno. No se piensa en la relación de estas medidas con otros parámetros.  Como los niveles de acidez y nitrógeno para cultivar el grano o las temperaturas y duraciones óptimas para tostarlo. Se depende de otros para estas mediciones.  Las mediciones, tanto para el café como para la seguridad de computación, implican muchos esfuerzos cada vez más interdependientes y estratégicos.  Puede que la gente no mida la seguridad más allá de analizar el contenido de los registros del cortafuegos.  Pero si no se entiende cómo otros miden la seguridad u otros valores empresariales, se será menos capaz de utilizar los datos para tomar buenas decisiones.  La medición consiste en entender por qué se quiere medir algo, qué es lo que se quiere medir, cómo medirlo y qué hacer con los datos.  A medida que la seguridad se vuelve cada vez más compleja y omnipresente.  Por ello, los profesionales de la seguridad no sólo protegen los activos de la empresa, sino que contribuyen a su éxito financiero y competitivo. |

# 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 solo 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. **Las métricas son un viaje, no el destino**: una vez establecido un programa de métricas de seguridad, preguntarse cómo los resultados han mejorado la comprensión de los sistemas y procesos de seguridad.
2. **Comprender no es diagnosticar**: conocer el porcentaje de contraseñas fáciles de descifrar o la proporción de computadores vulnerables no es suficiente si dicha información no permite mejorar la eficacia de la seguridad computacional. Incluso si la seguridad ha mejorado, pero sin saber a qué obedece la mejora, algo le falta al programa de métricas de seguridad.
3. **Las métricas no son conocimiento**: las métricas son depósitos de datos conceptuales que definen y estandarizan información. Al igual que las entradas de palabras bien definidas no transforman un diccionario en literatura: ¡Solo las personas pueden lograr estas cosas!
4. **No es cuestión de recopilar muchos datos**: un pequeño conjunto de datos, bien entendido y aplicado regularmente, es mucho más valioso que una montaña de datos sin utilizar.
5. **La medición es una actividad**: la medición implica realizar observaciones y recopilar datos para obtener una visión práctica de lo que se intenta comprender. La distinción es importante, porque las métricas no solo aportan información sobre la seguridad informática, sino también sobre los costes y los riesgos.
6. **Analizar y actuar**: la medición sin análisis y acción supone una pérdida de tiempo y dinero y contribuye a la incertidumbre y al riesgo en lugar de reducirlos. Conocer el problema y no actuar en consecuencia, lleva a una violación de la seguridad, que podría terminar siendo más perjudicial que la ignorancia que existía antes de que se recogieran los datos.

## 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:

### Utilizar la matriz para crear un prototipo de nuevas evaluaciones de riesgos

Ante los resultados, plantearse ¿por qué?, pensando en preguntas de seguimiento que conducen a nuevas mediciones:

* ¿Por qué es tan probable que el sistema se vea comprometido?
* ¿Por qué el impacto es tan grave en comparación con otros sistemas?

### Medir las diferencias de acuerdo

Comparar lo que piensan las diferentes personas de la organización sobre el riesgo, identificando las áreas en las que hay acuerdo o aquellas en las que hay amplia variación en las opiniones.

Este análisis permite descubrir dónde debe concentrar la organización sus esfuerzos de evaluación de riesgos, incluyendo dónde realizar actividades de medición más sofisticadas y sólidas.

## 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:

1. Reevaluando las métricas de seguridad



[Enlace de reproducción del video](https://youtu.be/aTO98EWWtjk)

|  |
| --- |
| **Síntesis del video: Reevaluando las métricas de seguridad** |
| Al desarrollar un programa de métricas, se debe considerar el entorno local, las necesidades específicas de la organización y los recursos asociados a la medición.  No es necesario que los programas sean grandes o exhaustivos para tener éxito; aunque sí deben ser mejores que lo que había antes del programa.  Una métrica enfocada, analizada y presentada adecuadamente, puede ser el catalizador de un cambio completo en la forma en que la organización gestiona su seguridad.  Al construir un programa de métricas de seguridad, lo que realmente se está estableciendo es un programa para analizar los datos de las mediciones de seguridad.  El análisis de las métricas de seguridad implica la identificación de herramientas y técnicas para crear inteligencia procesable y aprendizaje organizativo.  Recoger grandes cantidades de datos relacionados con las métricas sin un plan convincente de análisis y alineación con objetivos bien formulados es ineficaz.  Incluso puede resultar peligroso para la organización, llegando a considerar que cualquier dato relacionado con problemas de seguridad implica responsabilidad de abordarlo.  Un programa de métricas de seguridad debe estar diseñado para proporcionar una cantidad manejable de datos utilizables que la organización se comprometa a gestionar.  El sector de la seguridad utiliza hoy en día, varias métricas para medir aspectos de la seguridad informática de las organizaciones, tales como:  • Matrices de riesgo.  • Estadísticas de vulnerabilidad e incidentes de seguridad.  • Esperanza de pérdidas anuales (ALE).  • Retorno de la inversión (ROI).  • Costo total de propiedad (TCO).  Aunque estas métricas están ampliamente aceptadas, pueden ser muy limitadas en cuanto al valor que aportan a un programa de seguridad.  Con demasiada frecuencia, las medidas no se comprenden bien y apuntan a aspectos de la seguridad muy diferentes a lo que los usuarios creen estar midiendo.  En otras ocasiones, la mayoría de estas métricas parten de datos poco fiables que deben complementarse con datos no empíricos.  Aunque esto no significa que las conclusiones extraídas de estos datos sean falsas, sí significa que esas conclusiones deben ser sometidas a mayor cuestionamiento.  En algunos casos, quienes manipulan los datos para obtener resultados más favorables a sus objetivos individuales u organizativos abusan de estas métricas.  Finalmente, sobresalen como elementos importantes para el éxito de un programa de medición de la seguridad:  1) Los datos de calidad.  2) El enfoque de la seguridad como un proceso empresarial.  3) El respeto por las personas y las interacciones sociales. |

# “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

La imagen presenta el procedimiento de evaluación, el cual está compuesto por unos objetivos de evaluación, métodos y objetos de evaluación, declaraciones de determinación y funcionalidad del control de seguridad/privacidad.
A su vez la aplicación del procedimiento de evaluación a un control de seguridad, produce resultados de evaluación, que se reflejan en la eficacia del control.

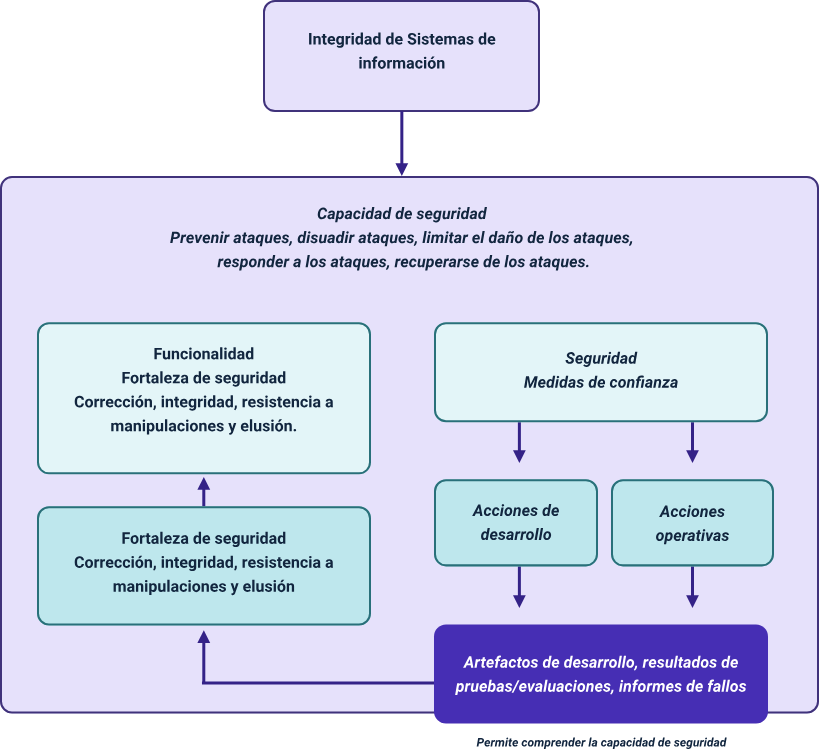
La evaluación de controles de seguridad, en tanto procedimiento sistemático, establece no solo objetivos de la evaluación misma, sino también métodos de aplicación. El control de la seguridad aporta resultados de evaluación que evidencian, o no, la eficacia del control.

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:

* **Especificaciones**: documentación (políticas, procedimientos, planes requisitos de seguridad y privacidad, especificaciones funcionales, diseños arquitectónicos) asociados a un sistema de información.
* **Mecanismos**: salvaguardas y contramedidas específicas de hardware, software o firmware empleadas en un sistema de información, es decir, los controles técnicos.
* **Actividades**: procesos relacionados con la protección de un sistema de información que involucran a las personas (por ejemplo, la realización de operaciones de copia de seguridad, la supervisión del tráfico de la red, la ejecución de un plan de contingencia).
* **Individuos**: personas que aplican las especificaciones, los mecanismos o actividades.

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. Tomado de J. Leighton (2019).

La integridad de los sistemas de información, traduce la capacidad de seguridad de una organización. Tal seguridad supone medidas de confianza, acciones de desarrollo y acciones operativas. Mediante artefactos de desarrollo, pruebas e informes, se fortalece permanentemente la seguridad y se preserva la integridad de los sistemas de información.

## 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:

1. **Revisar documentación**: verificación de documentos existente para el sistema o la aplicación bajo prueba. Estos documentos deben proporcionar las áreas principales para el escrutinio y la evaluación.
2. **Requisitos legales y reglamentarios**: cada sistema debe ajustarse a políticas y reglamentos, normalmente basados en los tipos de información utilizados, procesados o mantenidos por el sistema y la misión del sistema. Identificar áreas de conformidad y concordancia sustantiva entre el sistema, sus documentos y los requisitos externos.
3. **Realizar el análisis GAP (15 pasos)**: todos los documentos relevantes del sistema y de la documentación de apoyo.
4. **Visitar el lugar**: primera visita de verificación del estado del sistema y de los equipos, objetivo primordial para identificar áreas potenciales de preocupación o sospecha. Gestión de las expectativas del personal y la Dirección, sobre el proceso.
5. **Construir SAP y ROE**: desarrollar el Plan de Evaluación de Seguridad (SAP) que define los pasos, herramientas y técnicas de revisión que se aplicarán durante la evaluación. También se definen las Reglas de Compromiso (ROE) para toda la evaluación, incluyendo la realización de cualquier prueba externa, entrevistas e inspecciones según lo requerido por la organización.
6. **Aprobar SAP y ROE**: presentar el SAP y las ROE para su aprobación y aceptación al responsable de la contratación. La visita de evaluación propiamente dicha, no debe comenzar hasta haber recibido los documentos aprobados y firmados por medios oficiales.
7. **Realizar la evaluación**: una vez aprobados el SAP y las ROE, se programa la visita in situ para llevar a cabo las actividades de evaluación propiamente dichas. Importante preparación para la visita familiarizándose con las herramientas del oficio y documentación del sistema para realizar correctamente las entrevistas y los exámenes.
8. **Visita “in situ”**: suele comenzar con una reunión informativa con la dirección, en la que se discuten las expectativas de la visita, se reconfirma la programación de las entrevistas y se presenta el equipo al personal del lugar.
9. **Entrevistar al personal clave**: entrevistas con el personal operativo clave del sistema, el director de las instalaciones del lugar, el personal de seguridad tanto del lugar como del sistema, el propietario del sistema, los miembros del personal de administración del sistema del lugar y del sistema, así como cualquier desarrollador asociado con el sistema.
10. **Examinar el sistema**: Obtener una demostración por parte del personal para observar el procesamiento y los controles de seguridad en acción, así como las actividades de entrada y salida del sistema (control de acceso, identificación y autenticación, integridad, protección del sistema, comunicaciones).
11. **Llevar a cabo una inspección de recorrido de seguridad**: Verificación de controles físicos y ambientales, de mantenimiento, de protección de medios y de planificación de contingencias del sistema (controles de extinción y detección de incendios, sistema de calefacción, ventilación y aire acondicionado, servicios públicos y acceso físico, capacidad de alimentación de reserva de la ubicación empleada dentro del sistema).
12. **Probar el sistema con las herramientas definidas en SAP**: para obtener pruebas de cumplimiento y configuraciones de control de seguridad:

* Herramientas de escaneo: escáneres de bases de datos, de vulnerabilidad, de sitios web, mapeadores de red.
* Herramientas automatizadas: comprobadores de la integridad de los archivos, detección de redes inalámbricas, pruebas de penetración para comprobar conjuntos de controles de seguridad.

1. **Análisis inicial de los resultados**: una vez finalizada la ejecución de la(s) herramienta(s) a través de sus operaciones, revisar los resultados para identificar deficiencias o debilidades de alto o medio impacto. Además, se revisan los resultados de la prueba para asegurar que se ha completado con éxito.
2. **Informe de corrección para la toma de medidas**: Cada herramienta utilizada proporciona un método para la identificación de los problemas descubiertos. Esos datos se proporcionan al personal de administración del sistema, a través de informe que permita corregir cualquier deficiencia o debilidad de impacto significativo tan pronto como sea posible.
3. **Recibir pruebas del artefacto de esfuerzo de reparación**: el personal “in situ” del sistema permite ejecutar nuevamente las herramientas automatizadas para verificar la reparación o la prueba de la reparación mediante el uso de "capturas de pantalla" o informes de salida de los dispositivos. Estos documentos y artefactos se adjuntan o se incluyen en el SAR.
4. **Construir el SAR**: comienza durante la fase de pruebas revisando los resultados de los exámenes y las entrevistas. Finalizada dicha fase y entregado el Informe de reparación, se incluyen los resultados de los escaneos y otras pruebas realizadas. Finalmente, se incluyen todas las áreas, junto con una tabla completa de resultados por control.
5. **Revisar el SAR con el cliente**: se revisan los resultados preliminares para señalar cualquier área o elemento que pueda arreglarse, repararse o remediarse antes de la entrega final. A menudo, el cliente aborda algunas o todas estas áreas y proporciona documentación de apoyo adicional o prueba de la corrección, que se incluye en el SAR final.
6. **Desarrollar el SAR final**: Una vez terminadas todas las revisiones y discusiones, se completa el SAR en su versión final y se prepara el briefing para el AO que acompañará al informe.
7. **Elaborar la carta de certificación**: completado el SAR y las revisiones del SSP como resultado de la evaluación, se genera una Carta de Certificación para el AO indicando los resultados de la evaluación y la opinión del evaluador sobre los riesgos del sistema.
8. **Entregar el informe de evaluación y la carta de certificación al propietario del sistema y al cliente**: último paso del proceso que implica entregar el SAR final, la versión final del SSP y la Carta de recomendación al AO y al propietario del sistema para que tomen medidas.

## 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:

1. **Establecer una política de evaluación de la seguridad de la información**: la política debe identificar los requisitos de la organización para la realización de evaluaciones responsabilizando a las personas adecuadas para garantizar que las evaluaciones se realizan de acuerdo con estos requisitos.
2. **Aplicar una metodología de evaluación**: metodología repetible y documentada que proporcione:

* Coherencia y estructura a las evaluaciones.
* Acelere la transición del nuevo personal de evaluación.
* Aborde las limitaciones de recursos asociadas a las evaluaciones.
* Permita a las organizaciones maximizar el valor de las evaluaciones al tiempo que minimiza los posibles riesgos introducidos por ciertas técnicas de evaluación.

1. **Analizar los hallazgos y desarrollar técnicas de mitigación de riesgos para abordar los puntos débiles**: las organizaciones deben realizar un análisis de las causas raíz al finalizar una evaluación para poder traducir los resultados en técnicas de mitigación procesables. Estos resultados pueden indicar que las organizaciones deben abordar no sólo las debilidades técnicas, sino también debilidades en procesos y procedimientos.

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

La imagen presenta el RMF paso 4, evaluar los controles de seguridad, el cual está compuesto de 4 tareas:
Tarea 1: preparación de la evaluación, donde se desarrolla, revisa y aprueba un plan para evaluar los controles de seguridad.
Tarea 2: evaluación de los controles de seguridad, donde se evalúan los controles de seguridad, de acuerdo con los procedimientos de evaluación, definidos en el plan de evaluación de la seguridad.
Tarea 3: informe de evaluación de la seguridad, donde se prepara el informe de evaluación de la seguridad, documentando los problemas, conclusiones y recomendaciones de la evaluación de los controles de seguridad.
Tarea 4: acciones correctivas, donde se llevan a cabo las acciones correctivas iniciales en los controles de seguridad, de acuerdo con las conclusiones y recomendaciones del informe de evaluación de la seguridad.

En el marco de gestión de riesgos, el paso 4, consiste en evaluar los controles de seguridad. Las cuatro tareas de este son: preparación de la evaluación, evaluación de los controles de seguridad, informe de la evaluación de la seguridad y acciones correctivas.

### 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:

1. **Prueba**: es el proceso de ejercitar uno o más objetos de evaluación bajo condiciones específicas para comparar los comportamientos reales y los esperados.
2. **Examen**: comprobación, inspección, revisión, observación, estudio o análisis de uno o más objetos de evaluación para facilitar la comprensión, lograr una aclaración u obtener pruebas. Implica principalmente la revisión de documentos para identificar el diseño, instalación, configuración, funcionamiento y el mantenimiento previsto de los sistemas y la red, y su revisión y referencias cruzadas garantizan la conformidad y la coherencia.
3. **Entrevista**: discusiones con individuos o grupos dentro de una organización para facilitar la comprensión, lograr la aclaración o identificar la ubicación de las pruebas.
4. **Observación**: ofrece la oportunidad de documentar las actividades, el comportamiento y los aspectos físicos sin tener que depender de la voluntad y la capacidad de las personas para responder a las preguntas de la entrevista o aislar el documento exacto que es relevante para un control o riesgo concreto.
5. **Revisión de la documentación**: determina si los aspectos técnicos de las políticas y procedimientos están actualizados y son completos. La documentación incluye arquitecturas y requisitos de seguridad, planes de seguridad del sistema, acuerdos de autorización, memorandos de entendimiento y los acuerdos para las interconexiones del sistema, y planes de respuesta a incidentes.

### “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.

## “Software”

Revise, en la siguiente infografía, cada detalle sobre los métodos de evaluación y lineamientos establecidos en relación al “software”:

<https://ecored-sena.github.io/CF5_233109_Tratamiento_Riesgos_Ciberseguridad_Micro_Pequena_Mediana_Empresa/downloads/anexometodos.pdf>

# 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).

1. Ventajas del sistema de gestión de información y eventos de seguridad (SIEM)



[Enlace de reproducción del video](https://youtu.be/6o9Pwrbzn4E)

|  |
| --- |
| **Síntesis del video: Ventajas del sistema de gestión de información y eventos de seguridad (SIEM)** |
| El sistema SIEM es utilizado para supervisar, identificar, documentar y, a veces, responder a diferentes ataques de seguridad. Como los ataques de denegación de servicio (DDoS) intencionados y maliciosos y los brotes de virus.  Pero también otros eventos de seguridad menos obvios, como violaciones de las políticas, intentos de acceso no autorizado y los de atacantes altamente cualificados. Que sin la ayuda de un sistema SIEM pasarían completamente desapercibidos dada su sutileza y tendencia a oscurecerse por miles de eventos por segundo.  Un objetivo importante para el analista de seguridad que utiliza un sistema SIEM es reducir el número de alertas falsas-positivas. Otros sistemas de seguridad suelen alertar sobre muchos eventos falsos positivos que llevan a ignorar las alertas de verdaderos positivos, más raras y significativas.  El sistema SIEM reduce las alertas falsas positivas mediante la creación de filtros y reglas de eventos correlacionados. Y alerta sólo sobre aquellos eventos de seguridad altamente calificados, descartando la mayor parte de los eventos falsos positivos.  El SIEM también se puede utilizar para identificar varios tipos de problemas operativos dentro de una red. O necesidades rutinarias del sistema relacionadas con capacidad adicional, problemas de formación de los usuarios y aplicaciones con errores que requieren parches, actualizaciones o sustituciones.  Además de los usos internos, el sistema SIEM ha demostrado su utilidad a divisiones de “marketing”, propietarios de empresas e incluso gobiernos. Para supervisar y recibir alertas, casi en tiempo real, de actividad externa importante que podría indicar cambios significativos en su competencia y mercado.  Utilizado para recopilar inteligencia de mercado, empresarial o política, el sistema SIEM puede obtener información sobre actividades que de otro modo no se verían. |

## 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:

1. **Configuración de nodos**: envío de eventos relevantes del sistema y de las aplicaciones a una base de datos centralizada, gestionada por la aplicación SIEM.

SIEM analiza los datos y proporciona servicios de almacenamiento, organización, recuperación y archivo de registros. Los nodos incluyen sistemas informáticos que ejecutan varios sistemas operativos (Linux, UNIX, Windows) y sistemas y dispositivos de infraestructura de red (“routers”, conmutadores gestionados, cortafuegos, servidores proxy, sistemas de detección de intrusiones (IDS), sistemas de acceso remoto).

1. **Creación de filtros o reglas y temporizadores**: para auditar y validar el cumplimiento o identificar las violaciones a los requisitos de cumplimiento impuestos a la organización.

Las reglas podrían incluir: supervisión de la frecuencia de los cambios de contraseña, identificación de los parches del sistema operativo (SO) o de las aplicaciones que no se instalan, la frecuencia de auditoría de las actualizaciones del antivirus, el “antispyware” y el IDS.

1. **Correlación de eventos**: enseña al sistema a considerar varias condiciones antes de activar la alarma. Por ejemplo, un servidor que funciona al 100 % de utilización de la CPU podría responder a varias causas:

* Una aplicación fallida que ha bloqueado el servidor.
* Sobrecarga del sistema con actividad legítima indicando servicios o aplicaciones que deben ser distribuidos en servidores adicionales (cluster).
* Un gusano que ejecuta un ataque de denegación de servicio (DoS). Actividad momentánea y natural del servidor.

1. **Respuesta activa**: el SIEM toma automáticamente medidas correctivas ante las amenazas percibidas o las configuraciones erróneas, por ejemplo, añadiendo filtros de IP y de puertos en la lista de control de acceso (ACL) de un “router” o un cortafuegos.

Aunque hay algunos beneficios obvios de las respuestas automatizadas, sólo en una instalación madura y en un SIEM finamente ajustado debería implementarse su utilización. De lo contrario, el sistema SIEM podría estar respondiendo a una colección de eventos falsos positivos, convirtiéndose en un arma de doble filo.

1. **Seguridad de los puntos finales**: el sistema SIEM puede supervisar si el cortafuegos de un PC o servidor está funcionando e identificar cuándo se actualizaron por última vez las definiciones de AV o cuándo un nodo se infecta con spyware. Incluso puede gestionar la seguridad de los puntos finales, realizando mejoras en la seguridad del nodo en el sistema remoto, como la configuración de cortafuegos y la actualización y supervisión de productos AV, “antispyware” y “antispam” en los nodos del sistema.

## 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.

## 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:

La imagen nos presenta los modelos de negocio, los cuales son la forma más fácil de entender la dirección y funcionamiento de la empresa. Allí se encuentran los productos o servicios, las estrategias, las actividades, los valores y los objetivos.
Luego nos presenta el modelo de negocio de TI, donde se debe:
Entender desde una perspectiva empresarial, qué es lo más importante para la organización.
Proporcionar soluciones de seguridad que se ajusten al modelo de negocio de su organización.
Clasificaciones básicas de modelos de negocios aplicables a la mayoría de entornos empresariales: gobierno, comercial y universidades.

# 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:

1. **Prevención**: con base en la experiencia y adopción de buenas prácticas de ciberseguridad, el SOC debe apropiar medidas de prevención a nivel técnico y de conciencia en la organización. Entre las soluciones preventivas se pueden considerar aplicación de controles de seguridad (firewalls, antimalware, etc.), el monitoreo continuo de la seguridad, el análisis y gestión de las vulnerabilidades técnicas.
2. **Detección**: consiste en el monitoreo constante de los eventos para detectar amenazas, vulnerabilidades, intrusiones y fallos de seguridad, para responder de manera rápida y eficaz. La principal herramienta que apoya esta etapa son las SIEM.
3. **Análisis**: en esta etapa se deben analizar los eventos detectados para determinar si corresponden a amenazas reales o si son falsas alertas. Los sistemas SIEM ayudan en el proceso de análisis con su base de datos de conocimientos y experiencias anómalas, registradas previamente, así como en la configuración de las reglas de cumplimiento.
4. **Respuesta**: consiste en las acciones que se toman para responder frente a un evento o incidentes de ciberseguridad; las mismas deben estar planificadas de manera que se apliquen las medidas o controles de forma eficaz.

## 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.

## 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:

1. **Gestión de riesgos**: identificar y tomar decisiones para hacer frente a los riesgos de la organización. Desde la seguridad física de los activos hasta la corrección de las vulnerabilidades digitales que existen en el “software”. También aplica a la corrección de políticas deficientes y falta de educación en seguridad de los miembros de una organización.
2. **Gestión de la vulnerabilidad**: identificar y gestionar el riesgo de las vulnerabilidades técnicas: detección de vulnerabilidades en el software que se encuentra en los servidores, los ordenadores portátiles y los dispositivos IoT. La mayoría de los SOC utilizan escáneres de vulnerabilidad e inteligencia de amenazas externa para identificar las vulnerabilidades.
3. **Gestión de incidentes**: respuesta a eventos relacionados con seguridad: acciones como el aislamiento de los sistemas, la alerta a los miembros del equipo y la aplicación de medidas correctivas para resolver el problema. Tecnologías como las herramientas de orquestación, la inteligencia artificial y los “playbooks” se están haciendo muy populares para ayudar a los SOC en los servicios de respuesta a incidentes.
4. **Análisis**: análisis de varios tipos de artefactos, identificación de características, ingeniería inversa, análisis de vulnerabilidad/explotación, análisis causa raíz, reparación y análisis de mitigación. El análisis utiliza herramientas como IDA Pro para desmontar el “malware” y comprender su funcionamiento.
5. **Cumplimiento**: evaluar y mantener los requisitos de cumplimiento de la organización: tanto los requisitos obligatorios por ley (HIPAA y PCI DSS), como los objetivos impulsados por la organización (norma NIST o ISO), que no son exigidos por la ley, pero que podrían ser considerados como una política requerida por la organización o sus clientes.
6. **Análisis forense digital**: recopilación de pruebas tras el incidente para determinar la causa y preparar acciones legales. La ciencia forense digital se distingue de la respuesta a incidentes y el análisis, en el aspecto legal relativo a la forma en que se recogen las pruebas (si se manipula un archivo durante la investigación, se arruina cualquier posibilidad de utilizar esa prueba en un tribunal).
7. **Conciencia de la situación y de la seguridad**: proporcionar a la organización conciencia de su entorno operativo y de las posibles amenazas. Incluye educación sobre elementos críticos que podrían afectar los objetivos de la organización, amenazas potenciales y acciones contra el riesgo operativo y las amenazas.
8. **Investigación y desarrollo**: investigar el panorama de las amenazas en constante evolución, desarrollar nuevas herramientas y técnicas, y modificar las herramientas existentes para mejorar su eficacia.

# 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.

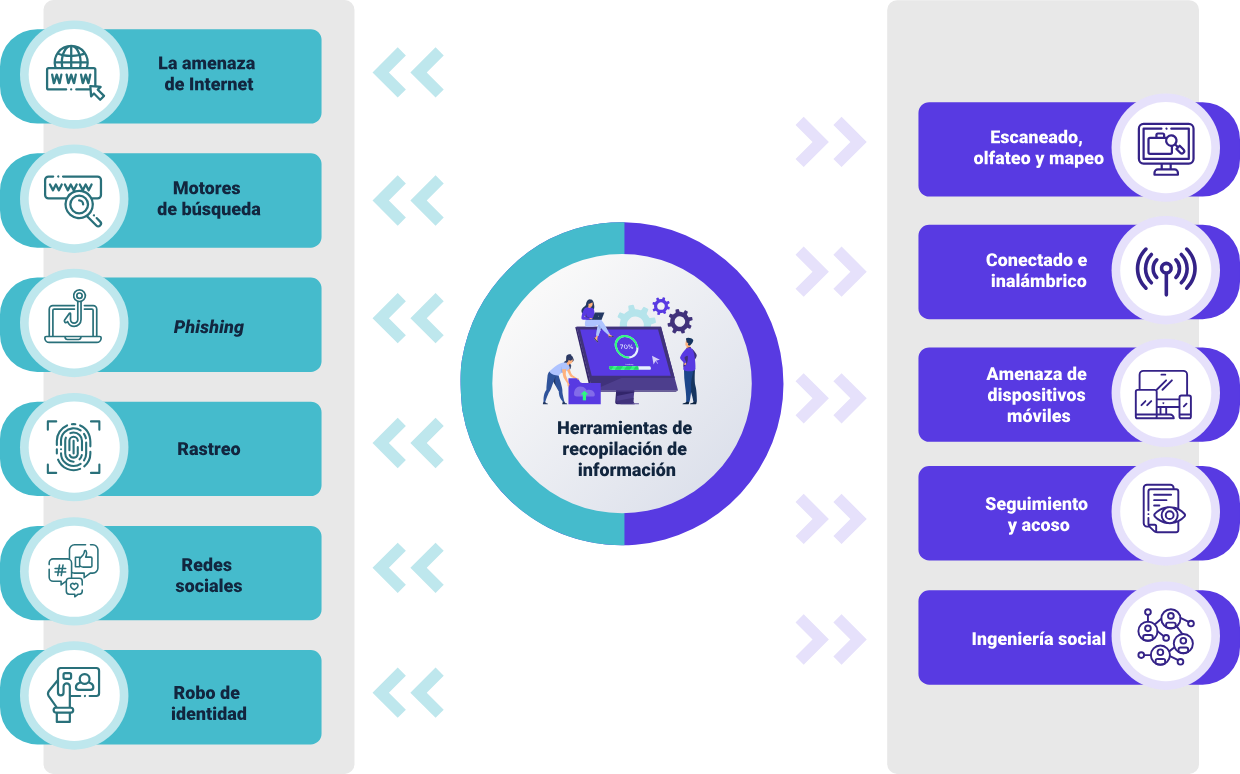
Esto tiene gran importancia en primer lugar, porque para poder atacar, hay que encontrar vectores en los que se pueda vulnerar el objetivo. Hoy día, con la tecnología digital es evidente el creciente vector de ataque. Una conversación telefónica, por ejemplo, puede ser almacenada digitalmente dentro 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.

## 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:



* **La amenaza de Internet**. Una o varias herramientas que permitan tomar datos desde sitio de internet como páginas web, formularios o servicios de aplicaciones.
* **Motores de búsqueda**. Herramienta para hacer consultas de información usando frases o palabras clave. Identificar aquellos motores que permitan consultas sin traer enlaces o programas maliciosos.
* **“Phishing”**. Práctica delictiva utilizada para tomar información bancaria y hacer fraudes a gran escala.
* **Rastreo**. Uso de aplicaciones de software que permite hacer el seguimiento de la huella digital de usuarios con propósitos poco éticos.
* **Redes sociales**. En estas aplicaciones web, los datos son el mayor tesoro, ya que se ofrecen de forma libre, pero pueden quedar expuestos para diferentes acciones.
* **Robo de identidad**. Actividad en donde se toma la información de un usuario y se usa de forma inapropiada en Internet y servicios de banca.
* **Escaneado, olfateo y mapeo**. Uso de herramientas y aplicaciones de “software”, para la intersección de paquetes que pasan por las redes de datos. La idea es capturar la información con fines de prevención o corrección.
* **Conectado e inalámbrico.** Se revisan todos los conceptos, facilidades y vulnerabilidades presentes en redes de datos, en función del medio de transmisión.
* **Amenaza de dispositivos móviles**. Los dispositivos móviles se han convertido en un punto de entrada a las redes de datos que pueden explotar las vulnerabilidades de la red o el sistema de información.
* **Seguimiento y acoso**. Técnicas para obtener información a través de acciones físicas de seguimiento e intimidación.
* **Ingeniería social**. Técnicas para obtener información sin que la persona se dé cuenta de que se está vulnerando sus opciones de seguridad.

## Características

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

1. **La amenaza de internet**: la red pública de Internet es una “mina de oro” para quienes realizar labores de inteligencia. Utilizada de forma no maliciosa resulta extremadamente útil, pero puede servir para reunir información y dirigir ataques. Otro punto es que una vez se sube algo en un servidor (entrada de blog, archivo de datos) podría permanecer allí durante mucho tiempo, posiblemente para siempre.
2. **Motores de búsqueda**: proporcionan gran cantidad de información a quienes saben cómo utilizarla. Las búsquedas de palabras clave y el refinamiento de los temas, así como el uso de herramientas y sitios web específicos, pueden dar a un atacante todo lo que necesita para comenzar la vigilancia de un objetivo.
3. **“**Phishing**”**: en el “phishing”, un atacante puede hacerse pasar por una fuente legítima en Internet para engañar, haciendo creer al usuario que está en la entidad que intenta visitar. Al buscar en Internet, puede encontrar (o ir directamente a) un sitio web en el que desea realizar una operación. Por ejemplo, una cuenta bancaria en línea para realizar una transacción.
4. **Rastreo**: otra forma de recopilar de información es a través de sitios web que rastrean quién es el usuario y de dónde viene. Esto puede utilizarse con fines de marketing, pero en manos de quienes desean hacer daño, puede utilizarse para rastrear intereses, ubicación, dispositivos digitales (como el PC) y datos de identidad.
5. **Redes sociales**: están apareciendo en masa ofreciendo una manera de hacer negocios, compartir datos, conocer personas, encontrar nuevas oportunidades. Pero, conlleva una gran responsabilidad en cuanto a la información que se comparte. No debería sorprender que cuando una residencia es robada durante, por ejemplo, un período de vacaciones, la primera pregunta que se haga sea: ¿sabía alguien que estaba fuera?
6. **Escaneado, olfateo y mapeo**: las redes cableadas se perciben más seguras que las inalámbricas, haciendo más difícil recopilar información por la dificultad de penetrar un cable para extraer información, pudiendo estropearlo y acabar con las señales que transportan la información. También producen por lo general una mayor velocidad de transmisión. Su principal debilidad: el tendido del cableado, costoso y más difícil de mantener.
7. **Conectado e inalámbrico**: examinan los niveles inferiores de las comunicaciones digitales, principalmente en la red a través de herramientas para capturar datos y realizar análisis a nivel de paquetes o escrutinio de puertos para reunir y verificar información sobre un objetivo.
8. **Amenaza de dispositivos móviles**: la mayor tendencia actual es el uso del dispositivo móvil, capaz de conectarse a las redes, incluida Internet, de forma inalámbrica. Pero fácilmente manipulable por un usuario malintencionado debido a, por ejemplo, la posibilidad de instalar aplicaciones de “software” (o apps, para abreviar) proveniente de muchas fuentes, que podría incluir “software” malicioso.
9. **Amenaza de datos (metadatos)**: no hay mayor amenaza que ser rastreado en línea. Por ejemplo, al hacer fotos a través de teléfono inteligente, la información se almacena en metadatos, que permiten archivar imágenes y saber cuándo y dónde fueron tomadas. Pero también, puede ser una fuente para que acosadores localicen ubicaciones exactas.

## Aplicación

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

* **Seguimiento y acoso**: una de las formas más antiguas de investigación, recopilación de información o técnica de acoso es seguir físicamente a alguien sin su conocimiento. Acechar a un objetivo se considera seguirlo, a veces para obtener información y a veces para hacerle daño.

No hay forma de explicar cómo se puede hacer esto sin decir que la clave es pasar desapercibido (es decir, ser sigiloso), permanecer fuera de la vista, pero no tanto como para perder.

* **Ingeniería social**: implica engañar a alguien a través de una conversación para obtener información particular. Por ejemplo, llamar desde un número de teléfono falsificado que parece confiable, contar cosas de interés, y a través de preguntas específicas lograr acceso a un sitio web o una cuenta bancaria.

Existen herramientas de “software” como Backtrack que pueden cargar programas de ingeniería social para la realización de dichos ataques.

* **Búsqueda en el contenedor de basura**: enseña al sistema a considerar varias condiciones antes de activar la alarma.

Consiste en rebuscar en la basura para recoger datos que se hayan desechado y que puedan contener información personal para utilizar maliciosamente.

Síntesis

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

Síntesis del componente formativo. Comienza con la evaluación de la ciberseguridad, la cual considera métricas y controles de seguridad, articulados en un modelo de seguridad, a través de testing y monitoreo, en integración con SIEM y SOC.
Este testing y monitoreo, permite evaluar la eficiencia del modelo de seguridad y la generación de alertas para enfrentar ataques al sistema, resultado de las técnicas y tácticas de recopilación de información, como son: rastreo, phishing, mapeo, ingeniería social, intervenciones y seguimiento.

Material complementario

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia | Tipo de material | Enlace del recurso |
| 2. “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. | Artículo | <https://www.researchgate.net/publication/224257991_Cyber-Physical_Security_of_a_Smart_Grid_Infrastructure> |
| 5. Técnicas de recopilación de información (“information gathering*”*) | Owasp Foundation. (2021). Vulnerability scanning tools. Owasp. | Página Web | <https://owasp.org/www-community/Vulnerability_Scanning_Tools> |
|  |  |  |  |

Glosario

**AAA**: autenticación, autorización y contabilidad.

**ACL**: listas de control de acceso.

**AWS**: nube de Amazon.

**AZURE**: nube de Microsoft.

**DHCP**: protocolo de configuración dinámica de host.

**DNS**: protocolo de sistema de nombres de dominio.

***“*Docker file*”***: archivo para configurar contenedores de Docker.

**DOS**: ataque de negación de servicio.

**IDS**: sistemas de detección de intrusos.

**PLC**: controlador lógico programable.

**SCD**: sistema de control distribuido.

**SCI**: sistema de control interno.

**Sistemas ERP**: estaciones de trabajo de usuarios finales.

**UI**: interfaz de usuario.

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>

Créditos

| Nombre | Cargo | Regional y Centro de Formación |
| --- | --- | --- |
| 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 |
| Hernando José Peña Hidalgo | Experto Temático | Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander |
| Diego E. Acevedo Guevara | Diseñador Instruccional | Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Centro de Diseño y Metrología - Regional Distrito Capital |
| Darío González | Corrector de Estilo | Centro de Diseño y Metrología - Regional Distrito Capital |
| Francisco José Lizcano Reyes | Desarrollador Fullstack | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Juan Daniel Polanco Muñoz | Diseñador de Contenidos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Carlos Eduardo Garavito Parada | Animador y Productor Multimedia | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| María Carolina Tamayo López | Locución | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Emilsen Alfonso Bautista | Actividad Didáctica | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Zuleidy María Ruíz Torres | Validador de Recursos Educativos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Luis Gabriel Urueta Álvarez | Validador de Recursos Educativos Digitales | Centro Industrial del Diseño y la Manufactura - Regional Santander |
| Daniel Ricardo Mutis | Evaluador para Contenidos Inclusivos y Accesibles | Centro Industrial del Diseño y la Manufactura - Regional Santander |