Seguimiento de la seguridad digital

Breve descripción:

Con el desarrollo de este componente, el aprendiz estará altamente capacitado en establecer indicadores, métricas y alcance de seguimiento de la seguridad digital, según estándares y metodologías nacionales e internacionales; de igual manera, en realizar el monitoreo de la seguridad digital de acuerdo con los indicadores y métricas establecidos.

Noviembre 2023

Tabla de contenido

Introducción

Para comenzar el estudio de este componente y enterarse de los contenidos, amplitud y ruta de aprendizaje del mismo, le invitamos a revisar el siguiente video:

Video 1. Seguimiento de la seguridad digital

Enlace de reproducción del video

Comentado [AF1]: Falta el video

Síntesis del video: Seguimiento de la seguridad digital
Le damos la bienvenida al estudio de este componente formativo. Mediante esta experiencia de aprendizaje estará en capacidad de establecer indicadores, métricas y alcances de seguimiento de la seguridad digital, según estándares y metodologías nacionales e internacionales.

Con el estudio responsable del mismo, fortalecerá sus habilidades para afianzará en medir la efectividad, la eficacia y la eficiencia de la seguridad de la información en una organización.

Tenga presente la importancia de la elaboración de artefactos de registro de monitoreo, de acuerdo con los controles de seguridad digital implementados. Ellos previenen y evitan la pérdida de datos estratégicos o información importante, ya que también ayudan a prevenir la disminución de desempeño, tanto de "hardware" como de "software", identificando fallas graves que necesitan corregirse.

Le invitamos a explorar todos los recursos que el componente tiene dispuesto para usted, procure llevar un registro de los elementos teóricos, conceptuales y prácticos que va asimilando en el recorrido del componente.

1. Métodos de métricas e indicadores de monitoreo

La adopción de métodos para la creación de métricas e indicadores de monitoreo está dirigido a la medición de la eficiencia, la efectividad y la eficacia de los componentes de gestión y de implementación, definidos en el plan estratégico de la seguridad y privacidad de la información. Estas métricas e indicadores ayudarán en la formulación de estrategias de mejora continua, permitiendo una mejor toma de decisiones.

Esta adopción de métricas e indicadores tiene como principales objetivos, los siguientes:

- ✓ Evaluar la efectividad de la implementación de los controles de seguridad.
- ✓ Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
- ✓ 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.
- ✓ Comunicar valores de seguridad al interior de la entidad.
- ✓ Servir como insumos al plan de análisis y tratamiento de riesgos.

Para fundamentar los conceptos abordados, se le recomienda indagar los lineamientos de la **ISO/IEC 27001 – ISO 27004** y la **Guía 9 de Indicadores de gestión para la seguridad de la información del MINTIC**, que encontrará en el material complementario.

1.1. Características de las métricas e indicadores

El escenario de la seguridad digital muestra cómo las amenazas cibernéticas evolucionan de manera permanente; el monitoreo de la seguridad de la información en las organizaciones ha de ser una rutina integral. Las métricas e indicadores orientadas a tal monitoreo, tienen una serie de características que vale la pena identificar, para una mejor aplicación y establecimiento de los mismos.

Esas características representativas son:

A. Evaluadores

Las métricas e indicadores son mecanismos o instrumentos utilizados para evaluar si se cumple o no con los objetivos estratégicos.

B. **Medidores**

Las métricas e indicadores son una unidad de medida gerencial que evalúa resultados de una organización, frente a sus responsabilidades y objetivos.

C. **Generadores de información**

Las métricas e indicadores son un generador de información que analiza el desempeño de cualquier proceso y verifica el cumplimiento, en términos de resultados.

D. **Generadores de alertas**

Las métricas e indicadores son un generador de alertas que determinan desviaciones en el cumplimiento de los objetivos.

1.2. Tipos de indicadores

Con los lineamientos de las normas ISO/IEC 27001, ISO/IEC 27004 y de la Guía 9 de indicadores de gestión para la seguridad de la información del MINTIC, se adopta una serie de indicadores para medir la gestión y el cumplimiento en el avance del modelo de seguridad digital.

Indicadores de gestión e indicadores de cumplimiento

Tanto las normas ISO/IEC 27001 e ISO/IEC 27004, así como la Guía 9 de indicadores de gestión para la seguridad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones, destacan la importancia de estos, para medir la gestión y el cumplimiento en el modelo de seguridad digital de las organizaciones. A continuación, algunas definiciones y orientaciones otorgadas por el MINTIC:

Se destacan, los tipos de indicadores que se enuncian y definen a continuación:

Indicadores de gestión

Están relacionados con las razones que permiten administrar un proceso o un sistema. Profundice a continuación sobre los indicadores de gestión:

1. **Organización de seguridad de la información**

   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 con la seguridad de la información, al interior de la organización.

   Objetivo: hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección.

2. **Cubrimiento del SGSI en activos de información**

   Permite determinar y hacer seguimiento al cubrimiento que se realiza al nivel de activos críticos de información de una organización y los controles aplicados.

   Objetivo: hacer un seguimiento a la inclusión de nuevos activos críticos de información y su control, dentro del marco de seguridad y privacidad de la información.

3. **Tratamientos de eventos relacionados en marco de seguridad y privacidad de la información:**

   Permite determinar la eficiencia en el tratamiento de eventos relacionados en la seguridad de la información. Los eventos serán reportados por los usuarios o determinados en las auditorías planeadas para el sistema.

Objetivo: reflejar la gestión y evolución del modelo de seguridad y privacidad de la información, al interior de la organización.

4. **Plan de sensibilización**

   Permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.

   Objetivo: establecer la efectividad de un plan de capacitación y sensibilización, previamente definido como medio para el control de incidentes de seguridad.

Indicadores de cumplimiento

Están relacionados con las razones que indican el grado de consecución de tareas. Revise a continuación más información sobre este tipo de indicadores:

1. **Cumplimiento de políticas de seguridad de la información en la organización**

   Objetivo: identificar el nivel de estructuración de los procesos de la organización orientados a la seguridad de la información.

2. **Identificación de lineamientos de seguridad de la organización**

   Es el grado de la seguridad de la información y los equipos de cómputo.

   Objetivo: medir el nivel de preparación del recurso humano y su apropiación, en cuanto a la seguridad de la información y los equipos de cómputo.

3. **Verificación del control de acceso**

   Es el grado de control de acceso.

   Objetivo: identificar la existencia de lineamientos, normas o estándares, en cuanto al control de acceso en la organización.

4. **Aseguramiento en la adquisición y mantenimiento de "software"**

   Es el grado de protección de los servicios de la organización.

   Objetivo: identificar la existencia de lineamientos, normas o estándares en cuanto a la adquisición o desarrollo de aplicaciones.

5. **Implementación de los procesos de registro y auditoría**

   Es el grado de existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.

   Objetivo: identificar la existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.

6. **Implementación de los procesos de registro y auditoría**

   Es el grado de implementación de los mecanismos encaminados a la detección de anomalías e irregularidades.

   Objetivo: medir el nivel de mecanismos encaminados a la detección de anomalías e irregularidades.

7. **Políticas de privacidad y confidencialidad**

   Grado de implementación de políticas privacidad y confidencialidad.

   Objetivo: identificar el nivel de implementación de políticas de privacidad y confidencialidad de la organización.

8. **Verificación de las políticas de integridad de la información**

   Es el grado de implementación de mecanismos para la integridad de la información.

   Objetivo: identificar el nivel de implementación de políticas, privacidad y confidencialidad de la organización.

9. **Políticas de disponibilidad del servicio y la información**

   Es el grado de cumplimiento de las políticas de disponibilidad del servicio y la información.

   Objetivo: identificar el nivel de implementación de políticas de disponibilidad del servicio y la información.

10. **Ataques informáticos a la organización**

    Porcentaje de ataques informáticos recibidos en la organización que impidieron la prestación de alguno de sus servicios.

    Objetivo: conocer el número de ataques informáticos recibidos.

2. "Testing" y monitoreo de la seguridad digital

La finalidad de las pruebas de efectividad, frente a la metodología, es comprobar o medir la eficiencia de la ejecución del modelo de seguridad en las entidades; la cual facilita a las entidades la comprensión del desarrollo de las pruebas, los objetivos y el beneficio que se gana al identificar sus etapas y gestionarlas.

Algunas generalidades del "testing" que se deben tener en cuenta, dado su nivel de importancia e implicación, estas son:

1. **Valoración múltiple y por etapas:** se desarrolla la metodología en etapas diferentes, que permiten definir qué tanto ha avanzado la organización con la implementación del modelo. Por medio de la valoración de diferentes aspectos, se podrán identificar vulnerabilidades y amenazas a las cuales está expuesta la entidad.
2. **Identificación de eventos:** se podrán identificar, al igual que las amenazas, las posibles debilidades en los controles implementados.
3. **Intención y necesidad:** los procedimientos de "testing" y monitoreo del modelo de seguridad y privacidad de la información, tienen como objetivo fundamental, proteger la integridad, disponibilidad y confidencialidad de la información de la organización.
4. **Implicaciones de la alta dirección:** los intereses de la alta dirección, son un factor externo de gran impacto, que se alinean con las pruebas de seguridad y privacidad y sus resultados, que en este caso se relacionan con los directivos de las entidades del estado, esto se demuestra en la capacidad que tengan las organizaciones para llevar a buen término la implementación del modelo de seguridad.
5. **Cumplimiento, aseguramiento e imagen:** cumplir con la normatividad vigente y llevar a la organización al siguiente nivel de seguridad, permite que sus procesos y atención al ciudadano brinden una buena imagen en la sociedad.

Guía No 1 (Guía metodológica de pruebas de efectividad) del MINTIC

Afiance sus conocimientos en lo relacionado con "testing" y monitoreo, visitando y leyendo, responsablemente, la guía.

Enlace del documento

2.1. Tipos de pruebas de efectividad

No existe una sola forma de hacer pruebas de efectividad ni tampoco un solo tipo de pruebas; esto significa que no habría marcos de referencia de los niveles de seguridad que se estarían evaluando. Entre otras cosas, un solo tipo de pruebas sería insuficiente para cubrir los diferentes tipos de comprobaciones existentes al interior de la organización. Una sola prueba o tipo de prueba, no tendría arqueo suficiente para evaluar todas las necesidades y eventos de la seguridad y privacidad de la información, que tuviera la entidad. (MINTIC, s.f.).

Se pueden determinar tres tipos de pruebas de efectividad, teniendo en cuenta el nivel de conocimiento del entorno de la organización, esto es:

1. **Pruebas con conocimiento nulo del entorno:** es una prueba que hace creer un atacante real, debido a que tiene muy poco, o nulo, conocimiento del objetivo.
2. **Pruebas con conocimiento medio del entorno:** aplica en el caso donde se tiene más información sobre el ambiente que será atacado, para la prueba de "pentesting"; por ejemplo, direcciones IP, sistemas operativos, arquitectura de red, etc., sin embargo, es información limitada. Esto, imita a alguna persona dentro de la red, con conocimiento básico de la misma.

3. **Pruebas con conocimiento completo del entorno:** se presenta cuando la información relacionada al sistema objetivo del ataque ya está clara para el "hacker". Principalmente se aplica para temas de auditoría.

2.2. Alcance de las pruebas de efectividad

La metodología de pruebas, desde el inicio de la ejecución, se enfoca en implementar una línea base del estado de seguridad de la organización, con el fin de facilitar la identificación de la brecha en la implementación del modelo de seguridad, teniendo como concepto de línea base, la primera medición.

Estos son algunos alcances de las pruebas de medición en las organizaciones, en relación con el plan de seguridad y privacidad de la información, otorgadas por el ministerio de tecnologías de la información y comunicaciones:

A. **¿Qué ofrecen las pruebas?**

   Las mediciones otorgan a la entidad, una percepción de seguridad que se presenta en la ejecución del modelo de seguridad.

B. **Seguridad de la información: ecosistema**

   La seguridad de la información ha de ser concebida como ecosistema, la cual presenta varios principios básicos que deberían ser valiosos en el momento de realizar pruebas para comprobar los avances en la implementación del modelo de seguridad y privacidad.

C. **¿Soluciones definitivas en seguridad?**

En términos figurativos, no existe una bala de plata para los inconvenientes de seguridad que pueda tener una organización. Un modelo de protección y seguridad, por más adecuado, nunca será 100 % determinante.

D. La seguridad: proceso, no producto

Una evaluación de seguridad es útil como primera fase, pero no es efectiva en evaluaciones más profundas, requeridas por una organización para mejorar sus niveles de seguridad en todas las áreas. La seguridad digital es un proceso, no un producto. MINTIC (s.f.).

2.3. Procedimiento de las pruebas

De la aplicación procedente, responsable y oportuna de las pruebas, depende en gran medida su efectividad y su potencial aprovechamiento. Las pruebas de efectividad han de realizarse por fases, siendo cada una de estas, una acción vinculada consecuentemente con las anteriores o con las posteriores.

Nota. Guía metodológica de pruebas de efectividad

Repase las fases secuenciales de aplicación de las pruebas de efectividad, en procesos de seguridad de la información, como lo propone MINTIC, explorando la información que se expone a continuación:

Fase de contextualización

La fase de contextualización se soporta en la identificación de alcances reales de las pruebas y de los procedimientos a ejecutar, con base en las necesidades identificadas.

Tal identificación puede darse por medio de preguntas como:

a. ¿Cuáles serán los objetivos a evaluar?
b. ¿Qué quiere alcanzar la entidad específicamente con estas pruebas?
c. ¿Si desea realizarlo en horas hábiles, no hábiles o fines de semana?
d. ¿Qué direcciones IP internas o externas serán objetivo de las pruebas? (Si aplica).
e. En caso de poderse vulnerar el sistema, ¿qué tipo de acciones posteriores solicita realizar? (Pueden ser pruebas de vulnerabilidades en la máquina comprometida, escalamiento de privilegios, etc.).
f. ¿Qué fechas de inicio y finalización de las actividades?
g. ¿Se incluirán temas de ingeniería social?
h. ¿Qué temas de ingeniería social pueden ser válidos para ejecutar estos procedimientos?

Estos son algunos aspectos de suma importancia, desde el ministerio de las TIC, y que se deben tener en cuenta en la fase de contextualización, esto es:

Ha de tenerse en cuenta que estas pruebas no identifican, solamente, una vulnerabilidad sobre un sistema específico o algún sistema desactualizado; su meta principal es identificar riesgos de seguridad de información.

La identificación de riesgos de seguridad que logran estas pruebas, la hacen a través de controles que serán evaluados. Así, tomar las medidas proactivas/preventivas para mitigar riesgos encontrados.

Otros aspectos importantes para la contextualización del procedimiento son:

- ✓ Establecer líneas de comunicación con administradores de cada sistema a evaluar.
- ✓ Reportes parciales de avance de las pruebas, con una frecuencia definida.
- ✓ Manejo de evidencias o soportes de las actividades.

Estas pruebas también miden la efectividad de un sistema de monitoreo o detección, es decir que, si se están realizando actividades de escaneo, ataques, infiltración, alteración de la información, exista una respuesta eficaz.

Fase de reconocimiento del objetivo

Entre más información pueda obtenerse, más puntos de explotación podrían encontrarse y aprovecharse en las siguientes fases. Para realizar este levantamiento de información pueden utilizarse los tres métodos denominados: pasivo, semi-pasivo y activo (enfocado a los sistemas de información).

Conozca, según la orientación del ministerio de tecnologías de la información y las comunicaciones, las especificaciones y aspectos particulares de los tres métodos para el levantamiento de información en la fase de reconocimiento del objetivo:

A. **Método pasivo:** aplica, si la recolección de la información no implica acceder a ningún sistema de la entidad o generar tráfico que pueda ser detectado por alguno de sus sistemas. Generalmente, es información que está disponible en otros sitios y puede estar desactualizada, sin embargo, puede llegar a ser útil.

B. **Método semi-pasivo:** en esta instancia, se apunta hacia los sistemas de la entidad, simulando ser tráfico normal proveniente de internet, sin emplear ningún método que pueda considerarse sospechoso por parte de los sistemas, es "camuflar el tráfico". Como por ejemplo consultas DNS simples para verificar los servidores públicos.

C. **Método activo:** este método de obtención de información es el más propenso a ser detectado por los sistemas de detección y monitoreo, comprenden actividades como: escaneo de puertos, análisis de vulnerabilidad a puertos abiertos y búsqueda de directorios, archivos o servidores adicionales que no estén públicamente disponibles. MINTIC (s.f.).

Fase de modelado de amenazas

"Esta fase maneja la relación "**Atacante Versus activo**"; es decir, el beneficio que el atacante puede obtener si logra su objetivo de penetrar el sistema y modificar, borrar, copiar o destruir algún activo de información". (MINTIC, s.f.).

A continuación, podrá identificar de manera más detallada esta relación, esto es:

1. **Enfocado en la entidad: qué pasa si…**

   Gestión del riesgo para determinar el apetito de riesgo de la entidad y para identificar los activos más críticos (o los que mayor impacto negativo pueden causar en caso de verse afectados). Este análisis busca resolver la incógnita “Que pasa si”, por ejemplo, que pasa si se divulga la información de mis sistemas de información, ¿si se vulnera la confidencialidad?, ¿Qué impacto tendría dicha divulgación?

2. **Enfocado en la entidad: considerar los activos…**

   - ✓ Datos de empleados y datos de clientes.
   - ✓ Sistemas de información e información financiera.
   - ✓ Información de mercadeo.
   - ✓ Políticas, planes y procedimientos.
   - ✓ Información técnica (diseños de infraestructura, información de configuración del sistema, cuentas de usuarios, cuentas de usuarios privilegiados).
   - ✓ Personas.
   - ✓ Información generada a través de los diferentes procesos de negocio.
   - ✓ Información de producto (investigación y desarrollo, patentes, entre otros).

3. **Enfocado en la entidad: normas y estándares**

   Para realizar una gestión de riesgos adecuada, se debe acudir a la “**Guía de gestión de riesgos de seguridad de la información**” del modelo de seguridad y privacidad de la información. Si la entidad cuenta con este análisis, es importante revisarlo, ya que puede permitir identificar y perfilar ataques posibles y si los controles implementados sí son suficientes.

4. **Enfocado en el atacante: agentes**

   Identificando los posibles agentes o grupos que podrían llegar a perpetrar algún tipo de ataque hacia la entidad. Dicha identificación está centrada en los siguientes grupos: Agentes de ataque internos y Agentes de ataque externo. Dentro de las poblaciones que más ataques pueden llegar a generar se encuentran los empleados inconformes y los empleados a nivel ejecutivo, que pueden llegar a aprovechar sus usuarios con privilegios adicionales para vulnerar el sistema para sus propios fines.

5. **Enfocado en el atacante: agentes internos**

   Los atacantes o agentes de ataque, internos, pueden llegar a ser:

   - ✓ Administradores, ejecutivos.
   - ✓ Administradores de infraestructura.
   - ✓ Desarrolladores.
   - ✓ Ingenieros.
   - ✓ Técnicos.
   - ✓ Contratistas.
   - ✓ Soporte remoto.

6. **Enfocado en el atacante: agentes externos**

   Los atacantes o agentes de ataque, externos, pueden llegar a ser:

   - ✓ Sociedades.
   - ✓ Competidores.
   - ✓ Contratistas.
   - ✓ Proveedores.
   - ✓ Crimen organizado.
   - ✓ “Hacktivistas”.

- ✓ Hackers tipo “Script Kiddies”.

MINTIC (s.f.).

Fase de análisis de vulnerabilidades

Dependiendo de la amplitud de los alcances propuestos, el análisis de vulnerabilidad puede variar desde analizar un servicio o host específico o a un inventario completo de máquinas.

Estos procesos de análisis pueden ejecutarse también de las siguientes maneras o métodos:

1. **Análisis activo**

   El análisis activo involucra tener un contacto directo con el objetivo a probar. Puede hacerse de manera automática o de manera manual bajo diversas actividades conjuntas.

2. **Método automatizado**

   Utiliza un “software” que interactúa con el objetivo; realiza varios procedimientos de análisis simultáneamente, dando ventajas significativas de tiempo y esfuerzos, respecto a los métodos manuales. Una ventaja es, por ejemplo, ejecutar un telnet hacia un puerto para verificar si este responde o está abierto, repetir este proceso para los más de 60 mil puertos es una labor tediosa y un “software” puede ejecutarla.

3. **Ejecutan el método automático**

   - ✓ Escáneres de puertos.
   - ✓ Escáneres basados en servicios.
   - ✓ Lectura de “banners”.

- ✓ Escáneres específicos para servicios web.
- ✓ "Software" para ataques o escaneo de fuerza bruta.
- ✓ Escáneres de red.
- ✓ Escáneres para tráfico de voz.
- ✓ Múltiples nodos de ataque.

4. **Investigación**

   Una vez se realiza la verificación de las vulnerabilidades con base en los métodos anteriores, es necesario investigar en las diferentes bases de datos para comprobar la veracidad de lo que se ha encontrado y las posibles maneras de apalancar o aprovechar las fallas identificadas.

5. **Fuentes de información del método investigación**

   - ✓ Bases de datos de vulnerabilidades (CVE).
   - ✓ Alertas o publicaciones de proveedores de plataformas.
   - ✓ Bases de datos de "exploits".
   - ✓ "Passwords" por defecto de plataformas específicas.
   - ✓ Guías de "hardening" (endurecimiento) para plataformas.
   - ✓ Investigación propia (empleando virtualización o duplicación de máquinas, por ejemplo).

6. **Consolidado de investigación**

   Una vez se realiza la investigación, se deben confirmar las vulnerabilidades encontradas en un archivo consolidado, con su respectiva justificación y los tipos de ataque que podrían ejecutarse con base a los mismos. MINTIC (s.f.).

La fase de análisis de vulnerabilidades implica, además, métodos como análisis de metadatos en archivos publicados en internet, que pueden contener información sobre el tipo de servidor, nombres de dominio, direccionamiento IP, etc. También incluye el monitoreo de tráfico o copiado de tráfico (espejo de puertos) para captura y posterior análisis. (MINTIC, s.f.).

Fase de explotación

Esta fase se centra puramente en obtener acceso al sistema, apalancando las debilidades identificadas en la etapa anterior o sobrepasando los controles de seguridad existentes.

Dentro de las técnicas de explotación más utilizadas se encuentran las siguientes:

1. **Evasión**

   Implica realizar las pruebas de penetración escapando de los sistemas de detección, pueden implicar desde seguridad física (evadir una cámara) hasta evadir un sistema tipo IDS/IPS.

2. **Ataques de precisión**

   Uso de ataques bien focalizados, es decir, no empezar a atacar objetivos de manera indiscriminada, sino bien estructurada y puntual.

3. **Ataques personalizados**

   Con base a tecnologías/medios de transmisión: Dependiendo del medio de transmisión (cableado, vía Wifi).

4. **“Exploits” adaptados o complementados**

   Tomar “exploits” ya existentes y adaptarlos para las plataformas o sistemas objetivos.

5. **“Exploits” communes**

   “Buffer overflow”, SEH (Structured Exception Handler), ROP (Return Oriented Programming).

6. **Crackeo de SSID (WIFI)**

   Movimientos enfocados a apalancar vulnerabilidades sobre este medio y sus protocolos de encriptación como (WEB, WPA, EAP-FAST, entre otros).

7. **Ataques al usuario (Ingeniería social)**

   Con base en los temas encontrados en la fase de modelado de amenazas, emplear los ataques de ingeniería social al personal de la organización para obtener “passwords”, documentación adicional, etc.

8. **Hombre en el medio (Man In-The-Middle)**

   Ataques de interceptación de tráfico, donde se suplanta el direccionamiento bien sea físico o IP.

9. **VLAN Hopping**

   Este método de ataque consiste en engañar a dispositivos conmutadores (switches) con el fin de ganar acceso a la red como un dispositivo confiable, los métodos más comunes son VLAN HOPPING y Switch Spoofing.

Existen aún más métodos de ataque, con los cuales se puede intentar lograr el objetivo de vulnerar o acceder a los sistemas. Una vez se logre el objetivo de ingreso, deberán documentarse los hallazgos de una manera evidente y concreta para utilizar la información como herramienta de mejora. (MINTIC, s.f.).

Fase de post-explotación

"Es importante tener en cuenta que, a este punto, ya se vulnera el sistema y no es necesario dañarlo o desestabilizar gravemente (a menos que el plan desde el principio así lo indique)". (MINTIC, s.f.).

Por lo tanto, se debe definir un alcance máximo a ejecutar para las siguientes acciones:

- ✓ Escalamiento de privilegios.
- ✓ Acceso a datos específicos (bases de datos, repositorios, "fileservers", ftp).
- ✓ Denegación de servicios (CRÍTICO).
- ✓ Obtención de "passwords" para otros sistemas.
- ✓ Acceso a "logs" de dispositivos.
- ✓ Ingreso a servidores Web, DNS, proxy, servidores de impresión.
- ✓ Acceso a directorios activos o LDAP, para obtener información de usuarios (cuentas de correo electrónico, extensiones o dependencias donde trabajan), información que puede emplearse para posteriores ataques de ingeniería social.
- ✓ Ingreso a las entidades certificadoras, que podría afectar la creación de certificados, revocación e incluso la inscripción de dichos certificados si se llega a comprometer la llave.
- ✓ Acceso a los sistemas de almacenamiento, para verificar información sobre tipos de "backup", medios empleados, etc.
- ✓ "Ping Sweeps" (Barridos A VLANS para identificar "hosts").
- ✓ Instalación de "exploits" remotos.

- ✓ Instalación de “backdoors” para posterior ingreso y que no se afecten por los reinicios de los “hosts”.
- ✓ Modificación de los servicios.

Fase de reporte

“Es necesario documentar todos los resultados obtenidos en cada fase, para tener soportes de las labores realizadas y a su vez la respectiva justificación de los resultados finales”. (MINTIC, s.f.).

Por lo anterior, es importante tener en cuenta las audiencias a las cuales se les presentará el reporte, dado que no es conveniente entrar en demasiados detalles cuando la audiencia será de tipo administrativo y así mismo cuando la audiencia es de tipo técnico, no se disponga de un reporte más preciso y específico.

Tipos de Reporte

A. Reporte gerencial

“El reporte gerencial enfoca un plan de trabajo para solucionar todas las falencias encontradas, pueden manejarse plazos trimestrales, semestrales y anuales para determinadas labores que requieran ejecutarse”. (MINTIC, s.f.).

Según las mismas orientaciones de MINTIC, este tipo de reporte debe contener la siguiente información:

- ✓ Introducción, justificación y objetivos alcanzados durante las pruebas.
- ✓ Calificación de riesgo, ubicando los activos que mayor riesgo pueden traer a la organización con base al criterio del ejecutor de la prueba de efectividad de los controles.

- ✓ Motivos o causa raíz de las vulnerabilidades encontradas, entre las cuales se pueden encontrar razones como:
    - Máquinas sin parches.
    - Sistemas operativos sin el "hardening" adecuado.
    - Máquinas con servicios activos no utilizados.
    - Contraseñas débiles o fáciles de adivinar.
    - Diseños o arquitecturas de sistemas inseguros, servicios de red sin "hardening".
    - "Firmware" de dispositivos obsoleto.

B. Reporte técnico

"Este reporte puede contener la información anterior, pero incluyendo los aspectos más importantes a nivel técnico, dado que quienes reciban esta información serían quienes ejecuten las acciones de mejora para cada vulnerabilidad encontrada". (MINTIC, s.f.).

Lo anterior, teniendo en cuenta:

- ✓ Recolección de información basada en recursos publicados por la propia entidad.
- ✓ Información recolectada en plataformas como Google, Bing, páginas de referencia, etc.
- ✓ Información que pudo ser recolectada en las plataformas publicadas como, estructura de la organización, unidades de negocio, mercados, proveedores etc.

- ✓ Inteligencia con el personal interno, donde se evidencia la información que pudo obtenerse por medio de ingeniería social (solo en primera instancia, no para solicitar claves o accesos).
- ✓ Vulnerabilidades encontradas (clasificadas bien sea por los servicios, plataformas o "hosts").
- ✓ Explotación de las vulnerabilidades (cuales fueron apalancadas o pudieron ser aprovechadas en cada host y cuáles no).
- ✓ Actividades de POST-Explotación efectuadas en cada "host" comprometido con la prueba.
- ✓ Una vez se finaliza el reporte, se espera que la entidad inicie con las actividades propuestas para cerrar las brechas y aumentar la efectividad de los controles implementados o se implementen otros que cumplan con las expectativas de seguridad de la información.

C. Informes y recomendaciones

"En esta fase ya se cuenta con la información resultante del levantamiento de información, pruebas, análisis y evidencias recolectados se han evidenciado las vulnerabilidades técnicas explotables y la línea base de seguridad de la entidad evaluada, su brecha frente a la norma ISO 27001 y en relación con mejores prácticas". (MINTIC, s.f.).

Estos son algunos aspectos clave que, sobre los informes, deben tenerse en cuenta y ser aplicados, según lo orientado y estipulado por el ministerio de las TIC:

- ✓ **Documentar las recomendaciones:** en cada uno de los análisis se han documentado las recomendaciones para mejorar o subsanar las

debilidades y hallazgos. Ello permitirá determinar el nivel de madurez y construir los informes de las pruebas técnicas y administrativas.

- ✓ **Requerimientos técnicos:** un informe del análisis realizado en la entidad, donde se refleje el estado de lo avanzado frente a los requerimientos de la norma ISO 27001, Gobierno en Línea y el Modelo de Seguridad y Privacidad de la Información del Ministerio TIC. Este informe también incluirá las recomendaciones a nivel de estrategia de implementación y coordinación para el fortalecimiento de la seguridad de la información en las entidades.
- ✓ **Resultados de las pruebas que incluyan:** categorización de cada tipo de vulnerabilidad, la amenaza a la seguridad que se expone, la causa del problema de seguridad, la técnica de prueba usada para encontrarla, la remediación de la vulnerabilidad, la calificación de riesgo de la vulnerabilidad (alta, media, baja). MINTIC (s.f.).

3. “Software”

Proteger la empresa u organización es más posible cuando se cuenta con herramientas de seguridad digital. Subestimar la importancia de una estrategia de ciberseguridad robusta, es un error que puede costar caro a las organizaciones.

Las estrategias de seguridad digital fortalecidas y desarrolladas bajo normas y estándares son la herramienta que garantiza la protección de las organizaciones.

Conozca, a continuación, algunos de los “software” que contribuyen a la seguridad digital, desde la prevención o la mitigación de amenazas:

A. **Nagios Network Analyzer**

Otorga un análisis extenso de su red y fuentes de tráfico en unión con las amenazas a la seguridad.

El "software" cuenta con una potente interfaz web que es fácil de usar y permite consolidar notificaciones y alertas, a continuación, se enseña un video que ayuda a ampliar el conocimiento.

B. **Ntopng**

Es una de las mejores herramientas de monitoreo de tráfico de red, cuenta con una interfaz web inteligente para explorar información sobre el tráfico histórico y en tiempo real, junto con los "hosts" activos.

C. **SolarWinds**

Cuenta con variedad de funciones y herramientas útiles diseñadas para traducir detalles finos en informes y gráficos completos.

D. **PRTG Network Monitor**

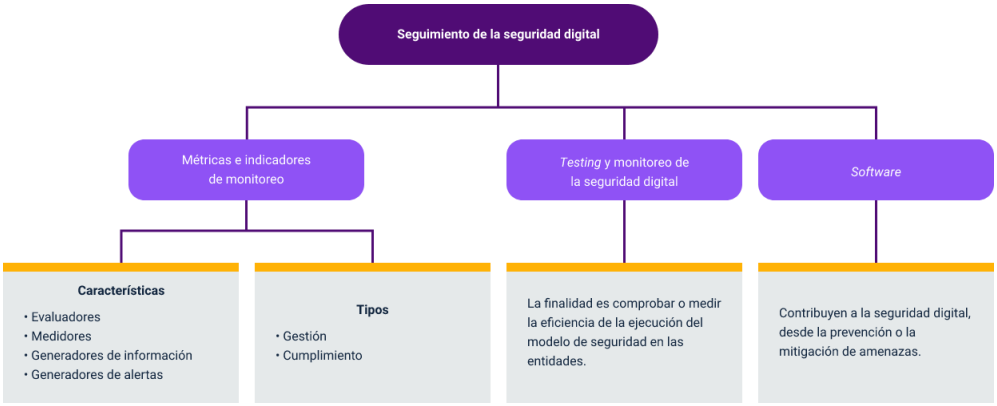
Tiene la capacidad de monitorear de manera eficiente sus dispositivos, sistemas y aplicaciones de red.

E. **Pandora FMS**

Sirve para supervisar cientos y miles de dispositivos, sistemas, aplicaciones y redes.

Síntesis

Toda empresa u organización debe propender por establecer una política que permita identificar, gestionar e implementar las acciones necesarias que permitan prevenir y mitigar los riesgos de seguridad digital, esto a través de monitoreos métodos e indicadores que permitan su seguimiento constante acorde a las métricas establecidas por la organización que generen seguridad digital.



Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1. Métodos de métricas e indicadores de monitoreo	Organización Internacional de Normalización (ISO). (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad*. (ISO 27001).	Norma técnica	https://www.iso.org/standard/27001
1. Métodos de métricas e indicadores de monitoreo	Organización Internacional de Normalización (ISO). (2016). *Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Seguimiento, medición, análisis y evaluación*. (ISO27004).	Norma técnica	https://www.iso.org/standard/64120.html
1. Métodos de métricas e indicadores de monitoreo	Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC). (2015). *Guía de indicadores de gestión para la seguridad de la información*.	Guía técnica	https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

Glosario

Activo: cualquier cosa que tenga valor para la organización. [NTC 5411-1:2006].

Amenaza: es toda aquella acción o serie de acciones, que aprovechan las vulnerabilidades para romper la seguridad de los sistemas.

Control: medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Política: toda intención y directriz expresada formalmente por la dirección.

Vulnerabilidad: se trata de aquella debilidad o fallo de seguridad que se presenta en un sistema de información, que puede estar compuesto por "software", "hardware" y otros componentes y servicios tecnológicos, generando riesgos de seguridad de la información.

Referencias bibliográficas

Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC). (s.f.). *Guía de indicadores de gestión para la seguridad de la información*. https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC). (s.f.). *Guía Metodológica de Pruebas de Efectividad*. https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

Organización Internacional de Normalización (ISO). (2013). *Seguridad de la información, ciberseguridad y protección de la privacidad.* (ISO 27001). https://www.iso.org/standard/27001

Organización Internacional de Normalización (ISO). (2016). *Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Seguimiento, medición, análisis y evaluación*. (ISO27004). https://www.iso.org/standard/64120.html

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal Gutiérrez	Responsable del equipo	Dirección General
Liliana Victoria Morales Gualdrón	Responsable de línea de producción	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Pablo Cesar Pardo Ortiz	Experto Temático	Regional Cauca - Centro de Teleinformática y Producción Industrial
Fabián Leonardo Correa Díaz	Diseñador Instruccional	Regional Tolima - Centro agropecuario La Granja
Andrés Felipe Velandia Espitia	Revisor Metodológico y pedagógico	Regional Distrito Capital - Centro de Diseño y Metrología
Rafael Neftalí Lizcano Reyes	Asesor Pedagógico	Regional Santander - Centro Industrial del Diseño y la Manufactura
Sandra Patricia Hoyos Sepúlveda	Revisión y corrección de estilo	Centro para la Industria de la Comunicación Gráfica
Gloria Amparo López Escudero	Adecuadora Instruccional	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información.
Alix Cecilia Chinchilla Rueda	Asesora Metodológica	Regional Distrito Capital - Centro de gestión de mercados, Logística y Tecnologías de la información.
Eulises Orduz Amezquita	Diseñador web	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información

Comentado [AF2]: Completar cuando actualicen los créditos.

Nombre	Cargo	Regional y Centro de Formación
Diego Fernando Velasco Güiza	Desarrollador Fullstack	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Nombre_responsable	Animador y Producción audiovisual	Regional Distrito Capital - Centro de Gestión De Mercados, Logística y Tecnologías de la Información
Carolina Coca Salazar	Evaluación de contenidos inclusivos y accesibles	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Lina Marcela Pérez Manchego	Validación de recursos educativos digitales	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información
Leyson Fabián Castaño Pérez	Validación de recursos educativos digitales	Regional Distrito Capital - Centro de Gestión de Mercados, Logística y Tecnologías de la Información