Guía Metodológica de Pruebas de Efectividad

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No. 1

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	06/05/2016	Versión inicial del documento

TABLA DE CONTENIDO

PÁG

DERECHOS DE AUTOR....4
AUDIENCIA....5
INTRODUCCIÓN....6
JUSTIFICACIÓN....7
GLOSARIO....8
OBJETIVOS....9
METODOLOGÍA DE PRUEBAS DE EFECTIVIDAD....10
ALCANCE....11
1. LEVANTAMIENTO DE INFORMACION....12
1.1 Revisiones Manuales....12
1.2 Identificación de Amenazas....13
2. PRUEBAS Y ANALISIS....14
2.1 Tipos de Pruebas de Efectividad....15
2.2 Alcance de las Pruebas....15
2.3 Procedimiento de Ejecución de Pruebas de Efectividad....16
2.3.1 Contextualización....16
2.3.2 Reconocimiento del Objetivo....17
2.3.3 Modelado de Amenazas....19
2.3.4 Análisis de Vulnerabilidades....20
2.3.5 Explotación....22
2.3.6 Reporte....24
3. INFORMES Y RECOMENDACIONES....27
3.1 Informes....27

1 DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27000 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

2 AUDIENCIA

Entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.

3 INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

En este sentido, dentro del marco de la estrategia de gobierno en línea, se ha elaborado el modelo de seguridad y privacidad de la información, el cual a lo largo de los últimos años se ha ido actualizando en función de las modificaciones de la norma técnica que le sirve de sustento: ISO 27001, así como las mejores prácticas y cambios normativos de impacto sobre el modelo.

A su turno el Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

4 JUSTIFICACIÓN

El Ministerio de las Tecnologías de la Información y las Comunicaciones, en concordancia con las actividades de la estrategia de gobierno en línea y con la implementación del modelo de seguridad y privacidad de la información, pone a disposición de las entidades, la siguiente guía, para que puedan tener una línea base durante los análisis en el recorrido de la implementación del modelo de seguridad y privacidad, de esta manera ayudar a proteger los bienes, activos, servicios, derechos y libertades dependientes del Estado.

5 GLOSARIO

- **ACTIVO:** Cualquier cosa que tenga valor para la organización. [NTC 5411-1:2006]
- **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.
- **SEGURIDAD DE LA INFORMACIÓN**. Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
- **POLÍTICA**. Toda intención y directriz expresada formalmente por la Dirección.
- **RIESGO**. Combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC Guía 73:2002]
- **ANÁLISIS DE RIESGOS**. Uso sistemático de la información para identificar las fuentes y estimar el riesgo. [ISO/IEC Guía 73:2002]
- **EVALUACIÓN DE RIESGOS**. Todo proceso de análisis y valoración del riesgo. [ISO/IEC Guía 73:2002]
- **VALORACIÓN DEL RIESGO**. Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo. [ISO/IEC Guía 73:2002]
- **GESTIÓN DEL RIESGO**. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. [ISO/IEC Guía 73:2002]
- **TRATAMIENTO DEL RIESGO**. Proceso de selección e implementación de medidas a para modificar el riesgo. [ISO/IEC Guía 73:2002]

6 OBJETIVOS

La presente guía tiene como finalidad, indicar los procedimientos de seguridad que pueden generarse durante el proceso de evaluación en los avances en la implementación del modelo de seguridad y privacidad de la información.

Se procura que las entidades tengan un enfoque de seguridad en el cual se incluya el desarrollo y mantenimiento de la misma, realizando mejoras en las áreas que se requiera.

Dependiendo de la entidad, dichos procedimientos pueden variar o si la entidad desea puede generar más procedimientos si lo considera conveniente.

7 METODOLOGÍA DE PRUEBAS DE EFECTIVIDAD

La metodología de pruebas de efectividad es una serie de actividades, que tienen por finalidad comprobar o medir la eficiencia de la implementación del modelo de seguridad en las entidades.

Esta metodología ha sido diseñada para ayudar a las entidades a entender y comprender, la realización de unas pruebas, los objetivos de las mismas y el beneficio que se obtiene al identificar sus etapas y gestionarlas.

Esta metodología es desarrollada en diferentes etapas que permiten concluir que tanto ha avanzado la entidad con la implementación del modelo; de esta manera, a través de la valoración de diferentes aspectos se permitirá identificar vulnerabilidades y amenazas a las cuales está expuesta la entidad, así como también posibles debilidades en los controles implementados.

Al igual que los demás procedimientos planteados en el modelo de seguridad y privacidad de la información, se busca proteger la disponibilidad, integridad y confidencialidad de la información de la entidad.

Un factor externo de mucho impacto, que se alinea con la ejecución de las pruebas de seguridad y privacidad y sus resultados, son los intereses de lo que se denomina Alta Dirección, que para nuestro caso son los directivos de las entidades del estado, estos se ven reflejados en las capacidades de las entidades de llevar a buen término la implementación del modelo de seguridad para dar cumplimiento a la normatividad vigente; así como llevar a la entidad al siguiente nivel de seguridad que permite que sus procesos y atención al ciudadano deje una buena imagen en la sociedad colombiana.

8 ALCANCE

La metodología busca desde el primer momento de la ejecución, crear una línea base del estado de seguridad de la entidad, es decir, facilitar la identificación de la brecha en la implementación del modelo de seguridad, entiéndase como línea base la primera medición; las siguientes mediciones darán a la entidad la percepción de seguridad que manifiestan en la implementación del modelo de seguridad.

Seguridad de la información como ecosistema tiene varios principios básicos que deberían ser importantes a la hora de hacer pruebas para verificar los avances en la implementación del modelo de seguridad y privacidad, básicamente no existe una bala de plata para los problemas de seguridad que pueda tener una entidad, una evaluación de seguridad si bien es cierto es útil como primera fase, no es efectiva en evaluaciones más profundas que requiera una entidad para mejorar sus niveles de seguridad en todas las áreas; esta es una razón de que la seguridad es un proceso, no un producto.

El alcance en la entidad es de total cobertura, dada la orientación del GEL, de la normatividad y demás, la seguridad y privacidad en la entidad debe desarrollarse de manera estratégica, debe tener un ciclo de vida, que permita llegar a las partes más expuestas al riesgo.

9 LEVANTAMIENTO DE INFORMACIÓN

En esta fase la entidad debe recopilar la información necesaria para iniciar la actividad, dicha información puede ser organizada por parte del equipo de seguridad de la información de la entidad.

La información recogida no solo debe permitir identificar los activos más importantes de la entidad, relacionados con los procesos de la misma, ya sea misionales o de apoyo. También me debe permitir el conocer el contexto de la entidad, es decir, el entorno donde se proyectan los objetivos de la entidad.

El grupo de personas que hace la recolección de información, debe reconocer el organigrama de la entidad, mapa de procesos, política de seguridad, manual de políticas, metodología de riesgos, identificación de riesgos, planes de gestión de riesgos, entre otros, esta información es la base para la identificación de la brecha de seguridad que tiene la entidad.

En esta fase también se debe identificar los grupos de interés, al interior de la entidad, como lo es control interno, tecnología, recursos humanos, calidad, comunicaciones, GEL, líderes de procesos.

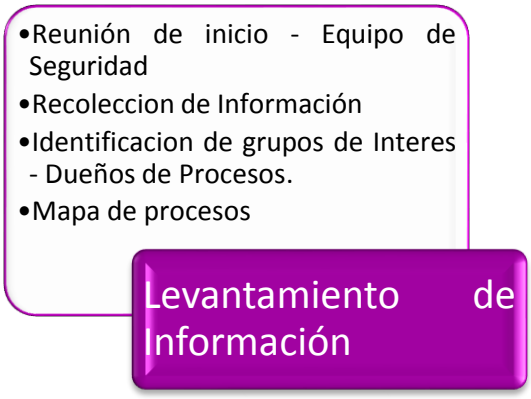

Imagen 1. Levantamiento de Información

Para entender mejor esta fase, tenga presente las actividades de revisiones manuales e identificación de amenazas.

9.1 REVISIONES MANUALES

Las revisiones son inspecciones manuales que la entidad debe realizar con el objetivo de identificar lo comprendido en seguridad por los servidores públicos, lo

realizado en seguridad en los procesos y el estado de las políticas de la entidad; dichas revisiones se hacen analizando la documentación, a través de reuniones con las personas a cargo de estos temas, dueños de los procesos.

Esta es una manera efectiva ya que a través de estas inspecciones se consigue identificar el porqué de las implementaciones de seguridad y sus controles en la entidad. Permite comprobar si las personas comprenden los procesos de seguridad, si se ha tomado conciencia de las políticas de seguridad y privacidad que tiene la entidad.

9.2 IDENTIFICACIÓN DE AMENAZAS

La identificación de amenazas no es otra cosa que la evaluación del riesgo que se realiza en la entidad, es decir, es la evaluación de las actividades donde se ven involucradas las personas, la infraestructura y los procesos; con el objetivo de identificar las amenazas que se ciernen sobre la entidad.

El resultado de estas actividades permite desarrollar planes de mitigación para las vulnerabilidades encontradas, orientar mejor los recursos y la ayuda a las áreas de la entidad que más lo requieren; la búsqueda de estas amenazas debe ser desde que se crean los procesos y durante su ciclo de vida.

Estas actividades deben tener un enfoque simple, es decir, descomponer los procesos a través de la evaluación manual, de manera que se sepa cómo funciona y su interrelación con las otras actividades.

- Definir y clasificar los activos de la entidad, evaluando su criticidad, sus posibles vulnerabilidades técnicas, operacionales y de gestión.
- Desarrollar una matriz con las amenazas potenciales, con sus vectores de ataque.
- Elaborar planes de mitigación para cada amenaza real.

El resultado de todo esto puede ser una serie de documentos, listas o diagramas, en los cuales se plasma los análisis de riesgo de la entidad y sus planes de mitigación a través de los controles sugeridos

Para el levantamiento de la información, se puede apoyar en el instrumento de diagnóstico y seguimiento que ha puesto a disposición de las entidades el Ministerio TIC.

10 PRUEBAS Y ANÁLISIS

En esta fase las entidades deben identificar los riesgos que se manifiestan a través de las debilidades en la implementación del modelo de seguridad y privacidad de la información y las vulnerabilidades que se presentan por la falta de controles de seguridad, que mitiguen los riesgos.

Estas pruebas están orientadas a evaluar la estructura de seguridad en la entidad.

Para esto las entidades deben revisar varios frentes de trabajo, como son el anexo A de la ISO 27001:2013, el ciclo de vida de la seguridad (PHVA), el nivel de madurez de la entidad de acuerdo a los niveles expuestos en el modelo de seguridad y privacidad y recomendaciones para que la entidad llegue a plasmar el concepto de Ciberseguridad.

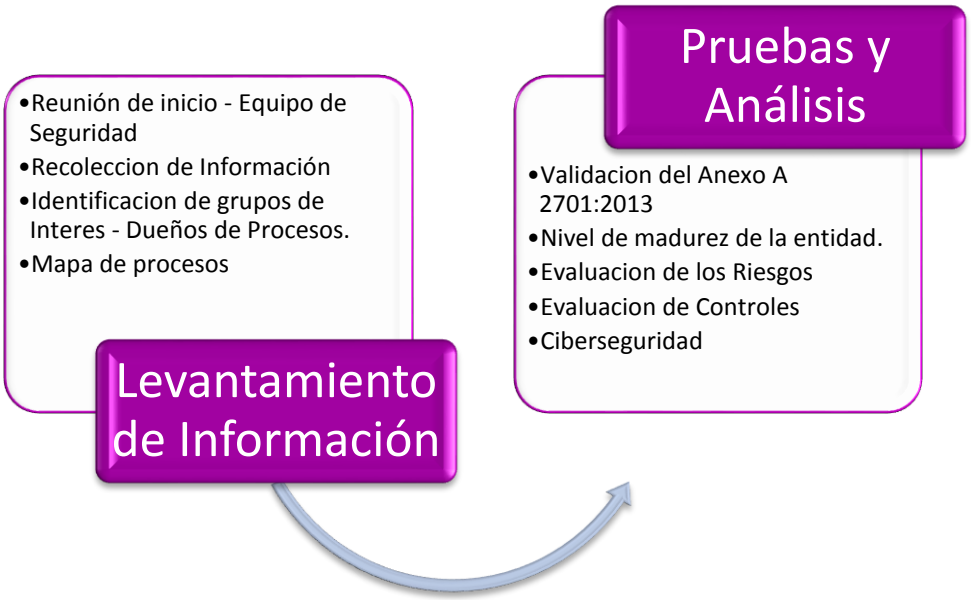

Imagen 2. Componentes de Levantamiento de Información y Pruebas y Análisis

Las pruebas de vulnerabilidad en resumen son unas técnicas empleadas para comprobar la seguridad de una entidad. Las pruebas son esencialmente las pruebas sobre aplicaciones, procesos y usuarios para encontrar vulnerabilidades.

Actualmente se encuentran diferentes técnicas y el cuándo usarlas, las cuales son necesarias para tener un marco de referencia del nivel de seguridad que estoy

evaluando; así como tampoco hay una sola técnica que cubra todas las comprobaciones necesarias para evaluar todo lo requerido por la entidad.

Una orientación objetiva al realizar la evaluación, le permite a la entidad de manera equitativa realizar actividades manuales como pruebas técnicas; esto dará como resultado la posibilidad de una comprobación completa de lo avanzado en la implementación del modelo de seguridad y privacidad.

Para entender mejor esta fase, tenga presente las siguientes recomendaciones metodológicas con las cuales se busca proteger la disponibilidad, integridad, y confidencialidad de la información.

10.2 TIPOS DE PRUEBAS DE EFECTIVIDAD

Pueden realizarse 3 tipos de pruebas de efectividad, basados en el nivel de conocimiento del entorno o infraestructura de la entidad objetivo:

- **Pruebas Con Conocimiento Nulo Del Entorno:** Es un tipo de prueba que simularía a un atacante real, ya que se basa en que tiene muy poco o nulo conocimiento del objetivo o su infraestructura.
- **Pruebas Con Conocimiento Medio Del Entorno:** Es cuando para la prueba de pentesting, se tiene más información sobre el ambiente que será atacado, es decir, direcciones IP, sistemas operativos, arquitectura de red etc… pero es información de igual manera limitada o media. Esto emula a alguna persona dentro de la red con conocimiento básico de la misma.
- **Pruebas Con Conocimiento Completo Del Entorno:** Es cuando el hacker tiene toda la información relacionada al sistema objetivo del ataque. Es generalmente para temas de auditoría.

10.3 ALCANCE DE LAS PRUEBAS

Deben existir reglas específicas para la ejecución de las pruebas de efectividad técnicas, para asegurar que dichas actividades no incurran en fallas mayores y se pueda afectar la infraestructura o las operaciones de la entidad. Dentro del alcance se pueden definir los siguientes aspectos:

1. **Plan De Trabajo:** Debe definirse durante cuánto tiempo se realizarán las pruebas, los sistemas que harán parte de las pruebas, las actividades específicas, los procedimientos de contingencia en caso de alguna afectación etc.…
2. **Insumos:** Que recursos son necesarios para realizar las actividades: Personal adicional, ventanas de tiempo, equipos etc…

3. **Responsables:** Quienes serán los encargados de efectuar las pruebas (sean proveedores o funcionarios de la entidad).
4. **Afectaciones Posibles:** El tipo de afectación que puede llegar a darse sobre cada sistema, también debe definirse si el objetivo es realizarlo en horario de producción o en horario de baja actividad laboral.
5. **Multas o Sanciones:** En caso de incumplir los parámetros anteriormente mencionados, deberán fijarse las sanciones disciplinarias o multas.

Estos alcances permitirán bien sea controlar internamente el desarrollo de las pruebas, como manejar los acuerdos de servicio con terceros que pueden llegar a realizar estos procedimientos.

10.4 PROCEDIMIENTO DE EJECUCIÓN DE PRUEBAS DE EFECTIVIDAD

Las pruebas de efectividad pueden realizarse por medio de las siguientes acciones de manera secuencial:

Imagen 3. Ciclo para la Ejecución de Pruebas de Efectividad Técnicas

10.4.1 Contextualización

Esta fase se basa en identificar los alcances reales de las pruebas y de los procedimientos a ejecutar con base a las necesidades identificadas:

Dicha identificación de necesidades, puede darse por medio de las siguientes preguntas.

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, que tipo de acciones posteriores solicita realizar (Pueden ser pruebas de vulnerabilidades en la máquina comprometida, escalamiento de privilegios etc)
f. 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?

Además de lo anterior, es importante tener en cuenta que estas pruebas no tienen como objetivo identificar solamente una vulnerabilidad sobre un sistema específico o algún sistema desactualizado, sino que la meta principal **es identificar los riesgos de seguridad de la información a través de los controles que serán evaluados a través de las pruebas**, para así tomar las medidas proactivas/preventivas para mitigar los riesgos encontrados.

Otros aspectos importantes para la contextualización del procedimiento son las siguientes:

- Establecer líneas de comunicación con los 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.

Un punto final a tener en cuenta, es que estas pruebas también deben medir la efectividad de un sistema de monitoreo o detección, es decir, si se están realizando actividades de escaneo, ataques, infiltración, alteración de la información, exista una respuesta eficaz.

10.4.2 Reconocimiento del Objetivo

Una vez se definen los alcances y necesidades, se procede con la fase de reconocimiento. Esta fase tiene por objetivo obtener tanta información del objetivo como sea posible para poder ser empleada en las fases de evaluación de vulnerabilidades y la fase de explotación.

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 3 métodos (enfocado a los sistemas de información):

- **PASIVO:** Este método 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.
- **SEMI-PASIVO:** En este punto, 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.
- **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
  - Búsqueda de directorios, archivos o servidores adicionales que no estén públicamente disponibles.

Otra información que puede obtenerse como punto de referencia contempla los siguientes temas:

- Relaciones con proveedores
- Acceso a información del personal, como extensiones telefónicas y direcciones de las sedes.
- Organigrama de la entidad.
- Direcciones de correo electrónico de funcionarios publicados en las páginas de la entidad.
- Bloques de direccionamiento IP adquirido.
- Tecnologías utilizadas por la compañía (información que puede obtenerse a través de ingeniería social hacia los proveedores).

- Identificar la presencia de equipos de respuesta a incidentes (CERT/CSIRT)
- Identificación de las instalaciones físicas.
- WHOIS lookups a través de LACNIC, RIPE, ARIN, IANA entre otros.

10.4.3 Modelado de Amenazas

Esta fase maneja la relación atacante vs activo, es decir, el atacante que beneficio puede obtener si logra su objetivo de penetrar el sistema y modificar, borrar, copiar o destruir algún activo de información.

En resumen, esta fase se centra en realizar un análisis desde 2 frentes:

ENFOCADO EN LA ENTIDAD: 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, ¿Se vulnera la confidencialidad?, ¿Qué probabilidad existe de que este evento se materialice?, ¿Qué impacto tendría dicha divulgación?

Dentro de la gestión de riesgos se incluyen o se deben considerar los siguientes activos:

- Datos De Empleados
- Datos De Clientes
- Sistemas De Información
- 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 etc.)

Para realizar una gestión de riesgos adecuada, se puede 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 si son suficientes.

ENFOCADO EN EL ATACANTE: Identificando los posibles agentes o grupos que podrían llegar a perpetrar algún tipo de ataque hacia la entidad. Dicha identificación está centrado en los siguientes grupos:

Internos	Externos
Empleados	Sociedades
Administrativos, Ejecutivos	Competidores
Administradores De Infraestructura	Contratistas
Desarrolladores	Proveedores
Ingenieros	Crimen Organizado
Técnicos	Hacktivistas
Contratistas	Hackers Tipo Script Kiddies
Soporte Remoto	

Tabla 1. Posibles Agentes de Ataque a una Organización.

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.

10.4.4 Análisis de Vulnerabilidades

Es el proceso de descubrir falencias en los sistemas y aplicaciones que pueden llegar a ser aprovechados por un atacante.

Dichas falencias pueden ser descubiertas a nivel del host o en la administración o configuración o diseño del mismo.

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 dos maneras:

- **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.

a. MÉTODO AUTOMATIZADO:

Se denomina método automatizado dado que se utiliza un software para que este haga la interacción con el objetivo, generalmente realiza varios procedimientos de análisis de manera simultánea, dando ventajas significativas de tiempo y esfuerzos respecto a los métodos manuales. Un ejemplo de las ventajas es por ejemplo ejecutar un telnet hacia un puerto para verificar si este responde o está abierto, repetir este procesos para los más de 60 mil puertos es una labor tediosa y un software puede ejecutarla.

Dentro de los métodos automáticos para análisis se encuentran:

- 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.

- **ANÁLISIS PASIVO**

Esto implica 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.

INVESTIGACIÓN:

Una vez se realiza la verificación de las vulnerabilidades con base a 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. Para ello se dispone de las siguientes fuentes de información:

- 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).

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.

10.4.5 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. **Enfoque de día zero:** Si se encuentra alguna vulnerabilidad nueva, idear la manera de aprovecharla para ejecutar algún ataque.
6. **Exploits comunes:** Buffer overflow, SEH (Structured Exception Handler), ROP (Return Oriented Programming)

7. **Crackeo De SSID (WIFI):** Movimientos enfocados a apalancar vulnerabilidades sobre este medio y sus protocolos de encripción como (WEB, WPA, EAP-FAST etc…)
8. **Ataques al usuario (Ingeniería social):** Con base a 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…
9. **Hombre en el medio (Man In-The-Middle):** Ataques de interceptación de tráfico, donde se suplanta el direccionamiento bien sea físico o IP.
10. **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.
11. **Análisis de código fuente:** (Puede ser tanto de aplicaciones como de sistemas operativos que dispongan de código abierto).

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.

10.4.6 Post-explotación

Una vez se encuentra comprometido el sistema o host (fase anterior), se procederá a identificar qué tipo de información puede obtenerse, a que otros sistemas de información se puede ingresar desde el sistema capturado, identificar opciones de configuración, información de red (direccionamiento IP de VLAN, servidores vecinos, direcciones físicas, etc.), todo esto con el objetivo principal de determinar el valor de la máquina para la organización.

Es importante tener en cuenta que a este punto ya se vulneró el sistema y no es necesario dañarlo o desestabilizarlo gravemente (a menos que el plan desde el principio así lo indique). 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 encripción 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.

10.4.7 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.

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.

REPORTE GERENCIAL:

Puede 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 faciles de adivinar.
    - Diseños o arquitecturas de sistemas inseguros, servicios de red sin hardening.
    - Firmware de dispositivos obsoleto.
- Plan de trabajo para solucionar todas las falencias encontradas, pueden manejarse plazos trimetrales, semestrales y anuales para determinadas labores que requieran ejecutarse.

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:

- 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 cuales 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.

Para el seguimiento a esta fase, se puede apoyar en el instrumento de diagnóstico y seguimiento que ha puesto a disposición de las entidades el Ministerio TIC.

11 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 los requisitos frente a al MSPI , Gobierno en Línea y en relación con mejores prácticas. De la misma forma en cada uno de los análisis se han documentado las recomendaciones para mejorar o subsanar las debilidades y hallazgos.

Lo anterior permitirá determinar el nivel de madurez y construir los informes de las pruebas técnicas y administrativas.

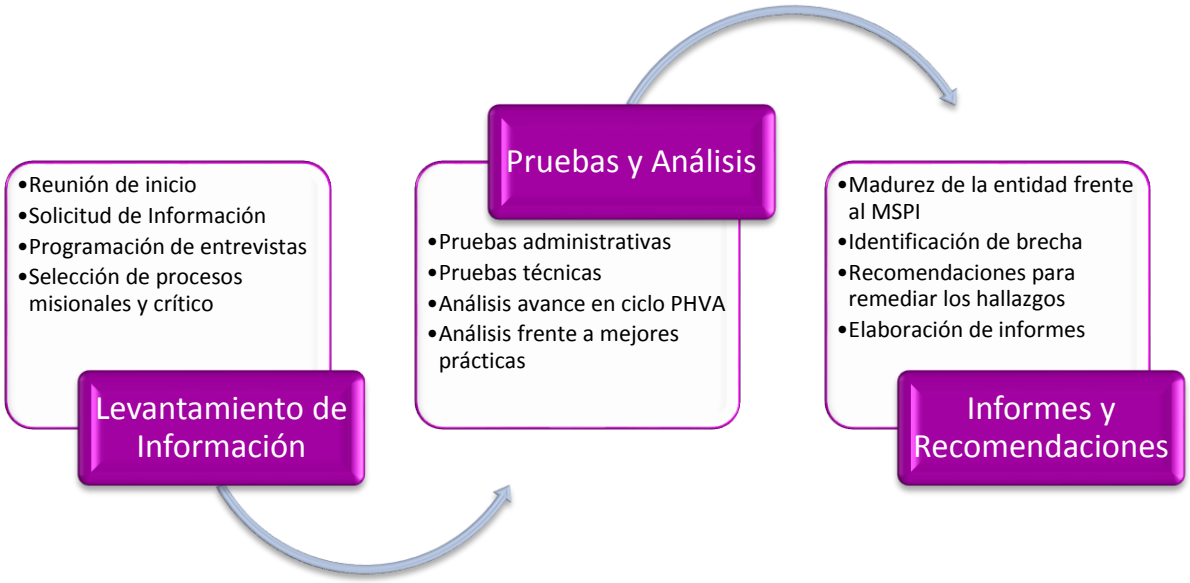

Imagen 4. Descripción de los 3 Componentes de la Metodología de Pruebas de Efectividad.

11.2 Informes

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.

Al sacar los resultados de las pruebas de seguridad, la recomendación es incluir la siguiente información:

- 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)

Para el seguimiento a esta fase, se puede apoyar en el instrumento de diagnóstico y seguimiento que ha puesto a disposición de las entidades el Ministerio TIC.