PEHPT™ Methodology

Illustrations

1. Justificación

La metodología **PEHPT™ Methodology** se define como la herramienta que permitirá el diseño, desarrollo e implementación de las soluciones del tipo Seguridad Informática – Ethical Hacker y Computo Forense.

Esta metodología ha sido desarrollada y patentada por Electronic Design and Technological Development for your future – ED&TD®; es revisada y ajustada continuamente conforme los avances tecnológicos así lo demanden.

2. Alcance

La metodología **PEHPT™ Methodology** tiene por alcance el constituirse en la herramienta central del diseño, desarrollo e implementación de nuestras soluciones en:

- Seguridad Informática
- Ethical Hacker
- Computo Forense

Garantizando de esta forma el 99.9%[1] en el objetivo primordial de salvaguardar, proteger y custodiar la información sensible de una organización y los medios electrónicos (hardware) donde esta es almacenada.

3. Objetivos

- Definir la ruta procedimental requerida para auditar la intranet como la extranet de una organización en términos de performance y seguridad informática propiamente dicha.

- Identificar las acciones correctivas y opciones de mejora que han de implementarse dentro de una consultoría a efectos de optimizar el

[1] Nunca se podrá garantizar el 100%, dado que el factor humano es el 0.1% de cualquier sistema de seguridad tanto informática como física.

performance y seguridad informática propiamente dicha, de los servicios de red ofertados mediante la intrante y extranet de la organización.

- Identificar las vulnerabilidades y brechas en la seguridad informática propiamente dicha de una organización y tomar las medidas preventivas requeridas y conforme estándares internacionales a fin de proteger la información[2].

- Garantizar la cadena de custodia de la prueba obtenida como prueba legal de la comisión de un delito informático.

- Salvaguardar, proteger y custodiar la información sensible de una organización y los medios electrónicos (hardware) donde esta es almacenada.

4. Definiciones

4.1. Delito Informático

Un delito informático o ciberdelito es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y/o dañar ordenadores, medios electrónicos y redes de Internet.[3]

4.2. Cadena de Custodia de la Prueba

La cadena de custodia de la prueba se define como el procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones.[4]

[2] Este es el activo más importante de cualquier organización.
[3] Tomado de URL: https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico. El 2016-08-08 a las 22:15 Hr. LMT.
[4] Tomado de URL: https://es.wikipedia.org/wiki/Cadena_de_custodia. El 2016-08-08 a las 22:16 Hr. LMT.

4.3. Intranet

Definida como la red computacional propia de una organización que implementa tecnologías similares a la Internet, permitiendo de esta manera compartir archivos, servicios de impresión, mensajería, consulta a bases de datos, telefonía y demás aplicaciones especializadas que se utilizan al interior de una organización.

4.4. Extranet

Definida como la red computacional que implementa como medio de conexión a la Internet para que usuarios específicos tales como clientes y/o proveedores accedan a los servicios y recursos de red, que ofrece la Intranet de la organización.

Cabe destacar que los empleados que se encuentran por fuera del marco de seguridad perimetral que ofrece la Intranet también acceden mediante la Extranet a la misma.

4.5. Performance

En términos generales hace alusión al rendimiento de un equipo y/o sistema. Y propiamente dicho en términos de:

Red Computacional: Determina cuales son los factores que hacen que la red no tenga un comportamiento conforme estándares internacionales aplicables a la categoría de cableado estructurado implementado en la infraestructura de red, en términos de:

1. Calidad de servicio
2. Calidad de la transmisión
3. Calidad del servicio a partir de la experiencia del cliente.

4.6. Ingeniería Social

Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.[5]

4.7. Servicios de Comunicaciones

Tales servicios de comunicaciones son:

1. Datos
2. Voz Analógica
3. Voz Digital
4. VoIP
5. Video Analógico
6. Video Digital
7. Multimedia
8. Señales de Control (Los nueve (09) subsistemas de un edificio inteligente)

4.8. Interoperabilidad

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define interoperabilidad como la habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada..

5. Responsables

Es responsabilidad de la División de Ingeniería.

[5] Tomado de URL: https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica). El 2016-08-08 a las 22:19 Hr. LMT.

En tal virtud de lo anterior, las responsabilidades se asignan de la siguiente manera, así:

Responsabilidad	Cargo
Eng. Hugo David Shlomoh Lopez Gonzalez	Gerente General – ED&TD® y Director de la División de Ingeniería

6. PEHPT™ Methodology

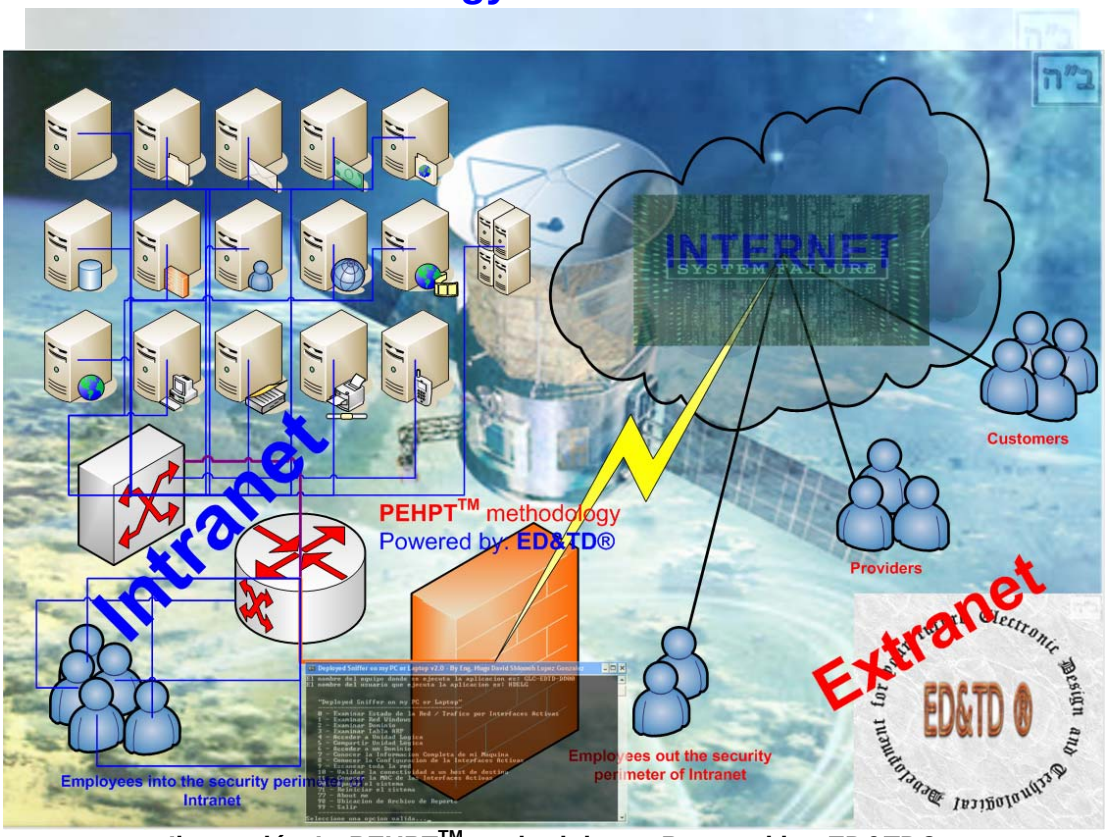

Ilustración 1 - PEHPT™ methodology - Powered by: ED&TD®

Siglo XXI, entendida la tecnología como el "*conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico*"[6], podemos decir que desde que hicimos dominio del fuego como gran avance

[6] 1ra acepción de la RAE, consultado el 2016-08-08 a las 16:28 Hr. LMT. Tomado de: http://dle.rae.es/?id=ZJ2KRZZ.

tecnológico de esa época, el campo de la informática es el segundo gran avance tecnológico de esta época.

Entendiendo la informática, la cual se soporta en otras tecnologías; como el tratamiento del activo más importante de una organización mediante el empleo de computadoras, podremos desarrollar las siguientes preguntas:

1. **¿Cual es el activo más importante de una organización?**

   El activo más importante de toda organización no es otro que la **INFORMACION**

2. **¿Que es información?**

   Entendida la información como un conjunto de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje[7].

   La información no es otra cosa que el conocimiento estructurado, y porque no decirlo de manera científica de los eventos físicos que observamos.

3. **¿Porque es el activo más importante?**

   A partir de la definición que propusimos y teniendo en cuenta que en el mundo empresarial, cuando se deben de tomar las decisiones sobre un cambio en la estrategia bien sea de producción o de mercadeo, el que posea la información en gran nivel de detalle en ese instante de tiempo (lo que llamaremos tiempo real) se traduce en un éxito financiero y/o económico para esa organización.

   Ese factor - Financiero y/o Económico - hace que la información sea el ACTIVO MAS IMPORTANTE de toda organización, llámese como se llame, sea cual sea su actividad económica.

Desarrolladas nuestras preguntas podremos entender el porque en la era de la informática debemos asegurar nuestro activo más importante como

[7] Tomado de wikipedia el 2016-08-08 a las 16:52 Hr. LMT. URL: https://es.wikipedia.org/wiki/Informaci%C3%B3n

cuando aseguramos nuestras instalaciones físicas; y para lograr ese objetivo debemos contemplar tres servicios, a saber:

- Seguridad Informática
- Ethical Hacker
- Computo Forense

A efectos de garantizar estos servicios antes contemplados, implementamos metodologías para el análisis de tráfico y desempeño de la red a nivel de capa física, enlace, red y transporte; y mediante técnicas de Ethical Hacking, se identifican las vulnerabilidades en la actual infraestructura computacional y de red instalada en la organización.

Bajo este contexto y definido cada servicio, podemos decir entonces que la **Seguridad Informática y el Ethical Hacking** son los **elementos de defensa preventivos** al momento de proteger ese activo tan valioso e importante de toda organización - la **INFORMACION** - y que el ***Computo Forense*** es el ***elemento de prueba judicial*** cuando ese activo ya fue comprometido.

PEHPT™ methodology, garantiza el 99.9% en el objetivo primordial de salvaguardar, proteger y custodiar la información sensible de una organización y los medios electrónicos (hardware) donde esta es almacenada. **ATENCION**: No olvidar que el otro 0.1% siempre será el factor humano.

Como ya mencionamos la metodología fue desarrollada y patentada por Electronic Design and Technological Development for your future - ED&TD® y se estructura en las siguientes fases:

1. Performance
2. Ethical Hacking – Pruebas de Penetración
3. Ethical Hacking – Aseguramiento de la Infraestructura Computacional

6.1. PEHPT™ methodology – Servicios que asegura

6.1.1. Seguridad Informática

Es el conjunto de estrategias tanto tecnológicas como de ingeniería social tendientes a identificar las vulnerabilidades presentes y futuras que la infraestructura computacional y de red actualmente instalada al seno de una organización puede presentar.

Todo ello, con el único fin de salvaguardar, proteger y custodiar la información sensible de una organización y los medios electrónicos (hardware) donde esta es almacenada.

Un estudio de Seguridad Informática tiene dos componentes radiculares a saber:

Auditoria: En este componente se audita tanto la intranet como la extranet de la organización en términos de performance y seguridad informática propiamente dicha.
Consultoría: Se identifican las acciones correctivas y opciones de mejora que han de implementarse para el óptimo performance y seguridad informática propiamente dicha, de los servicios de red ofertados mediante la intranet y la extranet de la organización.

6.1.2. Ethical Hacker

Es el procedimiento mediante el cual una organización a través de ataques a su infraestructura computacional y de red ***sin fines destructivos, dentro del marco legal vigente y bajo un ambiente controlado***; identifica sus vulnerabilidades y brechas en su seguridad informática propiamente dicha, a efectos; de tomar las medidas preventivas requeridas y conforme estándares internacionales a fin de proteger su activo más importante.

El Ethicak Hacking es conocido como pruebas de penetración (del ingles Penetration Testing) o pruebas de intrusión (del ingles Intrusion Testing) y quienes se desempeñan como hackers éticos son conocidos como Pen-Tester.

6.1.3. Computo Forense

Explotadas las vulnerabilidades y brechas en la seguridad informática propiamente dicha de una organización, esta; requiere conocer al detalle la respuesta a los siguientes interrogantes:

1. ¿Quien fue?
2. ¿Como lo hizo?
3. ¿Que se comprometio?

Estos interrogantes son resueltos mediante la implementación de técnicas y metodologías forenses a medios informáticos y de almacenamiento electrónico dentro de una infraestructura computacional y de red.

Este conjunto de técnicas y metodologías permiten que los datos que han sido identificados, preservados, analizados y presentados como prueba de la comisión de un delito informático tenga plena validez dentro de un proceso legal. En otros términos, es; garantizar la cadena de custodia de la prueba.

6.2. PEHP™ methodology – Fases

6.2.1. Performance

La necesidad de implementar una infraestructura de red al seno de una organización, no es otra que la de integrar los servicios de comunicaciones de la empresa, dichos servicios están directamente relacionados a la producción de la misma; dado que al mejorar los procesos de intercambio de la información y sus tareas conexas tales como: Manipulación concurrente de datos, seguridad de los sistemas de información (recuerde es el activo más importante), aumento en la taza de transferencia de archivos digitales, interoperabilidad entre departamentos y procedimientos, manejo de medios electrónicos, servicios de correspondencia, entre otros; el tiempo de respuesta entre el usuario y los procesos con los cuales interactúa mejoran considerablemente, lo cual se refleja en términos prácticos en un aumento en la producción de la misma.

Esta fase consta de las siguientes etapas:

1. Evaluación de la infraestructura de red
2. Evaluación de los requerimientos de red

3. Auditoria de la infraestructura de red
4. Informes y entregables

6.2.1.1. Evaluación de la infraestructura de red

Tiene como objeto, el identificar el estado actual de la red a nivel de infraestructura; para ello desarrollaremos las siguientes tareas:

1. Identificación de los edificios que conforman el campus de la organización.
2. Mapa de interconexiones físicas a nivel de campus y por edificio.
3. Esquema físico de la red.
4. Esquema lógico de la red.
5. Informe preliminar.

6.2.1.2. Evaluación de los requerimientos de red

Entendiéndose por requerimientos de red, todos aquellos requerimientos del negocio que nos indican cuales son las necesidades de tráfico interdepartamental, nivel de utilización y planes de expansión; para lo cual realizaremos las siguientes tareas:

1. Identificación de las aplicaciones que se ejecutan, determinando cuales son de uso corrientes y cuales de misión critica.
2. Identificación de los servicios de comunicaciones actualmente en uso en la organización.
3. Desempeño y análisis de trafico, y caracterización del trafico por servicio en función de los siguientes conceptos:
    a. Calidad de Servicio
    b. Calidad de la Transmisión
    c. Calidad del Servicio a partir de la experiencia del usuario
4. Determinar el Ancho de Banda requerido a nivel de campus y edificio, dimensionando los correspondientes enlaces.
5. Identificar las directrices organizacionales en cuanto al número de centros de red requeridos (centros de datos), administradores de red, conexión de grupos de trabajo, virtualización de redes tanto a nivel de intranet como de externet.
6. Informe preliminar.

6.2.1.3. Auditoria de la infraestructura de red

Fundamentado en el acopio de la información suministrada en las etapas anteriores y más aun en sus informes preliminares, se realizara la correspondiente autoría a la infraestructura de red, donde se listan las siguientes tareas:

1. Análisis del performance de la red, donde a partir de los requerimientos de red, determinamos:
    a. Conectividad.
    b. Transportabilidad.
    c. Fiabilidad.
    d. Redundancia.
2. Consideración de los problemas a nivel lógico, a partir de:
    a. Interoperabilidad.
    b. Enrutamiento.
    c. Segmentación.
3. Gestión de red, identificando las necesidades inmediatas como las de mediano y largo plazo.
4. Arquitectura de la infraestructura de red, analizando:
    a. Estándar de cableado estructurado implementado.
    b. Topología física y lógica de red.
    c. Recomendaciones para posibles migraciones.
5. Requerimiento a nivel de adecuaciones, donde:
    a. Se realiza una evaluación a los sistemas de energía actualmente existentes.
    b. Se revisan los niveles de tierras, los sistemas de puesta a tierra, y las salidas eléctricas.
    c. Se define el espacio para futuras ampliaciones.
    d. Se dan directrices para la estructura del tendido de cable.
    e. Se fijan las distancia entre los Cuartos de Cableado a los Centros de Datos o Cuartos de Telecomunicaciones.
    f. Se identifica la topología de los enlaces de datos.
    g. Se listan los requerimientos de hardware a nivel de equipos de conectividad activa y pasiva.
    h. Se establece el esquema de direccionamiento y segmentación.
6. Informe preliminar.

6.2.1.4. Informes y entregables

Mediante una la compilación sistemática de los diferentes informes preliminares, se redacta el informe final de la etapa de performance, donde se hace énfasis en:

1. Metodología implementada
2. Resultados obtenidos
3. Conclusiones
4. Recomendaciones
5. Anexos. Estos contemplan todos y cada uno de los archivos digitales productos de cada fase.

6.2.2. Ethical Hacking – Pruebas de Penetración

Mediante pruebas de penetración, podremos:

- Evaluar las vulnerabilidades a través de la identificación de las debilidades provocadas por una mala configuración en las aplicaciones.
- Analizar y categorizar las debilidades explotables, con base en el impacto potencial versus la amenaza sea realidad.
- Proveer recomendaciones fundamentado en las prioridades de la organización mitigando y en lo posible eliminado las vulnerabilidades, reduciendo el riesgo de ocurrencia de evento(s) desfavorable(s).

Las pruebas de penetración, se ejecutan en las siguientes etapas:

1. Recopilación de información
2. Descripción de la red
3. Exploración de los sistemas
4. Auditoria de las aplicaciones Web
5. Extracción de información
6. Acceso no autorizado a información sensible o crítica
7. Informes y entregables

6.2.2.1. Recopilación de información

En esta fase pretender generar el panorama de la red desde una vista holística, donde se integran: Infraestructura, Equipamiento y Usuarios; para con ello identificar los posibles objetivos que serán objeto de la prueba de penetración. Dentro de las tareas listadas contamos:

1. Identificación de los puntos débiles con el ánimo de encontrar los posibles agujeros de seguridad.
2. Análisis detallado de la infraestructura, equipamiento y perfiles de usuario.
3. Análisis de las políticas de seguridad informática actuales.
4. Informe preliminar.

6.2.2.2. Descripción de la red

Permite identificar la topología lógica y física en función de la seguridad informática, para lo cual realizaremos las siguientes tareas:

1. Identificación y listado de las plataformas computacionales instaladas, determinando cuales están activas, y cuales en uso; a nivel de:
    a. Sistemas Operativos.
    b. Servidores Bases de Datos.
    c. Servidores Web.
    d. Servidores de Correo Electrónico.
    e. Servidores de Aplicaciones.
    f. Servidores de Impresión.
    g. Servidores FTP.
    h. Servidores Proxy.
    i. Servidores de Voz.
    j. Entre otros.
2. Identificación de la configuración en los equipos:
    a. Servidores.
    b. De Conectividad Activa.
3. Identificación de los parámetros y políticas de control de acceso a los centros de datos o cuartos de telecomunicaciones y cuartos de cableado.
4. Informe preliminar.

6.2.2.3. Exploración de los sistemas

Son todos y cada uno de los escaneos realizados a cada uno de los equipos servidores y de conectividad activa previamente identificados en la etapa anterior. Listamos las siguientes tareas:

1. Escaneo a los dispositivos de conectividad activa y servidores
2. Escaneo a puertos conocidos.
3. Escaneo a puertos asociados.
4. Escaneo de vulnerabilidades.
5. Escaneo a la seguridad perimetral.
6. Escaneo de enumeración.
7. Escaneo a cada plataforma computacional.
8. Informe preliminar.

6.2.2.4. Auditoria de las aplicaciones web

Esta fase pretender identificar y validar el nivel de seguridad que posee la información que la organización facilita mediante los accesos vía la Internet. Se catalogan las siguientes tareas:

1. Identificación, listado y validación de los certificados de seguridad activos y/o en uso.
2. Escaneo de las vulnerabilidades presenten en los diferentes componentes, a saber:
    a. ActiveX.
    b. JavaScript.
    c. CGI's.
    d. Applets.
    e. Entre otros.
3. Informe preliminar.

6.2.2.5. Extracción de información

Análisis detallado y pormenorizado de los resultados obtenidos en la fase de: Exploración de los sistemas y Auditoria de las aplicaciones Web; a partir de las siguientes tareas:

1. Identificación, comprobación y clasificación de las vulnerabilidades.
2. Identificación, comprobación y clasificación de los errores en programación.
3. Comprobación e impacto de las configuraciones por defecto.
4. Identificación, comprobación e impacto de las políticas de seguridad informática implementadas.
5. Informe preliminar.

6.2.2.6. Acceso no autorizado a información sensible o crítica

Es la prueba de penetración como tal, y en tal virtud se realizaran:

1. **Pruebas de penetración con objetivo**: Evaluamos las vulnerabilidades en partes específicas en la infraestructura computacional.
2. **Pruebas de penetración sin objetivo**: Se examinan la totalidad de los componentes que conforman la infraestructura computacional.
3. **Pruebas de penetración a ciegas**: Realizadas a partir de la información publica de la organización.
4. **Pruebas de penetración informadas**[8]: Simulación de ataques realizados por individuos al seno de la organización que poseen información privilegiada.
5. **Pruebas de penetración externas**: Evaluamos los mecanismos seguridad perimetral implementados.
6. **Pruebas de penetración internas**: Evaluamos las políticas de seguridad informática implementadas.

Dado el alcance de **PEHPT™ methodology**, estas pruebas se ejecutaran bajo la modalidad de Red Teaming[9], para lo cual nos valdremos de técnicas de ingeniería social para obtener la información requerida a efectos de realizar el ataque.

Para estas pruebas de penetración, usaremos las siguientes metodologías:

[8] El nombre de la prueba deriva, del hecho puntual que la prueba parte del perfil de cargo de la organización; y no necesariamente que se informe a los usuarios de la misma de la realización de la prueba.
[9] El 'Red Teaming' es la modalidad de pruebas encubierta, donde solo un selecto grupo de ejecutivos de la organización, conocen de la misma. Esta modalidad es la mas real y evita que realicen cambios de ultima hora que hagan pensar que hay una mejora y/o un mayor nivel de seguridad de la organización.

1. OSSTMM (Open Source Security Testing Methodology Manual).
2. OWASP (Open Web Application Security Project).
3. PTF (Penetration Testing Framework).
4. ISSAF (Information System Security Assessment Framework)

La selección de estas metodologías obedece a dos factores primordiales:

- Son referencia en el mundo de la seguridad informática.
- Recomiendan las herramientas que se deben utilizar para realizar el penTest[10].

Las tareas de esta fase son:

1. Seis pruebas de penetración, a saber:
   a. Con objetivo.
   b. Sin objetivo.
   c. A ciegas.
   d. Informada.
   e. Externa.
   f. Interna.
2. Informe preliminar

6.2.2.7. Informes y entregables

Mediante una la compilación sistemática de los diferentes informes preliminares, se redactaran dos informes, a saber:

1. **Informe ejecutivo**: Orientado a la gerencia y directivos de la organización; donde se hará énfasis en:
   a. Metodología implementada.
   b. Resultados obtenidos.
   c. Conclusiones.
   d. Recomendaciones.
   e. Anexo Especial: Análisis de Vulnerabilidades[11].
   f. Anexos. Estos contemplan todos y cada uno de los archivos digitales productos de cada fase.

[10] Pruebas de penetración.
[11] El análisis de vulnerabilidades evalúa el impacto que estas tienen sobre la organización.

2. **Informe técnico**: El cual será para personal de administradores y/o responsables directos de la gestión y administración de la infraestructura computacional y de red de la organización; donde el énfasis se encuentra en:
    a. Falencias técnicas, operativas y procedimentales.
    b. Aplicación de buenas practicas de seguridad informática.

6.2.3. Ethical Hacking – Aseguramiento de la Infraestructura Computacional

Esta etapa propende por afianzar la buena imagen y reputación corporativa que la organización debe de proyectar.

Las etapas de esta fase, son:

1. Implementación del informe ejecutivo
2. Acceso no autorizado a información sensible o crítica
3. Informes y entregables

6.2.3.1. Implementación del informe ejecutivo

Como su nombre lo dice, se implementaran las recomendaciones del informe ejecutivo y de las propias manifestadas en el anexo especial 'Análisis de Vulnerabilidades'.

Las tareas a realizar son:

1. Listado de las tareas inherentes y derivadas del informe ejecutivo en su aparte de recomendaciones y anexo especial.
2. Ejecución de las tareas listadas en el numeral anterior.
3. Informe preliminar.

6.2.3.2. Acceso no autorizado a información sensible o crítica

Mediante esta etapa se propende por verificar que las vulnerabilidades que fueron remediadas en la etapa inmediatamente anterior, lo hubiese sido de

manera satisfactoria, de igual forma; se identifican nuevas vulnerabilidades no encontradas y visibles solo hasta la ejecución de la etapa anterior.

Las tareas son:

1. Seis pruebas de penetración, a saber:
    a. Con objetivo.
    b. Sin objetivo.
    c. A ciegas.
    d. Informada.
    e. Externa.
    f. Interna.
2. Informe preliminar

6.2.3.3. Informes y entregables

Mediante una la compilación sistemática de los diferentes informes preliminares, se entrega un informe ejecutivo donde se hace énfasis en:

1. Vulnerabilidades remediadas.
2. Vulnerabilidades encontradas y que no fueron remedidas.
3. Nuevas vulnerabilidades.
4. Recomendaciones.

7. Registros asociados

- Listado maestro de documentos de origen interno – **LR-00-00**

Change Control		
Date	**Version**	**Description**
2016–08–08	01	Original
2016–09–15	02	Chage of type

Version Control						
Version	**Elaborated**		**I review**		**Pass**	
	Date	**Name/Job**	**Date**	**Name/Job**	**Date**	**Name/Job**
01	2016–08–08	HDSLG/GM	2016–08–08	HDSLG/GM	2016–08–08	HDSLG/GM
02	2016-09-15	HDSLG/GM	2016-09-15	HDSLG/GM	2016-09-15	HDSLG/GM