Diagnóstico de Ethical Hacking para la Universidad Politécnica Salesiana

Pablo Mauricio Brito Bermúdez

Trabajo Final de Fin de Master (TFM)

Master Universitario en Seguridad de las TIC (MISTIC)

Ing. Pablo Brito Bermúdez.

PhD. Marco Antonio Lozano.

12 de Marzo del 2018

Licencias alternativas

Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Diagnóstico de Ethical Hacking en la Universidad Politécnica Salesiana*

Nombre del autor:	*Pablo Mauricio Brito Bermúdez*
Nombre del consultor/a:	*Pablo Mauricio Brito Bermúdez*
Nombre del PRA:	*Marco Antonio Lozano*
Fecha de entrega (mm/aaaa):	Junio/2018
Titulación::	*Trabajo Final de Fin de Master*
Área del Trabajo Final:	*Master Universitario en Seguridad de las TIC*
Idioma del trabajo:	*Español*
Palabras clave	*Ethical Hacking UPS*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

La seguridad de la información es necesario implementarla en toda institución es por eso que la Universidad Politécnica Salesiana ha decidido realizar una revisión mediante un análisis a su seguridad de la información, es por lo que se ha decido realizar un Ethical Hacking a la infraestructura haciendo uso de la metodología OSSTMM la misma que valida a todos los componentes involucrados en la seguridad de la información, reflejando en su estudio que la seguridad está en un término medio el mismo que refleja la constante evolución de la tecnología dentro de la institución por lo que es necesario siempre estar en constante mantenimiento de sus procedimientos y revisión de los activos implementados para mejorar su seguridad frente a nuevas brechas de nuevas aplicaciones que ingresan a dar servicio dentro de la red de la institución que pueden permitir obtener la información real a los usuarios pudiendo mantener la confidencialidad, integridad y disponibilidad necesaria que requiere para hacer uso de la misma en su trabajo diario. El uso de herramientas que ayudan a mantener información sobre la seguridad son aplicadas en este trabajo. La desmitificación de la seguridad de la información dentro de una empresa o institución es el 100% segura Y se ve reflejada dentro de este trabajo ya que las participaciones de los componentes de la información inciden en ella y existe siempre un eslabón débil como es el usuario final.

Abstract (in English, 250 words or less):

It is necessary to implement information security in all institutions, therefore Universidad Politecnica Salesiana has decided to analyze its information security through Ethical Hacking by using OSSTMM methodology, which validates all the components involved in information security. The study demonstrated that the security is at an average level and also shows the constant evolution of technology in the institution which is why it is necessary to constantly give its procedures maintenance and review the tools implemented to improve its security against new applications that provide services within the network of the institution and allow users to obtain real information and keep confidentiality, integrity and the availability needed to use the information in daily tasks. The use of tools that help keep information regarding security are applied in this work. The demystification of information security within a company or institution is 100% secure and is reflected in this work since the participation of the information components affect it and there is always a weak link as is the end user.

INDICE

Índice de Gráficos

Índice de Tablas

1 INTRODUCCIÓN

1.1 Contexto y justificación del trabajo

La institución donde se procederá a realizar el estudio del Ethical hacking es la Universidad Politécnica Salesiana (UPS), siendo esta una institución de educación superior privada con presencia nacional, su matriz está ubicada en la ciudad de Cuenca - Ecuador. Su trascendencia precede desde hace 20 años posicionado con renombre en el sistema educativo ecuatoriano, cuenta con carreras técnicas y sociales las mismas que son recibidas por alrededor de 6.000 estudiantes en la ciudad de Cuenca contando con una planta docente de alrededor de 400 docentes y 250 empleados en el área administrativa.

Al momento la Universidad Politécnica Salesiana tiene un servicio de sistema público mediante una página web donde entrega toda la información sobre su funcionamiento, noticias y actualidades, siendo este un método de acceso para los trámites de los alumnos, adicional al mismo maneja una intranet para los servicios de la planta docente y administrativa.

La Universidad Politécnica Salesiana ofrece el servicio de acceso al Internet a sus estudiantes y docentes mediante la red inalámbrica para consumir diferentes servicios públicos, siendo el acceso a la intranet únicamente mediante la red alámbrica desplegada por todos los campus que mantiene la Universidad.

Al ser una institución educativa la Universidad Politécnica Salesiana se halla a la vanguardia de la tecnología implementando y desarrollando continuamente nuevos servicios para el uso de sus estudiantes y colaboradores, con el compromiso de que estos sean de calidad y con alta seguridad en la información en las diferentes redes desplegadas para su uso.

El acceso a la información restringida o confidencial dentro de la web e intranet, es el valor intrínseco que maneja la Universidad por lo que se debe dar un mayor énfasis al momento de implementar los controles físicos y lógicos de seguridad dentro del campus así como desde sus accesos externos, por la valía de la información es necesario hacer una revisión a las posibles vulnerabilidades y amenazas que puede estar enfrentado a su infraestructura por pruebas indebidas de usuarios maliciosos con la finalidad de quebrantar su seguridad.

El uso de la ingeniería social se ha comprobado que va en aumento con la finalidad de conocer las claves de los usuarios, siendo necesario proceder a realizar un test de madurez en el conocimiento sobre ataques de ingeniería social especialmente a su planta docente y administrativa. Así mismo la búsqueda de acceso a la red inalámbrica por medio del portal cautivo con alteración del nombre de usuario es constante en la búsqueda de formas ilegales para su acceso por parte de los usuarios especialmente de los estudiantes por lo que es necesario realizar el testan a la página del portal cautivo.

Haciendo uso de mejores prácticas, recomendaciones que ofrecen diferentes estándares o metodologías de revisión se procederá a realizar el testing a las páginas

web disponibles así como a la infraestructura que muestre en las diferentes redes que tienen acceso los usuarios.

1.2 Objetivo del trabajo

El objetivo principal de este TFM es el de evaluar la seguridad a la infraestructura implementada en la Universidad Politécnica Salesiana con la finalidad de mitigar las vulnerabilidades hacia aplicaciones web y las amenazas posibles que pueden afectar a la triada CIA (Confidencialidad, Integridad y Disponibilidad) y al no el repudio de la información que la universidad maneja para su trabajo diario.

1.2.1 Objetivos Específicos

- Buscar información que no debería estar expuesta hacia el público que no tenga relación directa con la Universidad
- Evaluar accesos a las redes inalámbricas y alámbricas
- Evaluar conocimientos sobre ingeniería social y seguridad informática a los usuarios de la infraestructura de la Universidad
- Identificar vulnerabilidades en la infraestructura
- Identificar vulnerabilidades en la página web, subdominios principales e intranet que utiliza la UPS
- Identificar fortalezas y deficiencias de la infraestructura implementada que se evidencien en el pentesting
- Evaluar herramientas que sean de mejor uso para realizar este tipo de análisis
- Generar una metodología interna de pentesting que sirva a futuro para pruebas internas y externas, las mismas que sean realizadas periódicamente para evaluar el estado de seguridad de su infraestructura
- Obtener un conocimiento práctico de cómo realizar un pentesting de ethical hacking en una empresa o institución

1.3 Enfoque y metodología a seguir

Este TFM se enfoca a realizar una evaluación por medio de un pentesting de ethical hacking de forma escalonada de tipo caja negra hacia gris. Para lo cual se utilizará la metodología OSSTMM la misma que permitirá encontrar las vulnerabilidades más frecuentes a las que está expuesta la infraestructura de la universidad, teniendo por objetos de revisión los siguientes elementos de acceso a la información:

- Página web www.ups.edu.ec y subdominios principales
- Página de la intranet
- Red inalámbrica con su medio de acceso portal cautivo
- Test de manejo de ingeniería social para cuerpo docente y directivo de la Universidad
- Seguridad de la infraestructura en puntos de red libres o no custodiados por usuarios
- Seguridad física de acceso en equipos y claves de usuarios

Para la evaluación a las aplicaciones web se utilizará el estándar OWASP Top 10 – 2017 debido a que esta prueba va enfocada a la seguridad de aplicaciones.

Este estándar es utilizado con la finalidad de evaluar y para tomar las medidas de seguridad a través del proceso de desarrollo del pentesting, que nos ayuda para evidenciar el impacto de un software inseguro y a tomar decisiones para asegurar el mismo. Las características principales son:

- Pruebas a la aplicación web
- Comprobación del sistema de autenticación
- Pruebas de CSS (cross site scripting)
- Pruebas de CSRF (cross site request forgery)
- SQL Injection
- LDAP Injection
- Cookie Hijacking

Las fases de trabajo que se utilizará para realizar el pentesting constan de seis secciones principales para la fácil comunicación con el cliente. Estos cubren todo lo relacionado con una prueba de penetración:

- Herramientas requeridas
- Recolección de información
- Análisis de vulnerabilidades
- Explotación de ser necesario
- Post-explotación si es necesario
- Informes

1.4 Planificación del Trabajo

Para poder realizar el pentesting a los controles implementados internamente por la UPS para reducir las vulnerabilidades y amenazas que podrían afectar a la triada de la seguridad de la información CIA (Confidencialidad, Integridad y Disponibilidad), así como el no repudio de los recursos informáticos que maneja; se propone la siguiente planificación de trabajo:

- Pre compromiso del alcance del pentesting o auditoría
- Planeación y recolección de información, realizando un análisis corporativo y lógico de la red
- Modelado de amenazas identificando y clasificando los activos primarios y secundarios
- Identificación y clasificación de Vulnerabilidades hacia aplicaciones web, ataques de fuerza bruta, monitoreo de tráfico
- De ser necesario se realizará la explotación mediante la evasión de Firewall, IDS, IPS, identificando los exploits a medida, vulnerabilidades de Zero-Day, fuzzing, etc.
- Presentación de pruebas
- Escritura del documento de TFM que en este caso reemplazara al informe técnico y realización del informe ejecutivo, incorporando en el mismo las recomendaciones al tratamiento de vulnerabilidades y aseguramiento del sistema evaluado.

A continuación se procede a detallar la planificación mediante un diagrama de Gantt:

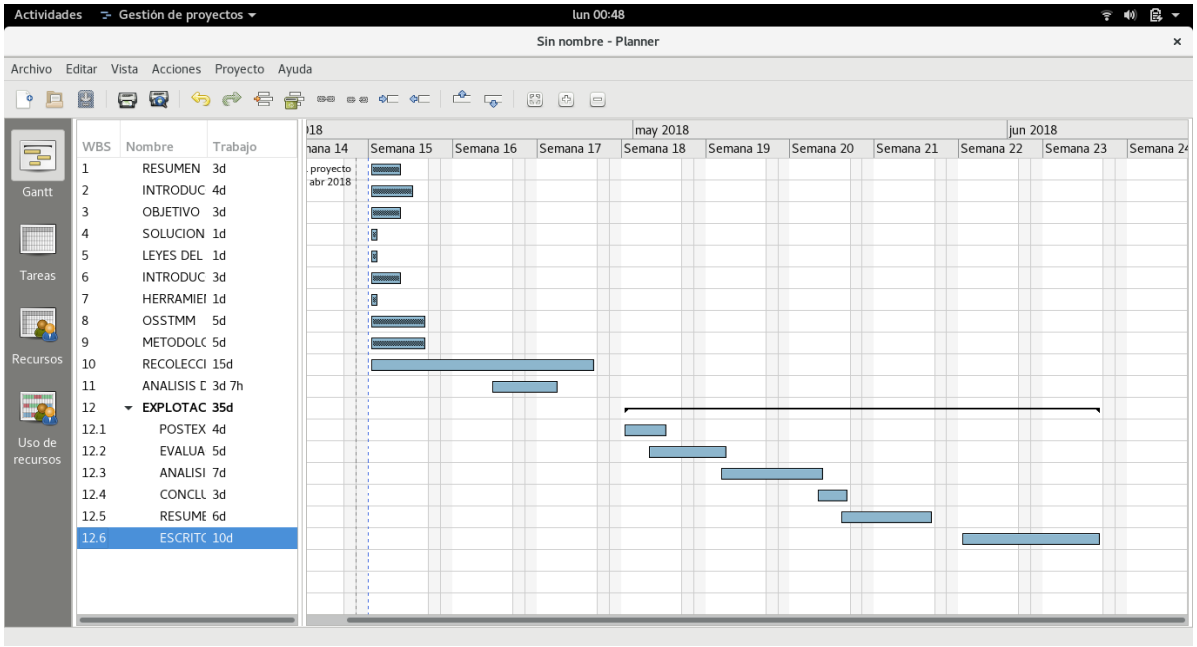


Gráfico 1.- Cronograma de Planificación
Fuente: Elaboración Propia

1.5 Breve sumario de productos obtenidos

Para la elaboración de la presente TFM seguiremos los siguientes capítulos donde iremos desglosando en forma detallada las referencias principales de cada uno de los ítems que se desarrollaran en este trabajo.

RESUMEN

CAPÍTULO 1: INTRODUCCION

1.1 Contexto y Justificación del trabajo
1.2 Objetivo del trabajo
1.3 Enfoque y metodología a seguir
1.4 Planificación del trabajo
1.5 Breve sumario de productos obtenidos
1.6 Breve descripción de los otros capítulos de la memoria
1.7 Marco Teórico
1.8 Introducción al Ethical Hacking
1.9 Metodología a utilizarse para el Ethical Hacking

CAPÍTULO 2: METODOLOGÍA

2.1 Hipótesis
2.2 Solución Propuesta
2.3 Historia y características de OSSTMM
2.4 Ventajas – Desventajas
2.5 Diseño y planificación de uso de la Metodología
2.6 Evaluación o realización mediante el Ethical Hacking
2.7 Reconocimiento
2.8 Enumeración
2.9 Revisión de Vulnerabilidades

CAPITULO 3: CONCLUSIONES Y RECOMENDACIONES

3.1 Conclusiones
3.2 Recomendaciones

BIBLIOGRAFÍA

1.6 Breve descripción de los otros capítulos de la memoria

Dentro del desarrollo del TFM se irá referenciando en los capítulos siguientes sobre los hechos que se vayan encontrando conforme vaya avanzando el trabajo del pentesting los mismos quedarán evidenciados dentro del capítulo elaborado:

CAPÍTULO 1: GENERALIDADES, en este capítulo se hace una introducción previa a como se encuentra el objeto de estudio al momento, los problemas que motivan el estudio de este TFM y de su objetivos que se proponen para encontrar una solución al trabajo realizado. También estará acompañada por parte teórica que hace referencia a los temas indicados. Es necesario conocer en este capítulo sobre las leyes y ordenanzas que el estado Ecuatoriano maneja frente al Ethical hacking, para no incumplir leyes que puedan afectar a este trabajo.

CAPÍTULO 2: METODOLOGÍA, en este capítulo se hace referencia a la metodología y herramientas con las que procederá a realizar el pentesting, así como la secuencia de las pruebas que se realizaran con la finalidad de hallar las vulnerabilidades respectivas hasta llegar a explotar esas amenazas y mantener privilegios para evidenciar problemas

que presente la infraestructura igualmente será acompañada con parte teórica sobre el tema indicado.

CAPITULO 3: ANÁLISIS DE RESULTADOS, en este capítulo se dará a conocer los resultados encontrados en el pentesting y cómo serán presentados a las autoridades de la institución para que sean valoradas y tomar sus correctivos respectivos.

CAPITULO 4: CONCLUSIONES Y RECOMENDACIONES, en base a los resultados obtenidos podemos dar las conclusiones y recomendaciones para asegurar la infraestructura de la Universidad Politécnica Salesiana, desde el punto de vista de revisor o autor del trabajo de TFM.

1.7 Marco Teórico

1.7.1 Leyes de Ethical Hacking en Ecuador

En la actualidad los equipos informáticos son utilizados en la mayoría de las actividades diarias de los seres humanos, generan gran información y son parte fundamental en el desarrollo de las empresas e instituciones a nivel mundial. Así mismo los delitos informáticos (cybercrimen) se han incrementado en gran cantidad a todo nivel especialmente en el robo de información personal y bancaria, con miras a realizar transacciones de forma fraudulenta suplantando a las personas que han sido víctimas de los delincuentes. En cuanto a nivel empresarial e institucional el robo sensible de información confidencial, ataques de denegación de servicios, acceso y control de redes para formar grandes grupos de bonnets con la finalidad de generar nuevos ataques son cada día más frecuentes, sin ser Ecuador la excepción al tema.

Con esta visión podemos darnos cuenta que existe dos formas de uso de los equipos informáticos el primero para la generación correcta y de forma legal de la información y la otra para perpetrar los cybercrímenes para obtener la información legal antes mencionada de forma anómala o por procedimientos ilegales, existiendo dos formas diferentes en las cuales se encuentran involucrados los equipos informáticos.

- Crímenes facilitados por computador.- cuando el equipo es utilizado como herramienta (acceso a archivos para generar fraudes, identificaciones falsas, copias sobre derechos de autor, etc.)
- Crímenes donde el computador es el objetivo.- con el crecimiento de la tecnología estos delitos se han sofisticado con el fin de dificultar la ubicación del criminal y víctima, jurisdicción del crimen y otros detalles. Su tratamiento en la recolección y manipulación de evidencias es muy diferente a la forencia tradicional.

En nuestro país la legislación define en su Código Integral Penal (COIP) los parámetros para no incurrir en los delitos antes mencionados el mismo que esta detallado en los siguientes artículos más destacados que hacen referencia a los delitos informáticos:

> ***Artículo 190.- Apropiación fraudulenta por medios electrónicos.-*** *En este artículo nos indica el tipo de sanción por tres años de prisión para el uso fraudulento de sistemas informáticos y redes con la finalidad de apropiarse de información ajena uso fraudulento de un sistema informático, redes electrónicas o telecomunicaciones para hacerse de información ajena considerada como un bien.*[1]
>
> ***Artículo 229.- Revelación ilegal de base de datos.-*** *En este artículo indica la sanción de uno a tres años de prisión por la violación de información secreta, intima o privada por medio de un*

1 Capítulo 2 - Delitos contra los derechos de libertad, sección novena, Delitos contra el derecho a la propiedad, COIP – Ecuador.

sistema o redes informáticas, apeorando la pena si es cometida en una institución pública y para empleados bancarios. [2]

Artículo 231.- Transferencia electrónica de activo patrimonial.- *En este artículo menciona la pena de reclusión de tres a cinco años por la modificación del funcionamiento de programas, sistemas informáticos o telemáticos*[3]

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- *Artículo donde da a conocer la pena de tres a cinco años para la persona que acceda en parte o a todo un sistema informático, telemático o de telecomunicaciones y manteniéndose dentro en contra de la persona que tiene el legítimo derecho*[4]

Luego de la revisión legal que existe en nuestro país con la finalidad de evitar incurrir en alguno de los temas antes mencionados es necesario hacer la solicitud para la aceptación y alcances del pentesting a realizarse en la Universidad por lo que se adjuntara como anexo el mismo.

1.8 Introducción al Ethical Hacking

En el Internet cada día nos informamos sobre el hallazgo de nuevos fallos de seguridad, extorsión cibernética, redes zombis, acosos y delitos mediante redes sociales, así como sitios que ofrecen herramientas y métodos para vulnerar sistemas informáticos como exploits; por lo que en la actualidad el problema de virus no es únicamente a lo que los administradores de Infraestructura y Redes deben cada día enfrentarse, actualmente el aumento de nuevas acciones para burlar la seguridad mediante phishing, spamming, pharming, etc., hace mantener la premisa de que un sistema informático puede ser cien por ciento seguro. Esto ha hecho que a nivel de Latinoamérica el porcentaje de crecimiento en la adquisición de herramientas de seguridad para infraestructura dentro de empresas e instituciones ha tenido una inversión este 2017 del 65%.[5]

La estadística de uso de las plataformas de redes sociales más utilizadas a nivel de Latinoamérica sigue manteniendo a YouTube como medio de entretenimiento, educación e información con el 95% de utilización, luego esta Facebook con un promedio de 89%, Twitter y LinkedIn con un 56 % cada uno, Instagram con el 47% y Skype con el 45%.

La Universidad Politécnica Salesiana igual que en el resto de Latinoamérica no es una excepción donde las plataformas de redes sociales son de gran uso dentro de la universidad teniendo así que el Facebook y YouTube son las plataformas más ocupadas dentro de la institución.

En cuanto a las proyecciones para este 2018 la revista ESET[6] para Latinoamérica nos presenta el panorama en que los ciberdelincuentes y grupos de espionaje mantendrán sus ataques con sus conocidas y trataran con nuevas amenazas, enfrentándose a organismos que están encargados de hacer cumplir las leyes y entidades de ciberseguridad que cada día encuentran en estrecha colaboración entre estas entidades para afrontar los diferentes ataques en que se

2 Capítulo tercero - Delitos contra los derechos del buen vivir - Sección tercera - Delitos contra la seguridad de los activos de los sistemas de información y comunicación, COIP – Ecuador.

3 Capítulo tercero - Delitos contra los derechos del buen vivir - Sección tercera - Delitos contra la seguridad de los activos de los sistemas de información y comunicación, COIP – Ecuador.

4 Capítulo tercero - Delitos contra los derechos del buen vivir - Sección tercera - Delitos contra la seguridad de los activos de los sistemas de información y comunicación, COIP – Ecuador.

5 Datos tomados de http://www.expreso.ec/ciencia-y-tecnologia/ecuador-2-0-en-cifras-DC1985720

6 Información tomada de: https://www.welivesecurity.com/wp-content/uploads/2017/12/ESET_Trends_Report_2018.pdf

hallan expuestas las diferentes infraestructuras siendo las tendencias de ataques más frecuentes los siguientes:

- **Aumento a ataques a la infraestructura crítica**.- las ciberamenazas irán en alza por la incorporación de dispositivos cada vez más interconectados, especialmente a los sistemas que son cruciales para el funcionamiento del estado y la sociedad como salud, energía, logística, etc.
- **Ataques a la cadena de suministros**.- las empresas grandes se protegen de los ciberataques mediante la adquisición de equipos que mejoran su seguridad, pero las pequeñas o medianas empresas que son proveedoras de bienes y servicios de las primeras son el objetivo buscado por los cyberdelincuentes para poder comprometer las infraestructuras más robustas por lo que el continuo peligro de las pymes es muy latente.
- **Piratería de la democracia**.- los procesos electorales han comenzado a ser atacados y esto va cada día en aumento por lo que debemos precautelar para evitar que los ciberataques puedan influenciar en gran forma los procesos electorales
- **Privacidad en la nueva era de la tecnología**: Las diferentes necesidades de consumo de los clientes mediante el uso de la tecnología, hace que los proveedores ingresen al mundo de la recolección de datos, aumentado el riesgo de privacidad de la información.

Todas estas pautas dadas nos ayudan a entender sobre los peligros latentes que cada día se enfrenta las diferentes infraestructuras ante la amenaza y peligro efectivo del cibercrimen. Ahora es momento de revisar el papel que juegan los diferentes actores frente al cibercrimen.

La palabra Hacker por muchos años ha sido mal interpretada dentro del ámbito informático ya que ha sido relacionado generalmente como la persona que realiza actos fuera de la ley en el uso de la tecnología, para lo cual existe una gran diferencia entre:

Hacker.- según la definición que brinda la RFC 1392 persona que disfruta con tener total conocimiento del funcionamiento interno de un sistema, computadoras y redes en particular. En función a su comportamiento podemos diferenciar los siguientes tipos de hackers:

- **Sombrero Blanco**.- definidos así a los hackers éticos los cuales utilizan sus habilidades en fines éticos y legales. Esos generan “pruebas de penetración” con la **debida autorización** de la persona que los contrata, adicionalmente informa como los atacantes pueden tener acceso con el fin de mejorar los mecanismos de defensa.
- **Sombrero Gris**.- es el hacker que no busca un beneficio personal o causar daño, actuando de forma no tan ética trata de comprometer la seguridad sin tener la autorización debida y en el caso de encontrar la falla no comenta a la empresa o institución afectada sino que lo divulga públicamente.
- **Sombrero Negro**.- Violan la seguridad informática con el fin de obtener un beneficio personal o simplemente con el fin de hacer daño u obtener ilegalmente información confidencial sobre una persona o una organización tales como: robo de número de tarjetas de crédito o recolección de datos personales para su venta a los ladrones de identidad, ellos caen ya en el campo del craking o cybercrimen.

Cracker.- según la definición que brinda la RFC 1392 personas que intenta acceder a los sistemas informáticos **sin autorización**. Estas personas a menudo son maliciosas, y tiene muchos medios a su disposición para irrumpir en los sistemas. Son totalmente opuestos a los hackers informáticos. Estos tienen diferentes motivaciones para realizar sus propósitos haciendo uso generalmente de rootkit, por lo que podemos diferenciarlos entre:

- **Script-kiddie**.- es una persona que recién comienza no es un profesional, no crea sino sigue un libreto está influenciado o trata de imitar a alguien.

- **Lammer**.- es una persona que en algún momento pudo efectivizar un ataque y se vuelve fanfarrón, no sabe mucho pero maneja el tema con la finalidad de hacer crecer su ego personal.
- **Defacer**.- persona dedicada a explotar fallos en sitios web
- **Newbie**.- persona novata que se encuentra con un manual o página donde hace referencia al tema de hacking y trata de usar sin conocer las consecuencias que puede acarrear en la infraestructura probada.
- **Hacktivistas**.- personas llevadas por motivación, política, social, venganza, defensa al consumidor, perpetran estos cybercrímenes, teniendo conciencia cierta de los daños que fomentara a la infraestructura intervenida.

Gráfico 2.- Diferencias entre Hacker y Cracker

Fuente: http://1.bp.blogspot.com/-WkR_U-7ihtc/VaHCMoVn1eI/AAAAAAAAACA/7AW1L7JFwEs/s400/hacker-cracker.png

Luego de haber clarificado esta constante confusión presentada durante largo tiempo podemos definir claramente el trabajo que realiza un Ethical Hacking que es la persona quien efectúa pruebas controladas a sistemas informáticos con la finalidad de busca o hallar vulnerabilidades en los sistemas, protegiéndolo de futuros ataques por otras personas no autorizadas las mismas que puedan aprovechar dichas amenazas existentes en las vulnerabilidades, explotándolas y afectando el funcionamiento normal del sistema con actividades maliciosas. Cabe recalcar que para este trabajo el hacker ético debe tener la autorización respectiva para poder llevar a cabo las pruebas necesarias.

Como grupo de buenas prácticas con las que un hacker ético debe realizar en cada una de sus pruebas se encuentran las siguientes

- No realizar pruebas de intrusión sobre un sistema sin el respaldo de un contrato o permiso escrito, cumplir los compromisos adquiridos sin realizar acciones fuera del ámbito del contrato
- Mantener la máxima confidencialidad de la información adquirida, de las vulnerabilidades detectadas en los sistemas y de la privacidad de los usuarios
- No responsabilizar al personal de la institución por algún fallo detectado
- Presentar reportes claros y adecuado sin manipulación de los resultados del análisis, llevando un formato ejecutivo que permita reflejar la calidad del análisis
- Mantener sus principios y valores como profesional ético, es decir, no aceptar ningún tipo de soborno

Por lo que es necesario que el hacker ético tenga el respectivo conocimiento de las formas como se perpetran estos crímenes mediante el conocimiento de los mecanismos de ataque que los cyberdelincuentes usan como técnicas o maneras de cumplir con su objetivo pudiendo obtener su cometido con los siguientes:

- **Virus y gusanos**.- son programas informáticos que afectan a dispositivos de almacenamiento de equipos, redes o un sistema completo, dejándolo fuera del control del usuario administrador de los equipos informáticos afectados.
- **Troyanos**.- son programas informáticos que parecen ser legítimos pero al ser ejecutados hacen al sistema anfitrión vulnerable para futuros ataques o daños en su sistema operativo, pudiendo destruir información de los discos de almacenamiento.
- **Mensaje spam**.- son correos electrónicos enviados sin consentimiento del receptor provocando problemas de congestionamiento con correo basura en los sistemas del receptor.
- **Denegación de servicios (DoS)**.- cuando los delincuentes se encargan de dejar sin servicio a una red, sistema o página web, mediante el envío masivo y constante de mensajes haciendo desbordar la capacidad de respuesta a estas peticiones
- **Malware**.- es el software que toma control de del ordenador de cualquier persona con múltiples finalidades como el de dañar o causar un mal funcionamiento del sistema, el extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo provocando el secuestro del mismo o anexándolo a una red más grande para fomentar ataques hacia otros objetivos o víctimas de la cyberdelincuencia
- **Scareware**.- software de engaño que viene en ventanas de publicidad fraudulenta haciendo uso de ingeniería social que nos obliga a descargar otro software de protección generalmente fraudulento en el cual puede hacerse de información sobre nuestra identidad y tarjetas de crédito o dañar y secuestrar nuestra información alojada en nuestros discos
- **Phishing**.- relacionadas con la clonación de páginas originales especialmente donde se puedan obtener usuarios y contraseñas provocando la confusión de acceso a los usuarios víctimas de estos ataques.
- **Carders**.- robo de tarjetas de crédito para su duplicación
- **Ataques cibernéticos**.- se presenta como un nuevo medio para guerras entre estados como el ataque al programa nuclear de Irán mediante el virus informático STUXNET, desactivando el enriquecimiento de uranio de las centrífugas

Como se evidencia en los diferentes tipos de ataques tienen la finalidad de afectar la información que tienen los diferentes dispositivos informáticos, por lo que la información debe presentar características intrínsecas que lo hacen valederas como determina la triada CIA (confidencialidad, integridad y disponibilidad) que son los principios básicos de la seguridad de la información para que los receptores o usuarios hagan de la información obtenida por su emisor, su materia prima para procesarla y generar una nueva información necesaria para el trabajo dentro de una institución o empresa, por lo que podemos encontrar diferentes categorías de ataques a la información los cuales podemos clasificarlos de la siguiente manera:

- **Interrupción**.- este ataque tiene como finalidad afectar la disponibilidad de información, rompiendo, dañando o saturando la capacidad de respuesta del servicio a las peticiones realizadas por los usuarios
- **Intercepción**.- ataque donde su finalidad es afectar o violentar la confidencialidad de la información, alguien (persona, equipo informático o un programa) no autorizado gana accesos sobre la información confidencial.
- **Modificación**.- ataque que se caracteriza por violentar la integridad de la información, alguien no solo gana accesos a la información sino que los modifica según sus necesidades
- **Fabricación**.- este ataque afecta la autenticidad de la información, alguien inserta objetos falsos en el sistema para entregar información diferente a los usuarios

1.9 Metodología utilizada para el Ethical Hacking

Este método inductivo – deductivo, realizado con un conjunto ordenado, de forma secuencial mediante procedimientos específicos bajo un criterio de actuación como un cracker, su finalidad es hacer que sus ataques sean efectivos al realizar una investigación exploratoria a las posibles vulnerabilidades que en un sistema pueden aparecer pese a tener implementado con lineamientos sobre políticas y procesos técnicos, con la finalidad de proteger su entorno informático.

El Hacker Ético realiza todas sus acciones dentro de la legalidad es decir para realizar sus pruebas deben previamente haber llegado a un acuerdo con el cliente sobre el tipo, extensión del pentesting y especialmente mantener un acuerdo o permiso para realizarlo, adicional el Ethical hacker presenta informes sobre los hallazgos encontrados en el pentesting a las personas responsables tanto de la parte técnica, como de la parte administrativa para que conozcan la situación actual de la seguridad en la empresa.

A diferencia del cracker que en primer lugar no tiene la autorización del acceso para las pruebas respectivas, y; adicional no emite ningún informe a las personas encargadas de la empresa sino que al contrario el borra huellas de acceso luego de haber logrado su objetivo de acceso ilegal al sistema afectado.

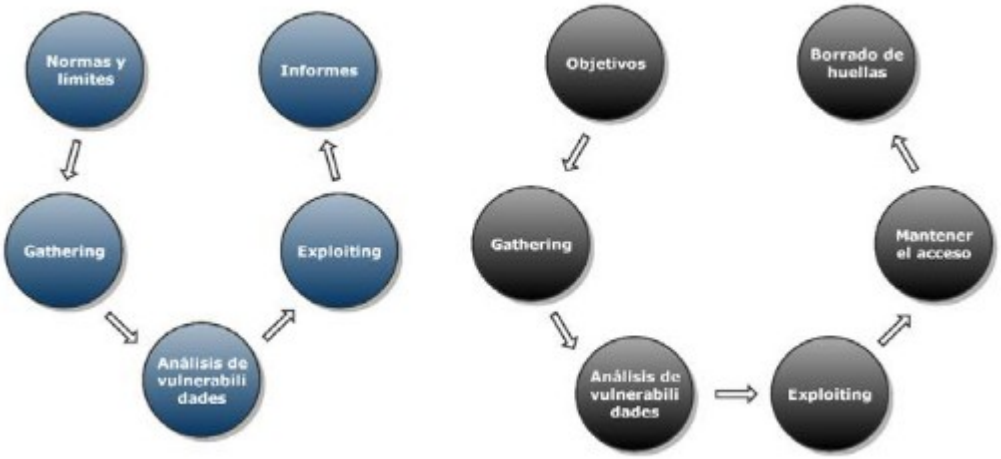


Gráfico 3.- Formas de visualización de un ataque

Fuente: Libro Seguridad en redes y sistemas.-Técnicas y conceptos sobre hacking y pentesting

En el gráfico podemos tener la diferencia en la metodología aplicada para una penetración realizada por un Ethical hacking representada en azul y la visión de un hacker que está representada en color obscuro.

Para poder comprender la metodología que realiza el Ethical hacking se describe cada uno de sus pasos:

1. Levantamiento de Información.- fase donde se levanta el convenio entre auditor y empresa para establecer los parámetros, límites y legalización del pentest. De esta manera pudiendo acceder a información personal o realizar ingeniería inversa o social al sistema y sus usuarios siempre manteniendo la privacidad de la información, adicional la revisión de las leyes y procedimientos del pentester con la finalidad de no violar la ley en ningún caso.
2. Recolección de la información o gathering.- Luego estar de acuerdo con los parámetros del pentesting, se comienza la recolección de información, siendo esta una fase muy importante dado que aquí se determina el éxito o fracaso del pentesting debido a los posibles falsos positivos que podamos obtener de la mayor información posible recolectada acerca de los sistemas, software, redes, metadatos,

configuraciones, versiones de sistemas operativos, información en redes sociales, información en internet, etc., que desean ser revisados; pudiendo esta información equivocada provocar la entrega de conclusiones inválidas al momento de escoger la mejor estrategia para la realización del pentester de la empresa testeada.

3. Análisis de las vulnerabilidades. Luego de la recolección minuciosa y eficaz sobre la infraestructura de la empresa testeada, se procede a realizar un análisis exhaustivo en busca de posibles vulnerabilidades o defectos susceptibles de ser explotados mediante el uso de herramientas creadas para dichas tareas, siendo en este punto un factor muy importante la experiencia y astucia del auditor.
4. Explotación de las vulnerabilidades. Es la fase donde queda evidenciada el ataque a las vulnerabilidades encontradas en la infraestructura testeada, mediante el uso de herramientas las mismas que pueden afectar el funcionamiento correcto de la infraestructura auditada por lo que el auditor debe tomar gran precaución para evitar perder el control de los objetivos acordados en las cláusulas del contrato.
5. Generador de los informes. Esta es una de las fases donde se diferencia con el cracker por la realización de documentos en los cuales se describen los procedimientos y acciones realizadas en cada una de las tres fases anteriores, con los resultados y alcances de los ataques encontrados, adicional se debe incluir las recomendaciones necesarias para solventar estos posibles fallos a la seguridad presentes en la infraestructura revisada. Se presentan dos tipos de informes un técnico donde se presenta los detalles técnicos y medidas óptimas para su mitigación de las vulnerabilidades halladas. En el segundo es un informe gerencial sin muchos detalles técnicos más con el afán de que cualquier persona pueda tomar conciencia de las deficiencias encontradas en la seguridad al momento de la realización del pentesting indicado, con sus recomendaciones generales.

Los objetivos de la metodología de trabajo del pentesting es evaluar a todos los componentes que están involucrados en la seguridad de la información como: usuarios, infraestructura, redes, equipos, sistemas, bases de datos, etc. Para el efecto, las fases que se utilizan en el Ethical Hacking son las siguientes:

1. Pre ataque.- fase donde se realiza la planeación y preparación del pentester, mediante el diseño de la mejor metodología a utilizarse con la información obtenida para la empresa a auditar
2. Ataque.- es la fase en donde se interactúa con la infraestructura o componentes involucrados en la generación de la información de la empresa o institución, aquí se obtiene los resultados de la planificación realizada para la ejecución del ataque
3. Post-ataque.- fase donde se realiza la reportería a todas las evidencias encontradas en el ataque, así como la limpieza de exploits y herramientas que ayudaron en la fase de ataque con la finalidad de dejar la infraestructura tal como se encontró, y puedan luego hacer las reparaciones sugeridas para mejorar la seguridad de la institución o empresa.

En la realización del pentesting existe tres tipos de testeo o formas de realizar la penetración a la empresa o institución auditada, esto en base a la información obtenida previa a la ejecución de la auditoría; las cuales son:

Caja Negra.- test de Penetración de Seguridad donde el técnico no cuenta con información sobre el sistema. Refleja de la mejor manera posible un ataque real. Es muy frecuente en pruebas de penetración a redes. Hay que descubrir equipos, sistemas, tecnologías de sitios web, etc.

White Box.- se entrega la información interna de las empresas. Proporcionan un mapa de red, firewalls, sistemas operativos, tipos de autenticación, usuarios, tecnología de sitios web, etc. Son realizadas generalmente por un equipo interno, pero ahora es más frecuente asignarlo a un equipo externo. Se convierte en parte fundamental del ciclo de

vida del desarrollo de software. No se invierte tiempo en la fase de descubrimiento (fingerprint)

Gray Box.- Mezcla características de las 2 anteriores. Test de Penetración de Seguridad donde el técnico cuenta con información limitada sobre el sistema. Se da a conocer alguna información al pentester. Sirve para profundizar en aquellos puntos críticos del sistema. Útil para conocer ataques que puede llegar hacer un usuario y privilegios a nivel interno. El cliente o empresa proporciona el nombre de su organización y una estructura interna de sus redes.

La prueba de forma escalonada es lo ideal para este tipo de pruebas ya que realiza las pruebas desde caja negra hacia caja gris, permitiendo probar ataques desde distintos perfiles.

Dependiendo de la ubicación o perfil del Pentester podemos tener los siguientes tipos de penetración:

Outsider o Test Externo.- el objetivo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema. Se realizan desde fuera del Firewall y consisten en penetrar la zona desmilitarizada (DMZ) para luego acceder a la red interna. Se compone de un elevado número de pruebas, entre las que se puede nombrar:

- Pruebas de usuarios y la "fuerza" de sus contraseñas.
- Captura de tráfico.
- Detección de conexiones externas y sus rangos de direcciones.
- Detección de protocolos utilizados.
- Scanning de puertos TCP, UDP e ICMP.
- Intentos de acceso vía accesos remotos, módems, Internet, etc.
- Análisis de la seguridad de las conexiones con proveedores, trabajadores remotos o entidades externas a la organización.
- Pruebas de vulnerabilidades existentes y conocidas en el momento de realización del Test.
- Prueba de ataques de Denegación de Servicio.

Insider o Test Interno.- Este tipo de testeo trata de demostrar cuál es el nivel de seguridad interno. Se deberá establecer que puede hacer un Insider y hasta donde será capaz de penetrar en el sistema siendo un usuario con privilegios bajos. Este Test también se compone de numerosas pruebas:

- Análisis de protocolos internos y sus vulnerabilidades.
- Autenticación de usuarios.
- Verificación de permisos y recursos compartidos.
- Test de los servidores principales (WWW, DNS, FTP, SMTP, etc.).
- Test de vulnerabilidad sobre las aplicaciones propietarias.
- Nivel de detección de la intrusión de los sistemas.
- Análisis de la seguridad de las estaciones de trabajo.
- Seguridad de la red.
- Verificación de reglas de acceso.
- Ataques de Denegación de Servicio

2 METODOLOGIA

2.1 Hipótesis

¿La seguridad de la Información en la Universidad Politécnica Salesiana es óptima?

2.2 Solución Propuesta

En este capítulo se analizará la metodología OSSTMM, la misma que ha sido seleccionada como guía de aplicación por sus ventajas que presenta para comprobar que los controles y medidas de seguridad implementada en la infraestructura de la Universidad ha sido desplegada correctamente, se propone realizar para su análisis un Pentesting basado en un Ethical Hacking utilizando la metodología OSSTMM, la misma ayudará a identificar vulnerabilidades que no puedan ser detectadas únicamente con un análisis de riesgos, es necesario demostrar que el peligro es real por medio de una simulación de ataque.

OSSTMM es la única que abarca todos los ámbitos, con lo que se convierte en la única posibilidad para cumplir con el objetivo de realizar un análisis completo de toda la seguridad de la organización. Posee métricas y explica cómo hay que hacer los informes, no cuenta con una guía técnica sobre cómo llevar a cabo las pruebas que propone, dando la facilidad para poder hacer uso de guías técnicas o manuales de buenas prácticas en la recolección de la información al momento del pentesting.

Los sistemas de información, a más de los servidores tienen un gran conjunto de elementos que conforman la plataforma para generar la información:

- Servidores
- Backups
- Administradores
- Usuarios
- Redes
- Estaciones de trabajo
- Señales Radioeléctricas
- Seguridad Física
- Entorno en general

2.3 Historia y características de la Metodología OSSTMM

OSSTMM es fruto del trabajo conjunto de varios profesionales de seguridad quienes aportaron para que en el 2001 junto a Pete Herzog como director general de a luz el nacimiento de esta norma.

Llamada así por su nombre en inglés Open Source Security Testing Methodology Manual, al estándar Manual de la Metodología Abierta de Testeo de Seguridad; siendo esta metodología la más utilizada al momento de realizar un pentesting, abarca el cumplimiento de varias normas entre ellas NITS, ISO 27001 – 27002 e ITIL, adicionalmente abarca procedimientos con bases legales y regulaciones inherentes al área de la industria del cliente, amenazas conocidas y la seguridad de la empresa. Por lo que representa un testing metodológico de seguridad que valida todos los pequeños detalles ya que individualmente no representan mucho pero que en su conjunto suman un riesgo potencial para la seguridad de una empresa. La limitación al alcance del testing de seguridad externo al interno radica fundamentalmente en los privilegios

de acceso, los objetivos, y los resultados asociados con el testing interno a interno. También esta metodología es utilizada para certificar a una organización en los requisitos que exige ISECOM.

La OSSTMM describe especificaciones sobre cuándo, que y cuales eventos serán testeados en todos los ámbitos que componen el mapa de seguridad de la gestión de seguridad de la información

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

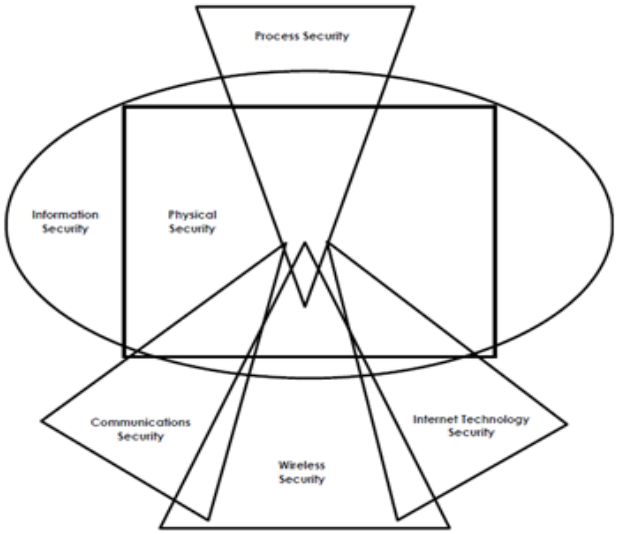


Gráfico 4.- Canales del OSSTMM

Fuente: Manual OSSTMM v2.1 (Pag23)

En esta metodología se diferencian seis tipos de test que pueden realizarse, siendo estos los siguientes:

- Blindaje o Ethical Hacking
- Doble blindaje, auditoría de Caja Negra o pruebas de Penetración
- Pruebas de Penetración
- De Caja Gris
- De doble Caja Gris
- Test Tamdem o Secuencial
- Inverso

OSSTMM utiliza Valores de la Evaluación de Riesgo (RAV), los mismos que realzarán los estados de seguridad actual de las empresas agregando dimensiones de frecuencia y un contexto de tiempo a los test de seguridad, manteniendo la compatibilidad con CVE. Para un rav, se requieren tanto el conteo como la operación.

- Vulnerabilidad
- Debilidad

- Filtrado de Información
- Preocupación
- Desconocidos

La metodología está realizada en un método jerárquico las mismas que se dividen en:

- Secciones.- son los puntos específicos del mapa de seguridad
- Módulos.- son el flujo de la metodología desde el punto de presencia de seguridad hacia otro, tiene una entrada (información usada en el desarrollo de la cada tarea) y salida (resultado de la tarea completada)
- Tareas.- son los test de seguridad o procesos que se realizan en cada módulo dependiendo de su entrada

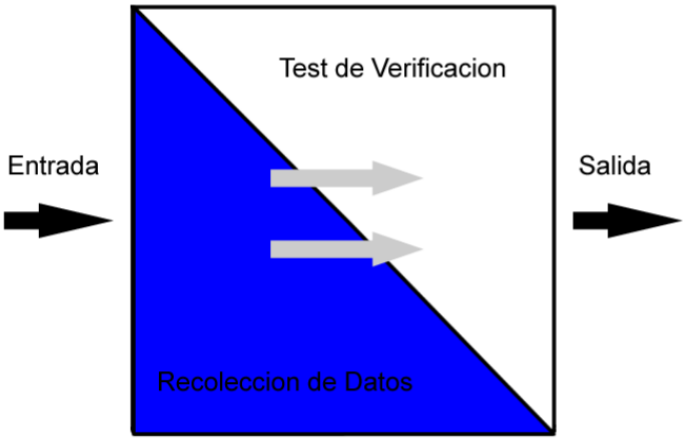


Gráfico 5.- Tareas de la Metodología OSSTMM

Fuente: Manual OSSTMM v2.1 (Pag32)

El proceso para el control del análisis de seguridad, requiere evaluar las dimensiones de seguridad que tiene en las áreas:

- Autenticación.- contar cada instancia de autenticación requerida para obtener acceso, requiere que el proceso de identificación y autorización sea el apropiado para cada mecanismo de control.
- Identificación.- contar cada instancia de métodos usados para determinar la responsabilidad y aseguramiento de todos los activos alcanzados
- Sometimiento.- contar cada instancia de acceso o confianza que estrictamente no permite que los controles se realice la interacción del usuario
- Continuidad.- contar cada instancia de acceso o confianza en el alcance del test que asegura la no interrupción entre la interacción del canal y vector causado, a pesar de fallo total. Es una buena medida sobre la capacidad de supervivencia, el equilibrio de carga y redundancia.
- Resistencia.- contar cada instancia de acceso o confianza en el alcance del test cuando no falle en abrir o proporcionar nuevos accesos en casos de fallos en la seguridad es decir fallar en forma segura.
- No Repudio.- medida que precautela que ninguna persona o sistema en la interacción en un momento particular pueda negar su participación. Requiere una correcta identificación y autorización.
- Confianza.- relación entre dos o más factores para mantener el contenido de sus interacciones no divulgadas dependiendo de su nivel de seguridad

- Privacidad.- proceso o método para mantener sin divulgar la interacción que se realiza entre por las partes o sistemas involucrados, esta debe ser conocida únicamente entre las dos partes involucradas
- Integridad.- contar las instancias de acceso o confianza con la que interactúa un proceso para verificar que la interacción entre personas o sistemas no sea alterado, redirigido, restringido, sin conocimiento de los involucrados
- Alarma.- contar las instancias de notificación apropiada y precisa frente a actividades anormales en cualquiera de las áreas del mapa de seguridad

La metodología presenta en el proceso de pruebas de seguridad las siguientes fases:

Fase	Consideraciones	Explicación
Inducción	- Compresión del alcance de auditoría - Logística para la auditoría - Detección activa de la verificación	El auditor comprende los requisitos, el alcance y las limitaciones dela auditoría
Interacción	- Considera la visibilidad de la auditoria - Verificación de accesos, de confianza, - Verificación de controles.	Se define el ámbito de la aplicación, la base de las pruebas de seguridad requiere el conocer el alcance y el ámbito en relación de los objetivos y activos.
Investigación	- Verificación de procesos, de configuración, - Validación de propiedad, - Revisión de segregación y de exposición - Exploración de la Inteligencia Competitiva.	El auditor va descubriendo información, cuya intención es descubrir la mala gestión de la información.
Intervención	- Verificación de la cuarentena, - Verificación de privilegios - Validación de continuidad - Revisión de alertas - Registros	Se centran en la penetración y perturbación. Es por lo regular la fase final de las pruebas de seguridad, y esta no puede realizarse mientras las otras no se hayan realizado.

Tabla 1.-Procesos de prueba OSSTMM (fuente propia)

2.4 Ventajas y Desventajas

Las ventajas que ofrece el usar esta metodología son las siguientes:

- Utiliza métricas que son imprescindibles para poder gestionar la seguridad de la información, ofreciéndonos los parámetros necesarios para saber si la empresa auditada cuenta con un nivel de seguridad aceptable frente a posibles ataques.
- OSSTMM es una metodología que ha ganado un gran reconocimiento y es certificable, por lo que son exigencias al momento de elegir auditores para realizar las pruebas
- No se embarca únicamente al ámbito digital, proponiendo la realización de pruebas en el ámbito físico y humano.

Las desventajas que presenta la metodología son los siguientes:

- Requiere la obtención de una gran cantidad de información para poder sacar las métricas, requiriendo tiempo y experiencia para poder obtener esta información de forma correcta.
- OSSTMM cubre todos los aspectos de la seguridad de una empresa por lo que puede resultar muy genérica y abstracta.

2.5 Diseño y Planificación de la Metodología OSSTMM

Se deben tener ciertas consideraciones al momento de realizar un Pentesting cuando es de caja negra, los sistemas que no logren ser comprometidos pueden tener vulnerabilidades ocultas que solo son visibles desde una posición administrativa. La presencia de falsos negativos y falsos positivos se incrementa.

El pentester no debe solucionar las vulnerabilidades, ya que se presenta un conflicto de interés, solo debe limitarse a realizar recomendaciones para solucionarlas, y en caso de ser necesario, se realizará una nueva auditoría para verificar que hayan sido corregidas.

Para el pentesting que se va a realizar, se debe mantener los parámetros definidos en el documento de la suscripción del pentesting y su autorización, por lo que no debe salirse del alcance de la prueba, como línea de trabajo no se debe actuar de forma no-ética, ni dejar de reportar algún hallazgo encontrado, hay que recordar que el Ethical hacking debe cumplir con las leyes locales, regionales y nacionales, adicional se plantea el uso del tipo de test escalonado (la misma que hace uso de los tipos de testing de caja gris a negra) dentro del Ethical Hacking, para lo cual debemos tomar las siguientes consideraciones generales para evaluar la infraestructura y aplicaciones desplegadas:

Tipo Test	Revisión	Alcance u Objetivo
Caja Negra	➢ DNS ➢ Puertos ➢ Servidores Web ➢ Conexiones seguras ➢ Sistemas de validación de usuarios ➢ Intrusión a bases de datos ➢ Intrusión a intranet ➢ Servicios en la nube	➢ Footprinting ➢ Scanning ➢ Enumeración ➢ Análisis de vulnerabilidades automatizado y procesos manuales ➢ Comprobación ➢ Penetración ➢ Escalamiento
Caja Gris	➢ DNS ➢ Puertos ➢ Servidores Web ➢ Sistemas de validación de usuarios ➢ DMZ ➢ Intrusión a intranet ➢ Servicios en la nube ➢ Test de fuerza bruta	➢ Total

Tabla 2.-Tipos de Pentesting (fuente propia)

La metodología OSSTMM evalúa la seguridad desde todos los puntos de vista, para la realización del pentesting a la institución se hará mediante revisión de los principales módulos y tareas que actúan en los diferentes canales que nos ayuden a evaluar de forma clara como se encuentra al momento la seguridad de la información implementada en la Universidad Politécnica Salesiana, La metodología OSSTMM ofrece varios módulos de revisión en los diferentes canales que en el capítulo de realización práctica del pentesting será definido cuales y como realizarlos.

Se debe tener en cuenta que puede presentarse riesgos en el desarrollo de la metodología al momento de realizar el levantamiento de información especialmente en las tareas para ciertos

canales en el que el analista no está totalmente familiarizado por lo que se prevé mantener reuniones permanentes con el área auditada con la finalidad de despejar dudas y poder resolverlas de forma adecuada.

La interacción entre los módulos, secciones y canales que utiliza la metodología OSSTMM se puede observar en el ANEXO 1

2.5.1 Herramientas a utilizarse

El pentesting automatizado se realiza a través de herramientas que permiten facilitar la labor del pentester. Por ejemplo, Nessus provee una solución de revisión de vulnerabilidades automatizada. A continuación se presenta algunas herramientas automatizadas que son utilizadas en los pentesting.

Nombre	Características
Zenmap	El poderoso Nmap gráfico, multiplataforma con muchas opciones para escaneo de equipos y puertos que se encuentran en una red
Burp	Utilizada para pruebas de penetración gráfica de aplicaciones web, permite utilizar un proxy entre su navegador y la aplicación destino modificando el tráfico para realizar las pruebas respectivas como nuevos intentos de conexión, envío de solicitudes, pruebas de aleatoriedad de tokens de sesión
Nessus	Software para escáner de vulnerabilidades. Incluye perfiles agresivos que puede combinar scritps experimentales, probar servicios basados en SSL, etc. Se puede combinar también con Nikto para potenciar sus resultados.
OpenVas	Similar al Nessus pero de distribución gratuita para diferente tipos de escaneo su configuración se realiza con un módulo manager, el mismo que sirve para predefinir los tipos de escaneo a redes, host que se desee. Mantiene un base de datos mediante MySQL o SQLite para guardar los resultados
Arachni	Herramienta gráfica para escaneo de vulnerabilidades para equipos móviles. De código abierto para Linux o Mac OS X, utiliza scripting para todo el sitio web pudiendo probar activamente aplicaciones web
Acunetix	Especializada en el escaneo de vulnerabilidades para webs

Tabla 3.-Herramientas automáticas para Pentesting (fuente propia)

El pentesting manual se realiza probando y construyendo directamente las vulnerabilidades. Existen muchas vulnerabilidades que no pueden ser conseguidas con herramientas autómatas, ya que estas no entienden muy bien el alcance y/o el riesgo que es adaptado a una organización específica. Entre las principales herramientas tenemos las siguientes:

Nombre	Características
Ping	Herramienta manual que sirve para verificar conectividad de un equipo en la red
Dig	Herramienta encargada de hallar los DNS, para ayuda en la resolución de dns de las diferentes páginas web
Nmap	Herramienta poderosa para realizar varios procesos como encontrar puertos o servicios abiertos en servidores, descubrimiento de IPs activos en una red, etc.
ZenMap	Herramienta gráfica del Nmap
Netcat	La navaja suiza para supervisar el tráfico de red, tiene opciones de sniffer, abrir, escuchar los puertos TCP y UDP
tcpdump	Herramienta snnifer en modo texto para revisar tráfico de una red
Wireshark	Herramienta gráfica del Tcpdum
cupp	Herramienta para generación de diccionarios a medida.
crunch	Generador de diccionarios.

Tabla 4.-Herramientas manuales para Pentesting (fuente propia)

Podemos encontrar herramientas que vienen dentro de diferentes suites para realizar los análisis a las diferentes secciones que integran la infraestructura a ser auditada, muchos de ellos los podemos encontrar en modo Open Source como Kali o también en herramientas de pago como Acunetix, también se hará uso de las guías para las diferentes pruebas de pruebas como OWASP que se utilizará para la revisión de aplicaciones web, OFFENSIVE SECURITY, Penetration Testing Framework 0.59 que nos proporcionan guías para la recolección de información las mismas que serán aplicadas en los diferentes tareas para validar los controles que la Metodología OSSTMM requiere como herramientas manuales de revisión, por lo que para este trabajo de pentesting se utilizara herramientas automatizadas, complementadas con herramientas de chequeos manuales. En la mayor parte de la evaluación se hará uso de herramientas open source y se probara con algunas herramientas especializadas de pago.

2.6 EVALUACIÓN O REALIZACIÓN DEL PROYECTO MEDIANTE EL ETHICAL HACKING

Para la realización práctica del pentesting tenemos que realizar la revisión previa del estado de seguridad y como se encuentra estructurado al momento la infraestructura de la institución, así como definimos el análisis de riesgo para los activos.

2.6.1 Mapa de la seguridad UPS (confidencial)

La seguridad informática es un componente fundamental para la seguridad de la información institucional por lo que se necesita diferenciar los diferentes activos que intervienen dentro de la infraestructura para dar los diferentes servicios a los usuarios:

Seguridad en red de datos: En esta sección la seguridad se centra en aquellos equipos de red que permiten protegerla de comunicaciones o accesos no autorizados a determinados servicios e información confidencial. Los elementos que ofrecen este tipo de seguridad en la red son los firewalls, proxy, switches de capa tres, estando también la red inalámbrica ya que implica un gran riesgo en la seguridad de la infraestructura

Seguridad en ordenadores: En esta sección se tiene lo que concierne a la seguridad en estaciones de trabajo, equipos portátiles, y la seguridad de los servidores instalados en la red. El enfoque principal está en los equipos que trabajan como servidores, y en donde se maneja información crítica para los procesos de la Universidad.

Seguridad física: Esta sección comprende la seguridad en las oficinas, en los cuartos de comunicaciones y datacenter donde se encuentran los servidores. En esta área los aspectos críticos son los controles de seguridad en el acceso a equipos, también factores que puedan afectar la integridad y disponibilidad de ellos como equipos para climatización, sensores, etc.

Seguridad en aplicaciones: Esta es una de las secciones más críticas, y se encuentra separada en tres diferentes áreas, una de ellas son las aplicaciones desarrolladas en la Universidad, otra son los sistemas operativos instalados en servidores y demás equipos de trabajo, y por último están las bases de datos donde se administra toda la información confidencial de la Universidad.

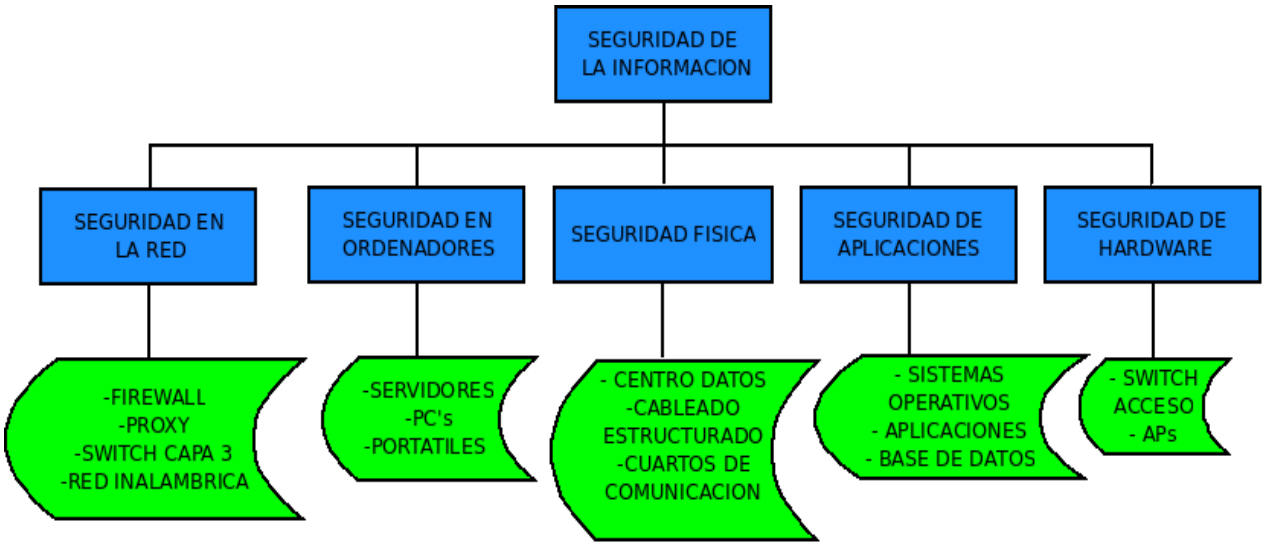


Gráfico 6.- Seguridad Informática de la Institución (confidencial)

Fuente: Elaboración Propia

Seguridad en hardware: Esta área cubre todos los equipos activos utilizados para interconectar los distintos segmentos de red y que no son un factor muy críticas en la prestación de seguridad en la red, como son los switchs de acceso o capa dos.

Uno de los principales problemas de seguridad está dado por los usuarios entre ellos los administradores de activos que muchas veces participan únicamente como usuario saltándose ciertos parámetros de seguridad que falta de conocimiento o por

negligencia hacen uso de los sistemas operativos y activos sin la seguridad correcta pudiendo ocasionar consecuencias graves para la información institucional y a la integridad de ellos.

2.6.2 Análisis de Variables

La necesidad de definir una metodología para realizar el diagnóstico de la seguridad en la red de datos de la Universidad, desde el punto de vista de ingeniería conlleva a analizar unas variables que son la base para el desarrollo de la presente investigación, estas son y representan las amenazas, vulnerabilidades y los riesgos asociados a los activos en la red.

EXPOSICIÓN DEL ACTIVO

En la realización del análisis de riesgos frente a la exposición del activo es el alcance que puede tener sobre los posibles daños que pueda causar la combinación de una amenaza y una vulnerabilidad de un activo se clasifica con los siguientes criterios:

NIVEL DE EXPOSICION DEL ACTIVO	
Pérdida grave o total del activo	ALTA
Pérdida limitada o moderada	MEDIA
Pérdida menos o no hay pérdida	BAJA

Tabla 5.-Nivel exposición activo (fuente propia)

NIVEL DE IMPACTO

Es la repercusión negativa que acarrea la pérdida de un activo dentro de la institución por la explotación de la vulnerabilidad o ejecución de la amenaza, se clasifica por:

NIVEL DE IMPACTO					
Tipo de Activo	ALTO	3	Impacto MEDIO	Impacto ALTO	Impacto ALTO
	MEDIO	2	Impacto BAJO	Impacto MEDIO	Impacto ALTO
	BAJO	1	Impacto BAJO	Impacto BAJO	Impacto MEDIO
			1	2	3
			BAJO	MEDIO	ALTO
			NIVEL DE EXPOSICION		

Tabla 6.-Nivel de impacto (fuente propia)

PROBABILIDAD DE LA AMENAZA

Hace referencia a la probabilidad de que una amenaza se ejecute aprovechándose de una vulnerabilidad en el activo. Su clasificación:

- Alta.- los factores para que se ejecute esa amenaza es fácil para su explotación y no requiere de un alto conocimiento técnico.
- Media.- los factores desencadenante de la amenaza es un poco más complejo, pero no necesita de privilegios de acceso especiales ni de un conocimiento técnico alto.
- Bajo.- para que se ejecute esta amenaza se requiere conocimientos técnicos altos y privilegios de accesos especiales

CRITERIOS DE PROBABILIDAD DE LA AMENAZA
ALTA
- Ejecutable remotamente - Los privilegios de acceso son anónimos - Método de explotación publicado en Internet - Requiere de pocos conocimientos técnicos para ejecutar la amenaza - Las condiciones son favorables para que se ejecute la amenaza
MEDIA
- No puede ejecutarse remotamente - Los privilegios de acceso son de usuario - El método de explotación no está publicado en Internet - Requiere de especialistas para que pueda ejecutar la amenaza - Las condiciones no favorecen la ejecución de la amenaza - Sin posibilidad de ejecutar el ataque a la vulnerabilidad de forma automática -Incendio en cuartos de comunicación de acceso -Robo de Aps
BAJA
- Su ejecución es imposible de forma externa - Los privilegios de acceso son de administradores y especiales - Método de explotación no publicado en Internet - Los conocimientos técnicos del atacante son altos para explotar la vulnerabilidad - Las condiciones no favorecen la ejecución de la amenaza - Sin posibilidad de ejecutar el ataque a la vulnerabilidad de forma automática

Tabla 7.-Criterios de probabilidad de amenaza (fuente propia)

NIVEL DE RIESGO

Es el posible daño que puede generar por la efectivización de la amenaza aprovechándose de una vulnerabilidad, por lo que las redes de datos de la Universidad Politécnica Salesiana se encuentran expuestas a varias amenazas como todas las redes de datos a nivel mundial, por lo que están asociados a un riesgo de dos tipos de orígenes los mismos que son:

- Naturales.- son todos los riesgos que se generan por fenómenos naturales o ambientales como terremotos, inundaciones, etc. Para los cuales se debe estar correctamente protegido mediante construcciones civiles apropiadas por la infraestructura de telecomunicaciones.
- Técnicas.- son los riesgos que se producen por intervención del personal técnico los cuales generalmente pueden ser producidos por fallos en la configuración de equipos y aplicaciones

La existencia de un riesgo está determinado por la presencia de al menos una amenaza y una vulnerabilidad, y puede ser interpretado por la siguiente ecuación:

RIESGO = AMENAZA × VULNERABILIDAD

Para poder hallar el nivel de riesgo de un activo es necesario conocer todos los factores que en el intervienen: nivel de exposición del activo, nivel de impacto según clasificación de activo y la probabilidad de ocurrencia de una amenaza.

CLASIFICACION DEL RIESGO					
IMPACTO	ALTO	3	Riesgo MEDIO	Riesgo ALTO	Riesgo ALTO
	MEDIO	2	Riesgo BAJO	Riesgo MEDIO	Riesgo ALTO
	BAJO	1	Riesgo BAJO	Riesgo BAJO	Riesgo MEDIO
			1	2	3
			BAJO	MEDIO	ALTO
			NIVEL DE PROBABILIDAD		

Tabla 8.-Clasificación del riesgo (fuente propia)

El nivel de riesgo de un activo puede ser representado por la fórmula

$$Nivelderiesgo = \sum \frac{Clasificaciódelriesgo}{Cantidaddeamenazas}$$

2.6.2 Ámbito y limitación de OSSTMM

En el documento de metodología para el testeo de seguridad se define como un conjunto de reglas y lineamientos para CUANDO, QUE y CUALES eventos serán revisados y dependiendo de los privilegios de acceso, objetivos y los resultados asociados al pentesting.

La presente metodología para diagnóstico de la seguridad informática se encuentra limitada al diagnóstico en los activos dentro de la categoría de servidores, firewall, Proxy, switches de capa 3 y red inalámbrica, que hace parte de la red de datos de la Universidad Politécnica Salesiana en su campus el Vecino.

La metodología OSSTMM mantiene el presente esquema para la verificación y revisión de las vulnerabilidades respecto a los diferentes activos:

- Levantamiento de información del activo según el canal
- Análisis de vulnerabilidades del activo
- Evaluación de riesgos
- Informe final

LEVANTAMIENTO DE LA INFORMACIÓN

Esta información valida todos los aspectos relacionados con un activo, sus interactores y características intrínsecas de su comportamiento frente a todos los canales del OSSTMM, con la finalidad de obtener el máximo de información para poder evaluar la seguridad frente a la confidencialidad, disponibilidad, autenticidad y el no repudio del activo, precautelando la información institucional como su valor institucional.

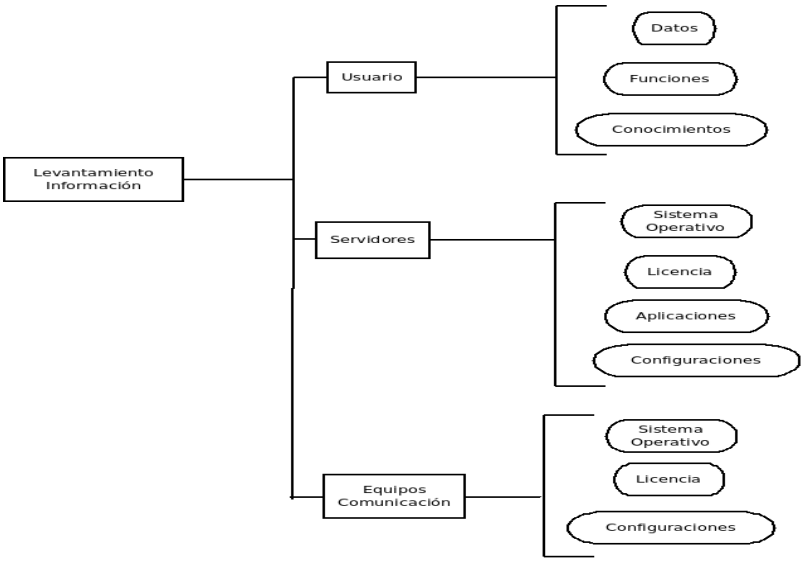


Gráfico 7.- Recolección de Información de activos

Fuente: Elaboración propia

ANÁLISIS DE VULNERABILIDADES

En esta fase se realizara la revisión, enumeración, comprobación y verificación de vulnerabilidades de los activos de la institución según los módulos revisados para cada uno de los canales de estudio valorando tres aspectos importantes de que pueden afectar a la información acceso, servicio y autenticación dentro de la red datos

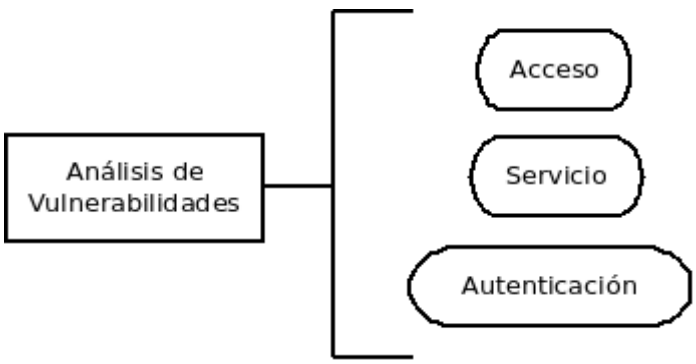


Gráfico 8.- Análisis de vulnerabilidades del activo

Fuente: Elaboración Propia

EVALUACIÓN DE RIESGOS

Fase donde se hace énfasis a los riesgos que representan las vulnerabilidades encontradas en cada uno de los activos estudiados de la infraestructura de la institución, estos representan:

- Riesgos técnicos.- hace referencia a calidad del activo frente a los aspectos de configuración, desconocimientos técnicos, falta de mantenimiento y evolución de la tecnología
- Robo de información.- es importante ya que afecta directamente a la triada de la información como es integridad, confidencialidad y disponibilidad que brinda el mismo en la institución
- Riesgos económicos.- son las incertidumbres que causan con el factor económico por el rendimiento de la inversión tecnológica

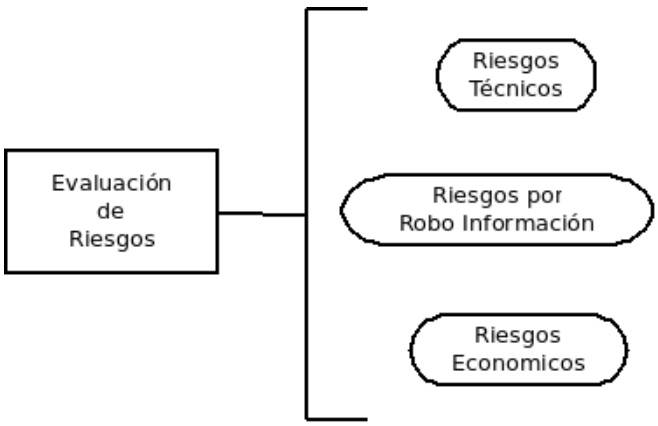


Gráfico 9.- Análisis de riesgos

Fuente: Elaboración propia

ELABORACIÓN DE REPORTES

Es la fase donde se plasma por escrito los datos hallazgos encontrados.

A continuación se realiza un mapeo donde se puede determinar cómo afectan las limitaciones frente a la seguridad operativa en cada una de las categorías que pueden ser auditados los activos.

CATEGORIA	SEGURIDAD OPERATIVA	LIMITACIONES
OPERACIONES	Visibilidad	Exposición
	Acceso	Vulnerabilidades

<table>
<tr><td colspan="2"></td><td>Confianza</td><td></td></tr>
<tr><td rowspan="6">CONTROLES</td><td rowspan="5">Clase A
Interactivos</td><td>Autenticación</td><td rowspan="5">Debilidades</td></tr>
<tr><td>Indemnización</td></tr>
<tr><td>Resistencia</td></tr>
<tr><td>Subyugación</td></tr>
<tr><td>Continuidad</td></tr>
<tr><td rowspan="5">Clase B
Procesos</td><td>No repudio</td><td rowspan="5">Preocupación</td></tr>
<tr><td>Confidencialidad</td></tr>
<tr><td>Privacidad</td></tr>
<tr><td>Integridad</td></tr>
<tr><td>Alarma</td></tr>
<tr><td colspan="4">Anomalías</td></tr>
</table>

Tabla 9.-Limitaciones del OSSTMM – Fuente OSSTMM v3, (Pag29)

2.6.3 Análisis y pruebas con OSSTMM para la infraestructura de la Universidad Politécnica Salesiana

Para realizar el pentesting dentro de la Universidad en base a la metodología del OSSTMM se procede a definir las tareas que se realizarán en los diferentes métodos para validar en cada uno de los canales que la metodología evalúa a la infraestructura en su conjunto para ello de las tareas y módulos que presentan la metodología se escogieron los siguientes que se desarrollaran a lo largo del pentesting y que se apegan más para dar con el objetivo de este trabajo que es el de evaluar la seguridad de la infraestructura de la Universidad Politécnica Salesiana en las fechas en la que se realiza la tarea de recolección y análisis de la información, lo cual podemos ver en el ANEXO 2

2.6.4 Ambientes de pruebas del revisor frente a la infraestructura

El ambiente de pruebas hace relación a la visibilidad del revisor frente a la infraestructura, desde las siguientes ubicaciones que el revisor pueda examinar.

Gráfico 10.- Pruebas del revisor visibilidad outsider

Fuente: Elaboración propia

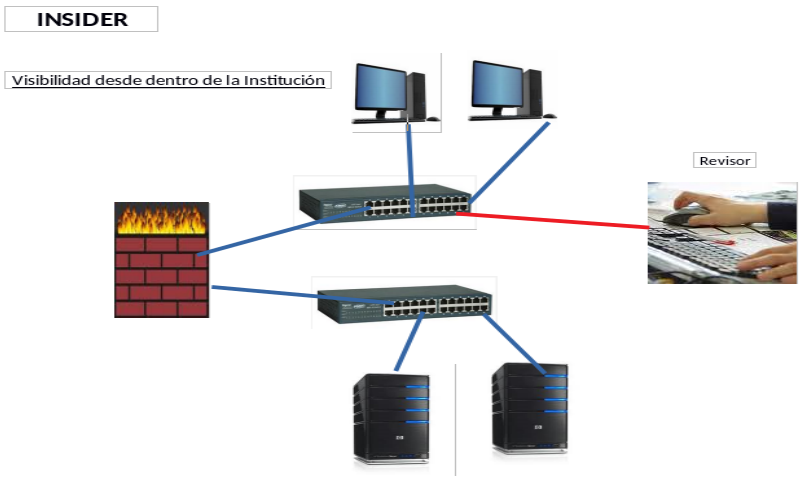


Gráfico 11.- Pruebas del revisor visibilidad insider

Fuente: Elaboración Propia

2.6.5 Formatos para la recolección de la información

Para el levantamiento de información es necesario validar en la revisión a los usuarios manteniendo como objetivo el llegar a conocer su nivel de conocimiento sobre informática y seguridad de la información

DATOS USUARIO	CARGO	TIEMPO DE TRABAJO	TITULO PROFESIONAL	CONOCIMIENTOS SOBRE INFORMATICA	CONOCIMEINTO DE SEGURIDAD INFORMATICA	CONOCIMIENTOS EN SEGURIDAD DE LA INFORMACION	CONOCE SOBRE LA POLITICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACION	QUE PROCEDIEMNTO DE SEGURIDAD DE LA INFORMACION UTILIZA			A TENIDO CAPACITACION EN SEGURIDAD DE LA INFORMACION

Tabla 10.-Encuesta usuarios (fuente propia)

Herramientas: entrevistas y cuestionarios.
Análisis: Las reglas deben concordar con la política de seguridad informática de la Universidad
Revisión: Monitoreo, procedimientos su documentación y actualizaciones de reglas

Servidores.- nuestro objetivo es conocer las aplicaciones y su nivel de seguridad que son aplicados según su sensibilidad, así como el entorno físico donde están desplegados los equipos. Por lo que se aplicara la siguiente plantilla para obtener la información

Server	IP	MAC	Aplicaciones	Sistema Operativo	Puertos Abiertos	Puertos Cerrados	Puertos Filtrados	Ataques de Fuerza Bruta	Vulnerabilidades	Cuarto de Comunicación	Cableado Estructurado	Acceso seguro a ubicación

Tabla 11.-Revisión servidores (fuente propia)

Herramientas: ping, dnsmap, dnsenum, theharvester, NMAP, ACUNETIX, OWASP, Metaesploit Framework
Análisis: Las reglas deben concordar con la política de seguridad informática de la Universidad
Revisión: Monitoreo, documentación y actualizaciones de reglas

Equipos de comunicación.- se necesita hacer la búsqueda de información para recabar la información del filtrado de tráfico hacia y desde la red a Internet, Lan, Wan. Es necesario también conocer el entorno físico donde se encuentran instalados los equipos. Por lo que se utilizara la siguiente plantilla

Equipo	IP	MAC	Accesibilidad	Red Oculta	Puertos Abiertos		Puertos Filtrados	Bloqueos de Direcciones	Ataques de Fuerza bruta	Vulnerabilidades	Cuarto de Comunicación	Cableado Estructurado	Acceso hacia el equipo

Tabla 12.-Revisión equipos comunicación (fuente propia)

Herramienta: NMAP, ping, traceroute,
Análisis: Las reglas deben concordar con la política de seguridad informática de la Universidad
Revisión: Monitoreo, documentación y actualizaciones de reglas

Switch Capa Tres.- se busca identificar los problemas de seguridad asociados a la segmentación por VLANs, las vulnerabilidades del switch como ataques de ARP spoofing, ataques en protocolos VTP, CDP, STP, etc.

Equipo	IP	MAC	Accesibilidad	VLAN´s	Pruebas de ARP Spoofing	Cuarto de comunicaciones	Cableado estrcuturado

Tabla 13.-Revisión switch capa 3 (fuente propia)

Herramienta: Ettercap, Wireshark, Yersinia
Análisis: Las reglas deben concordar con la política de seguridad informática de la Universidad
Revisión: Monitoreo, documentación y actualizaciones de reglas

Seguridad Inalámbrica.- es importante su análisis debido que la red está expuesta físicamente a cualquier persona dentro del campo de cobertura, por lo que es necesario revisar la seguridad física y lógica al acceso a los diferentes AP's, su cifrado y método de contención de ingreso, mapeo de la red y acceso al usuario administrador del AP.

Equipo	IP	MAC	Redes Encontradas	Encriptación	Método de acceso	Seguridad Física de APs	Visibilidad

Tabla 14.-Revisión red inalámbrica (fuente propia)

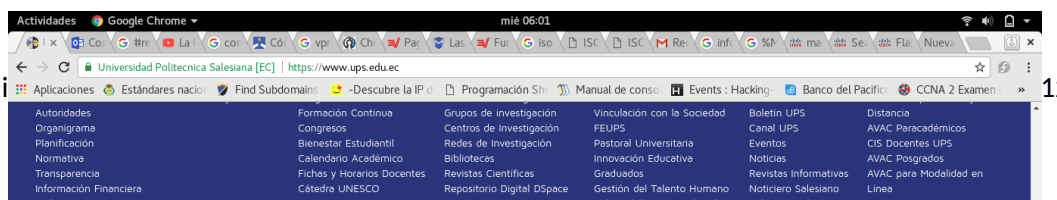
Herramienta: Wireshark, aircrack, NetStumbler
Análisis: Las reglas deben concordar con la política de seguridad informática de la Universidad
Revisión: Monitoreo, documentación de APs y actualizaciones

2.7 FASE 1: RECONOCIMIENTO

RECOLECCION DE INFORMACIÓN PÚBLICA

En la fase de reconocimiento, se recolecta toda la información pública disponible en internet sobre ups.edu.ec, el fin es recopilar la mayor cantidad de información desde visibilidad outsider como insider de la institución. Para ello se utilizó diferentes métodos y herramientas.

Método: **FOOTPRINTING**	Observaciones: **Descubrimiento pasivo**
Herramienta: **Google**	Visibilidad: **Outsider**



Entre la información más relevante que se encuentra podemos hallar las siguientes de las autoridades y direcciones de ubicación de las sedes:

EMAIL			
email	**Usuario**	**Cargo**	**Teléfono y extensiones**
jhxxx@ups.edu.ec	Jxxx Hxxx Gxxx	Rector	28xxx - 1100
ltxxx@ups.edu.ec	Lxxx Txxx Pxxx	Vicerrector Académico General	28xxx - 1200
fpxxx@ups.edu.ec	Fxxx Pxxx Axxx	Vicerrector Docente	28xxx - 1106
jpxxx@ups.edu.ec	Jxxx Pxxx Sxxx Gxxx	Vicerrector de Investigación	28xxx - 1101
cvxxx@ups.edu.ec	Céxxx Vxxx Vxxx	Vicerrector sede Cuenca	28xxx - 1167
jjxxx@ups.edu.ec	Jxxx Jxxx Bxxx	Vicerrector sede Quito	39xxx – 2208
abxxx@ups.edu.ec	Axxx Bxxx Gxxx	Vicerrector sede Guayaquil	04xxx - 4499
dpxxx@ups.edu.ec	Jxxx Dxxx Pxxx Rxxx	Vicerrector Posgrados	28xxx - 1120

Tabla 15.-Información en página www.ups.edu.ec - (fuente propia)

Esta es una información valiosa con la finalidad de seguir investigando para poder hacer a futuro un ataque de ingeniería social.

Las principales fuentes de información pública donde se puede encontrar la información acerca de la Universidad son las siguientes:

Descripción	Url
Facebook	https://www.facebook.com/ViveUPS/
Twitter	https://twitter.com/upsalesiana
Youtube	https://www.youtube.com/watch?v=IKrps2np-9Q
Página Web	https://ups.edu.ec
Linkedin	https://www.linkedin.com/school/universidad-politecnica-salesiana/

Tabla 16.-Fuentes públicos de información de la Universidad Politécnica Salesiana (fuente propia)

Método: **FOOTPRINTING**	Observaciones: **Descubrimiento pasivo**
Herramienta: **WHOIS, DMITRY, www.whois.com**	Visibilidad: **Outsider**

En el uso de estas herramientas se presenta algo curioso al realizar la búsqueda de forma manual en primer lugar no se encontró información referente a la universidad, luego al hacer uso de la herramienta dmitry se presenta información de la IP pública y del ISP o proveedor del servicio de internet, mientras que cuando se utilizó la herramienta www.whois.com de internet se obtuvo información del contacto técnico y comercial de la institución con las direcciones obtenidas luego se podrá hacer más consultas.

1 Herramienta: **whois**

[root@localhost]# whois www.ups.edu.ec

[Preguntando whois.nic.ec]

[No se puede conectar al anfitrión remoto]

[root@]# whois ups.edu.ec

[Preguntando whois.nic.ec]

[No se puede conectar al anfitrión remoto]

2 Herramienta: **dmitry**

HostIP:xxx.xxx.xxx.75

HostName:www.ups.edu.ec

Gathered Inet-whois information for xxx.xxx.xxx..75

---

inetnum: xxx.xxx.xxx/20

status: allocated

aut-num: N/A

owner: Txxx S.A

ownerid: EC-TESA-LACNIC

responsible: Txxx S. A.

address: Kxxxy Nxxxte MZ, 109,

address: 59342 - Guayaquil -

country: EC

phone: +593 4 268xxxx5 [101]

owner-c: TRS4

tech-c: SEL

abuse-c: SEL

inetrev: xxx.xxx.xxx./22

nserver: SRV1.TExxxET.NET

nsstat: 20180414 AA

9nslastaa: 20180414

nserver: SRV2.TExxxxET.NET

nsstat: 20180414 AA

nslastaa: 20180414

created: 20041021

changed: 20041021

nic-hdl: SEL

person: Cxxxx Mxxxx

e-mail: networking@TExxxxET.EC

address: Kennedy Norte MZ, 109, Solar 21

address: 59342 - Guayaquil -

country: EC

phone: +593 42xxxxx55 [4601]

created: 20021004

changed: 20170323

nic-hdl: TRS4

person: Cxxx Mxxx

e-mail: networking@TExxxxET.EC

address: Kennedy Norte MZ 109 SL 21, ,

address: - Guayaquil - GU

country: EC

phone: +593 4 26xxx5 [4601]

created: 20111025

changed: 20140602

% whois.lacnic.net accepts only direct match queries.

% Types of queries are: POCs, ownerid, CIDR blocks, IP

% and AS numbers.

Gathered Inic-whois information for ups.edu.ec

Unable to connect: Socket Connect Error

ERROR: Connection to InicWhois Server ec.whois-servers.net failed

3 Herramienta **www.whois.com**

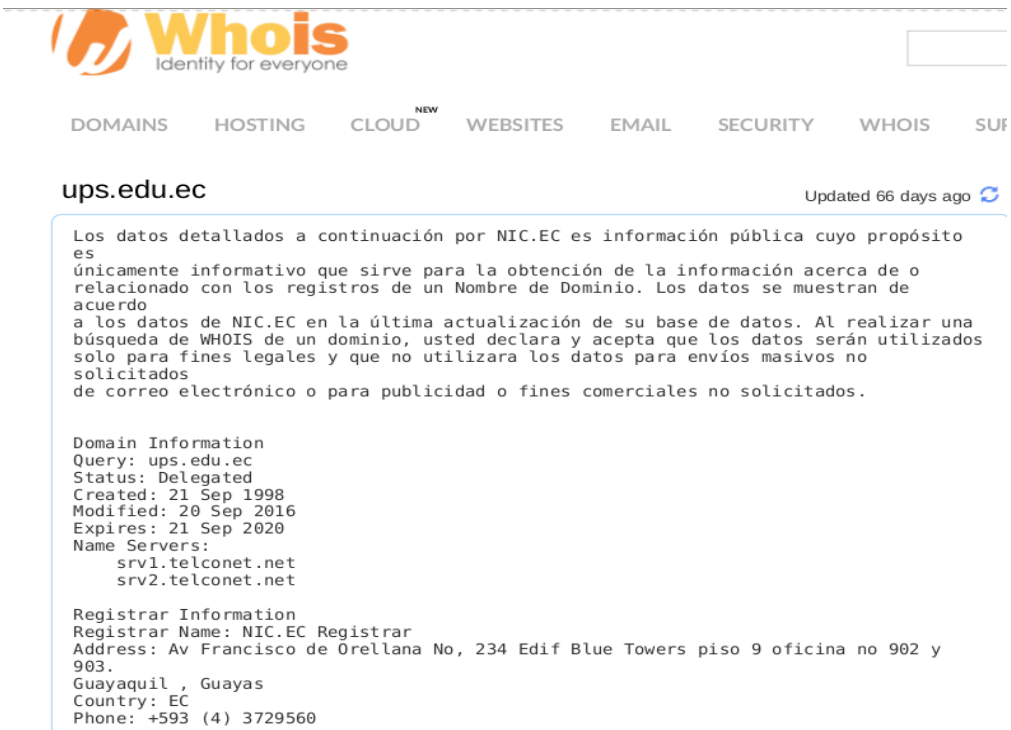


Gráfico 13.- Información correspondiente al DNS de la UPS

Fuente: www.whois.com

La información encontrada es la siguiente:

CUENTA	OBSERVACION
axxx@ups.edu.ec	Contacto técnico
xxxx@ups.edu.ec	Contacto Financiero

Tabla 17.-Información encontrada en www.whois.com (fuente propia)

Método: **FOOTPRINTING**	Observaciones: **Descubrimiento pasivo**
Herramienta: **www.monitis.com/traceroute/**	Visibilidad: **Outsider**

Con esta herramienta se puede conocer que el servicio de hosting es realizado por una empresa propia de ECUADOR, se llega en 20 saltos

Método: **FOOTPRINTING**	Observaciones: **Descubrimiento pasivo**
Herramienta: **Kali - TheHarvester**	Visibilidad: **Outside**

Esta herramienta ayuda a encontrar direcciones de correo institucionales, nombres de subdominios que se encuentran en diferentes fuentes públicas.

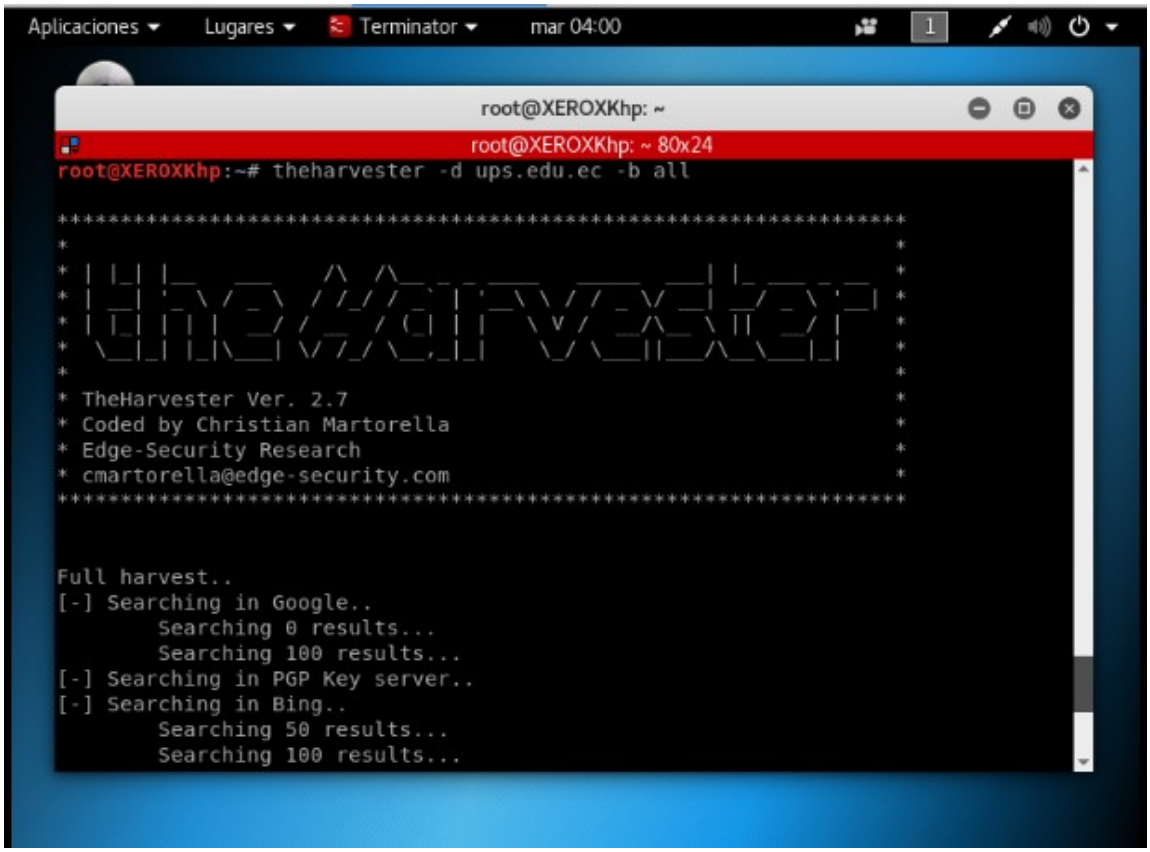


Gráfico 14.- Información con TheHarvester

Fuente: Elaboración propia

Se obtuvo la siguiente información:

EMAIL		
email	**Usuario**	**Observación**
aaxxx@ups.edu.ec		
ajxxx@ups.edu.ec	xxx	coincide con whois
apxxx@ups.edu.ec		
cbxxx@ups.edu.ec		
clxxx@ups.edu.ec		
clxxx@ups.edu.ec		
cpxxx@est.ups.edu.ec		
ctxxx@ups.edu.ec		
dhxxx@ups.edu.ec		
ecxxx@ups.edu.ec		
eqxxx@ups.edu.ec		
erxxx@ups.edu.ec		
fpxxx@ups.edu.ec	xxx	coincide con página web
jpxxx@ups.edu.ec		
mmxxx@est.ups.edu.ec		
pbxxx@ups.edu.ec		
pcxxx@ups.edu.ec		
pxxxx43784-web-@ups.edu.ec		
pxxxx607883-web-@ups.edu.ec		
srxxx@ups.edu.ec		Asocia a una cuenta de dirección administrativa en página web
svxxx@ups.edu.ec		Asocia a una cuenta de dirección administrativa en página web
svixxx@ups.edu.ec		Asocia a una cuenta de dirección administrativa en página web
wpxxx@ups.edu.ec		
DIRECCIONES RELACIONADAS		
IP	**NOMBRE SERVER**	
xxx,xxx.225.12	alexxx.ups.edu.ec	
xxx.xxx.89.77	altxxx.ups.edu.ec	
xxx.xxx.225.198	caxxx.ups.edu.ec	
xxx.xxx.243.235	dsxxx.ups.edu.ec	
xxx.xxx.42.76	idxxx.ups.edu.ec	
xxx.xxx.89.77	lagxxx.ups.edu.ec	
xxx.xxx..223.195	quixxx.ups.edu.ec	
xxx.xxx..225.194	servxxx.ups.edu.ec	
xxx.xxx.199.89	virxxx.ups.edu.ec	
xxx.xxx.89.75	www.ups.edu.ec	
HOST VIRTUALES		
xxx.xxx.225.198	www.ups.edu.ec	
xxx.xxx.199.89	virxxx.ups.edu.ec	

xxx.xxx.89.75	www.ups.edu.ec	

Tabla 18.-Información encontrada con TheHarvester (fuente propia)

La información encontrada es valiosa con la finalidad de seguir investigando para poder hacer a futuro un ataque de ingeniería social, revisión de servicios para futuros ataques.

Método: **FOOTPRINTING**	Observaciones: **Descubrimiento activo**
Herramienta: **FOCA**	Visibilidad: **Outsider**

Esta herramienta provee mayor información, sobre usuarios y documentos que se hallan expuestos a la información pública, de la revisión realizada se encuentran información de planes de mejoramiento de carreras, información de colaboradores, dominios relacionados a ups.edu.ec,

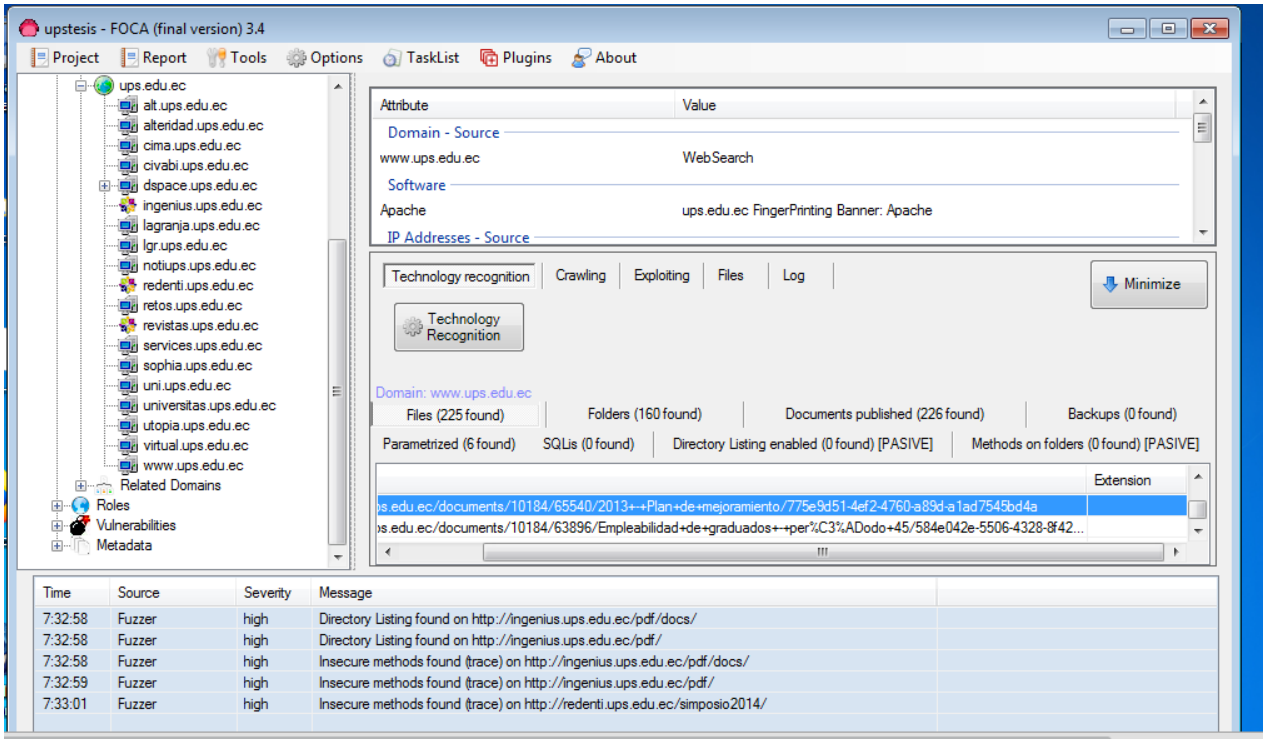


Gráfico 15.- Información de FOCA

Fuente:

Foca nos ayuda a revisar posibles vulnerabilidades con las que podemos luego hacer comprobaciones manuales para confirmar el nivel de vulnerabilidades presentes:

La información encontrada mediante esta herramienta podemos destacar la siguiente:

REDES		
RED	**IP**	**Observación**
xxx.xxx.0.0	xxx.xxx.199.89	Desplegado NGINX, pto 80
xxx.xxx.0.0	xxx.xxx.55.110	Desplegado en Apache/2.2.15 (CentOS), pto 80
xxx.xxx.0.0	xxx.xxx.225.11	Pto HTTPS
	xxx.xxx.243.235	Desplegado Apache, ptos 80 y 443
xxx.xxx.89.0	xxx.xxx.89.75	Desplegado en Apache, ptos 80 y 443, varios subdominios
DOMINIOS		
RED	**IP**	**Observación**
altxxx.ups.edu.ec	xxx.xxx.89.75	Desplegado en Apache, ptos 80 y 443
altexxx.ups.edu.ec	xxx.xxx.89.77	Desplegado en Apache/2.2.15 (CentOS), ptos 80 y 443
cimxxx.ups.edu.ec	xxx.xxx.89.75	Desplegado en Apache, ptos 80 y 443
cibxxx.ups.edu.ec	xxx.xxx.89.75	Desplegado en Apache, ptos 80 y 443
dspxxx.ups.edu.ec	xxx.xxx.243.235	Desplegado en Apache, ptos 80 y 443
ingxxx.ups.edu.ec	xxx.xxx.89.77	Desplegado en Apache/2.2.15 (CentOS), ptos 80 y 443
lagxxx.ups.edu.ec	xxx.xxx.89.77	Desplegado en Apache/2.2.15 (CentOS), ptos 80 y 443
lgrxxx.ups.edu.ec	xxx.xxx.89.75	Desplegado en Apache, ptos 80 y 443
notxxx.ups.edu.ec	xxx.xxx.89.75	Desplegado en Apache, ptos 80 y 443
redxxx.ups.edu.ec	xxx.xxx.55.110	Desplegado en Apache/2.2.15 (CentOS), ptos 80 y 443
retxxx.ups.edu.ec	xxx.xxx.89.75	Desplegado en Apache/2.2.15 (CentOS), ptos 80 y 443
revxxx.ups.edu.ec	xxx.xxx.89.77	Desplegado en Apache/2.2.15 (CentOS), ptos 80 y 443
serxxx.ups.edu.ec	xxx.xxx.225.11	Desplegado en Apache/2.2.15 (CentOS), ptos 80 y 443
sopxxx.ups.edu.ec	xxx.xxx.89.77	Desplegado en Apache/2.2.15 (CentOS), ptos 80 y 443
unixxx.ups.edu.ec	xxx.xxx.89.75	Desplegado en Apache, ptos 80 y 443
univvxx.ups.edu.ec	xxx.xxx.89.77	Desplegado en Apache/2.2.15 (CentOS), ptos 80 y 443
utoxxx.ups.edu.ec	xxx.xxx.89.75	Desplegado en Apache, ptos 80 y 443
virtxxx.ups.edu.ec	xxx.xxx.199.89	Desplegado NGINX, pto 80
www.ups.edu.ec	xxx.xxx.89.75	Desplegado en Apache/2.2.15 (CentOS), ptos 80 y 443
VULNERABILIDADES		
EQUIPO	**TIPO**	**OBSERVACION**
xxx.ups.edu.ec	Lista Directorios	Realizar otras pruebas para su confirmación
ups.edu.ec	Métodos Inseguros	Realizar otras pruebas para su confirmación
xxx.ups.edu.ec	Métodos Inseguros	Realizar otras pruebas para su confirmación
xxx.ups.edu.ec	Métodos Inseguros	Realizar otras pruebas para su confirmación
xxx.ups.edu.ec	Métodos Inseguros	Realizar otras pruebas para su confirmación
DOCUMENTOS		
DOCUMENTOS	**TIPO**	**OBSERVACION**
varios	1116 documentos con formatos xls, doc, pdf	Son archivos que mantiene información sobre horarios de clase, planes de mejoras, cv de empleados, formularios de inscripción

Tabla 19.-Información obtenida con FOCA (fuente propia)

Método: **FOOTPRINTING**	Observaciones: **Descubrimiento pasivo**
Herramienta: **MALTEGO**	Visibilidad: **Outsider**

Herramienta que ayuda a registrar información de personas, correos y relaciones directas que se encuentran relacionadas con el dominio ups.edu.ec y la página www.ups.edu.ec por medio de transformaciones, es valiosa para luego poder generar diccionarios para ataques o utilizar ingeniería social para vulnerar la infraestructura.

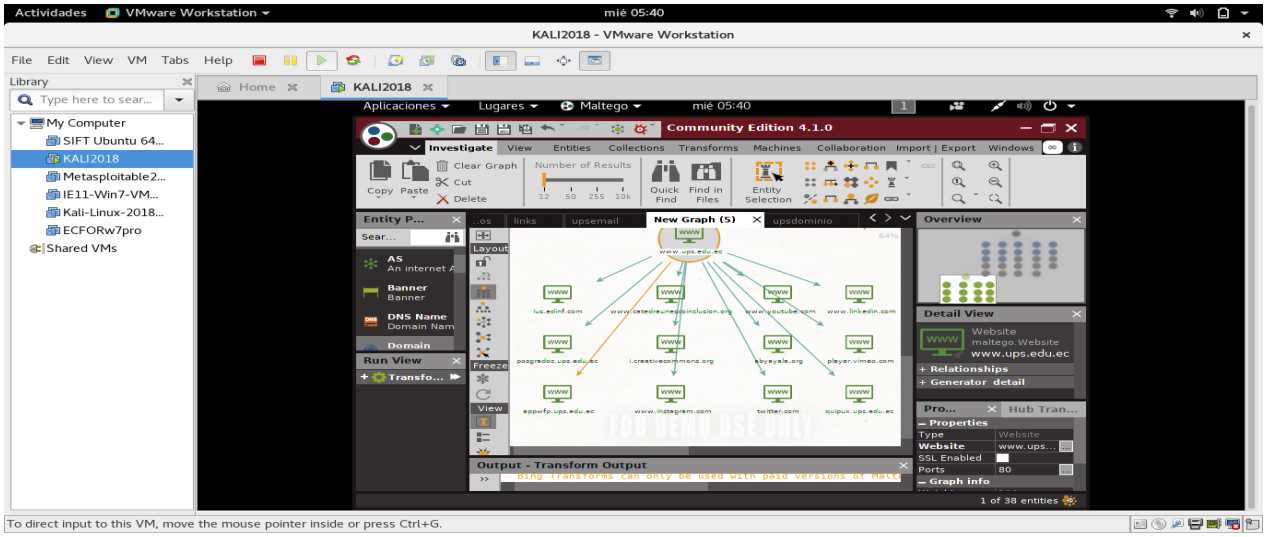


Gráfico 16.- Información de Maltego

Fuente:

La información nueva recuperada para poder hacer revisiones para recabar mayor información son las siguientes:

RELACIONES		
DOMINIO		**Observación**
ius.edinf.com		Red universal de universidades salesianas
twitter.com		Red social
www.youtube.com		Red social
www.universia.com.ec		Red educativa
abyayala.org		editorial
vimeo.com		Red social
www.instagram.com		Red social
i.creativecommons.org		
www.facebook.com		Red social
EMAILS		
CUENTA		**Observación**
jmxxx@ups.edu.ec		Docente universidad
caxxx@ups.edu.ec		Docente universidad
dhxxx@ups.edu.ec		Docente universidad
emxxx@ups.edu.ec		Docente universidad
bgxxx@ups.edu.ec		Docente universidad
mcxxx@ups.edu.ec		Docente universidad
rzxxx@ups.edu.ec		Docente universidad
start@ups.edu.ec		
PERSONAS		
NOMBRE	**CORREO**	**Observación**
PXX J	ajxxx@ups.edu.ec	Empleado universidad
Axxx Axxx	aaxxx@ups.edu.ec	Empleado universidad
Mxxx Vxxx Mxxx	mmxxx@ups.edu.ec	Empleado universidad
Wxxx	wpxxx@ups.edu.ec	Empleado universidad
Exxx	erxxx@ups.edu.ec	Empleado universidad
Cxxx		
Cxxx Axxx Lxxx Jxxx	clxxx@ups.edu.ec	Empleado universidad
Exxx Qxxx Pxxx	eqxxx@ups.edu.ec	Empleado universidad
Axxx Jxxx Pxxx Rxxx	apxxx@ups.edu.ec	Empleado universidad
Cxxx Bxxx	cbxxx@ups.edu.ec	Empleado universidad
Cxxx Axxx Lxxx Ixxx	clxxx@ups.edu.ec	Empleado universidad

Tabla 20.-Información encontrada con MALTEGO (fuente propia)

Método: **FINGERPRINTING (confidencial)**	Observaciones: **Descubrimiento pasivo**
Herramienta: **PING y NSLOOKUP**	Visibilidad: **Insider**

Para esta prueba se encontró un punto de red en una de las salas de conferencia donde nos entregó una IP de un servicio DHCP y se procedió a realizar pruebas insider a la red interno encontrando las siguientes novedades:

```
[root@localhost britop71]# ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted].3.34  netmask 255.255.255.128  broadcast [redacted].3.127
        inet6 fe80::3bd:350:db28:d345  prefixlen 64  scopeid 0x20<link>
        ether a4:4c:c8:4e:56:0a  txqueuelen 1000  (Ethernet)
        RX packets 3043790  bytes 3794201825 (3.5 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1479542  bytes 176164679 (168.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xef200000-ef220000
```

Gráfico 17.- Información IFCONFIG

Fuente: Elaboración propia

De

```
[root@localhost britop71]# ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted].3.34  netmask 255.255.255.128  broadcast [redacted].3.127
        inet6 fe80::3bd:350:db28:d345  prefixlen 64  scopeid 0x20<link>
        ether a4:4c:c8:4e:56:0a  txqueuelen 1000  (Ethernet)
        RX packets 3043790  bytes 3794201825 (3.5 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1479542  bytes 176164679 (168.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xef200000-ef220000
```

Gráfico 18.- Información de NSLOOKUP

Fuente: Elaboración propia

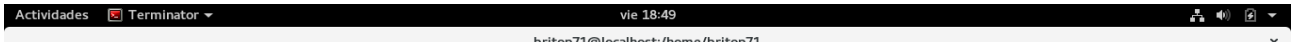
donde se pudo hallar la siguiente información

RELACIONES				
DOMINIO	**IP**	**PRUEBAS ICMP**		**Observación**
		PING	**TRACEROUTE**	
ups.edu.ec	xx.xxx.1.8	NO	NO	Servidor no responde
	xx.xxx.5.50	NO	NO	Servidor no responde
	xx.xxx.42.47	NO	NO	Servidor no responde
Servidor DNS	xx.xxx.1.157	NO	NO	Servidor no responde

Tabla 21.-Información insider de www.ups.edu.ec (fuente propia)

Método: **FOOTPRINTING - Red Inalámbrica (confidencial)**	Observaciones: **Descubrimiento activo**
Herramienta: **aircrack**	Visibilidad: **Insider**

Aircrack nos ayuda a realizar la auditoría a la red inalámbrica mediante el uso de una tarjeta inalámbrica que tiene la opción de trabajar en modo monitor para poder sniffear las redes desplegadas dentro del campus Vecino, para comenzar a revisar podemos



obtener las siguientes redes de la Universidad, como se puede visualizar en un AP se irradia varias redes

La información preliminar encontrada tenemos la siguiente:

REDES		
RED	**ENCRIPTACION**	**Observación**
UPS_EVxxx	WPA2 con PSK	
UPS_COxxx	WPA2 con PSK	
UPS_DOxxx	Open	Solicita para su acceso un portal cautivo
UPS_ESxxx	Open	Solicita para su acceso un portal cautivo
eduroam	WPA2 con MGT	

Tabla 22.-Información de la red inalámbrica (fuente propia)

2.8 FASE 2: ENUMERACIÓN:

En la fase de recolección de datos se pudo obtener correos institucionales, nombres de empleados, información sobre documentos públicos, datos del hosting, datos de APs y redes inalámbricas, etc.; información valiosa para poder continuar ingresando o conociendo a la infraestructura de forma más profunda.

Método: **ESCANEO DE PUERTOS (confidencial)**	Observaciones: **Descubrimiento activo**
Herramienta: **NMAP, dnsmap, dnsenum** comando: **nmap -sS -sV -O -f -iL serverext.txt -oN pruebasextups.txt** comando: **nmap -f -A -sV -O -f -iL serverext.txt -oN pruebasextupsf.txt**	Visibilidad: **Outsider**

Mediante la herramienta NMAP y los resultados antes obtenidos se pudo generar un listado de servidores que se descubrieron externamente para revisar la información de sus servicios, sistema operativo y puertos que están visibles, esta información nos ayudará a verificar y corroborar los resultados antes mostrados:

Gráfico 20.- Información de NMAP

Fuente: Elaboración propia

Luego de la ejecución del comando se pudo hallar la siguiente información ANEXO 3

Método: **ESCANEO DE PUERTOS (confidencial)**	Observaciones: **Descubrimiento activo**
Herramienta: **NMAP, dnsmap, dnsenum** comando: **nmap -sS -sV -O -f -iL serverint.txt -oN pruebasintups.txt** comando: **nmap -f -A -sV -O -f -iL serverint.txt -oN pruebasintups.txt**	Visibilidad: **Insider**

La información encontrada desde la red interna a la página web www.ups.edu.ec es la siguiente:

SERVIDORES						
DOMINIO	**IP**	**SISTEMA OPERATIVO**	**Revisión**			
			PTO	**SERVICIO**	**VERSION**	**Observación**
wxxx.ups.edu.ec	xxx.xxx.1.8		80/tcp	HTTP		OPEN unfiltered
			443/tcp	SSL/HTTPS		OPEN unfiltered
			67/udp	dhcps		filtered
			68/udp	dhcpc		filtered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
	xxx.xxx.5.50		2000/tcp	cisco-sccp		OPEN
			5060/tcp	sip		OPEN
			8008/tcp	http		OPEN
			3268/tcp	globalcatLDAP		OPEN
			3269/tcp	globalcatLDAPssl		OPEN
			3389/tcp	ms-wbt-server		OPEN
			49153/tcp	unknown		OPEN
			49154/tcp	unknown		OPEN
			49155/tcp	unknown		OPEN
			49158/tcp	unknown		OPEN
			49159/tcp	unknown		OPEN
	xxx.xxx.42.47		80/tcp	http		OPEN unfiltered
			443/tcp	https		OPEN unfiltered

Tabla 23.-Información de wxx.ups.edu.ec con NMAP (fuente propia)

En base al descubrimiento de la IP de wxxx.ups.edu.ec, se procede a realizar otras b úsquedas de servidores internos obteniendo los siguientes resultados:

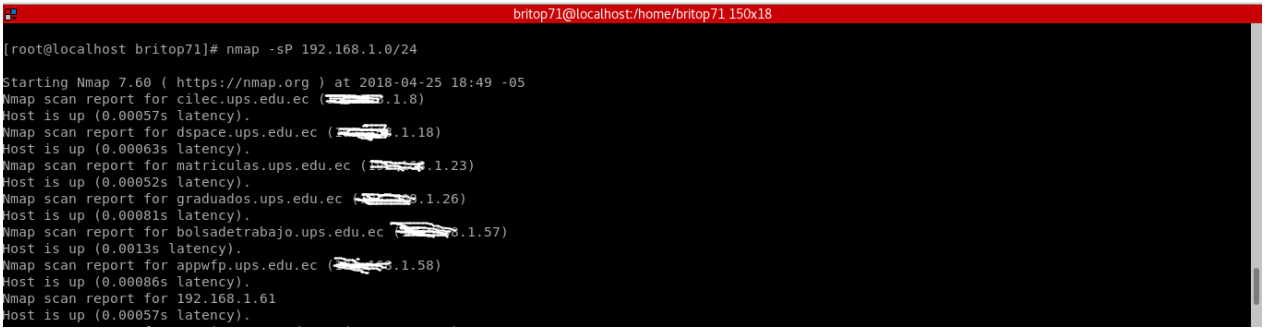


Gráfico 21.- Información de Ping Sweep

Fuente: Elaboración propia

Haciendo uso del nmap se obtuvo la siguiente información de los servidores internos que se presentan en el ANEXO 4.

Cabe recalcar que cuando se realiza una inspección en la red inalámbrica nos da como sistema operativo Cisco 2500-series Wireless LAN Controller (AireOS), Cisco 2500- or 5500-series Wireless Controller.

El resultado de puertos y servicios obtenidos en la infraestructura mediante el uso de nmap se puede observar en el ANEXO 5

2.8 FASE 3: REVISION VULNERABILIDADES

En la fase anterior se pudo recabar información sobre los servicios desplegados por la infraestructura, ahora tenemos que proceder a realizar la revisión de posibles vulnerabilidades que se encuentran presente en su puerta de ingreso institucional que es la página web e intranet, mediante herramientas automáticas y comprobaciones manuales

Método: **COMPROBACION DE VULNERABILIDADES (confidencial)**	Observaciones: **Descubrimiento activo**
Herramienta: **ACUNETIX**	Visibilidad: **Outsider**

Esta herramienta nos permite hallar las vulnerabilidades que se encuentran implementadas en la página web www.ups.edu.ec, entrega un reporte de OWASP TOP 2017, es una herramienta de pago cuyo costo es alto y en su versión de prueba no entrega datos precisos donde se encuentra la vulnerabilidad dentro de la página, pero si nos ayuda a sondear como se encuentra en general la misma.

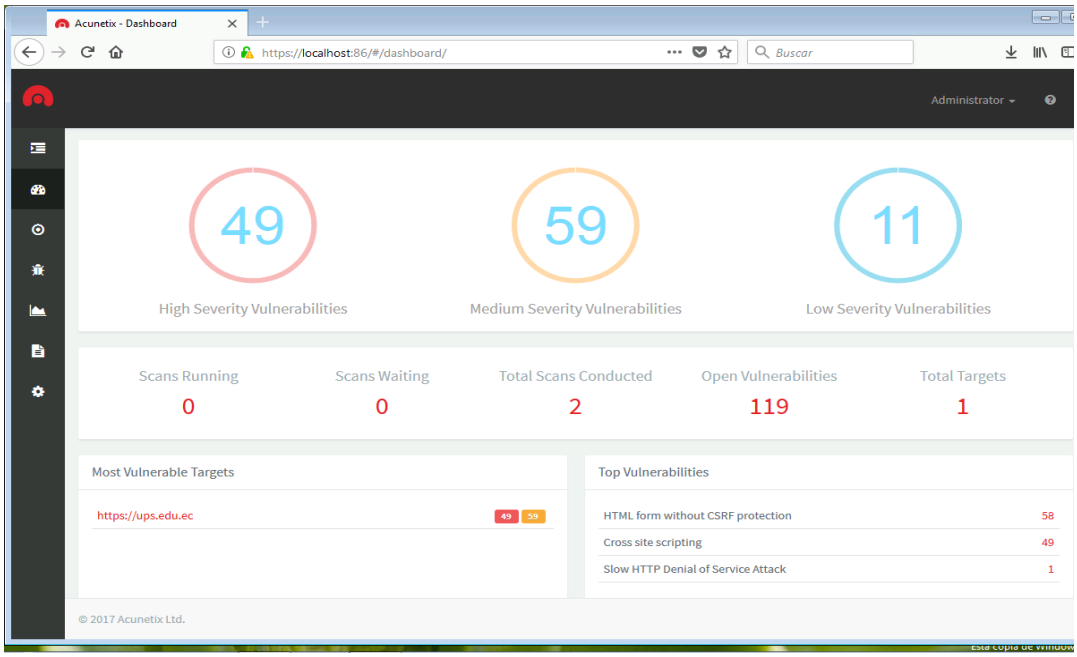


Gráfico 22.- Información ACUNETIX outsider

Fuente: Elaboración propia

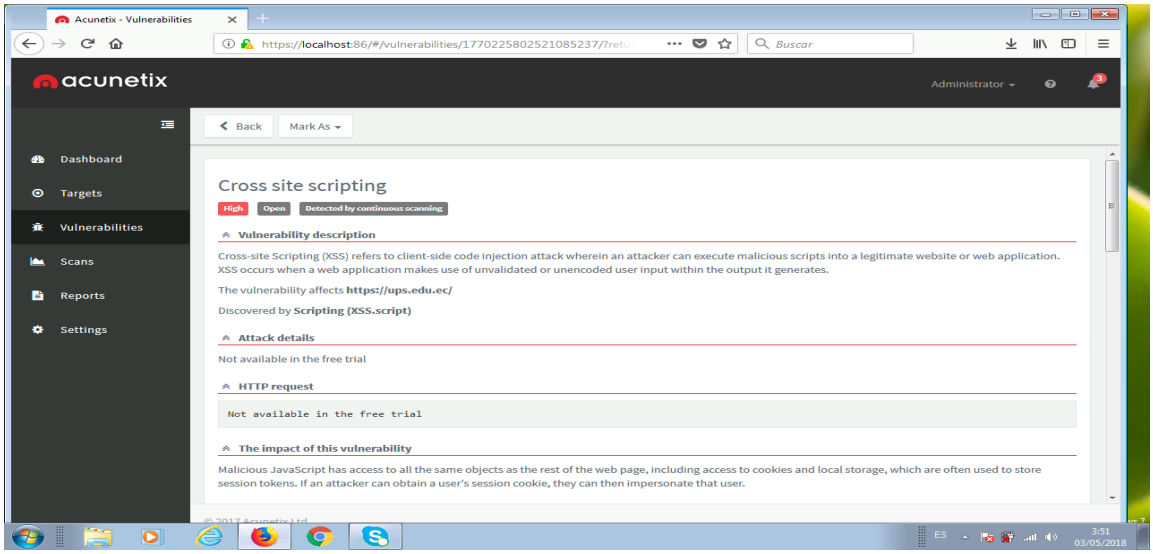
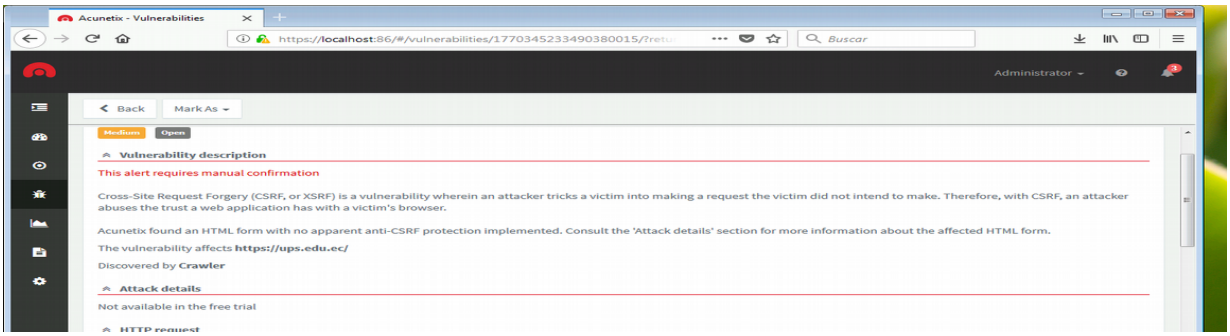


Gráfico 23.- Información sobre ALTO RIESGO ACUNETIX

Fuente: Elaboración propia



La información encontrada sobre las vulnerabilidades de la página son las siguientes:

VULNERABILIDAD	DESCRIPCION	CRITICIDAD	# ALERTAS	SERVICIO
Sensitive Data Exposure(A3)	Muchas aplicaciones web y API tienen una debilidad de no protegen adecuadamente los datos confidenciales, como financieros, de salud y PII. Los atacantes pueden robar o modificar esos datos débilmente protegidos para realizar fraude con tarjetas de crédito, robo de identidad u otros delitos. Los datos sensibles pueden ser comprometidos sin protección adicional, como cifrado en reposo o en tránsito, y requiere precauciones especiales cuando se intercambia con el navegador.	**CWE-16 - MEDIA**	427	WEB SERVER
- Security Misconfiguration(A6)	La mala configuración de seguridad es el problema más común. Esto es comúnmente el resultado de configuraciones predeterminadas inseguras, configuraciones incompletas o ad hoc, almacenamiento en la nube abierta, encabezados HTTP mal configurados y mensajes de error detallados que contienen información sensible. No solo se deben configurar correctamente todos los sistemas operativos, marcos, bibliotecas y aplicaciones, sino debe ser parcheado y actualizado de manera oportuna.	**CWE-16 - MEDIA**		WEB SERVER
- Using Components with Known Vulnerabilities(A9)	Los componentes, como bibliotecas, marcos y otros módulos de software, casi siempre se ejecutan con todos los privilegios. Si es vulnerable componente se explota, dicho ataque puede facilitar la pérdida de datos graves o la toma del servidor. Aplicaciones que usan componentes con las vulnerabilidades conocidas pueden socavar las defensas de las aplicaciones y permitir un rango de posibles ataques e impactos.	**CWE-16 - MEDIA**		WEB SERVER
- Cross Site Scripting (XSS)(A7)	Las fallas XSS ocurren siempre que una aplicación incluye datos no confiables en una nueva página web sin la validación o escape adecuado, o actualiza una página web existente con datos proporcionados por el usuario mediante una API de navegador que puede crear HTML o JavaScript. XSS permite atacantes para ejecutar scripts en el navegador de la víctima que pueden secuestrar sesiones de usuario, desfigurar sitios web o redirigir al usuario a Sitios Maliciosos.	**CWE-79 - ALTA**	49	WEB SERVER

Tabla 24.-Información de vulnerabilidades con ACUNETIX outsider (fuente propia)

Método: **COMPROBACION DE VULNERABILIDADES (confidencial)**	Observaciones: **Descubrimiento activo**
Herramienta: **ACUNETIX**	Visibilidad: **Insider**

La información encontrada sobre las vulnerabilidades de la página del intranet son las siguientes:

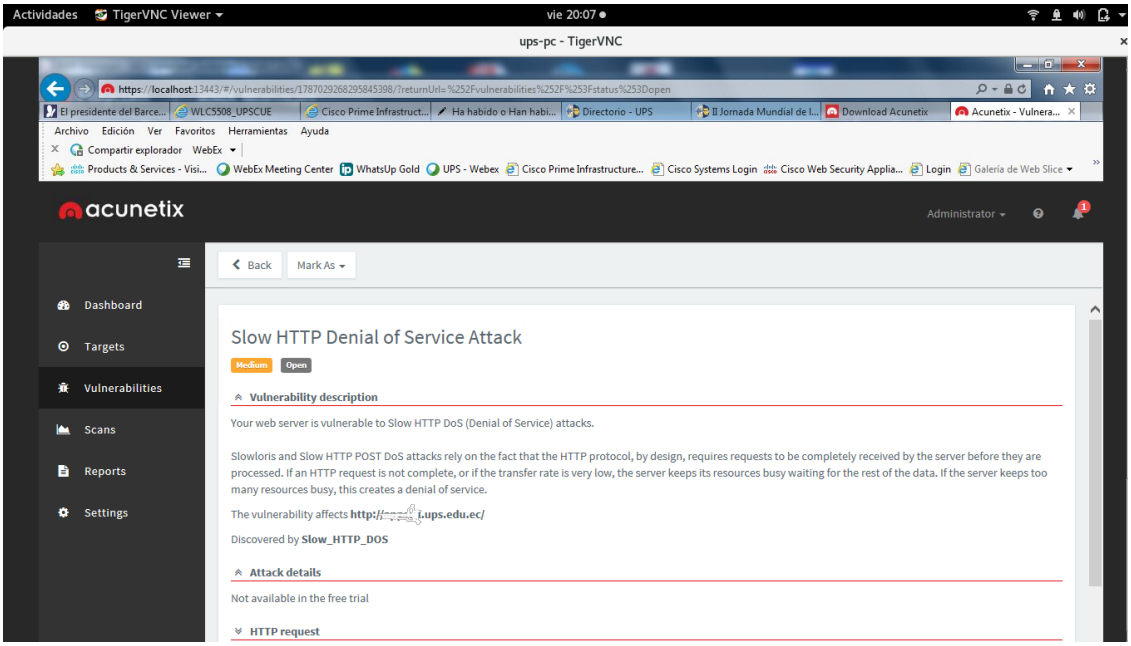


Gráfico 25.- Información de ACUNETIX sobre vulnerabilidad en Intranet

Fuente: Elaboración propia

La información encontrada sobre las vulnerabilidades de la página son las siguientes:

VULNERABILIDAD	DESCRIPCION	CRITICIDAD	# ALERTAS	SERVICIO
Slow HTTP Denial of Services	Los ataques DoS se basan en el hecho de que el protocolo HTTP, por diseño, requiere que las solicitudes sean completamente recibidas por el servidor antes de ser procesadas. Si una solicitud HTTP no está completa, o si la tasa de transferencia es muy baja, el servidor mantiene sus recursos ocupados esperando el resto de los datos. Si el servidor mantiene demasiados recursos ocupados, esto crea una denegación de servicio.	**CVSS – 5.3 MEDIA**	9	WEB SERVER
Error message on page	Esta página contiene un mensaje de error / advertencia que puede revelar información confidencial. El mensaje también puede contener la ubicación del archivo que produjo la excepción no controlada. Esto puede ser un falso positivo si el mensaje de error se encuentra en las páginas de documentación.	**CWE-16 - MEDIA**		WEB SERVER

Tabla 25.-Información de vulnerabilidades con ACUNETIX insider (fuente propia)

Método: **COMPROBACION DE VULNERABILIDADES (confidencial)**	Observaciones: **Descubrimiento activo**
Herramienta: **NMAP** comando: **nmap -sS -sV --script vuln (IPpagweb)**	Visibilidad: **Outsider**

Herramienta que ayuda a comprobar información adicional sobre las vulnerabilidades más conocidas y que puedan afectar a la página web www.ups.edu.ec

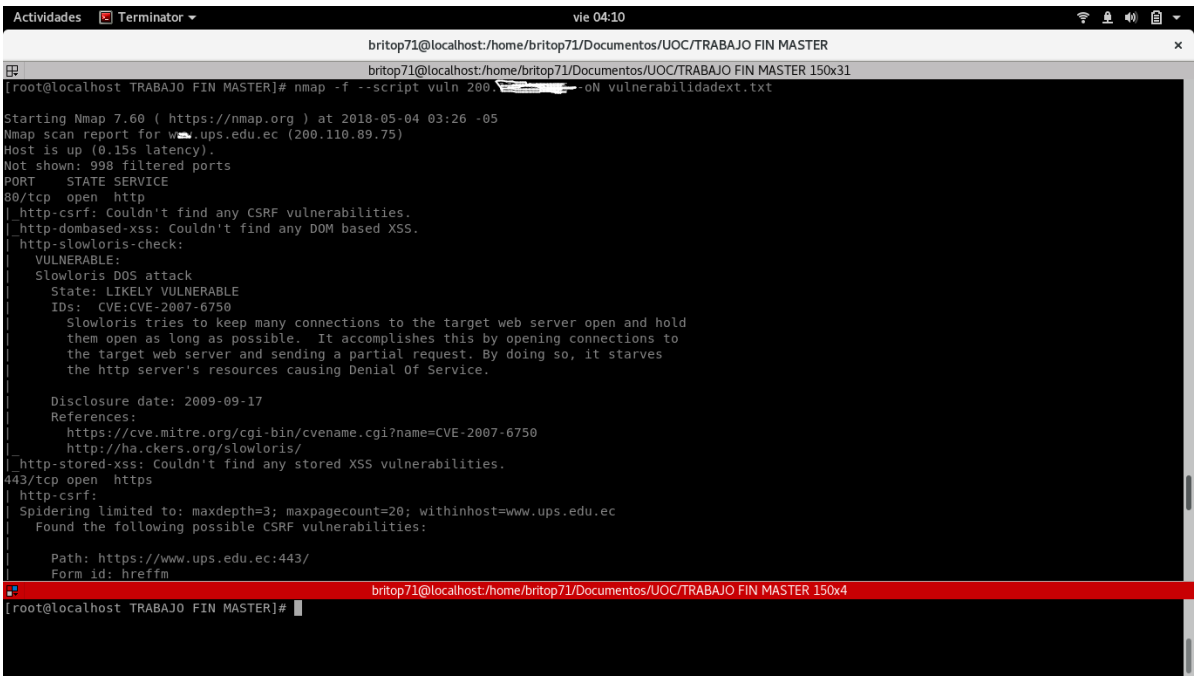


Gráfico 26.- Información sobre vulnerabilidades con NMAP web

Fuente Elaboración propia

La información encontrada sobre las vulnerabilidades de la página son las siguientes:

VULNERABILIDAD	DESCRIPCION	DETALLE	CRITICIDAD	SERVICIO
CVE-2007-6750	Slowloris DOS attack	Slowloris intenta mantener abiertas y retenidas muchas conexiones al servidor web objetivo se abren el mayor tiempo posible. Lo logra abriendo conexiones al servidor web objetivo y enviando una solicitud parcial. Al hacerlo, se queda y los recursos del servidor http que causan la denegación de servicio.	**MEDIA**	HTTP
Possible CSRF vulnerabilities: https://wxxx.ups.edu.ec:443/ https://wxxx.ups.edu.ec/web/guest/admisiones https://wxxx.ups.edu.ec/web/guest/tour-virtual-360 https://wxxx.ups.edu.ec/web/guest/-como-hacer-investigacion-	Cross-Site Request Forgery (CSRF)	El CSRF (*Cross-site request forgery*) es un tipo de *exploit* malicioso de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía. Esta vulnerabilidad es conocida también por otros nombres como XSRF, enlace hostil, ataque de un click, cabalgamiento de sesión, y ataque automático.	**MEDIA**	HTTPS - 443
CVE-2014-3704	SSL/TLS MITM vulnerability (CCS Injection)	OpenSSL antes de 0.9.8za, 1.0.0 antes 1.0.0m y 1.0.1 antes 1.0.1h no restringe adecuadamente el procesamiento de los mensajes ChangeCipherSpec, lo que permite a los atacantes man-in-the-middle desencadenar el uso de una clave maestra de longitud cero en ciertas comunicaciones OpenSSL-to-OpenSSL, y consecuentemente secuestrar sesiones u obtener información sensible, a través de un handshake TLS diseñado, también conocido como la vulnerabilidad de "Inyección CCS".	**ALTA**	HTTPS - 443
ssl-dh-params	Diffie-Hellman Key Exchange Insufficient Group Strength	Los servicios de seguridad de la capa de transporte (TLS) que usan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que usan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques pasivos de escuchas ilegales.	**MEDIA**	

Tabla 26.-Comprobación de vulnerabilidades con NMAP outsider (información propia)

Método: **COMPROBACION DE VULNERABILIDADES (confidencial)**	Observaciones: **Descubrimiento activo**
Herramienta: **OWASP ZAP**	Visibilidad: **Outsider**

Este escaneo ayuda a comprobar información adicional sobre las vulnerabilidades más conocidas y que puedan afectar a la página web www.ups.edu.ec.

Nota: esta prueba se realizó pero la misma presentó muy invasiva, por lo que se procedió a parar la misma, no hubo alertas de la misma en equipos de borde por monitoreo sino advirtieron del mismo por la lentitud de la página y se revisó en logs del servidor, por lo que no se pudo sacar un reporte completo.

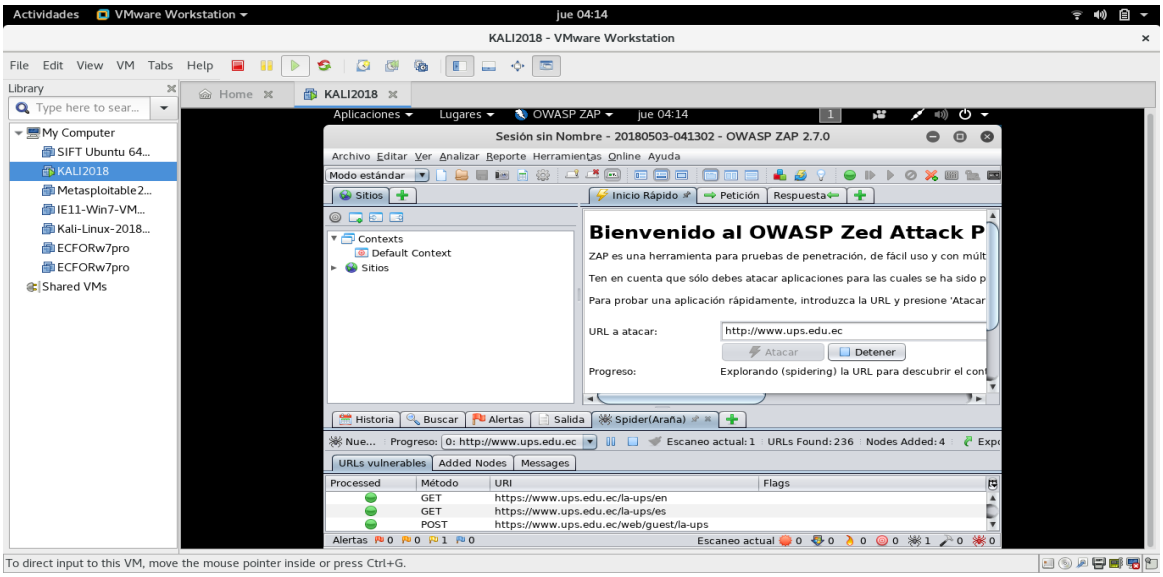


Gráfico 27.- Información de OWASP

Fuente: Elaboración propia

	ivo
Herramienta: **NMAP** comando: **nmap -sS -sV --script vuln (IPpagweb)**	Visibilidad: **Insider**

Se realiza una comprobación manual para revisar la página web wxxx.ups.edu.ec con la finalidad de encontrar posibles vulnerabilidades

```
Nmap done: 1 IP address (1 host up) scanned in 588.39 seconds

C:\Users\ups>nmap -sS -sV --script vuln [redacted].101.8 -oN intranet.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-03 17:53 Hora est. Pacífico,
Sudamérica
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for appswl.ups.edu.ec (172.16.101.8)
Host is up (0.0068s latency).
Not shown: 875 closed ports, 121 filtered ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Oracle Application Server 11g httpd
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /forms/: Potentially interesting folder
|   /manual/: Potentially interesting folder
|   /reports/: Potentially interesting folder
```

La información encontrada sobre las vulnerabilidades de la página www.ups.edu.ec son las siguientes ANEXO 5

La información encontrada para la intranet (xxx.xxx.101.8) sobre las posibles vulnerabilidades de la página es la siguiente:

VULNERABILIDAD	DESCRIPCION	DETALLE	CRITICIDAD	SERVICIO
CVE-2007-6750	Slowloris DOS attack	Slowloris intenta mantener abiertas y retenidas muchas conexiones al servidor web objetivo se abren el mayor tiempo posible. Lo logra abriendo conexiones al servidor web objetivo y enviando una solicitud parcial. Al hacerlo, se queda y los recursos del servidor http que causan la denegación de servicio.	**MEDIA**	HTTP

Tabla 27.-Información de vulnerabilidades con NMAP intranet (fuente propia)

Método: **COMPROBACION DE VULNERABILIDADES (confidencial)**	Observaciones: **Descubrimiento pasivo**
Herramienta: **ISO 27002, entrevistas, revisiones visuales, chequeos**	Visibilidad: **Insider**

Un factor importante para en la seguridad de la información comprende el conocimiento, compromiso y uso de procedimientos que la institución posee para que los usuarios especialmente que hacen uso de los activos críticos de la Universidad con la finalidad de que realicen un trabajo de óptimo y seguro para evitar provocar de forma inconsciente o sin ánimo de afectar el trabajo diario de la institución, daños o afecciones graves a la infraestructura que puedan desembocar a un fallo general de magnitud alta

dentro de la institución. Es por eso que en base a lo revisado se ha obtenido la siguiente revisión a los controles propuestos por la ISO 27002 la misma que hace referencia a la seguridad de la información, la cual se adicionará como anexo de este trabajo, se puede ver en el ANEXO 8.

Declaración de Aplicabilidad Vigente para el: dd/mm/aaaa

Leyenda (para la selección de controles y razón por la que se seleccionaron):

LR: **requerimientos legales,**CO: **obligaciones contractuales,**BR/BP: **requerimientos del negocio/mejores prácticas adoptadas ,**RRA: **resultado de la valoración de riesgos;**TSE: hasta cierto punto

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/BP	RRA	
Cláusula	Sección	Objetivo de control / control							
5 Políticas de Seguridad	5.1	Dirección de la alta gerencia para la seguridad de la información							
	5.1.1	Políticas de seguridad de la información	si				x	3/5	existe publicada la política en la pagina web sin difusión
	5.1.2	Revisión de las políticas de seguridad de la información	si				x	2/5	no se actualiza de forma constante la política
6 Organización de la Seguridad de la Información	6.1	Organización interna							
	6.1.1	Roles y responsabilidad de seguridad de la información	si				x	2/5	definido de forma general
	6.1.2	Segregación de deberes	no				x	0/5	no esta definidas las tareas
	6.1.3	Contacto con autoridades	no				x	0/5	no hay un procedimiento
	6.1.4	Contacto con grupos de interés especial	no				x	0/5	no hay un procedimiento
	6.1.5	Seguridad de la información en la gestión de proyectos	si				x	2/5	no se cumple adecuadamente pese a existir un procedimiento
	6.2	Dispositivos móviles y teletrabajo							
	6.2.1	Política de dispositivos móviles	no				x	0/5	no existe una política definida para los dispositivos móviles
	6.2.2	Teletrabajo	no	no se utiliza este sistema					
	7.1	Previo al empleo							
	7.1.1	Verificación de antecedentes	si		x		x	3/5	lo realiza GTH, no enfatiza en la seguridad de la información
	7.1.2	Términos y condiciones del empleo	si		x		x	3/5	lo realiza GTH, no enfatiza en la seguridad de la información
	7.2	Durante el empleo							

Gráfico 29.- Información de la infraestructura según los controles ISO 27001

Método: **COMPROBACION DE VULNERABILIDADES (confidencial)**	Observaciones: **Descubrimiento activo**
Herramienta: **aicrack-ng, cruch**	Visibilidad: **Insider**

Para la realización de esta prueba se escogió hacer pruebas en la red UPS_EVENTOS además fue necesario realizar una pequeña investigación mediante ingeniería social para conocer la estructura de la clave de acceso (combinaciones frecuentes de letras que utilizan) a esta red que se encuentra protegida con WPA2, para lo cual se generó un diccionario personalizado mediante la herramienta **crunch** de la cual se obtuvo el archivo dicUPS.txt, con el que se trabajó para hallar la clave luego de capturar tráfico de la red y esperar que un usuario se conecte a la red inalámbrica, obteniéndose el resultado efectivo al hallar la clave **Uxxx-xxx.**

```
[root@localhost britop71]# crunch 9 9  abcefghijklmnopqrstuwxyz1234567890-. -t U%%-%%,,. > /home/britop71/Documentos/dicUPS.txt
Crunch will now generate the following amount of data: 67600000 bytes
64 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 6760000
[root@localhost britop71]# ls -l /home/britop71/Documentos/dicUPS.txt
-rw-r--r--. 1 root root 67600000 abr 20 21:24 /home/britop71/Documentos/dicUPS.txt
[root@localhost britop71]#
```

Gráfico 30.- Creación de diccionario personalizado con CRUNCH

Fuente: Elaboración propia

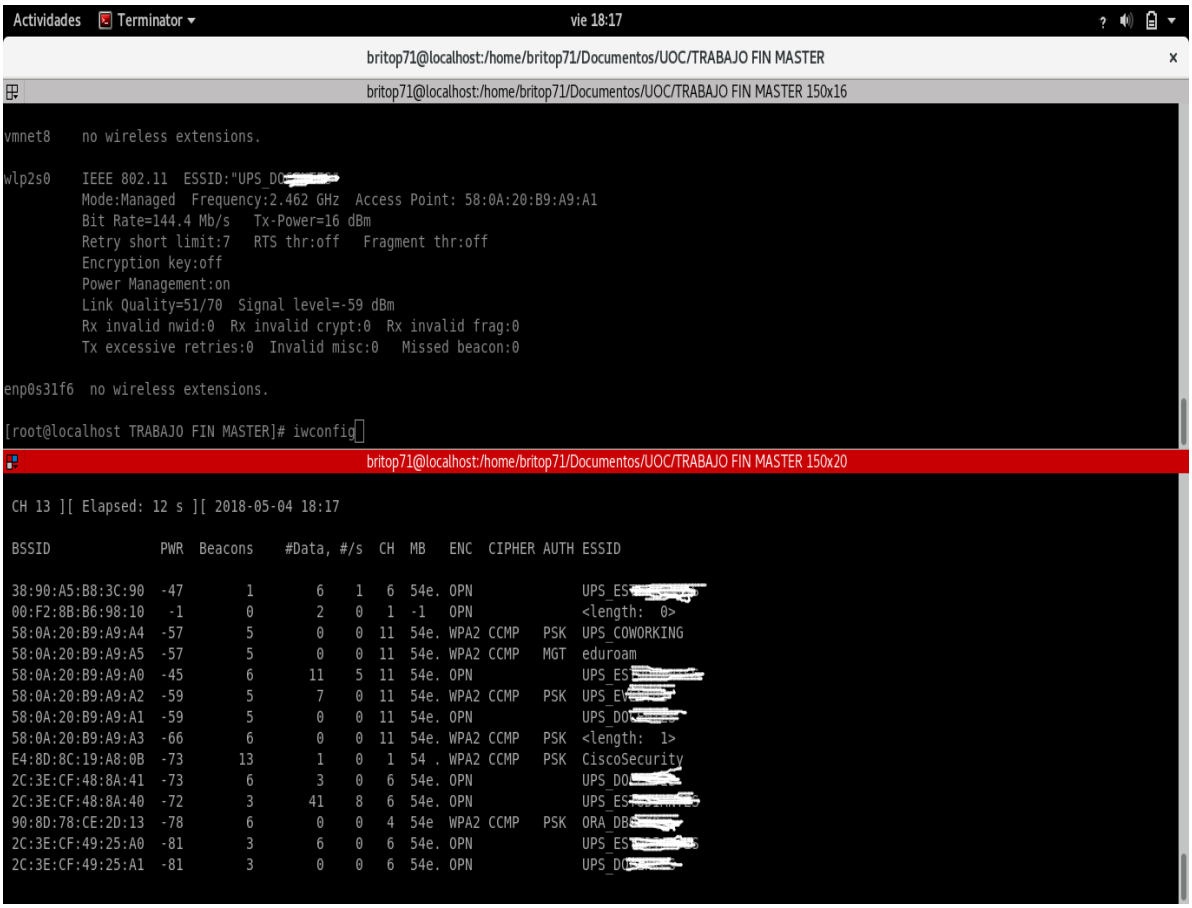
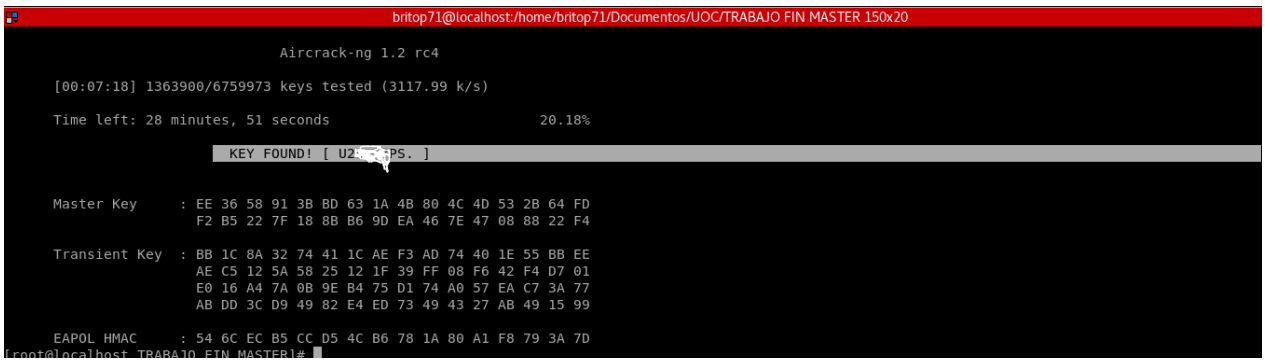


Gráfico 31.- Escaneo de redes inalámbricas de la Universidad

Fuente: Elaboración propia



Método: **COMPROBACION DE VULNERABILIDADES**	Observaciones: **Descubrimiento pasivo**
Herramienta: **Phishing**	Visibilidad: **Insider - Outsider**

La infraestructura de la Universidad constantemente está sujeta a ataques de phishing, lamentablemente donde muchos usuarios estudiantes y administrativos han sido presas de estos ataques, pese a que constantemente es enviado recordatorios por parte de la Secretaría de Tecnología sobre estos tipos de ataques

De: Manuel Fernando Paladines Jaramillo
Enviado: miércoles, 30 de mayo de 2018 3:42
Para: Cristian Teodoro Diaz Gutierrez
Asunto: Urgente (

ID de notificación: 0.866645843
Email: @ups.edu.ec.

Acaba de detectarse un virus VTB en su carpeta de correo, inicie sesión con el nuevo escáner de la aplicación UPS 2018 GVTFX Secure Outlook para eliminar el virus de su cuenta de correo electrónico (@ups.edu.ec) y proteger sus archivos importantes.

Debe realizar esta acción para eliminar el Virus VTB de sus carpetas de correo electrónico con el escáner de la aplicación UPS Outlook 201 GVTFX Secure Outlook, o su cuenta de correo electrónico terminará inmediatamente para evitar la propagación del virus en nuestro registro de correo web.

Escanee con el escáner de la aplicación Secure Outlook GVTFX de UPS 2018 ¡AQUÍ!

www.ups.edu.ec
Helpdesk, Universidad Politécnica Salesiana.
Copyright ©2018 Universidad Politécnica Salesiana

Gráfico 33.- Ataques de Phishing

Fuente: Elaboración propia

Método: **REVISION DE VULNERABILIDADES**	Observaciones: **Descubrimiento pasivo**
Herramienta: **revisión de información recabada**	Visibilidad: **Insider - Outsider**

Hasta el momento se han identificado los servidores, sus servicios y puertos que se presentan en la infraestructura, por lo que se validará posibles vulnerabilidades que existen y se probaran si alguna de ellas se hace efectiva esto depende de que existan más capas de seguridad implementadas en la infraestructura de la universidad.

Las posibles vulnerabilidades que pueden encontrarse en la infraestructura por los sistemas operativos implementado en los servidores y versiones de sus servicios, para lo cual procederemos a revisar las posibles vulnerabilidades que afectan a estos tipos de plataformas y servicios, para luego pasar comprobar si pueden ser explotadas algún servicio se adjunta en el ANEXO 7

2.8.1 Calificación de la Escala de Riesgo

De lo revisado y analizado en el pentesting se puede indicar que las posibles amenazas a las que la infraestructura es expuesta son las siguientes:

AMENAZA	VULNERABILIDAD	NIVEL
Incendio - Vandalismo	Las construcciones del MDF y cuartos de comunicación permite que estén debidamente aislados de agentes y posibles contaminantes para que se ha afectado por esta amenaza	BAJO
Inundaciones	Las construcciones del MDF y cuartos de comunicación permite que estén debidamente aislados de afecciones por amenazas de agua	BAJO
Interrupción del Servicio	Versión de sistemas operativos y servicios, presentan vulnerabilidades, adicional la falta de una gestión adecuada a la continuidad del servicio, puede producir una afección severa al servicio	ALTO
Persona mal intencionada	Persona que quiera hacer daño física a equipos de comunicación y servidores es totalmente nulo ya que los cuartos están debidamente protegidos y el control hacia ellos.	BAJO
Acceso no autorizado	El acceso físico de los proveedores a de comunicación se lleva de manera correcta. En cuanto al uso de claves para acceso a diferentes servicios debe ser de forma más segura con la finalidad de que se maneje un correcta auditoría en el acceso a activos	MEDIO
Información de equipos que protege el firewall	El firewall permite revisar la información de equipo internos a los cuales el protege. Adicional en los sistemas operativos y de servicios	BAJO
Suplantación	Los switch permiten la suplantación de equipos por medio de mac	MEDIO
Robo de información	Problemas de DNS Spoofing, falta de protocolos de cifrado para el intercambio de información confidencial	MEDIO
Robo de equipos	Equipos de APs externos no tiene la seguridad contra robos	MEDIO
Ataque de un cracker	Existe vulnerabilidades encontradas en el estudio, que pueden facilitar a la consecución del ataque tanto interna como externamente	ALTO

Tabla 28.-Posibles amenazas que afecten la infraestructura de la UPS (fuente propia)

En base a la valoración de los impactos y probabilidad de que las amenazas se hagan efectivas aprovechándose de las vulnerabilidades para los activos de la infraestructura

de la Universidad Politécnica Salesiana se puede calcular el riesgo al que se encuentran sometidos los activos principales de la universidad:

TIPO	ACTIVO	IMPACTO (infraestructura)	PROBABILIDAD (amenaza)	NIVEL DE RIESGO
RED	ROUTER	ALTO	BAJA	RIESGO MEDIO
	FIREWALL	ALTO	BAJA	RIESGO MEDIO
	SWITCH CAPA 3	ALTO	BAJA	RIESGO MEDIO
	WLC	ALTO	BAJA	RIESGO MEDIO
	APs	MEDIO	MEDIO	RIESGO MEDIO
SERVIDORES	SERVIDORES	CRITICO	MEDIO	RIESGO MEDIO
FISICA	CENTRO DATOS	ALTO	BAJA	RIESGO MEDIO
	CABLEADO ESTRUCTURADO	CRITICO	MEDIO	RIESGO MEDIO
	CUARTOS DE COMUNICACION	CRITICO	BAJA	RIESGO MEDIO
APLICACIONES	SISTEMAS OPERATIVOS	ALTO	BAJA	RIESGO MEDIO
	APLICACIONES	ALTO	BAJA	RIESGO MEDIO
	BASES DE DATOS	ALTO	BAJA	RIESGO MEDIO
HARDWARE	SWITCH ACCESO	CRITICO	BAJA	RIESGO MEDIO

Tabla 29.-Nivel de Riesgo de la infraestructura (fuente propia)

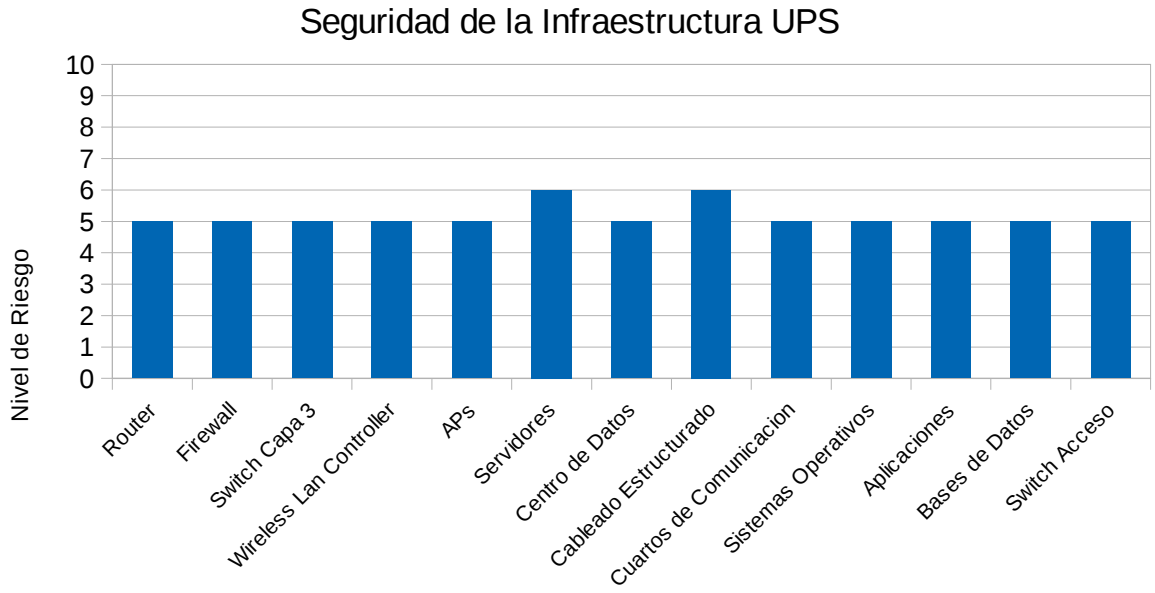


Gráfico 34.- Seguridad de la Infraestructura de la Universidad Politécnica Salesiana Cuenca

Fuente: Elaboración propia

Se realiza la revisión de manera más minuciosa a la página web e intranet, que son activos muy importantes de la institución, porque en su servicio se encuentran los sistemas financieros y académicos.

ACTIVO	AMENAZA	NIVEL	IMPACTO	PROBABILIDAD	NIVEL de RIESGO
Página web	Incendio - Vandalismo	BAJO	CRITICO	MEDIO	MEDIO
	Inundaciones	BAJO			MEDIO
	Interrupción del Servicio	ALTO			CRITICO
	Persona mal intencionada	BAJO			MEDIO
	Acceso no autorizado	MEDIO			MEDIO
	Información de equipos que protege el firewall	BAJO			MEDIO
	Suplantación	MEDIO			MEDIO
	Robo de información	MEDIO			MEDIO
	Robo de equipos	BAJO			MEDIO
	Ataque de un cracker	ALTO			CRITICO
Página intranet	Incendio - Vandalismo	BAJO	CRITICO	MEDIO	MEDIO
	Inundaciones	BAJO			MEDIO
	Interrupción del Servicio	ALTO			CRITICO
	Persona mal intencionada	BAJO			MEDIO
	Acceso no autorizado	MEDIO			MEDIO
	Información de equipos que protege el firewall	BAJO			MEDIO

	Suplantación	MEDIO			MEDIO
	Robo de información	MEDIO			MEDIO
	Robo de equipos	BAJO			MEDIO
	Ataque de un cracker	ALTO			CRITICO

Tabla 30.-Nivel de riesgo de la página web e intranet UPS (fuente propia)

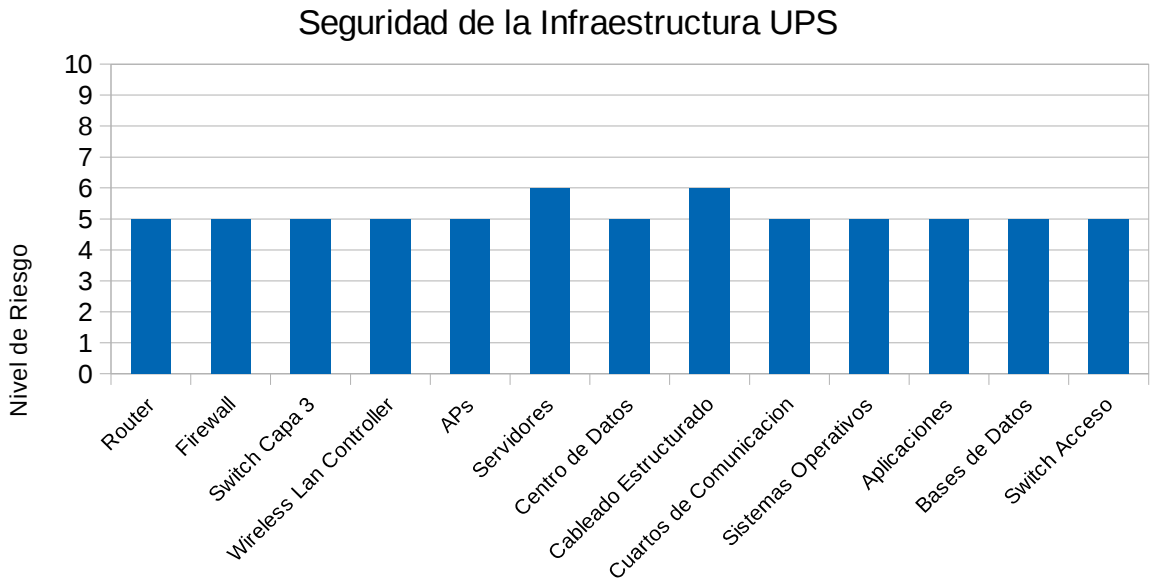


Gráfico 35.- Seguridad de activos críticos UPS

Fuente: Elaboración propia

NIVEL DE RIESGO
ALTO 9-10
CRITICO 7-8
MEDIO 3-6
BAJO 1-2

3 CONCLUSIONES Y RECOMENDACIONES

3.1 CONCLUSIONES

Luego de haber realizado el pentesting se obtuvo como conclusiones las siguientes:

- ✓ Se desmitifica la falsa sensación de que la infraestructura de una institución o empresa es 100% segura.
- ✓ La seguridad de la información depende de todos sus componentes (usuarios, políticas, procedimientos, activos) y si uno de ellos falla se ve comprometida la seguridad.
- ✓ El eslabón más débil en la seguridad de la información generalmente es el usuarios por lo cual hay que capacitarle y actualizarle constantemente en temas de seguridad.
- ✓ La metodología OSSTMM es la más aconsejada para poder evaluar la infraestructura de una institución o una empresa ya que ella hace una revisión de cada elemento mediante sus canales de revisión donde revisa a todos los componentes de la infraestructura.
- ✓ El Ethical Hacking es una herramienta que debe ser implementada en la institución con la finalidad de que periódicamente se esté probando la seguridad de la información con la finalidad de revisar el uso de la política de la información y procedimientos que aseguran la información que es un bien muy valioso para el funcionamiento de cualquier institución.
- ✓ Es necesario que en la institución se apoye en los controles de la ISO 27001 con la finalidad de mejorar su seguridad de la información, a miras a una próxima certificación.
- ✓ Es necesario realizar una evaluación de riesgos de la infraestructura cada vez que un activo sea puesto en producción.
- ✓ La continuidad del servicio dentro de la infraestructura es imprescindible para lograr la calidad de servicio óptimo entregado por TI hacia la comunidad universitaria.
- ✓ En cuanto al uso de herramientas para pentesting es necesario complementar la revisión de las herramientas automáticas con las manuales para tener claro las posibles vulnerabilidades que puede tener un activo.

3.2 RECOMENDACIONES

Las recomendaciones que se entrega para poder mejorar las vulnerabilidades encontradas en la infraestructura son las siguientes:

SERVIDORES		
SISTEMA OPERATIVO O SERVICIO	**VULNERABILIDAD**	**RECOMENDACION**
Linux 2.6.32	LINUX KERNEL 2.6.32 IP_REPOPTS DENEGACIÓN DE SERVICIO **CVE-2013-2224**	- Actualización del sistema operativo, Las futuras actualizaciones de kernel para Red Hat Enterprise Linux 5 y Red Hat Enterprise Linux 6 pueden abordar este problema.
Apache httpd 2.2.15	Aplicación con afección a vulnerabilidad **CVE-2010-2068** Reflejo de memoria sin inicializar en mod_auth_digest	- Apache httpd 2.2 tiene un fin de vida útil desde diciembre de 2017 y no debe utilizarse. - Se recomienda a los usuarios actualizar a la versión comercial admitida actualmente para abordar problemas conocidos.
Apache Tomcat / Coyote JSP engine 1.1	Aplicación con afección a vulnerabilidad **CVE-2010-0738** Reflejo de memoria sin inicializar en mod_auth_digest	- Se aconseja a todos los usuarios de JBEAP 4.2 en Red Hat Enterprise Linux 5 que actualicen a estos paquetes actualizados. - Revisar: http://community.jboss.org/wiki/SecureTheJmxConsole
Ngnx 1.12.2	Aplicación con afección a vulnerabilidad **CVE-2017-7529**	- Habilitar parche - Revisar: https://nginx.org/download/patch.2017.ranges.txt
OPEN SSH 7.4 (protocol 2.0)	Aplicación con afección a vulnerabilidad **CVE-2016-10009**	- Actualizar versión del sistema operativo o instalar el parche respectivo
Apache httpd 2.215 ((Centos); SSL-only mode)	Aplicación con afección a vulnerabilidad **CVE-2014-0160**	- 1 Actualizar el OPENSSL - 2 Revocar todas las claves privadas y volver a generarlas - 3 revocar certificados y volverlos a generar - 4 luego las contraseñas deben ser cambiadas - Revisar: https://www.csoonline.com/article/2142700/vulnerabilities/vulnerabilities-heartbleed-cve-2014-0160-an-overview-of-the-problem-and-the-resources-needed-to.html
Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)	Aplicación con afección a vulnerabilidad **CVE-2013-4248**	- Actualizar a php-upgrade-5.4.18 o php 5.5.2 - Revisar https://bugzilla.redhat.com
Apache httpd 2.2.15 ((CentOS) mod_jk/1.2.40 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips)	Aplicación con afección a vulnerabilidad **CVE-2011-1473**	- Esta vulnerabilidad se ha corregido en la versión 2.2.20 y corregida posteriormente en 2.2.21. Se recomienda actualizar a la versión 2.2.21 (o posterior).
Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips mod_cluster/1.3.1.Final)	Aplicación con afección a vulnerabilidad **CVE-2014-0160**	- 1 Actualizar el OPENSSL - 2 Revocar todas las claves privadas y volver a generarlas - 3 revocar certificados y volverlos a generar - 4 luego las contraseñas deben ser cambiadas - Revisar: https://www.csoonline.com/article/2142700/vulnerabilities/vulnerabilities-heartbleed-cve-2014-0160-an-overview-of-the-problem-and-the-resources-needed-to.html
Apache httpd 2.2.29 ((Unix) mod_ssl/2.2.29 OpenSSL/1.0.1e-fips mod_bwlimited/1.4)	Aplicación con afección a vulnerabilidad **CVE-2014-0160**	- 1 Actualizar el OPENSSL - 2 Revocar todas las claves privadas y volver a generarlas - 3 revocar certificados y volverlos a generar - 4 luego las contraseñas deben ser cambiadas - Revisar: https://www.csoonline.com/article/2142700/vulnerabilities/vulnerabilities-heartbleed-cve-2014-0160-an-overview-of-the-problem-and-the-resources-needed-to.html
Dovecot pop3d	Aplicación con afección a	- Actualizar a la versión dovecot 2.2.34, dovecot 2.3.1

	vulnerabilidad **CVE-2017-15132**	
Dovecot imapd	Aplicación con afección a vulnerabilidad **CVE-2017-15132**	- Actualizar a la versión dovecot 2.2.34, dovecot 2.3.1
MySQL (unauthorized)	Aplicación con afección a vulnerabilidad **CVE-2012-2122**	- Revisar actualizaciones -Revisar los requisitos de acceso a la base de datos y eliminar base MySQl expuesta a la red - Hacer uso de ACL por IP para redes confiables - Dar acceso solo a usuarios de confianza - Monitoreo de sistemas afectados
Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.7)	Aplicación con afección a vulnerabilidad **CVE-2012-0550**	- Instalar parche - Oracle ha creado una solución para esta vulnerabilidad que se ha incluido como parte del Aviso de actualización de parches críticos: abril de 2012. Security-Assessment.com recomienda aplicar el último parche proporcionado por el proveedor. -Leer http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html
OpenSSH 5.3 (protocol 2.0)	Aplicación con afección a vulnerabilidad **CVE-2012-0814**	- Actualizar software a la versión OpenSSH 5.7 o superiores que ya vienen con un parche para esta vulnerabilidad.
Pure-FTPd	Aplicación con afección a vulnerabilidad **CVE-2014-6271**	- Oracle-solaris-11-2-upgrade-shell-bash-4-1-17-0-175-2-5-0-2-0
Oracle Application Server 11g httpd	Aplicación con afección a vulnerabilidad **CVE-2007-6750** **CVE-2011-3192**	- Para mitigar esta vulnerabilidad, debe permitir el acceso de la administración a los productos F5 solo a través de una red segura y restringir el acceso de la línea de comando para los sistemas afectados a los usuarios de confianza. -Se requiere la actualización a la última versión
Oracle WebLogic Server (Servlet 2.5; JSP 2.1)	Aplicación con afección a vulnerabilidad **CVE-2007-6750** **CVE-2011-3192**	- Para mitigar esta vulnerabilidad, debe permitir el acceso de la administración a los productos F5 solo a través de una red segura y restringir el acceso de la línea de comando para los sistemas afectados a los usuarios de confianza. -Se requiere la actualización a la última versión

CONTROLES ISO 27001		
CONTROL	**VULNERABILIDAD**	**RECOMENDACION**
5 Políticas de Seguridad|	Falta de conocimiento de la política	- Es necesario una estrategia para dar a conocer, actualizar y enseñar al usuario sobre la política de seguridad institucional dentro de la Universidad, la misma que debe ser apoyados por las autoridades de la institución.
6 Organización de la Seguridad de la Información	No existe responsables definidos para monitorear y trabajar de lleno en la seguridad de la información	- Es necesario mantener un organigrama sobre el personal que se encargue de la gestión de la seguridad de la información con la finalidad de conocer quien debe actuar en un incidente y que su procedimiento sea definido, según los requerimientos de la institución.
7 Seguridad en los Recursos Humanos	Hasta el momento no se ha presentado ninguna afectación producida por un ex-empleado, pero puede llegar a ser crítica especialmente en el área de tecnología	- Es necesario que los empleados tengan conocimiento y ponga en práctica cumpliendo las normas y políticas sobre la seguridad de la información, durante el ingreso y finalización de relaciones laborales con la institución, pudiendo de esta manera proteger los intereses institucionales.
8 Gestión de Activos	La pérdida o copia de información sensible de la universidad, o personal de un usuario puede acarrear problemas en la confidencialidad de la información	- Se requiere tener definido los activos y sus usuarios, con la finalidad de que se aplique la custodia responsable sobre los mismos, para asegurar la información evitando su divulgación, modificación, eliminación o destrucción de activos; si estas acciones no son autorizadas.
9 Control de Acceso	Es necesario un mantener una mejora continua de los mismos para evitar quedar obsoletos.	- Es necesario que la gestión del control de accesos a los activos sea constantemente actualizada mediante un procedimiento de cese de funciones con recursos humanos y TI con la finalidad de dar de baja la cuenta de usuarios y retirar de los activos que estuvieron a su cargo la información sensible de la institución. Así mismo se debe proceder cuando el usuario cambia de rol laboral dentro de la institución.
10 Criptografía	Es necesario tener un procedimiento de criptografía	- Es necesario implementar controles criptográficos especialmente al momento de envío de información confidencial dentro institución entre

	por medio de llaves para evitar préstamos o uso de claves de usuarios no autorizados	las autoridades y los usuarios que manejen la información sensible, pudiendo ser implementado un sistema como AxCrypt, Gpg4win.
11 Seguridad Física y del Entorno	Existe cierto cableado estructurado sin la debida protección por lo que puede ser cortado, produciendo un fallo de servicio a un grupo de usuarios.	- Es necesario canalizar el cableado estructurado que este expuesto por canaletas que se encuentran dentro de aulas, salas, oficinas y especialmente dar una prioridad al cableado que sea externo emplazarlo en canaletas metálicas. - Cuartos de comunicación deben estar limpios y retirado todo elemento que pueda causar algún conato de incendio.
12 Seguridad en las Operaciones	La revisión de procedimientos establecidos son correctos, es necesario que se los ponga en práctica para que los mismos no afecten a la seguridad de la información, el monitoreo es fundamental para hacer seguimiento de problemas	- Es necesario el uso correcto de los procedimientos que se tiene implementados con la finalidad de realizar una mejor gestión sobre la seguridad de la información - Mantener el registro de los incidentes que se suscitan sobre la seguridad de la información con la finalidad de contrarrestar si alcanza a tornarse en un problema. - Evitar la explotación de vulnerabilidades técnicas desde el interior que son las más devastadoras mediante el hardening a los activos que se incorporan a la infraestructura
13 Seguridad en las Comunicaciones	Es necesario implementar procedimientos formales y una política de transferencia para la información.	- Afinamiento de la seguridad en la transferencia de información especialmente la sensible dentro de la institución y fuera de ella con la finalidad de que esta sea reflejada en los controles implementados en los equipos de seguridad tanto a nivel de WAN y LAN.
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	Antes de ser puesto en producción cualquier aplicación esta debe ser probada no solo en su parte funcional sino de seguridad de la información con la finalidad de que presente vulnerabilidades por problemas de programación.	- La seguridad de la información debe ser implementada en todo el ciclo de vida del desarrollo de un software y deben ser incluido como requisitos especialmente para los servicios públicos. - Asegurar los datos que se utilizan en las fases de pruebas.
15 Relaciones con Proveedores	La gestión del servicio de los proveedores es importante para mantener un seguimiento constante de la calidad del servicio ofrecida a la institución	- Es necesario la implementación de un procedimiento de proveedores con la finalidad de garantizar la protección de los activos accesibles al proveedor y mantener un SLA de seguridad de seguridad de la información con ellos.
16 Gestión de Incidentes de Seguridad de la Información	Es muy importante que se tenga procedimientos formales con la finalidad de que los usuarios tomen las acciones correctivas necesarias antes de los incidentes se conviertan en problemas	- Se requiere procedimientos frente a la administración de incidentes de seguridad de la información que puedan presentarse dentro de la institución y realizarse la gestión respectiva en cuanto a su actualización y mantenimiento, debido al avance de la tecnología y la implementación de aplicaciones constantes dentro de la institución.
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	Se necesita el establecimiento y correcto funcionamiento del sitio alterno y los equipos de redundancia que brinde la posibilidad de continuar trabajando cuando uno de los componentes informáticos principales presente algún daño o incidente.	- La continuidad del servicio es imprescindible por lo que es necesario las constantes pruebas de los activos redundantes que sirven para dar soporte a la disponibilidad del servicio, adicional debe estar implementado la seguridad de la información dentro de la gestión de la continuidad aplicada a cada uno de los activos participantes.
18 Cumplimiento	Se necesita manejar en todos los aspectos de la información los temas de protección y seguridad de la información especialmente por los datos sensibles de carácter personal que se utilizan en la institución	- Se requiere la implementación de seguridad de la información especialmente cuando se comparte información legal, normativa o contractual con otras instituciones con la finalidad de evitar incumplimientos de ley frente a las políticas y procedimientos institucionales.
RED		
INFRAESTRUCTURA	**VULNERABILIDAD**	**RECOMENDACION**
RED LAN	De lo revisado las posibles vulnerabilidades que pueden ser afectados se encuentran dentro de los parámetros	- Si bien la enumeración de servidores no es una vulnerabilidad muy problemática, es necesario proceder a mejorar las reglas de ACL implementadas, adicional como otra medida de protección seria la implementación de un firewall para acceso a servidores internos.

	normales como (afección por corte de cable que afectaría a un grupo de usuarios, enumeración de servidores, atención de restricciones en puntos no atendidos)	- Es necesario implementar para cada servidor una restricción a nivel de capa 2 por mac para su acceso - Implementar en los puertos donde se conecten los usuarios seguridad por capa2 o mac - Es necesario que se establezca una política o procedimiento para los puntos desatendidos como en salas de sesiones (estas deberían estar en una VLAN que no puedan acceder a servidores solo acceso a internet) y puntos adicionales dentro de las oficinas o laboratorios (puede mantenerse en la VLAN especial o poner en shutdown el puerto) - Mantener un registro de accesos a los diferentes servidores para usuarios externos del área de TI con la finalidad de llevar una auditoría y bitácora respectiva de permisos temporales. - Los permisos deben darse según procedimiento donde se refleje autorizaciones, tiempo de acceso. - Habilitar logs de servidores con la finalidad de monitorear la seguridad de acceso. - Los accesos entre usuarios de TI y servidores deben realizarlos por llaves (privadas y pública) entre usuarios y servidores, para mayor seguridad. - A futuro consolidar en un solo syslog todos los eventos de equipos de comunicación con la finalidad de que el monitoreo sea más efectivo, así como la prevención y atención a los posibles eventos sea ejecutados oportunamente.
RED INALAMBRICA Red que da servicio interno para la Universidad	En la revisión se pudo visualizar Aps que no tienen seguridad frente a robos de equipos, adicional se mantiene un portal cautivo que a veces presenta la pantalla genérica de cisco, pudiendo facilitar el acceso a intrusos	- Implementación de cámaras para seguridad de los APs - Revisar el portal cautivo del wireless lan controler, ya que a veces presenta la autenticación por default - Las claves para la red de eventos no debe manejarse con un mismo patrón por mucho tiempo ya que puede facilitar la creación de diccionarios particulares y encontrar la clave respectiva. - Afinamiento de wireless lan controller, con la finalidad de que no estén expuestas las redes más allá de los límites de la institución. - De ninguna manera permitir el acceso a servidores internos y críticos mediante este recurso, trabajarlo a nivel de VLANs el bloqueo respectivo. - Tratar que este recurso sea únicamente para acceso a Internet. - Accesos especiales con procedimiento respectivo y autorización de jefe de área y de sistemas.

GLOSARIO

Pentesting (Penetration Testing).- es la labor que se realiza para comprobar en varios entornos buscando fallas, con la finalidad de hallar fallos en la seguridad o vulnerabilidades en una infraestructura con la finalidad de prevenir ataques externos.

CSS (Cross Site Scripting).- o XSS permite en los controles de ejecución de Java Script de una víctima, abrir vectores de ataque pudiendo tomar el control remoto del navegador.

CSRF (Cross Site Request Forgery).- hace uso del parámetro vulnerado con la finalidad de montar un enlace modificado embebiendo el HTML o del script.

SQL Injection.- se apoya en las vulnerabilidades que presentan las aplicaciones web que rescatan datos de una base de datos mediante parámetros mal formados.

LDAP Injectión.- recupera valores de una base de datos de usuarios LDAP haciendo un ataque para revelar información sensitiva sobre sus usuarios.

Cookie Hijacking.- es el secuestro de una sesión realizada por un usuario y poder hacer uso de la misma el atacante para su beneficio.

Bonnet.- conjunto de red o robots que han sido infectados para usar las características de sus equipos de forma remota y potenciar un ataque masivo o en mayor escala.

Exploits.- es el uso de secuencias de código para explotar vulnerabilidades de equipos, permitiendo acciones beneficiosas para un atacante.

Fuzzing.- técnica de fuerza bruta para probar datos inesperados de forma aleatoria en una aplicación con la finalidad de que pueda ser atacada una vulnerabilidad.

Zero-Day.- código o exploit nuevo que no es detectado por los antivirus o equipos de seguridad.

ISO.- Sistema Internacional de Estandarización que norma productos en vareas áreas a nivel internacional.

ITIL.- IT Infraestructure Library marco de referencia para el uso de mejores prácticas en la administración de servicios de TI.

RFC (Request For Comments).- Publicaciones del Internet Engineering Task Force que norman para el funcionamiento del Internet

Puertos.- en informática hace referencia a la interfaz lógica utilizada para transferrir datos

TCP (Protocolo de Control de Transmisión).- protocolo orientado a la comunicación, fundamental de Internet TCP/IP que realiza un control de la transmisión de datos.

UDP (Protocolo de Datagrama de Usuario).- protocolo de transporte no orientado a la conexión que no utiliza detección de errores. Usado para trasmisiones de tiempo real.

WWW (Red de Informática Mundial).- sistema lógico de acceso mundial que proporciona información mediante páginas web

ICMP (Protocolo de control de Mensajes de internet).- envía mensajes con la finalidad de verificar si un equipo está activo haciendo uso de mensajes de error.

DNS (Sistema de Nombres de Dominio).- sistema jerárquico de base de datos que trasladan los nombres de páginas web a valores de números de IP donde se encuentran alojadas las diferentes páginas.

FTP (Protocolo de Transferencia de Archivos).- protocolo que se utiliza para la transferencia de archivos entre equipos conectados en una red.

SMTP (Protocolo de Transferencia de Correo Simple).- protocolo para el intercambio de correo entre 2 o más equipos informáticos.

BIBLIOGRAFIA

Herzog Pete, *OSSTMM3 The Open Sorce Security Testing Methodology Manual*, Developed by ISECOM

Manual para comprender y entender el funcionamiento de la metodología OSSTMM

González Pérez, Pablo, Germán, Sánchez Garcés, José Miguel, Soriano de la Cámara. (2013) : *Pentesting con Kali*, Madrid: 0xWORD.

Útil para hacer uso de la herramienta Kali y poder realizar las comprobaciones manuales del testing, mediante el uso de varias de sus aplicaciones.

McClure Sturat, Joel Scambray, Kurtz George, 2010: *HACKERS 6 Secretos y soluciones de seguridad en redes*, Madrid: Mac Graw Hill.

Ayuda con pautas para conocer algunos tipos de ataques y su aseguramiento.

Aharoni Mati, 2007: *Offensive Securitty Lab Exercises v.2.0*, Vitalie Andriyo Dobrovolschi.

Útil para conocer comandos y scripts para el pentesting

Aharoni Mati, (varios autores más), Tutorial de Metasploit Framework de Offensive-Securitty, cyberlocos.net

Manual de uso de exploits con fines de prueba

Calderón Pale Paulino, *Mastering the Nmap Scripting Engine Master the Nmap Scripting Engine and the art of developing NSE scripts*, www.allittebooks.com

Pdf muy interesante sobre el uso de scripts para la herramienta NMAP

ISO 20072.ES. Disponible en iso270072.es/ido27002.html, visitada el (15 abril del 2018)

Página que nos ayuda en la descripción y controles de la norma ISO 27002

ANEXOS

ANEXO 1 CANALES DEL OSSTMM			
PRUEBAS DE SEGURIDAD HUMANAS			
Módulo	**TAREA**	**DESCRIPCION**	**REVISAR**
Revisión Postura	- Revisar y verificar las políticas, legislaciones y regulaciones implementadas	- Mantienen políticas sobre la seguridad de la información, sobre el uso y propiedad intelectual de activos de la Universidad	- Directrices para seguridad de la información - Revisar organización interna -Revisar Política sobre control de accesos - Revisar documentos con firmas sobre la confidencialidad del uso de activos
Logística	-Revisar los canales o medios de comunicación del activo hacia el receptor para limitar la revisión	- Que función cumple el activo en la infraestructura	- Revisar si mantiene inventario de equipos y su función
Detección Activa	- Monitoreo y control de las tareas sobre la gestión de calidad del activo hacia el usuario y modo de almacenamiento de sus registros	- Procedimiento de uso del activo	- Revisar la gestión para la responsabilidad sobre activos en aspectos de: - Monitoreo del activo - Supervisión del activo - Operación del activo
Verificación de Visibilidad	- Determinar los objetivos del activo dentro de la infraestructura	- Que función cumple el activo en la infraestructura	- Revisar la clasificación de activos y sus interacciones con: Acceso de identificación Personal Enumeración
Verificación Acceso	- Registrar los procesos correctos y fallas en la gestión de acceso a los activos	- Como se realiza el acceso o interactuación hacia el activo en la infraestructura	- Enumerar los puntos de acceso en interacción de activos con el usuario -Verificar accesos de proveedores de servicios hacia activos
Verificación de Confianza	- Evaluar y documentar la gestión de acceso a los activos en base a la relación de confianza	- Los procedimientos antiguos o jerárquicos de acceso a activos son verificados con una gestión correcta o son pasados por alta	- Verificar seguridad en accesos de activos con usuarios no responsables o no autorizados (externas al área) por medio de: Declaraciones falsas Fraude Phishing
Verificación Controles	- Enumerar y probar los procedimientos implementados con la finalidad de cumplir con los controles reales a los activos	- Control implementado y sus rutinas para acceder a los activos	- Revisar los requisitos de la institución para el control de accesos a activos - Revisar la gestión del acceso a usuarios, sistemas y aplicaciones - Existe auditoria frente a los accesos - Revisar responsabilidades y procedimientos de operación - Verificar si se mantiene controles: Criptográficos Copias de seguridad

			Control del software en explotación Control de código maligno
Verificación Entrenamiento	- Evaluar el conocimiento de a cerca de la seguridad informática y de la información en la institución	- Conocer y diferenciar sobre la seguridad informática y de la información	- Revisar si conoce la política institucional de seguridad de la información - Frecuencia de capacitación sobre la seguridad de la información Conciencia Secuestro - Diferencia entre información confidencial y pública de la institución
Verificación Propiedad	- Verificar el grado en que la administración de un activo con propiedad intelectual de la institución es usado dentro o fuera de la infraestructura	- Existe clausulas y gestión sobre los derechos de la propiedad intelectual institucional	- Política de uso de dispositivos para la movilidad - Procedimiento sobre manejo de soportes de almacenamiento -Procedimientos para la entrega de activos - Procedimientos para el traslado de activos
Revisión de Segregación	- Identificar los niveles de información privada definido en la postura	- Conocer como están aplicados los derechos de privacidad en la información y en qué medida está desplegada	Privacidad Mapeo de Contención Información Evidente Divulgación Limitaciones
Verificación Accesos	- Revisar el cumplimiento de accesos según la política institucional lo define	- Conocer la forma de acceso en la interconexión con el activo	- Verificar la gestión de accesos a activos de la información según los niveles de contención mediante: Privilegios Identificación. Autorización Estalación
Verificación Exposición	- Identificación de información de libre acceso del activo dentro del canal elegido	- Buscar información del activo en fuentes públicas	- Revisar la definición del activo especialmente de la información frente a los intereses de la institución
Inteligencia Competitiva	- Buscar Información de libre acceso que pueda dañar o afectar en medios externos o de la competencia	- Definir la existencia de mayor valor sobre los procesos y objetivos del activo, que influyan en las decisiones de la competencia	- Buscar posibles relaciones entre usuarios y personas externas de la institución con afinidad en instituciones de educación mediante redes sociales
Verificación Aislamiento	- Determinar y medir el uso del aislamiento del activo dentro del canal	- Determinar la efectividad de los controles de autenticación y sometimiento en base de listas blancas y negras	- Revisar la seguridad del activo según su clasificación frente a los demás activos del canal

Auditoría Privilegios	- Verificación de la gestión de procesos para identificación, autorización de accesos, así como de las deficiencias de su aplicación como en correos o llamadas telefónicas	- Buscar la forma de interactuación de los activos	- Validar los tipos de privilegios para alcanzar los activos respectivos mediante: Identificación Autorización Escalamiento Discriminación.
Continuidad del servicio	- Verificar que al producirse algún error en un activo este no interfiera o detenga el trabajo de la institución	- Buscar la continuidad del canal frente a una falla del canal	- Verificar procedimientos para continuación del negocio - Verificar redundancia de activos - Verificar registro de alarmas frente a situaciones anómalas que permitan el pronto accionar de los usuarios encargados de los activos de seguridad
PRUEBAS DE SEGURIDAD FÍSICA			
Revisión Postura	- Revisar y verificar las políticas, legislaciones y regulaciones de implementaciones según estándares implementadas sobre climatización, sanidad ambiental y fenómenos naturales	- Buscar lineamientos sobre la seguridad física dentro de la institución	- Revisar - Políticas de seguridad física al acceso de los diferentes departamentos de la institución
Revisión de Logística	- Verificar que la gestión física a la seguridad de activos se encuentre correctamente implementada que medios tiene para detectar irregularidades		- Revisar los tipos de controles físicos
Verificación de Acceso	- Revisar pruebas para la enumeración de puntos de acceso para interactuar con los objetivos y activos dentro del alcance. Esta auditoría se limita a la interacción del alcance únicamente para proteger los derechos de propiedad de terceros.	- Formas seguras para acceder a los activos En este módulo se busca verificar las medidas de seguridad del perímetro para los activos de la red.	- Revisar - Áreas de acceso a activos sean seguras mediante el uso de cámaras, puertas especiales para acceso - Áreas de ubicación de activos sean protegidas de amenazas externas y ambientales - Procedimiento de uso, traslado y mantenimiento de activos entre las diferentes áreas
			Tarea 1: Verificar los controles de acceso físico o las paredes del área deben estar sólidas y sin ninguna brecha que facilite cualquier violación. O Las puertas y ventanas del cuarto deben tener cerradura. O Presencia de un sistema de control de intrusos. O Registro de la entrada de visitantes. o El equipo se encuentra ubicado de manera que evite que Cualquiera sin autorización pueda manipular las conexiones. o El equipo se encuentra protegido en

			un gabinete con Cerradura o un cuarto con cerradura en la puerta y ventanas.
			Tarea 2: Verificar las protecciones contra amenazas físicas. o Se evita tener elementos que propaguen o provoquen un Incendio dentro del cuarto. o Se cuenta con equipo contra incendio apropiado y acorde con Los requerimientos que exige el cuarto. o Se debería contar con sistemas para el monitoreo de las Condiciones ambientales.
			Tarea 3: Verificar el cableado en los equipos. O Los cables se encuentran debidamente rotulados. O Los cables se encuentran ordenados. o Los cables están protegidos evitando cualquier interceptación O daño físico.
			Tarea 4: Verificar que el cuarto cumpla con los estándares apropiados para el buen funcionamiento de los sistemas de información.
Verificación de Confianza	- Evaluar y documentar la gestión de seguridad física de acceso a los activos en base a la relación de confianza a los activos sin la necesidad de identificación o autenticación	- Testear y documentar la gestión implementación de controles al acceso de activos de forma tergiversada, como miembro de otro departamento, fraudulenta como personal especializado. Las faltas de identificación, abusos en el uso de los recursos valiéndose de niveles de confianza si presentación de las respectivas credenciales	- Revisar - Ubicación de áreas públicas de atención a personal externo sea fuera de áreas de trabajo - Identificación para personal de visita fuera de la institución - Identificación de usuarios que prestan servicios temporales dentro de las áreas tecnológicas
Alerta y Registros	- Un análisis de la brecha entre las actividades llevadas a cabo con la prueba y la verdadera profundidad de esas actividades registradas o desde las percepciones de terceros, tanto humanos como mecánicos.	- Registros y monitores de movimiento hacia los diferentes activos	- Revisar la existencia de registros del acceso, traslado, retiro o cambio de activos
PRUEBAS DE SEGURIDAD WIRELESS			
Revisión Postura	- Revise y documente cualquier sistema, software y aplicaciones de servicio que requieran cuidado especial debido al alto uso, inestabilidades o		- Revisar y verificar las políticas legislaciones y regulaciones implementadas, así como los acuerdos y acuerdos de nivel de servicio (SLA) con proveedores de servicios y otros.

	una alta tasa de cambio.		
Demás Métodos			- Para la revisión de los demás métodos que pertenecen a este canal es necesario realizar pruebas de penetración de las diferentes redes.
Alerta y Registros	- Comprobar si los controles están en su lugar para bloquear las señales (bloqueo) o alertar sobre actividades no autorizadas.		-Verificar y enumerar el uso de un sistema de advertencia localizado localmente donde el personal detecta una situación sospechosa sospecha de intentos de elusión, ingeniería social o actividad fraudulenta. - Documentar la gestión de registro de esta información
PRUEBAS DE SEGURIDAD TELECOMUNICACIONES			
Revisión Postura	- Revise y documente cualquier sistema, software y aplicaciones de servicio que requieran cuidado especial debido al alto uso, inestabilidades o una alta tasa de cambio.		- Revisar y verificar las políticas legislaciones y regulaciones implementadas, así como los acuerdos y acuerdos de nivel de servicio (SLA) con proveedores de servicios y otros. - Resoluciones que rigen la interceptación de telecomunicaciones
Demás Métodos			- Revisar falencias en la red cableada u IEE 802.3 - Para la revisión de los demás métodos que pertenecen a este canal es necesario realizar pruebas de penetración de las diferentes redes.
Alerta y Registros	- Comprobar si los controles están en su lugar para bloquear las señales (bloqueo) o alertar sobre actividades no autorizadas.		-Verificar y enumerar el uso de un sistema de advertencia localizado localmente donde el personal detecta una situación sospechosa sospecha de intentos de elusión, ingeniería social o actividad fraudulenta. - Documentar la gestión de registro de esta información
PRUEBAS DE SEGURIDAD RED DE DATOS			
Revisión Postura	- Revise y documente cualquier sistema, software y aplicaciones de servicio que requieran cuidado especial debido al alto uso, inestabilidades o una alta tasa de cambio.		- Revisar y verificar las políticas legislaciones y regulaciones implementadas, así como los acuerdos y acuerdos de nivel de servicio (SLA) con proveedores de servicios y otros. - Resoluciones que rigen la interceptación de telecomunicaciones - Revisar antigüedad del software
Demás Métodos			- Forma de gestionar la seguridad de datos mediante mesa de ayuda - Para la revisión de los demás métodos que pertenecen a este canal para las aplicaciones se realizaran mediante pruebas de penetración de las diferentes redes.

Alerta y Registros	- Comprobar si los controles están en su lugar para bloquear las señales (bloqueo) o alertar sobre actividades no autorizadas.		-Verificar y enumerar el uso de un sistema de advertencia localizado localmente donde el personal detecta una situación sospechosa sospecha de intentos de elusión, ingeniería social o actividad fraudulenta. - Documentar la gestión de registro de esta información

ANEXO 2

MODULOS ESCOGIDOS PARA LA EVALUACION

PRUEBAS DE SEGURIDAD HUMANAS

Módulo	TAREA	DESCRIPCION	REVISAR
Revisión Postura	- Revisar y verificar las políticas, legislaciones y regulaciones implementadas	- Mantienen políticas sobre la seguridad de la información, sobre el uso y propiedad intelectual de activos de la Universidad	- Directrices para seguridad de la información - Revisar organización interna -Revisar Política sobre control de accesos - Revisar documentos con firmas sobre la confidencialidad del uso de activos
Logística	-Revisar los canales o medios de comunicación del activo hacia el receptor para limitar la revisión	- Que función cumple el activo en la infraestructura	- Revisar si mantiene inventario de equipos y su función
Detección Activa	- Monitoreo y control de las tareas sobre la gestión de calidad del activo hacia el usuario y modo de almacenamiento de sus registros	- Procedimiento de uso del activo	- Revisar la gestión para la responsabilidad sobre activos en aspectos de: - Monitoreo del activo - Supervisión del activo - Operación del activo
Verificación de Visibilidad	- Determinar los objetivos del activo dentro de la infraestructura	- Que función cumple el activo en la infraestructura	- Revisar la clasificación de activos y sus interacciones con: Acceso de identificación Personal Enumeración
Verificación Acceso	- Registrar los procesos correctos y fallas en la gestión de acceso a los activos	- Como se realiza el acceso o interactuación hacia el activo en la infraestructura	- Enumerar los puntos de acceso en interacción de activos con el usuario -Verificar accesos de proveedores de servicios hacia activos
Verificación de Confianza	- Evaluar y documentar la gestión de acceso a los activos en base a la relación de confianza	- Los procedimientos antiguos o jerárquicos de acceso a activos son verificados con una gestión correcta o son pasados por alta	- Verificar seguridad en accesos de activos con usuarios no responsables o no autorizados (externas al área) por medio de: Declaraciones falsas Fraude Pichinga

Verificación Controles	- Enumerar y probar los procedimientos implementados con la finalidad de cumplir con los controles reales a los activos	- Control implementado y sus rutinas para acceder a los activos	- Revisar los requisitos de la institución para el control de accesos a activos - Revisar la gestión del acceso a usuarios, sistemas y aplicaciones - Existe auditoria frente a los accesos - Revisar responsabilidades y procedimientos de operación - Verificar si se mantiene controles: Criptográficos Copias de seguridad Control del software en explotación Control de código maligno
Verificación Entrenamiento	- Evaluar el conocimiento de a cerca de la seguridad informática y de la información en la institución	- Conocer y diferenciar sobre la seguridad informática y de la información	- Revisar si conoce la política institucional de seguridad de la información - Frecuencia de capacitación sobre la seguridad de la información. Conciencia Secuestro - Diferencia entre información confidencial y pública de la institución
Verificación Propiedad	- Verificar el grado en que la administración de un activo con propiedad intelectual de la institución es usado dentro o fuera de la infraestructura	- Existe clausulas y gestión sobre los derechos de la propiedad intelectual institucional	- Política de uso de dispositivos para la movilidad - Procedimiento sobre manejo de soportes de almacenamiento -Procedimientos para la entrega de activos - Procedimientos para el traslado de activos
Revisión de Segregación	- Identificar los niveles de información privada definido en la postura	- Conocer como están aplicados los derechos de privacidad en la información y en qué medida está desplegada	Privacidad Mapeo de Contención Información Evidente Divulgación Limitaciones
Verificación Accesos	- Revisar el cumplimiento de accesos según la política institucional lo define	- Conocer la forma de acceso en la interconexión con el activo	- Verificar la gestión de accesos a activos de la información según los niveles de contención mediante: Privilegios Identificación. Autorización Escalamiento
Verificación Exposición	- Identificación de información de libre acceso del activo dentro del canal elegido	- Buscar información del activo en fuentes públicas	- Revisar la definición del activo especialmente de la información frente a los intereses de la institución
Inteligencia Competitiva	- Buscar Información de libre acceso que pueda dañar o afectar en medios externos o de la competencia	- Definir la existencia de mayor valor sobre los procesos y objetivos del activo, que influyan en las decisiones de la competencia	- Buscar posibles relaciones entre usuarios y personas externas de la institución con afinidad en instituciones de educación mediante redes sociales

Verificación Aislamiento	- Determinar y medir el uso del aislamiento del activo dentro del canal	- Determinar la efectividad de los controles de autenticación y sometimiento en base de listas blancas y negras	- Revisar la seguridad del activo según su clasificación frente a los demás activos del canal
Auditoría Privilegios	- Verificación de la gestión de procesos para identificación, autorización de accesos, así como de las deficiencias de su aplicación como en correos o llamadas telefónicas	- Buscar la forma de interactuación de los activos	- Validar los tipos de privilegios para alcanzar los activos respectivos mediante: Identificación Autorización Escalamiento Discriminación.
Continuidad del servicio	- Verificar que al producirse algún error en un activo este no interfiera o detenga el trabajo de la institución	- Buscar la continuidad del canal frente a una falla del canal	- Verificar procedimientos para continuación del negocio - Verificar redundancia de activos - Verificar registro de alarmas frente a situaciones anómalas que permitan el pronto accionar de los usuarios encargados de los activos de seguridad
PRUEBAS DE SEGURIDAD FÍSICA			
Revisión Postura	- Revisar y verificar las políticas, legislaciones y regulaciones de implementaciones según estándares implementadas sobre climatización, sanidad ambiental y fenómenos naturales	- Buscar lineamientos sobre la seguridad física dentro de la institución	- Revisar - Políticas de seguridad física al acceso de los diferentes departamentos de la institución
Revisión de Logística	- Verificar que la gestión física a la seguridad de activos se encuentre correctamente implementada que medios tiene para detectar irregularidades		- Revisar los tipos de controles físicos
Verificación de Acceso	- Revisar pruebas para la enumeración de puntos de acceso para interactuar con los objetivos y activos dentro del alcance. Esta auditoría se limita a la interacción del alcance únicamente para proteger los derechos de propiedad de terceros.	- Formas seguras para acceder a los activos En este módulo se busca verificar las medidas de seguridad del perímetro para los activos de la red.	- Revisar - Áreas de acceso a activos sean seguras mediante el uso de cámaras, puertas especiales para acceso - Áreas de ubicación de activos sean protegidas de amenazas externas y ambientales - Procedimiento de uso, traslado y mantenimiento de activos entre las diferentes áreas
			Tarea 1: Verificar los controles de acceso físico; o las paredes del área deben estar sólidas y sin ninguna brecha que facilite cualquier violación; o las puertas y ventanas del cuarto deben tener cerradura. O Presencia de un sistema de control de intrusos. O Registro de la entrada de visitantes.

			o El equipo se encuentra ubicado de manera que evite que Cualquiera sin autorización pueda manipular las conexiones. o El equipo se encuentra protegido en un gabinete con Cerradura o un cuarto con cerradura en la puerta y ventanas.
			Tarea 2: Verificar las protecciones contra amenazas físicas. o Se evita tener elementos que propaguen o provoquen un Incendio dentro del cuarto. O Se cuenta con equipo contra incendio apropiado y acorde con los requerimientos que exige el cuarto. O Se debería contar con sistemas para el monitoreo de las condiciones ambientales.
			Tarea 3: Verificar el cableado en los equipos. O Los cables se encuentran debidamente rotulados. O Los cables se encuentran ordenados. O Los cables están protegidos evitando cualquier interceptación o daño físico.
			Tarea 4: Verificar que el cuarto cumpla con los estándares apropiados para el buen funcionamiento de los sistemas de información.
Verificación de Confianza	- Evaluar y documentar la gestión de seguridad física de acceso a los activos en base a la relación de confianza a los activos sin la necesidad de identificación o autenticación	- Testear y documentar la gestión implementación de controles al acceso de activos de forma tergiversada, como miembro de otro departamento, fraudulenta como personal especializado. Las faltas de identificación, abusos en el uso de los recursos valiéndose de niveles de confianza si presentación de las respectivas credenciales	- Revisar - Ubicación de áreas públicas de atención a personal externo sea fuera de áreas de trabajo - Identificación para personal de visita fuera de la institución - Identificación de usuarios que prestan servicios temporales dentro de las áreas tecnológicas
Alerta y Registros	- Un análisis de la brecha entre las actividades llevadas a cabo con la prueba y la verdadera profundidad de esas actividades registradas o desde las percepciones de terceros, tanto humanos como mecánicos.	- Registros y monitores de movimiento hacia los diferentes activos	- Revisar la existencia de registros del acceso, traslado, retiro o cambio de activos
PRUEBAS DE SEGURIDAD WIRELESS			

Revisión Postura	- Revise y documente cualquier sistema, software y aplicaciones de servicio que requieran cuidado especial debido al alto uso, inestabilidades o una alta tasa de cambio.		- Revisar y verificar las políticas legislaciones y regulaciones implementadas, así como los acuerdos y acuerdos de nivel de servicio (SLA) con proveedores de servicios y otros.
Demás Métodos			- Para la revisión de los demás métodos que pertenecen a este canal es necesario realizar pruebas de penetración de las diferentes redes.
Alerta y Registros	- Comprobar si los controles están en su lugar para bloquear las señales (bloqueo) o alertar sobre actividades no autorizadas.		-Verificar y enumerar el uso de un sistema de advertencia localizado localmente donde el personal detecta una situación sospechosa sospecha de intentos de elusión, ingeniería social o actividad fraudulenta. - Documentar la gestión de registro de esta información
PRUEBAS DE SEGURIDAD TELECOMUNICACIONES			
Revisión Postura	- Revise y documente cualquier sistema, software y aplicaciones de servicio que requieran cuidado especial debido al alto uso, inestabilidades o una alta tasa de cambio.		- Revisar y verificar las políticas legislaciones y regulaciones implementadas, así como los acuerdos y acuerdos de nivel de servicio (SLA) con proveedores de servicios y otros. - Resoluciones que rigen la interceptación de telecomunicaciones
Demás Métodos			- Revisar falencias en la red cableada u IEE 802.3 - Para la revisión de los demás métodos que pertenecen a este canal es necesario realizar pruebas de penetración de las diferentes redes.
Alerta y Registros	- Comprobar si los controles están en su lugar para bloquear las señales (bloqueo) o alertar sobre actividades no autorizadas.		-Verificar y enumerar el uso de un sistema de advertencia localizado localmente donde el personal detecta una situación sospechosa sospecha de intentos de elusión, ingeniería social o actividad fraudulenta. - Documentar la gestión de registro de esta información
PRUEBAS DE SEGURIDAD RED DE DATOS			
Revisión Postura	- Revise y documente cualquier sistema, software y aplicaciones de servicio que requieran cuidado especial debido al alto uso, inestabilidades o una alta tasa de cambio.		- Revisar y verificar las políticas legislaciones y regulaciones implementadas, así como los acuerdos y acuerdos de nivel de servicio (SLA) con proveedores de servicios y otros. - Resoluciones que rigen la interceptación de telecomunicaciones - Revisar antigüedad del software

Demás Métodos			- Forma de gestionar la seguridad de datos mediante mesa de ayuda - Para la revisión de los demás métodos que pertenecen a este canal para las aplicaciones se realizaran mediante pruebas de penetración de las diferentes redes.
Alerta y Registros	- Comprobar si los controles están en su lugar para bloquear las señales (bloqueo) o alertar sobre actividades no autorizadas.		-Verificar y enumerar el uso de un sistema de advertencia localizado localmente donde el personal detecta una situación sospechosa sospecha de intentos de elusión, ingeniería social o actividad fraudulenta. - Documentar la gestión de registro de esta información

ANEXO 3
DESCUBRIMIENTO EN SERVIDORES OUTSIDER

DOMINIO	IP	SISTEMA OPERATIVO	Observación			
			PTO	SERVICIO	VERSION	Observación
	xxx.xxx.225.12	Linux 2.6.X| 3.X (91%)	80/tcp	HTTP	APACHE HTTP	OPEN
			443/tcp	SSL/HTTPS	APACHE HTTP	OPEN
			25/tcp	SMTP		FILTRADO
axxx.ups.edu.ec host: pxxx.ups.edu.ec	xxx.xxx.89.77	Linux 2.6.32 (91%)	80/tcp	HTTP	Apache httpd 2.2.15	OPEN
			443/tcp	SSL/HTTPS	Apache httpd 2.2.15 ((CentOS))	OPEN
			8080/tcp	HTTP	Apache Tomcat/Coyote JSP engine 1.1	OPEN
			25/tcp	SMTP		FILTRADO
cxxx.ups.edu.ec	xxx.xxx.225.198	Linux 2.6.32 (89%)	80/tcp	HTTP	Apache httpd 2.2.15	OPEN
			443/tcp	SSL/HTTPS	Apache httpd 2.2.15	OPEN
			8080/tcp	HTTP	Apache Tomcat/Coyote JSP engine 1.1	OPEN
			25/tcp	SMTP		FILTRADO
	xxx.xxx.243.235	Linux 2.6.32 (91%)	80/tcp	HTTP	Apache httpd 2.2.15	OPEN
			443/tcp	SSL/ATTPS	Apache httpd 2.2.15	OPEN
			25/tcp	SMTP		FILTRADO
vps-1406505-x.dattaweb.com	xxx.xxx.42.76	FreeBSD 9.0-RELEASE (89%)	80/tcp	HTTP	nginx 1.12.2	OPEN unfiltered
			443/tcp	HTTPS		CLOSED unfiltered
			3389/tcp	ms-wbt-server		CLOSED unfiltered
			4848/tcp	appserv-http		CLOSED unfiltered
			5432/tcp	postgresql	PostgreSQL DB	OPEN unfiltered

			8080/tcp open	HTTP-proxy	Apache Tomcat/Coyote JSP engine 1.1	OPEN unfiltered
qxxx.ups.edu.ec	xxx.xxx223.195	Linux 2.6.32 (91%)	80/tcp	HTTP	Apache httpd 2.2.15	OPEN
			443/tcp	HTTPS	Apache httpd 2.2.15 ((CentOS))	OPEN
			25/tcp	SMTP		FILTRADO
exxx.ups.edu.ec host: servicesapp.ups.edu.ec	xxx.xxx.225.194	Linux 2.6.32 (91%)	80/tcp	HTTP	Apache httpd 2.2.15	OPEN
			443/tcp	HTTPS	Apache httpd 2.2.15 ((CentOS))	OPEN
			5666/tcp	tcpwrapped		
			25/tcp	SMTP		FILTRADO
vxxx.ups.edu.ec	xxx.xxx.199.89	Vodavi XTS-IP PBX (87%) Linux 2.6.8 (Debian, x86) (87%)	22/tcp	ssh	OpenSSH 7.4 (protocol 2.0)	OPEN unfiltered
			80/tcp	HTTP	nginx	OPEN unfiltered
			443/tcp	HTTPS		CLOSED unfiltered
			587/tcp	submission		CLOSED unfiltered
www.ups.edu.ec	xxx.xxx.89.75	Linux 2.6.32 (91%)	80/tcp	HTTP	APACHE HTTP	OPEN
			443/tcp	SSL/HTTPS	APACHE HTTP	OPEN
			25/tcp	SMTP		FILTRADO
www.bxxx.ups.edu.ec	xxx.xxx.243.234	Linux 2.6.32 (91%)	80/tcp	HTTP	Apache httpd 2.2.15	OPEN
			443/tcp	HTTPS	Apache httpd 2.2.15 ((CentOS))	OPEN
			25/tcp	SMTP		FILTRADO
ec2-54-69-154-224.us-west-2.compute.amazonaws.com	xxx.xxx.154.224	HP P2000 G3 NAS device (90%) Linux 2.6.18 (88%)	22/tcp	ssh	OpenSSH 5.3 (protocol 2.0)	OPEN unfiltered
			80/tcp	http	Apache httpd 2.2.15 ((Red Hat))	OPEN unfiltered
			465/tcp	smtps		CLOSED unfiltered
			3306/tcp	mysql	MySQL (unauthorized)	OPEN unfiltered
host-181-39-29-196.telconet.net host: hxxx.ups.edu.ec	xxx.xxx.29.196	Linux 2.6.32 (91%)	80/tcp	http	Apache httpd 2.2.15	OPEN
			443/tcp	ssl/http	Apache Tomcat/Coyote JSP engine 1.1	OPEN
			8443/tcp	ssl/http	Apache httpd 2.2.15 ((CentOS); SSL-only mode)	OPEN
			25/tcp	SMTP		FILTRADO
mxxx.cue.ups.edu.ec	xxx.xxx.89.76	Linux 3.16 (85%) Foundry Networks BigIron 8000 switch (IronWare 07.8.02eT53) (89%)	80/tcp	http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/ 5.4.16)	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/ 5.4.16)	OPEN unfiltered

sxxx.ups.edu.ec	xxx.xxx.225.11	Linux 2.6.32 (91%)	80/tcp	HTTP	Apache httpd 2.2.15	OPEN
			443/tcp	HTTPS	Apache httpd 2.2.15 ((CentOS))	OPEN
			5666/tcp	tcpwrapped		
			25/tcp	SMTP		FILTRADO
	xxx.xxx243.236	Foundry Networks BigIron 8000 switch (IronWare 07.8.02eT53) (89%)	443/tcp	ssl/http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips mod_cluster/1.3.1.Final)	OPEN unfiltered
			8443/tcp	ssl/http	Apache httpd 2.2.15 ((CentOS) mod_jk/1.2.40 mod_ssl/2.2.15 OpenSSL/ 1.0.1e-fips)	OPEN unfiltered
	xxx.xxx.55.101	Linux 2.6.39 (89%)	21/tcp	ftp	Pure-FTPd	OPEN
			26/tcp	rsftp		CLOSED
			53/tcp	domain?		OPEN
			80/tcp	http	Apache httpd 2.2.29 ((Unix) mod_ssl/2.2.29 OpenSSL/1.0.1e-fips mod_bwlimited/1.4)	OPEN
			110/tcp	pop3	Dovecot pop3d	OPEN
			143/tcp	imap	Dovecot imapd	OPEN
			443/tcp	ssl/http	Apache httpd 2.2.29 ((Unix) mod_ssl/2.2.29 OpenSSL/1.0.1e-fips mod_bwlimited/1.4)	OPEN
			465/tcp	smtps?		OPEN
			993/tcp	imaps?		OPEN
			995/tcp	pop3s?		OPEN
			3306/tcp	mysql	MySQL (unauthorized)	OPEN
			8080/tcp	http-proxy		CLOSED
			25/tcp	SMTP		FILTRADO
host-181-39-29-194.telconet.net host: bxxx.ups.edu.ec	xxx.xxx.29.194	Linux 2.6.32 (88%)	80/tcp	http	Apache httpd 2.2.15	OPEN
			443/tcp	ssl/http	Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.7)	OPEN
			8088/tcp	http	Apache Tomcat/Coyote JSP engine 1.1	OPEN
			25/tcp	SMTP		FILTRADO
axxx.ups.edu.ec	xxx.xxx.89.77	Linux 2.6.32 (91%)	80/tcp	http	Apache httpd 2.2.15	OPEN
			443/tcp	ssl/http	Apache httpd 2.2.15 ((CentOS))	OPEN
			8080/tcp	http	Apache Tomcat/Coyote JSP engine 1.1	OPEN
			25/tcp	SMTP		FILTRADO

ANEXO 4 DESCUBRIMIENTO EN SERVIDORES INSIDER						
DOMINIO	IP	SISTEMA OPERATIVO	Observación			
			PTO	SERVICIO	VERSION	Observación
dxxx.ups.edu.ec	xxx.xxx.1.18	Linux 2.6.32	80/tcp	HTTP	Apache httpd	OPEN unfiltered
			443/tcp	SSL/HTTPS	Apache httpd	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
mxxx.ups.edu.ec	xxx.xxx.1.23	Linux 2.6.32	443/tcp	https		CLOSED unfiltered
			8443/tcp	ssl/http	Apache httpd 2.2.15 ((CentOS) mod_jk/1.2.40 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips)	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
gxxx.ups.edu.ec	xxx.xxx1.26	Linux 2.6.32 (94%)	80/tcp	http	Apache httpd 2.4.6 ((CentOS) PHP/7.0.24 OpenSSL/1.0.2k-fips)	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd 2.4.6 ((CentOS) PHP/7.0.24 OpenSSL/1.0.2k-fips)	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
bxxx.ups.edu.ec	xxx.xxx.1.57	Linux 2.6.32	80/tcp	http	Apache httpd 2.2.15	OPEN unfiltered
			443/tcp	ssl/http	Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.7)	OPEN unfiltered
			8088/tcp	http	Apache Tomcat/Coyote JSP engine 1.1	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
axxx.ups.edu.ec	xxx.xxx.1.58	Linux 2.6.32	80/tcp	http	Apache httpd 2.2.15	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd 2.2.15 ((CentOS))	OPEN unfiltered

			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
	xxx.xxx.1.61	Linux 2.6.32	80/tcp	http	Apache httpd	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd	OPEN unfiltered
			8080/tcp	http	Apache Tomcat/Coyote JSP engine 1.1	OPEN unfiltered
			9080/tcp	glrpc		unfiltered
sxxx.ups.edu.ec	xxx.xxx1.64	Linux 2.6.32 (98%)	80/tcp	http	Apache httpd 2.2.15	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd 2.2.15 ((CentOS))	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
axxx.ups.edu.ec	xxx.xxx.1.68	Linux 2.6.32	80/tcp	http	Apache httpd	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
Host: sxxx.ups.edu.ec	xxx.xxx.1.70	Linux 2.6.32	80/tcp	http	Apache httpd 2.2.15	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd 2.2.15 ((CentOS))	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
qxxx.ups.edu.ec	xxx.xxx.1.81	Linux 2.6.32	80/tcp	http	Apache httpd 2.2.15	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd 2.2.15 ((CentOS))	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
bxxx.ups.edu.ec	xxx.xxx.1.83	Netgear ReadyNAS 3200 NAS device (Linux 2.6) (95%)	80/tcp	http-proxy	EZproxy web proxy	OPEN
			2040/tcp	lam		CLOSED
			2041/tcp	interbase		CLOSED
			2042/tcp	isis		CLOSED
			2043/tcp	isis-bcast		CLOSED
			2045/tcp	cdfunc		CLOSED
			2046/tcp	sdfunc		CLOSED
			2047/tcp	dls		CLOSED
			2048/tcp	dls-monitor		CLOSED
			2049/tcp	nfs		CLOSED
			2065/tcp	http-proxy	EZproxy web proxy	OPEN
			2068/tcp	http-proxy	EZproxy web proxy	OPEN
			2099/tcp	http-proxy	EZproxy web proxy	OPEN

			2100/tcp	http-proxy	EZproxy web proxy	OPEN
			2103/tcp	http-proxy	EZproxy web proxy	OPEN
			2105/tcp	http-proxy	EZproxy web proxy	OPEN
			2106/tcp	http-proxy	EZproxy web proxy	OPEN
			2107/tcp	http-proxy	EZproxy web proxy	OPEN
			2111/tcp	http-proxy	EZproxy web proxy	OPEN
			2119/tcp	http-proxy	EZproxy web proxy	OPEN
			2121/tcp	http-proxy	EZproxy web proxy	OPEN
			2126/tcp	http-proxy	EZproxy web proxy	OPEN
			2135/tcp	http-proxy	EZproxy web proxy	OPEN
			2144/tcp	http-proxy	EZproxy web proxy	OPEN
			2160/tcp	http-proxy	EZproxy web proxy	OPEN
			2170/tcp	http-proxy	EZproxy web proxy	OPEN
			2179/tcp	http-proxy	EZproxy web proxy	OPEN
			2190/tcp	http-proxy	EZproxy web proxy	OPEN
			2191/tcp	http-proxy	EZproxy web proxy	OPEN
			2196/tcp	http-proxy	EZproxy web proxy	OPEN
			2200/tcp	http-proxy	EZproxy web proxy	OPEN
			2222/tcp	http-proxy	EZproxy web proxy	OPEN
			2251/tcp	http-proxy	EZproxy web proxy	OPEN
			2260/tcp	http-proxy	EZproxy web proxy	OPEN
			2288/tcp	http-proxy	EZproxy web proxy	OPEN
			2301/tcp	http-proxy	EZproxy web proxy	OPEN
			2323/tcp	http-proxy	EZproxy web proxy	OPEN
			2366/tcp	http-proxy	EZproxy web proxy	OPEN
			2381/tcp	http-proxy	EZproxy web proxy	OPEN
			2382/tcp	http-proxy	EZproxy web proxy	OPEN
			2383/tcp	http-proxy	EZproxy web proxy	OPEN
			2393/tcp	http-proxy	EZproxy web proxy	OPEN
			2394/tcp	http-proxy	EZproxy web proxy	OPEN
			2399/tcp	http-proxy	EZproxy web proxy	OPEN
			2401/tcp	cvspserver		CLOSED
			2492/tcp	http-proxy	EZproxy web proxy	OPEN
			2500/tcp	http-proxy	EZproxy web proxy	OPEN
			2522/tcp	http-proxy	EZproxy web proxy	OPEN
			2525/tcp	http-proxy	EZproxy web proxy	OPEN
			2557/tcp	http-proxy	EZproxy web proxy	OPEN
			2601/tcp	http-proxy	EZproxy web proxy	OPEN
			2602/tcp	http-proxy	EZproxy web proxy	OPEN
			2604/tcp	http-proxy	EZproxy web proxy	OPEN
			2605/tcp	http-proxy	EZproxy web proxy	OPEN
			2607/tcp	http-proxy	EZproxy web proxy	OPEN

			2608/tcp	http-proxy	EZproxy web proxy	OPEN
			2638/tcp	http-proxy	EZproxy web proxy	OPEN
			2701/tcp	http-proxy	EZproxy web proxy	OPEN
			2702/tcp	http-proxy	EZproxy web proxy	OPEN
			2710/tcp	http-proxy	EZproxy web proxy	OPEN
			2717/tcp	http-proxy	EZproxy web proxy	OPEN
			2718/tcp	http-proxy	EZproxy web proxy	OPEN
			2725/tcp	http-proxy	EZproxy web proxy	OPEN
			2800/tcp	http-proxy	EZproxy web proxy	OPEN
			2809/tcp	http-proxy	EZproxy web proxy	OPEN
			2811/tcp	http-proxy	EZproxy web proxy	OPEN
			8080/tcp	http-proxy		CLOSED
			9080/tcp	glrpc		CLOSED
Host: pxxx.ups.edu.ec	xxx.xxx.1.84		80/tcp	http	Apache httpd 2.2.15	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd 2.2.15 ((CentOS))	OPEN unfiltered
			8080/tc	http	Apache Tomcat/Coyote JSP engine 1.1	OPEN unfiltered
			9080/tcp	glrpc		unfiltered
axxx.ups.edu.ec	xxx.xxx.1.87	Linux 2.6.32 (98%)	80/tcp	http	Apache httpd 2.4.6 ((CentOS) mod_jk/1.2.40 OpenSSL/1.0.2k-fips)	OPEN unfiltered
			443/tcp	ssl/http	Oracle GlassFish 4.1 (Servlet 3.1; JSP 2.3; Java 1.7)	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
www.bxxx.ups.edu.ec	xxx.xxx1.91	Linux 2.6.32 (98%)	80/tcp	http	Apache httpd 2.2.15	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd 2.2.15 ((CentOS))	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
	xxx.xxx.1.95	Netgear ReadyNAS 3200 NAS device (Linux 2.6) (93%)	80/tcp	http	Apache httpd 2.4.6 ((CentOS) mod_jk/1.2.40 OpenSSL/1.0.1e-fips)	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
axxx.ups.edu.ec	xxx.xxx.1.103	Linux 2.6.32	80/tcp	http	Apache httpd 2.2.15 ((CentOS))	OPEN unfiltered
			8080/tcp	http	Apache Tomcat/Coyote JSP engine 1.1	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
sexxx.ups.edu.ec	xxx.xxx.1.131	Linux 2.6.32	80/tcp	http	Apache httpd 2.2.15	OPEN unfiltered

			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
	xxx.xxx1.160	Netgear ReadyNAS 3200 NAS device (Linux 2.6) (95%)	80/tcp	http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips mod_cluster/1.3.1.Final)	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips mod_cluster/1.3.1.Final)	OPEN unfiltered
			8080/tcp	http-proxy		CLOSED unfiltered
			9080/tcp	glrpc		CLOSED unfiltered
	xxx.xxx.1.184		80/tcp	http		unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
axxx.ups.edu.ec	xxx.xxx.1.199	Linux 2.6.32 (94%)	80/tcp	http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)	OPEN unfiltered
			443/tcp	ssl/http	Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)	OPEN unfiltered
			8080/tcp	http-proxy	Apache Tomcat/Coyote JSP engine 1.1	OPEN unfiltered
			9080/tcp	glrpc		unfiltered
	xxx.xxx.1.200	Linux 2.6.32	80/tcp	http	Apache httpd 2.4.6 ((CentOS) mod_jk/1.2.40)	OPEN unfiltered
			8080/tcp	http	Oracle GlassFish 4.1 (Servlet 3.1; JSP 2.3; Java 1.7)	OPEN unfiltered
			443/tcp	https		unfiltered
			9080/tcp	glrpc		unfiltered
sxxx.ups.edu.ec	xxx.xxx1.238	Linux 2.6.32	80/tcp	http	Apache httpd 2.2.15	OPEN unfiltered
			443/tcp	ssl/http	Oracle GlassFish 3.1.2.2 (Servlet 3.0; JSP 2.2; Java 1.7)	OPEN unfiltered
			8080/tcp	http-proxy		unfiltered
			9080/tcp	glrpc		unfiltered
vxxx.ups.edu.ec	xxx.xxx.199.89	F5 BIG-IP load balancer (92%)	80/tcp	http	nginx	OPEN unfiltered
			443/tcp	https		OPEN unfiltered
	xxx.xxx.1.2	Linux 2.6.18 (88%),	80/tcp	http		OPEN unfiltered
			443/tcp	https		OPEN unfiltered
	xxx.xxx.101.8	Linux 2.6.32 - 3.10	80/tcp	http	Oracle Application Server 11g httpd	OPEN
			7001/tcp	http	Oracle WebLogic Server	OPEN

					(Servlet 2.5; JSP 2.1)	
			9001/tcp	http	Oracle WebLogic Server (Servlet 2.5; JSP 2.1)	OPEN
			9002/tcp	http	Oracle WebLogic Server (Servlet 2.5; JSP 2.1)	OPEN

ANEXO 5
RESULTADO DEL DESCUBRIMIENTO DE PUERTOS

RESUMEN DE ESCANEO DE PUERTOS visibilidad OUTSIDER

IP HOST	HOSTNAME	SISTEMA OPERATIVO	PUERTOS				REVISAR
			OPEN	FILTER	SIN FILTRO	CLOSED	
xxx.xxx.225.12	axxx.ups.edu.ec	Linux 2.6	80, 443	25			Pto. Filtrado sin servicio
xxx.xxx.89.77	pxxx.ups.edu.ec	Linux 2.6	80, 443, 8080	25			Pto. Filtrado sin servicio
xxx.xxx.225.198	cxxx.ups.edu.ec	Linux 2.6	80, 443, 8080	25			Pto. Filtrado sin servicio
xxx.xxx.243.235	dxxx.ups.edu.ec	Linux 2.6	80, 443	25			Pto. Filtrado sin servicio
xxx.xxx.42.76	ixxx.ups.edu.ec	FreeBSD 9.0-RELEASE (89%)	80, 5432, 8080			443, 3389, 4848	Pto. Filtrado sin servicio
xxx.xxx.223.195	qxxx.ups.edu.ec	Linux 2.6	80, 443	25			Pto. Filtrado sin servicio
xxx.xxx.225.194	exxx.ups.edu.ec	Linux 2.6	80, 443, 5666	25			Pto. Filtrado sin servicio
xxx.xxx.199.89	vxxx.ups.edu.ec	Linux 2.6.8 (Debian, x86 87%)	22, 80			443, 587	Pto. Filtrado sin servicio
xxx.xxx.89.75	www.ups.edu.ec	Linux.2.6.32	80, 443	25			Pto. Filtrado sin servicio
xxx.xxx.243.234	www.bxxx.ups.edu.ec	Linux.2.6.32	80, 443	25			Pto. Filtrado sin servicio
xxx.xxx.154.224	ec2-54-69-154-224.us-west-2.compute.amazonaws.com	HP P2000 G3 NAS device (90%) Linux 2.6.18 (88%)	22, 80, 3306,			465	Pto. Filtrado sin servicio
xxx.xxx.29.196	hxxx.ups.edu.ec	Linux.2.6.32 (91%)	80, 443, 8443	25			Pto. Filtrado sin servicio
xxx.xxx.89.76	mxxx.cue.ups.edu.ec	Linux 3.16 (85%)	80, 443				Pto. Filtrado sin servicio
xxx.xxx.225.11	sxxx.ups.edu.ec	Linux.2.6.32 (91%)	80, 443, 5666	25			Pto. Filtrado sin servicio
xxx.xxx.243.236		Foundry Networks	443, 8443				Pto. Filtrado sin servicio

xxx.xxx.55.101		Linux 2.6.39	21, 53, 80, 110, 143, 465, 993, 995, 3306,	25		26, 8080	Pto. Filtrado sin servicio, si todos los servicios están desplegados
xxx.xxx.29.194	bxxx.ups.edu.ec	Linux.2.6.32 (91%)	80, 443, 8080	25			Pto. Filtrado sin servicio

RESUMEN DE ESCANEO DE PUERTOS visibilidad INSIDER

IP HOST	HOSTNAME	SISTEMA OPERATIVO	PUERTOS				OBSERVACION
			OPEN	FILTER	SIN FILTRO	CLOSED	
xxx.xxx.1.8	www.uxxx.edu.ec	Linux 2.6.32	80, 443,		8080, 9080		Pto. sin Filtrado
xxx.xxx.5.50	www.uxxx.edu.ec		200, 5060, 8008, 3268, 3269, 3389, 49153, 49154, 49155, 49158, 49159				Pto. sin Filtrado, y si todos los servicios desplegados son necesarios
xxx.xxx.42.47			80, 443				Pto. sin Filtrado
xxx.xxx.1.18	dxxx.ups.edu.ec	Linux 2.6.32	80,		8080, 9080	443,	Pto. sin Filtrado
xxx.xxx.1.23	mxxx.ups.edu.ec	Linux 2.6.32	443, 8443		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.26	gxxx.ups.edu.ec	Linux 2.6.32	80, 443		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.57	bxxx.ups.edu.ec	Linux 2.6.32	80, 443, 8088		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.58	axxx.ups.edu.ec	Linux 2.6.32	80, 443		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.61	cxxx.ups.edu.ec	Linux 2.6.32	80, 443		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.64	sxxx.ups.edu.ec	Linux 2.6.32	80, 443		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.68	axxx.ups.edu.ec	Linux 2.6.32	80, 443		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.70	sxxx.ups.edu.ec	Linux 2.6.32	80, 443		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.81	qxxx.ups.edu.ec	Linux 2.6.32	80, 443		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.83	bxxx.ups.edu.ec	Linux 2.6	80, 2065, 2068, 2099, 2100, 2103, 2105, 2106, 2107, 2111, 2119,			2040, 2041, 2042, 2043, 2045, 2046, 2048, 2049, 2401, 8080, 9080	Pto. Cerrados sin servicios eliminar

			2121, 2126, 2135, 2144, 2160, 2170, 2179, 2179, 2190, 2191, 2196, 2200, 2222, 2251, 2260, 2288, 2301, 2323, 2366, 2381, 2382, 2383, 2393, 2394, 2399, 2492, 2500, 2522, 2525, 2601, 2602, 2604, 2605, 2607, 2608, 2638, 2701, 2702, 2710, 2717, 2718, 2725, 2800, 2809, 2811,				
xxx.xxx.1.84	pxxx.ups.edu.ec	Linux 2.6.32	80, 443, 8080		9080		Pto. sin Filtrado
xxx.xxx.1.87	axxx.ups.edu.ec	Linux 2.6.32	80, 443		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.91	www.bxxx.ups.edu.ec	Linux 2.6.32	80, 443		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.95		Linux 2.6	80		8080, 9080		Pto. sin Filtrado
xxx.xxx.1.103	axxx.ups.edu.ec	Linux 2.6.32	80, 443, 8080		9080, 8080		Pto. sin Filtrado
xxx.xxx.1.131	sxxxx.ups.edu.ec	Linux 2.6.32	80		9080, 8080		Pto. sin Filtrado
xxx.xxx.1.160		Linux 2.6	80, 443			8080, 9080	Pto. Cerrados sin servicio eliminar
xxx.xxx.1.184					80, 8080, 9080		Pto. sin Filtrado

xxx.xxx.1.199	axxx.ups.edu.ec	Linux 2.6.32	80, 443, 8080		9080		Pto. sin Filtrado
xxx.xxx.1.200		Linux 2.6.32	80, 8080		9080, 443		Pto. sin Filtrado
xxx.xxx.199.89	vxxx.ups.edu.ec	F% BIG-IP load balancer	80			443	Pto. sin Filtrado
xxx.xxx.1.2	mxxx.ups.edu.ec	Linux 2.6.18 (88%)	80, 443				Pto. sin Filtrado
xxx.xxx.101.8		Linux 2.6.32-3.10	80, 7001, 9001, 9002				Pto. sin Filtrado

ANEXO 6

VULNERABILIDADES halladas en www.ups.edu.ec OUTSIDER

VULNERABILIDAD	DESCRIPCION	DETALLE	CRITICIDAD	SERVICIO
CVE-2007-6750	Slowloris DOS attack	Slowloris intenta mantener abiertas y retenidas muchas conexiones al servidor web objetivo se abren el mayor tiempo posible. Lo logra abriendo conexiones al servidor web objetivo y enviando una solicitud parcial. Al hacerlo, se queda y los recursos del servidor http que causan la denegación de servicio.	**MEDIA**	HTTP
Http-csrf: https://ixxx.ups.edu.ec:443/ https://ixxx.ups.edu.ec:443/web/guest/bienestar-estudiantil https://ixxx.ups.edu.ec:443/evento-listado https://ixxx.ups.edu.ec:443/noticias?articleId=11635365&version=1.0 https://ixxx.ups.edu.ec:443/web/guest/noticias-archivo https://ixxx.ups.edu.ec:443/web/guest/autoridades https://ixxx.ups.edu.ec:443/web/guest/consultar-ficha-horario https://ixxx.ups.edu.ec:443/web/guest/lineas-de-investigacion https://ixxx.ups.edu.ec:443/web/guest/asociacionismo-salesiano-universitario https://ixxx.ups.edu.ec:443/web/guest/boletin-salesiano https://ixxx.ups.edu.ec:443/web/guest/investigacion	*Cross-site request forgery*	Un ataque CSRF fuerza al navegador validado de una víctima a enviar una petición a una aplicación web vulnerable, la cual entonces realiza la acción elegida a través de la víctima. Al contrario que	**MEDIA**	ssl/http Apache httpd

https://ixxx.ups.edu.ec:443/web/guest/carreras-grado https://ixxx.ups.edu.ec:443/evento?calendarBookingId=11589534 https://ixxx.ups.edu.ec:443/web/guest/tour-virtual-360 https://ixxx.ups.edu.ec:443/web/guest/centros-de-investigacion		en los ataques XSS, los cuales explotan la confianza que un usuario tiene en un sitio en particular, el cross site request forgery explota la confianza que un sitio tiene en un usuario en particular.		
Possible sqli for queries: https://ixxx.ups.edu.ec:443/web/guest/consultar-ficha-horario?	SQL INJECCION	Un ataque por inyección SQL consiste en la inserción o "inyección" de una consulta SQL mediante comandos por medio de los datos de entrada desde el cliente hacia la aplicación, cuando es exitoso puede leer información sensible desde la base de datos.	**MEDIA**	HTTP
Possible sqli for forms: https://ixxx.ups.edu.ec/web/guest/consultar-ficha-horario?	SQL INJECCION	Un ataque por inyección SQL consiste en la inserción o "inyección" de una consulta SQL mediante comandos por medio de los datos de entrada desde el cliente hacia la aplicación, cuando es exitoso puede leer información sensible desde la base de datos.	**MEDIA**	HTTPS
http-trace: TRACE is enabled	HTTP TRACE / TRACK Methods Allowed	El servidor web remoto es compatible con los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan	**MEDIA**	HTTP

		para la depuración de las entradas de los usuarios. En este caso se debe desactivar ya que mediante él se puede ejecutar un ataque web del tipo XSS: Cross-site scripting, un tipo de vulnerabilidad comúnmente encontrada en Servidores Web (Tomcat, Apache, etc.).		
ssl-dh-params:	Diffie-Hellman Key Exchange Insufficient Group Strength	Los servicios de seguridad de la capa de transporte (TLS) que usan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que usan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques pasivos de escuchas ilegales.	**MEDIA**	TLS

ANEXO 7

REVISION DE VULNERABILIDADES EN INFRAESTRUCTURA

REVISION DE POSIBLES VULNERABILIDADES EN SERVIDORES

SISTEMA OPERATIVO O SERVICIO	VULNERABILIDAD	DESCRIPCION	EXPLOIT	CVSS v3 VALOR
Linux 2.6.32	LINUX KERNEL 2.6.32	Una vulnerabilidad clasificada como	Linux Kernel 2.6.32 < 3.x (CentOS 5/6) - 'PERF_EVENTS' Local Privilege	**6 (medi**

	IP_REPOPTS DENEGACIÓN DE SERVICIO **CVE-2013-2224**	problemática fue encontrada en Linux Kernel 2.6.32. Una función desconocida del componente IP_REPOPTS es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase denegación de servicio. Esto tiene repercusión sobre la disponibilidad.	Escalation (1) Linux Kernel 2.6.x - 'pipe.c' Local Privilege Escalation (2) Linux Kernel 2.6.32-rc1 (x86-64) - Register Leak	**o)**
Apache httpd 2.2.15	Aplicación con afección a vulnerabilidad **CVE-2010-2068** Reflejo de memoria sin inicializar en mod_auth_digest	Apache httpd 2.2 tiene un fin de vida útil desde diciembre de 2017 y no debe utilizarse. mod_proxy_http.c en mod_proxy_http en Apache HTTP Server 2.2.9 a 2.2.15, 2.3.4-alpha y 2.3.5-alpha en Windows, NetWare y OS / 2, en ciertas configuraciones que involucran grupos de trabajadores proxy, no detectar adecuadamente los tiempos de espera, lo que permite a los atacantes remotos obtener una respuesta potencialmente sensible destinada a un cliente diferente en circunstancias oportunistas a través de una solicitud HTTP normal.	Apache HTTPD: Timeout detection flaw (mod_proxy_http) (CVE-2010-2068)	**5 (medio)**
Apache Tomcat / Coyote JSP engine 1.1	Aplicación con afección a vulnerabilidad **CVE-2010-0738** Reflejo de memoria sin inicializar en mod_auth_digest	El reconocimiento que realizamos nos permite elegir los módulos de Metasploit que creamos. En primer lugar, tenemos una página de inicio de sesión; esto nos proporciona una forma de crear credenciales de inicio de sesión de fuerza bruta. En segundo lugar, tenemos una interfaz WebDAV y una posible vía para cargar un shell PHP. En tercer lugar, el servidor funciona de forma similar al servidor Apache y es susceptible a los ataques de denegación de servicio.	tomcat mgr login msf > use auxiliary/scanner/http/tomcat_mgr_login Automated Metasploit File Upload use exploit/multi/http/tomcat_mgr_upload	**7.5 (critico)**
Ngnx 1.12.2	Aplicación con	Se está usando nginx /	[Exploit] CVE-2017-7529 / Nginx -	**5**

	afección a vulnerabilidad **CVE-2017-7529**	1.12.2 que tiene una vulnerabilidad de desbordamiento de enteros. Las versiones de Nginx desde 0.5.6 hasta, e incluyendo, 1.13.2 son vulnerables de desbordamiento de enteros en el módulo de filtro de rango nginx, lo que resulta en una fuga de información potencialmente confidencial desencadenada por una solicitud especialmente diseñada. Al usar nginx con módulos estándar, esto permite que un atacante obtenga un encabezado de archivo de caché si se devolvió una respuesta desde el caché. En algunas configuraciones, un encabezado de archivo de caché puede contener la dirección IP del servidor back-end u otra información sensible.	Remote Integer Overflow Vulnerability # 15	**(medio)**
OPEN SSH 7.4 (protocol 2.0)	Aplicación con afección a vulnerabilidad **CVE-2016-10009**	La vulnerabilidad de la ruta de búsqueda no confiable en ssh-agent.c en ssh-agent en OpenSSH antes de 7.4 permite a los atacantes remotos ejecutar módulos arbitrarios locales PKCS # 11 al aprovechar el control sobre un socket de agente reenviado.	OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	**7.5 (critico)**
Apache httpd 2.215 ((Centos); SSL-only mode)	Aplicación con afección a vulnerabilidad **CVE-2014-0160**	Las (1) implementaciones TLS y (2) DTLS en OpenSSL 1.0.1 antes 1.0.1g no manejan adecuadamente los paquetes Heartbeat Extension, lo que permite a los atacantes remotos obtener información sensible de la memoria del proceso a través de paquetes diseñados que activan una sobre-lectura del búfer. Como se demostró al leer claves privadas, relacionadas con d1_both.c y t1_lib.c, también conocido como el error Heartbleed.	OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support) OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure	**5 (medio)**
Apache httpd 2.4.6 ((CentOS)	Aplicación con	La función openssl_x509_parse en	PHP Vulnerability: CVE-2013-4248	**4.3**

OpenSSL/1.0.2k-fips PHP/5.4.16)	afección a vulnerabilidad **CVE-2013-4248**	openssl en el módulo OpenSSL en PHP antes de 5.4.18 y 5.5.x antes de 5.5.2 no maneja adecuadamente un carácter '\ 0' en un nombre de dominio en el campo Nombre alternativo del sujeto de un X.509 certificado, que permite a los atacantes man-in-the-middle falsificar servidores SSL arbitrarios a través de un certificado elaborado por una autoridad de certificación legítima		**(bajo)**
Apache httpd 2.2.15 ((CentOS) mod_jk/1.2.40 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips)	Aplicación con afección a vulnerabilidad **CVE-2011-1473**	Mozilla Network Security Services (NSS) 3.x, con ciertas configuraciones de la opción SSL_ENABLE_RENEGOTIATION, no restringe adecuadamente la renegociación iniciada por el cliente dentro de los protocolos SSL y TLS, lo que podría facilitar que los atacantes remotos causen una denegación de servicio (CPU consumo) realizando muchas renegociaciones dentro de una única conexión	SUSE Linux Security Vulnerability: CVE-2011-1473	**4.3 (bajo)**
Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips mod_cluster/1.3.1.Final)	Aplicación con afección a vulnerabilidad **CVE-2014-0160**	Las (1) implementaciones TLS y (2) DTLS en OpenSSL 1.0.1 antes 1.0.1g no manejan adecuadamente los paquetes Heartbeat Extension, lo que permite a los atacantes remotos obtener información sensible de la memoria del proceso a través de paquetes diseñados que activan una sobre-lectura del búfer. Como se demostró al leer claves privadas, relacionadas con d1_both.c y t1_lib.c, también conocido como el error Heartbleed.	OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support) OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure	**5 (medio)**
Apache httpd 2.2.29 ((Unix) mod_ssl/2.2.29 OpenSSL/1.0.1e-fips mod_bwlimited/1.4)	Aplicación con afección a vulnerabilidad **CVE-2014-0160**	Las (1) implementaciones TLS y (2) DTLS en OpenSSL 1.0.1 antes 1.0.1g no manejan adecuadamente los paquetes Heartbeat Extension, lo que permite a los atacantes remotos	OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support) OpenSSL TLS Heartbeat Extension -	**5 (medio)**

		obtener información sensible de la memoria del proceso a través de paquetes diseñados que activan una sobre-lectura del búfer. Como se demostró al leer claves privadas, relacionadas con d1_both.c y t1_lib.c, también conocido como el error Heartbleed.	'Heartbleed' Memory Disclosure	
Dovecot pop3d	Aplicación con afección a vulnerabilidad **CVE-2017-15132**	Este módulo explota una vulnerabilidad de inyección de comando contra Dovecot con Exim usando la opción "use_shell". Utiliza la dirección del remitente para inyectar comandos arbitrarios, ya que esta es una de las variables controladas por el usuario. Se ha probado con éxito en Debian Squeeze utilizando el Exim4 predeterminado con los paquetes comunes de dovecot.	exploit/linux/smtp/exim4_dovecot_exec use auxiliary/scanner/pop3/pop3_version	**5 (medio)**
Dovecot imapd	Aplicación con afección a vulnerabilidad **CVE-2017-15132**	Este módulo explota una vulnerabilidad de inyección de comando contra Dovecot con Exim usando la opción "use_shell". Utiliza la dirección del remitente para inyectar comandos arbitrarios, ya que esta es una de las variables controladas por el usuario. Se ha probado con éxito en Debian Squeeze utilizando el Exim4 predeterminado con los paquetes comunes de dovecot.	exploit/linux/smtp/exim4_dovecot_exec use auxiliary/scanner/pop3/pop3_version	**5 (medio)**
MySQL (unauthorized)	Aplicación con afección a vulnerabilidad **CVE-2012-2122**	Este módulo explota una vulnerabilidad de omisión de contraseña en MySQL para extraer los nombres de usuario y los hashes de contraseña cifrados de un servidor MySQL. Estos hash se almacenan como botín para agrietamiento posterior.	auxiliary/scanner/mysql/ mysql_authbypass_hashdump	**5.1 (medio)**
Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.7)	Aplicación con afección a vulnerabilidad **CVE-2012-0550**	Este módulo inicia sesión en un servidor GlassFish (código abierto o comercial) utilizando varios métodos (como	Oracle GlassFish Server - REST Cross-Site Request Forgery Sun/Oracle GlassFish Server -	**6.8 (medio)**

		omisión de autenticación, credenciales predeterminadas o inicio de sesión proporcionado por el usuario) y despliega un archivo de guerra malicioso para obtener la ejecución remota de código. Ha sido probado en Glassfish 2.x, 3.0, 4.0 y Sun Java System Application Server 9.x. Las versiones más nuevas de GlassFish no permiten el acceso remoto (Secure Admin) de forma predeterminada, pero se requiere para su explotación.	Authenticated Code Execution (Metasploit)	
OpenSSH 5.3 (protocol 2.0)	Aplicación con afección a vulnerabilidad **CVE-2012-0814**	La función auth_parse_options en auth-options.c en sshd en OpenSSH antes de 5.7 proporciona mensajes de depuración que contienen las opciones del comando authorized_keys, que permite a los usuarios autenticados remotos obtener información potencialmente confidencial leyendo estos mensajes, como lo demuestra la cuenta de usuario compartido requerida por Gitolite. NOTA: esto puede cruzar los límites de los privilegios porque una cuenta de usuario puede no tener acceso intencionalmente al shell o al sistema de archivos, y por lo tanto puede no tener una forma admitida de leer un archivo authorized_keys en su propio directorio de inicio.	OpenSSH Vulnerability: CVE-2012-0814	**3.5 (medio)**
Pure-FTPd	Aplicación con afección a vulnerabilidad **CVE-2014-6271**	Este módulo explota la vulnerabilidad Shellshock, un error en la forma en que el shell Bash maneja las variables de entorno externo. Este módulo se dirige al servidor FTP Pure-FTPd cuando se compiló con el indicador --with-extauth y se usa un script Bash externo para la autenticación. Si el servidor no está configurado de esta manera, el exploit fallará,	exploit/multi/ftp/pureftpd_bash_env_exec	**10 (alto)**

		incluso si la versión de Bash en uso es vulnerable.		
Oracle Application Server 11g httpd	Aplicación con afección a vulnerabilidad **CVE-2007-6750** **CVE-2011-3192**	Una vulnerabilidad de denegación de servicio en Apache HTTPD, que se aplica a los productos de Oracle HTTP Server basados en Apache 2.0 o 2.2. Esta vulnerabilidad puede ser remotamente explotable sin autenticación, es decir, puede explotarse a través de una red sin la necesidad de un nombre de usuario y contraseña. Un usuario remoto puede aprovechar esta vulnerabilidad para afectar la disponibilidad de los sistemas sin parche.	auxiliary/dos/http/apache_range_dos	**5 (medio)**
Oracle WebLogic Server (Servlet 2.5; JSP 2.1)	Aplicación con afección a vulnerabilidad **CVE-2007-6750** **CVE-2011-3192**	Ataque de denegación de servicios por medio de peticiones Range especialmente manipulados, originando un consumo alto de memoria	auxiliary/dos/http/apache_range_dos	**5 (medio)**

REVISION DE POSIBLES VULNERABILIDADES POR CONTROLES

CONTROL	DESCRIPCION	VULNERABILIDAD	VALOR
5 Políticas de Seguridad|	El desconocimiento de la política puede provocar serios inconvenientes por uso indebido de los recursos informáticos de la Universidad	Falta de conocimiento de la política	**3 (medio)**
6 Organización de la Seguridad de la Información	Falta de especificaciones claras sobre la definición de roles frente a la seguridad de la información	No existe responsables definidos para monitorear y trabajar de lleno en la seguridad de la información	**4 (crítico)**
7 Seguridad en los Recursos Humanos	Falta una gestión específica sobre la seguridad de la información	Hasta el momento no se ha presentado ninguna afectación producida por un ex-empleado, pero puede llegar a ser crítica especialmente en el área de tecnología	**3 (medio)**
8 Gestión de Activos	Se necesita tener un mejor control sobre los activos es necesario dejar especificado los procedimientos para mejorar el control del uso dentro y fuera de la	La pérdida o copia de información sensible de la universidad, o personal de un usuario puede acarrear problemas en la confidencialidad de la información	**4 (crítico)**

	Universidad		
9 Control de Acceso	Existe procedimientos implementados	Es necesario un mantener una mejora continua de los mimos para evitar quedar obsoletos.	**3 (medio)**
10 Criptografía	Es una herramienta que ayuda a la seguridad en el acceso a recursos e información confidencial de la Universidad	Es necesario tener un procedimiento de criptografía por medio de llaves para evitar préstamos o uso de claves de usuarios no autorizados	**4 (crítico)**
11 Seguridad Física y del Entorno	La seguridad de los equipos de infraestructura (switch, router, Aps, servidores) son importantes para el desarrollo de las labores diarias de la institución, por lo que la su seguridad debe estar respaldad para evitar cualquier inconveniente	Existe cierto cableado estructurado sin la debida protección por lo que puede ser cortado, produciendo un fallo de servicio a un grupo de usuarios.	**3 (medio)**
12 Seguridad en las Operaciones	Las operaciones de TI son importantes para la seguridad de la información	La revisión de procedimientos establecidos son correctos, es necesario que se los ponga en práctica para que los mismos no afecten a la seguridad de la información, el monitoreo es fundamental para hacer seguimiento de problemas	**3 (medio)**
13 Seguridad en las Comunicaciones	La transferencia de información especialmente sensible a los diferentes usuarios debe ser acompañada de procedimientos formales y la gestión correcta en la red	Es necesario implementar procedimientos formales y una política de transferencia para la información.	**4 (crítico)**
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	El desarrollo y la compra de software para aplicaciones de la institución deben ser implementado en cada ciclo de vida del software la seguridad de la información	Antes de ser puesto en producción cualquier aplicación esta debe ser probada no solo en su parte funcional sino de seguridad de la información con la finalidad de que presente vulnerabilidades por problemas de programación.	**3 (medio)**
15 Relaciones con Proveedores	La relación con los proveedores debe ser implementado mediante requerimientos de seguridad para proteger la información institucional	La gestión del servicio de los proveedores es importante para mantener un seguimiento constante de la calidad del servicio ofrecida a la institución	**3 (medio)**
16 Gestión de Incidentes de Seguridad de la Información	La gestión de incidentes de seguridad es muy importante al momento de hallar problemas de operación de los diferentes servicios que	Es muy importante que se tenga procedimientos formales con la finalidad de que los usuarios tomen las acciones correctivas necesarias antes de los incidentes se conviertan en problemas	**3 (medio)**

	brinda la Universidad		
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	La continuidad de la seguridad de la información es un tema muy importante cuando se presenta problemas de interrupción del servicio por problemas de seguridad informática	Se necesita el establecimiento y correcto funcionamiento del sitio alterno y los equipos de redundancia que brinde la posibilidad de continuar trabajando cuando uno de los componentes informáticos principales presente algún daño o incidente.	**5 (alto)**
18 Cumplimiento	Dar cumplimiento con las normas nacionales en cuanto a la seguridad de la información	Se necesita manejar en todos los aspectos de la información los temas de protección y seguridad de la información especialmente por los datos sensibles de carácter personal que se utilizan en la institución	**3 (medio)**

REVISION DE POSIBLES VULNERABILIDADES POR SERVICIOS DE RED

INFRAESTRUCTURA	DESCRIPCION	VULNERABILIDAD	VALOR
RED LAN	Red que da servicio interno para la Universidad	De lo revisado las posibles vulnerabilidades que pueden ser afectados se encuentran dentro de los parámetros normales como (afección por corte de cable que afectaría a un grupo de usuarios, enumeración de servidores, atención de restricciones en puntos no atendidos)	**3 (medio)**
RED INALAMBRICA, Red que da servicio interno para la Universidad	Red que da servicio interno para la Universidad	En la revisión se pudo visualizar Aps que no tienen seguridad frente a robos de equipos, adicional se mantiene un portal cautivo que a veces presenta la pantalla genérica de cisco, pudiendo facilitar el acceso a intrusos	**3 (medio)**

ANEXO 8

VERIFICACION de CONTROLES

Declaración de Aplicabilidad Vigente para el: 04/jun/2018

Leyenda (para la selección de controles y razón por la que se seleccionaron):

LR**: requerimientos legales,** CO**: obligaciones contractuales,** BR/BP**: requerimientos del negocio/mejores prácticas adoptadas ,**RRA**: resultado de la valoración de riesgos;** TSE: hasta cierto punto

ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)	Controles seleccionados y razones de selección				Comentarios (visión general de la implementación)
					LR	CO	BR/ BP	RRA	
Cláusula	**Sección**	**Objetivo de control / control**							
5 Políticas de Seguridad	5.1	Dirección de la alta gerencia para la seguridad de la información							
	5.1.1	Políticas de seguridad de la información	si				x	3/5	existe publicada la política en la página web sin difusión
	5.1.2	Revisión de las políticas de seguridad de la información	si				x	2/5	no se actualiza de forma constante la política
6 Organización de la Seguridad de la Información	6.1	Organización interna							
	6.1.1	Roles y responsabilidad de seguridad de la información	si				x	2/5	definido de forma general
	6.1.2	Segregación de deberes	no				x	0/5	no está definidas las tareas
	6.1.3	Contacto con autoridades	no				x	0/5	no hay un procedimiento
	6.1.4	Contacto con grupos de interés especial	no				x	0/5	no hay un procedimiento
	6.1.5	Seguridad de la información en la gestión de proyectos	si				x	2/5	no se cumple adecuadamente pese a existir un procedimiento
	6.2	Dispositivos móviles y teletrabajo							
	6.2.1	Política de dispositivos móviles	no				x	0/5	no existe una política definida para los dispositivos móviles
	6.2.2	Teletrabajo	no	no se utiliza este sistema					

7 Seguridad en los Recursos Humanos	7.1	Previo al empleo							
	7.1.1	Verificación de antecedentes	si		x		x	3/5	lo realiza GTH, no enfatiza en la seguridad de la información
	7.1.2	Términos y condiciones del empleo	si		x		x	3/5	lo realiza GTH, no enfatiza en la seguridad de la información
	7.2	Durante el empleo							
	7.2.1	Responsabilidades de la Alta Gerencia	si				x	2/5	se debe hacer el seguimiento respectivo
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	si				x	2/5	falta de concienciar y capacitar a los usuarios
	7.2.3	Proceso disciplinario	no		x		x	0/5	no existe el procedimiento por falta a la seguridad de la información
	7.3	Terminación y cambio de empleo							
	7.3.1	Término de responsabilidades o cambio de empleo	si				x	2/5	no se utiliza ningún procedimiento seguro especial
8 Gestión de Activos	8.1	Responsabilidad de los activos							
	8.1.1	Inventario de activos	si		x	x	x	5/5	se mantiene inventarios
	8.1.2	Propiedad de activos	si		x	x	x	5/5	se mantiene la información de activos y departamentos ligados
	8.1.3	Uso aceptable de los activos	no				x	0/5	no existe procedimiento adecuado
	8.1.4	Devolución de activos	si				x	4/5	existe procedimiento
	8.2	Clasificación de la información							
	8.2.1	Clasificación de la información	si		x	x	x	4/5	no existe procedimiento actualizado
	8.2.2	Etiquetado de la información	si		x		x	3/5	no existe procedimiento actualizado
	8.2.3	Manejo de activos	si				x	2/5	no existe procedimiento específico
	8.3	Manejo de medios							
	8.3.1	Gestión de medios removibles	no				x	0/5	no existe procedimiento
	8.3.2	Eliminación de medios	no				x	0/5	no existe procedimiento
	8.3.3	Transporte de medios físicos	no				x	0/5	no existe procedimiento
9 Control de Acceso	9.1	Requerimientos de negocio para el control de acceso							

	9.1.1	Política de control de acceso	si				x	2/5	existe procedimiento pero sin actualización en base a su necesidad
	9.1.2	Acceso a redes y servicios de red	si				x	2/5	existe procedimiento pero sin actualización en base a su necesidad, por falta de actualización de cambios de usuario
	9.2	Gestión de accesos de usuario							
	9.2.1	Registro y baja del usuario	si				x	5/5	existe el procedimiento
	9.2.2	Provisión de acceso a usuarios	si				x	5/5	existe el proceso formal
	9.2.3	Gestión de derechos de acceso privilegiados	si				x	5/5	existe el proceso formal
	9.2.4	Gestión de información de autenticación secreta de usuarios	si				x	5/5	existe el proceso formal
	9.2.5	Revisión de derechos de acceso de usuarios	si				x	4/5	proceso se debe realizar con mayor frecuencia
	9.2.6	Eliminación o ajuste de derechos de acceso	si				x	3/5	no queda registros
	9.3	Responsabilidades del usuario							
	9.3.1	Uso de información de autenticación secreta	no				x	0/5	no existe ningún procedimiento formal de buenas prácticas
	9.4	Control de acceso de sistemas y aplicaciones							
	9.4.1	Restricción de acceso a la información	si				x	5/5	existe el proceso adecuado
	9.4.2	Procedimientos de inicio de sesión seguro	si				x	5/5	existe el proceso adecuado
	9.4.3	Sistema de gestión de contraseñas	si				x	5/5	existe el proceso adecuado
	9.4.4	Uso de programas y utilidades privilegiadas	si				x	5/5	existe el proceso adecuado
	9.4.5	Control de acceso al código fuente del programa	si				x	4/5	existe el proceso adecuado, pero es necesario adecuar auditoria
10 Criptografía	10.1	Controles criptográficos							
	10.1.1	Política en el uso de controles criptográficos	no				x	0/5	no existe ningún procedimiento
	10.1.2	Gestión de llaves	no				x	0/5	no existe ningún procedimiento
11 Seguridad Física y del Entorno	11.1	Áreas seguras							
	11.1.1	Perímetro de seguridad físico	si			x	x	5/5	existe el proceso adecuado

	11.1.2	Controles físicos de entrada	si			x	x	3/5	existe los controles adecuados, pero se debe ser un poco más estrictos en su permisividad de acceso
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	si			x	x	5/5	existe la seguridad adecuado
	11.1.4	Protección contra amenazas externas y del ambiente	si			x	x	5/5	existe protección adecuada
	11.1.5	Trabajo en áreas seguras	si			x	x	5/5	existe áreas seguras en Informática
	11.1.6	Áreas de entrega y carga	no			x	x	0/5	no existe definido un lugar de recepción
	11.2	Equipo							
	11.2.1	Instalación y protección de equipo	si				x	5/5	existe la protección adecuada
	11.2.2	Servicios de soporte	si				x	5/5	existe protección a fallas de suministro
	11.2.3	Seguridad en el cableado	si				x	3/5	Falta asegurar en ciertas áreas de accesibilidad publica
	11.2.4	Mantenimiento de equipos	si				x	5/5	Se realiza mantenimiento adecuado especialmente en los equipos del Datacenter
	11.2.5	Retiro de activos	si				x	3/5	no existe ningún procedimiento formal de buenas prácticas
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	si				x	3/5	no existe ningún procedimiento formal de buenas prácticas
	11.2.7	Eliminación segura o reúso del equipo	si				x	3/5	no existe ningún procedimiento formal de buenas prácticas
	11.2.8	Equipo de usuario desatendido	si				x	3/5	no existe ningún procedimiento formal de buenas prácticas
	11.2.9	Política de escritorio limpio y pantalla limpia	no				x	0/5	no existe una política de buenas prácticas
12 Seguridad en las Operaciones	12.1	Procedimientos Operacionales y Responsabilidades							
	12.1.1	Documentación de procedimientos operacionales	si				x	4/5	falta compromiso de hacer uso de los procedimientos
	12.1.2	Gestión de cambios	si				x	5/5	existe un procedimiento mediante helpdesk
	12.1.3	Gestión de la capacidad	si				x	5/5	existe un procedimiento mediante helpdesk

	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	si				x	2/5	falta de implementar una política y procedimiento formal
	12.2	Protección de Software Malicioso							
	12.2.1	Controles contra software malicioso	si				x	4/5	procedimiento formal, pero falta de concientización a usuarios
	12.3	Respaldo							
	12.3.1	Respaldo de información	si				x	5/5	existe un proceso formal
	12.4	Bitácoras y monitoreo							
	12.4.1	Bitácoras de eventos	si				x	4/5	existe procedimientos con herramientas y manuales para recolección de eventos de los activos
	12.4.2	Protección de información en bitácoras	si				x	5/5	existe la gestión en el manejo de bitácoras
	12.4.3	Bitácoras de administrador y operador	si				x	4/5	el procedimiento se cumple a cabalidad, es necesario correlacionar información de varios equipos
	12.4.4	Sincronización de relojes	si				x	4/5	Reloj de algunos equipos deben ser actualizados
	12.5	Control de software operacional							
	12.5.1	Instalación de software en sistemas operacionales	si				x	4/5	se debe acompañar siempre del análisis de riesgos de los cambios a realizarse en los activos
	12.6	Gestión de vulnerabilidades técnicas							
	12.6.1	Gestión de vulnerabilidades técnicas	si				x	4/5	falta monitoreo constante
	12.6.2	Restricciones en la instalación de software	si				x	3/5	falta de implementar una política y procedimiento formal
	12.7	Consideraciones de auditoria de sistemas de información							
	12.7.1	Controles de auditoría de sistemas de información	si				x	3/5	no existe implementado en todos los activos
13 Seguridad en las Comunicaciones	13.1	Gestión de seguridad en red							
	13.1.1	Controles de red	si				x	5/5	se tiene implementado seguridades y buenas prácticas

	13.1.2	Seguridad en los servicios en red	si				x	4/5	revisar los mecanismos de seguridad de los SLAs internos y externos
	13.1.3	Segregación en redes	si				x	5/5	se realiza mediante VLAN
	13.2	Transferencia de información							
	13.2.1	Políticas y procedimientos para la transferencia de información	si				x	3/5	falta de implementar una política y procedimiento formal
	13.2.2	Acuerdos en la transferencia de información	si				x	3/5	falta de implementar una política y procedimiento formal
	13.2.3	Mensajería electrónica	si				x	3/5	falta de implementar una política y procedimiento formal
	13.2.4	Acuerdos de confidencialidad o no-revelación	si				x	3/5	falta de implementar una política y procedimiento formal
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14.1	Requerimientos de seguridad en sistemas de información							
	14.1.1	Análisis y especificación de requerimientos de seguridad	si				x	4/5	sin uso total del procedimiento
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	si				x	5/5	aplicación de protección de la información
	14.1.3	Protección de transacciones en servicios de aplicación	si				x	5/5	aplicación de protección de la información
	14.2	Seguridad en el proceso de desarrollo y soporte							
	14.2.1	Política de desarrollo seguro	si				x	4/5	se debe actualizar procedimientos
	14.2.2	Procedimientos de control de cambios del sistema	si				x	4/5	se debe actualizar procedimientos
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	si				x	4/5	se debe actualizar procedimientos
	14.2.4	Restricción de cambios en paquetes de software	no				x	0/5	sin uso de procedimiento
	14.2.5	Principios de seguridad en la ingeniería de sistemas	si				x	3/5	se debe actualizar procedimientos
	14.2.6	Entorno de desarrollo seguro	si				x	4/5	se debe actualizar procedimientos
	14.2.7	Desarrollo tercerizado	si				x	4/5	se debe actualizar procedimientos
	14.2.8	Pruebas de seguridad del sistema	no				x	0/5	falta de implementar una política y procedimiento formal

	14.2.9	Pruebas de aceptación del sistema	si				x	5/5	se realiza con usuario final
	14.3	Datos de prueba							
	14.3.1	Protección de datos de prueba	si				x	4/5	lo realizan con bases de pruebas
15 Relaciones con Proveedores	15.1	Seguridad de la información en relaciones con el proveedor							
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	si				x	3/5	se debe actualizar procedimientos
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	si				x	3/5	falta de implementar una política y procedimiento formal
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	si				x	3/5	se debe actualizar procedimientos
	15.2	Gestión de entrega de servicios de proveedor							
	15.2.1	Monitoreo y revisión de servicios del proveedor	si		x		x	4/5	falta de implementar una política y procedimiento formal
	15.2.2	Gestión de cambios a los servicios del proveedor	si		x		x	4/5	se debe actualizar procedimientos , mediante SLA
16 Gestión de Incidentes de Seguridad de la Información	16.1	Gestión de incidentes de seguridad de la información y mejoras							
	16.1.1	Responsabilidades y procedimientos	si				x	3/5	falta de implementar una política y procedimiento formal
	16.1.2	Reporte de eventos de seguridad de la información	si				x	3/5	falta de implementar una política y procedimiento formal
	16.1.3	Reporte de debilidades de seguridad de la información	no				x	2/5	falta de implementar una política y procedimiento formal
	16.1.4	Valoración y decisión de eventos de seguridad de la información	si				x	3/5	falta de implementar una política y procedimiento formal
	16.1.5	Respuesta a incidentes de seguridad de la información	si				x	3/5	falta de implementar una política y procedimiento formal
	16.1.6	Aprendizaje de incidentes de seguridad de la información	si				x	3/5	falta de implementar una política y procedimiento formal
	16.1.7	Colección de evidencia	si				x	3/5	falta de implementar una política y procedimiento formal
17 Aspectos de	17.1	Continuidad de la seguridad de la información							

Seguridad de la Información para la Gestión de la Continuidad del Negocio	17.1.1	Planeación de la continuidad de la seguridad de la información	si				x	3/5	se debe actualizar procedimientos
	17.1.2	Implementación de la continuidad de la seguridad de la información	si				x	3/5	se debe actualizar procedimientos
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	si				x	3/5	se debe actualizar procedimientos , se necesita hacer pruebas periódicas
	17.2	Redundancias							
	17.2.1	Disponibilidad de facilidades de procesamiento de información	si				x	3/5	falta en ciertos activos
18 Cumplimiento	18.1	Cumplimiento con Requerimientos Legales y Contractuales							
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	no				x	0/5	no se ha socializado
	18.1.2	Derechos de propiedad intelectual (IPR)	no				x	0/5	no existe ningún procedimiento
	18.1.3	Protección de registros	no				x	0/5	no existe ningún procedimiento
	18.1.4	Privacidad y protección de información personal identificable (PIR)	si		x		x	3/5	falta de implementar una política y procedimiento formal
	18.1.5	Regulación de controles criptográficos	no				x		no existe ningún procedimiento
	18.2	Revisiones de seguridad de la información							
	18.2.1	Revisión independiente de seguridad de la información	no		x		x	0/5	no se ha realizado hasta el momento una revisión de la seguridad de forma profunda
	18.2.2	Cumplimiento con políticas y estándares de seguridad	si		x		x	4/5	especialmente con buenas prácticas
	18.2.3	Revisión del cumplimiento técnico	si		x		x	4/5	falta de implementar una política y procedimiento formal