UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA

Seguridad de la Información en las Actividades Académicas Virtuales de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la UTA.

Proyecto de Trabajo de Graduación. Modalidad: Proyecto de investigación, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

SUBLÍNEA DE INVESTIGACIÓN:
Seguridad de Unidades Informáticas

Autor: Christian Alejandro Aldas Falcón
Tutor: Ing. David Omar Guevara Aulestia, Mg.

Ambato – Ecuador
2017

APROBACIÓN DEL TUTOR

En mi calidad de tutor del Trabajo de Investigación sobre el tema: "Seguridad de la Información en las Actividades Académicas Virtuales de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la UTA.", del señor Christian Alejandro Aldas Falcón, estudiante de la Carrera de Ingeniería en Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato Diciembre, 2017

EL TUTOR

Ing. David Guevara Aulestia, Mg.

AUTORÍA

El presente Proyecto de Investigación titulado: "Seguridad de la Información en las Actividades Académicas Virtuales de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la UTA.", es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Diciembre, 2017

Christian Alejandro Aldas Falcón

CC: 180460922-8

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato Diciembre, 2017

Christian Alejandro Aldas Falcón

CC: 1803735289

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Dennis Chicaiza e Ing. Félix Fernández, revisó y aprobó el Informe Final del Proyecto de Investigación titulado: "Seguridad de la Información en las Actividades Académicas Virtuales de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la UTA.", presentado por el señor Christian Alejandro Aldas Falcón de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

PRESIDENTA DEL TRIBUNAL

Ing. Dennis Chicaiza, Mg.
DOCENTE CALIFICADOR

Ing. Félix Fernández, Ph D.
DOCENTE CALIFICADOR

DEDICATORIA

La presente Tesis está dedicada a Dios, ya que gracias a Él he logrado concluir mi carrera.

A mi madre y mi hermana que con sus palabras de aliento me han sabido guiar con sabiduría y amor en cada paso de mi vida.

Además, a cada una de esas personas que con sus palabras de aliento me han sabido apoyar en este largo camino.

Christian Alejandro Aldas Falcón

AGRADECIMIENTO

A Dios quien con su infinito y divino amor me ha dado la fuerza y el coraje de perseguir mis sueños.

A mi familia por cada palabra de fe y de aliento que me supieron dar para no doblegarme ante las adversidades.

A mi tutor Ing. David Guevara que con su guía se convirtió en el pilar más importante de la presente investigación.

A mis compañeros de trabajo, universidad y amigos que con su apoyo me ayudaron a conseguir este peldaño en mi vida profesional.

Christian Alejandro Aldas Falcón

ÍNDICE

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

En la actualidad, la información es uno de los principales valores de cualquier organización, pero también uno de sus puntos más vulnerables, sin ser la excepción las plataformas de educación virtual.

Por esta razón la presente investigación está enmarcada en solucionar dichas vulnerabilidades de la mano de Magerit V3 que siendo una metodología de análisis y gestión de vulnerabilidades de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de implantación y uso de las tecnologías de la información., nos permitirá que la información almacenada dentro de la plataforma virtual de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial sea confiable y cumpla estándares de seguridad.

Magerit propone concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos, así también ofrece un método sistemático de análisis de riesgos derivados del uso de tecnologías de la información y comunicación.

Asimismo, nos permite estudiar los riesgos que un sistema puede soportar y el entorno asociado al mismo, Magerit propone también la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en las organizaciones.

Es por ello que se propone un manual de buenas prácticas de seguridad a partir de las recomendaciones que Magerit nos sugiere y que a su vez el Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato tendrá a disposición.

ABSTRACT

At present, information is one of the main values of any organization, but also one of its most vulnerable points, without being the exception virtual education platforms.

For this reason the present investigation is framed in solving these vulnerabilities of the hand of Magerit V3 that being a methodology of analysis and management of vulnerabilities of the Information Systems elaborated by the Superior Council of Electronic Administration to minimize the risks of implantation and use of the information technologies., will allow us that the information stored within the virtual platform of the Faculty of Systems, Electronics and Industrial Engineering is reliable and meets safety standards.

Magerit proposes to raise awareness among those responsible for information organizations about the existence of risks and the need to manage them, as well as offering a systematic method of analyzing risks derived from the use of information and communication technologies.

It also allows us to study the risks that a system can support, and the environment associated with it, Magerit also proposes to carry out an analysis of the risks involved in assessing the impact that a breach of security has on organizations.

That is why a manual of good security practices is proposed based on the recommendations that Magerit suggests and which in turn the Directorate of Distance and Virtual Education of the Technical University of Ambato will have available.

INTRODUCCIÓN

El presente proyecto de investigación se enfoca en el análisis de vulnerabilidades y la elaboración de un manual de buenas prácticas de seguridad informática basadas en Magerit V3.

CAPÍTULO I, "EL PROBLEMA", se describe el problema que será sujeto de investigación, así como su respectiva justificación y el planteamiento de objetivos.

CAPÍTULO II, "MARCO TEÓRICO", se presentan los antecedentes investigativos que fungirán como sustento a la presente investigación así también una propuesta de solución al problema planteado.

CAPÍTULO III, "METODOLOGÍA", se define la modalidad de investigación además de plantear los lineamientos en los que se basará la investigación.

CAPÍTULO IV, "DESARROLLO DE LA PROPUESTA", se presenta cada uno de los pasos a seguir en el desarrollo de la investigación utilizando la metodología planteada en el capítulo anterior, además se elabora el manual de buenas prácticas a partir de la metodología Magerit V3.

CAPÍTULO V, "CONCLUSIONES Y RECOMENDACIONES", se presentan las conclusiones de los resultados de la investigación y se emiten recomendaciones a partir del manual de buenas prácticas de seguridad elaborado en el capítulo anterior.

CAPÍTULO I

EL PROBLEMA

1.1. Tema

Seguridad de la Información en las Actividades Académicas Virtuales de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la UTA.

1.2. Planteamiento del problema

Las actividades académicas se desenvuelven en torno a un mundo de grandes expectativas científicas y de constantes cambios tecnológicos, en donde es necesario el cambio de una sociedad industrial por una sociedad de las informaciones conocida también como la sociedad del conocimiento. En base a esta realidad existe la necesidad de explotar el trabajo autónomo estudiantil, esto, por las reales exigencias del desarrollo científico y de la informática en la actualidad. La palabra autónomo en la educación hace referencia a la actividad del estudiante que, realizada tanto dentro como fuera del aula, desarrolla la autonomía, libertad e independencia.

La educación en el país ha tenido importantes cambios, fundamentados en la incorporación de las tecnologías de información en las actividades académicas. Las universidades se enfocan en construir amplios campos internos, infraestructura tecnológica, bibliotecas con libros virtuales, así como aulas inteligentes, con presentaciones multimedia y el uso y desarrollo de las plataformas educativas [1].

La seguridad de la Información que se almacena procesa y transmite en los entornos virtuales de aprendizaje, es una necesidad subestimada, se hace necesario tomar en cuenta la protección de los datos con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

Los riesgos contra la seguridad de los datos en las actividades educativas son muchos y diversos debido a la gran cantidad de amenazas y vulnerabilidades existentes. Por ello, los responsables del manejo de esta información deben estar pendientes de los peligros y costes asociados a una posible pérdida de información, es por esto que deben cumplir con las normas de protección de datos y las regulaciones asociadas para asegurarlas, como son la creación de sistemas de gestión de la seguridad de la información, identificar los alcances de ataques contra la seguridad de la información y contramedidas a estos, conocer e implementar controles de seguridad a nivel de acceso físico y lógico ante posibles ataques y fugas de información y desarrollar políticas de seguridad de la información todo esto basándose en las buenas prácticas existentes para el efecto.

Con la incorporación de nuevas herramientas en las plataformas de educación virtual como el chat, el streaming de video y los sistemas de voz sobre IP, el surgimiento de nuevas formas de interacción en línea como las redes sociales y los teléfonos inteligentes, los estudiantes tienen una integración más rápida y efectiva de los procesos educativos a las plataformas virtuales. Al mismo tiempo estas nuevas tecnologías van de la mano con nuevos riesgos, que, si no son identificados y mitigados de manera apropiada, generan vulnerabilidades que pueden afectar la seguridad de la información, afectando así al proceso educativo.

En la Universidad Técnica de Ambato los docentes utilizan como herramienta de apoyo al proceso de enseñanza-aprendizaje, los Entornos Virtuales de Aprendizaje (EVA), para lo cual usan la aplicación Moodle en el desarrollo de las aulas virtuales. En vista a que en las aulas virtuales existen diferentes tipos de actividades como tareas y evaluaciones es necesario que estas no sean visualizadas por otras personas, ni alteradas por ningún medio.

En base a lo indicado se plantea realizar un análisis de Moodle que es la herramienta usada por la Universidad para el desarrollo de los EVA, también se plantea efectuar al mismo una comparación con otras plataformas de concepción libre usadas para crear entornos virtuales de aprendizaje. Para completar la investigación se realizarán simulacros virtualizados de ataques a la plataforma usada por la Universidad. Finalmente se diseñará un conjunto de Buenas Prácticas de seguridad para la información de las actividades académicas virtuales, elaborada a partir de recomendaciones, normativas, guías y estándares nacionales e internacionales, para ser aplicadas por los administradores, docentes y estudiantes directamente involucrados con el EVA.

1.3. Delimitación

Área académica: Administrativas Informática

Línea de Investigación: Normas y Estándares

Sublínea de Investigación: Seguridad de Unidades Informáticas

Delimitación temporal: El trabajo de investigación se desarrollará en un período de seis meses posteriores a la aprobación por parte del Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Delimitación espacial: La presente investigación se llevará a cabo en la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la Universidad Técnica de Ambato.

1.4. Justificación

La seguridad de la información se ha tornado un punto crítico en toda empresa, no quedando de lado las actividades educativas de las instituciones de educación superior. Es importante fundamentar científicamente el problema planteado para tener el conocimiento teórico sobre los temas a tratar durante el proceso de investigación, pues es sobre este que se construye todo el trabajo. Una buena base teórica formará la plataforma sobre la cual se construye el análisis de los resultados obtenidos en el trabajo, sin ella no se puede analizar los datos que se van a obtener durante la Investigación.

La base teórica o marco conceptual tiene el propósito de dar a la investigación un sistema coordinado y coherente de conceptos que permitan abordar el problema, en la presente Investigación se tratarán temas de interés relacionados con la seguridad de la información, las actividades académicas virtuales en las instituciones de educación superior y las buenas prácticas para la seguridad de la Información.

Para mitigar este problema de manera eficiente y con un alto impacto es necesario llevar adelante un proceso de gestión de la seguridad de la información con un análisis a fondo de los riesgos que permita incorporar las nuevas tecnologías de seguridad que ayuden a minimizar las amenazas más importantes sin perder facilidad de uso.

Las instituciones de educación superior dependen completamente de los datos que maneja en sus sistemas informáticos, esto hace necesario que se preste mayor atención a la disponibilidad, confidencialidad e integridad de los mismos, garantizando la continua prestación de sus servicios, así como la certeza de tener su información segura y sus sistemas protegidos, siendo los beneficiaros tanto estudiantes como docentes de la Carrera.

La propuesta está encaminada a que las actividades educativas en entornos virtuales, se realicen de forma más segura, dando la posibilidad a que tanto docentes como estudiantes tengan la confianza necesaria para trabajar en dichos entornos y la certeza de que tareas, evaluaciones y calificaciones obtenidas no han sido visualizadas por otras personas, al ser este tema necesario la carrera de Ingeniería en Sistemas Informáticos y Computacionales de la Universidad Técnica de Ambato prestará todas las facilidades para el estudio siendo **factible** la investigación planteada.

1.5. Objetivos

1.5.1. Objetivo General

Implementar la Seguridad de la Información en las Actividades Académicas Virtuales de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la UTA.

1.5.2. Objetivos Específicos

- Identificar las actividades en los Entornos Virtuales de aprendizaje que se desarrollan en la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la UTA.
- Analizar la Seguridad de la Información en la plataforma Moodle usada en la UTA mediante ataques virtualizados.
- Desarrollar un conjunto de buenas prácticas de seguridad para la información de las actividades académicas virtuales, elaborada a partir de recomendaciones, normativas y estándares.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes Investigativos

En la tesis [2] Marco de trabajo de representación y reúso de requisitos de seguridad, el autor, indica que es necesario la integración de otros análisis y estándares de seguridad, como ISO 27001, incluyendo también otras técnicas de seguridad.

En el trabajo investigativo [3] Entornos Virtuales para la formación práctica de estudiantes de educación: implementación, experimentación y evaluación de la plataforma aula web, el autor indica que la mayoría de los estudiantes cuenta con los recursos adecuados para poder acceder fácilmente a Internet desde su casa principalmente además de contar con un ordenador de trabajo con todas las herramientas necesarias para poder desarrollar un modelo de formación semipresencial. Además, los estudiantes controlan y utilizan habitualmente las TIC principalmente en su trabajo diario, usándolo como herramienta de búsqueda de información y para facilitar las comunicaciones. Finalmente señala que valoran positivamente de una manera general la utilización de la plataforma en la asignatura en la que han realizado su experiencia y piensan que es útil en las asignaturas relacionadas con la educación.

En la investigación Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato [4] señala que el personal administrativo, docentes y estudiantes realizan sus funciones acorde a la información que brindan los sistemas de la universidad, por lo tanto, es importante que la información y centros de procesamiento tengan restringido el acceso, estableciendo lineamientos de seguridad para la información.

Dentro de la Universidad Técnica de Ambato en la Dirección de Educación a Distancia y Virtual ya se ha realizado un análisis de vulnerabilidades por el estudiante Jorge Sánchez Freire con el tema "Análisis de vulnerabilidades y diseño de procesos correctivos de la página web de la Dirección de Educación a Distancia y Virtual de la Universidad Técnica de Ambato" cuyo enfoque está basado en errores cometidos por los usuarios principalmente y la vulnerabilidad que representan los fallos de control de parte de la administración para el manejo de datos por parte de quienes utilizan la aplicación web, la presente investigación tiene como base realizar un análisis de vulnerabilidades con un enfoque hacia la revisión de vulnerabilidades internas dentro de la administración y sus configuraciones, así también como el uso correcto del cifrado de las comunicaciones.

2.2.Fundamentación Teórica

2.2.1. Seguridad de la Información

La interconectividad e interoperabilidad de dispositivos en las redes, ha situado a la seguridad de los sistemas de información el principal elemento, se hace imprescindible que las necesidades de seguridad potenciales sean tomadas en cuenta [5].

El desarrollo de las TIC en los sistemas de información ha obligado a que se tome medidas para impedir, prevenir, detectar y corregir las violaciones de la seguridad que se produce durante la transmisión de la información [6].

La seguridad de información es muy importante y crucial en las organizaciones, por lo que es necesario una constante evaluación para determinar los beneficios y los factores de más impacto. La tendencia de las Universidades en la actualidad es realizar todas sus actividades y procesos en forma automatizada y virtual, teniendo como usuarios a todos los docentes y estudiantes, siendo necesario un mayor control de la seguridad de sus datos [7].

Las organizaciones necesitan una estabilidad y mayor grado de protección enfocada a la seguridad informática para proteger y minimizar las amenazas a su información. Aun cuando existen diferentes maneras de proteger sus datos el principal problema es la desinformación que tienen las organizaciones para la toma de decisiones, por lo tanto, se identifica la necesidad de desarrollar un modelo que permita aplicar buenas prácticas para establecer la seguridad en equipos de seguridad informática proporcione información eficaz y eficiente sobre recomendaciones, estrategias y planes para tener un nivel de seguridad alto en su información [8].

Al respecto [9], propuso una metodología que permite la disminución de tiempo y costos de implementación de un sistema de gestión para estas empresas en el mediano plazo, en conformidad con la norma ISO 27001 dando cumplimiento a las buenas prácticas según lo establecido en la norma ISO 27002.

Desarrollar una función de seguridad de la información en las organizaciones permite tener los mecanismos, las estrategias y acciones que le permiten hacer realidad las metas operativas de la seguridad de la información, para prevenir ataques, tener control de spam, antivirus, entre otras, protegiendo así la infraestructura tecnológica de riesgos que atentan contra la confidencialidad, integridad y disponibilidad [10].

Objetivos de la Seguridad

La Seguridad es la capacidad de un producto de software para proteger los datos e información de manera que personas o sistemas no autorizados no puedan leerlos o modificarlos y que el acceso no sea denegado a personal autorizado [10].

Los Objetivos de la seguridad son:

1. *Disponibilidad y accesibilidad* de los sistemas y datos para su uso autorizados. Es un requisito necesario para garantizar que el sistema trabaje puntualmente, con prontitud y que no se deniegue el servicio a ningún usuario autorizado.

2. *Integridad*. Se encarga de garantizar que la información del sistema no haya sido alterada por usuarios no autorizados, evitando la pérdida de consistencia.
3. *Confidencialidad de datos y de la información del sistema.* Es el requisito que intenta que la información privada o secreta no se revele a individuos no autorizados.
4. *Responsabilidad a nivel individual.* Es el requisito que permite que puedan trazarse las acciones de una entidad de forma única. Es un requisito de la política de la organización y soporta de forma directa el no repudio, la disuasión, el aislamiento de fallos, la detección y la prevención de intrusos.
5. *Confiabilidad*. Es la garantía en que los cuatro objetivos anteriores se han cumplido adecuadamente [5].

Problemas de Seguridad informática.

Con la explotación de Internet, es técnicamente posible pinchar un enlace de comunicaciones e interceptar el contenido de los datos TCP/IP que por él se transmiten. Cuando se envía información privada, es vital garantizar que los datos sean recibidos exclusivamente por su destinatario, y que la identidad sea la esperada.

Internet constituye un canal de comunicaciones inseguro fácilmente accesible en cualquier punto intermedio por un posible atacante. Es por esto por lo que se deben tomar las precauciones para proteger los elementos que hacen parte de la red como infraestructura e información, la más afectada por delincuentes cibernéticos.

Riesgos Informáticos

Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma [11]. Ante un riesgo, una organización puede optar por tres alternativas:

- Asumirlo sin hacer nada.
- Aplicar medidas para disminuirlo o anularlo.
- Transferirlo.

A la hora de dotar de seguridad a un sistema de información, hay que tener en cuenta todos los elementos que lo componen, analizar el nivel de vulnerabilidad de cada uno de ellos ante determinadas amenazas y valorar el impacto que un ataque causaría sobre todo el sistema.

Existen varios estándares y normativas de gestión de riesgo informático pero la más usada es Magerit.

Magerit

Magerit es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, esta metodología se fundamenta en que la gestión de los riesgos es la base en las guías de buen gobierno, enfocada principalmente a entidades de Administración Pública ofrece un método sistemático para analizar los riesgos derivados del uso de las Tics. Actualmente se encuentra en la versión 3 lanzada en el 2012. Se encuentra dividida en tres partes, la primera describe la estructura del modelo de gestión de riesgos, la segunda propone criterios para la identificación y valuación de los activos y ofrece un listado con las amenazas y controles aplicables y la última ofrece una guía de técnicas comúnmente utilizadas en los procesos de análisis de riesgos [13].

Vulnerabilidad

En seguridad informática la vulnerabilidad es cualquier debilidad de un activo que incide de alguna manera en el normal funcionamiento de un sistema informático. Estas debilidades, por lo general están relacionadas a fallos en aplicaciones o en la configuración del sistema operativo, a descuidos en la utilización de los sistemas y otros. El no usar protección frente a fallos eléctricos o carecer de mecanismos de

protección frente a ataques informáticos como antivirus o cortafuegos son ejemplos de vulnerabilidades [7].

Se debe controlar toda vulnerabilidad en la institución, ya que siempre será un riesgo potencial para la seguridad del área informática. Algunas vulnerabilidades permiten privilegios, con lo que un atacante podría conseguir más accesos de los previstos, implicando en varios casos llegar a tener los mismos privilegios que los administradores, pudiendo controlar el sistema [14].

Elementos vulnerables en un sistema de información.

Seguridad está asociado a certeza, falta de riesgo o contingencia, no siendo posible la certeza absoluta, estando el riesgo siempre presente, la seguridad absoluta no es posible siendo un problema integral que no puede no puede ser tratado aisladamente [13].

Los datos constituyen el principal elemento a proteger en una institución, en vista a que es el más amenazado y el más difícil de recuperar. Para proteger los datos las medidas de seguridad que deben establecerse comprenden el hardware, el sistema operativo, las comunicaciones, los controles organizativos y legales [13].

Muchos programas y sistemas informáticos poseen una serie de errores de programación producidos por la rapidez en el diseño o por el escaso tiempo de pruebas, estos pueden ser aprovechados para realizar un ataque. Estos errores son verdaderas vulnerabilidades que ponen en peligro la seguridad de los datos [14].

Pruebas de penetración

En la revista [17] el termino Pent Test o Test de penetración es un procedimiento compuesto por un conjunto de técnicas y métodos que simulan el ataque a un sistema para evaluar la seguridad de los sistemas informáticos, redes y aplicaciones. Es necesario realizar un Pent test ya que en toda empresa o institución siempre existe la posibilidad de sufrir ataques, es por eso importante descubrir las fallas.

Entre las diferentes herramientas se incluyen desde scanner de puertos, complejos algoritmos para descifrar claves, sistemas de intrusión por fuerza bruta, herramientas de Sniffing de redes y penetración de firewalls, así como también herramientas de escaneo de vulnerabilidades de aplicaciones web y mucho más.

Tipos de Pent Test

La revista [17] propone la existencia de los siguientes tipos de Pent Test:

- Pruebas de penetración con objetivo: se buscan las vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización.
- Pruebas de penetración sin objetivo: consisten en examinar la totalidad de los componentes de los sistemas informáticos pertenecientes a la organización.
- Pruebas de penetración a ciegas: en estas pruebas sólo se emplea la información pública disponible sobre la organización.
- Pruebas de penetración informadas: aquí se utiliza la información privada, otorgada por la organización acerca de sus sistemas informáticos.
- Pruebas de penetración externas: son realizas desde lugares externos a las instalaciones de la organización.
- Pruebas de penetración internas: son realizadas dentro de las instalaciones de la organización con el objetivo de evaluar las políticas y mecanismos internos de seguridad de la organización.

Amenazas

La revista de investigación [17] defina como la posibilidad de que ocurra cualquier tipo de evento o acción que puede producir un daño ya sea material o inmaterial sobre los elementos de un sistema de información se le conoce como amenaza. La Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento. Estos eventos pueden causar alteraciones a la información de la organización ocasionándole pérdidas materiales, económicas, de información, y de prestigio.

En el glosario de la ISO 27000, la amenaza es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización. Existen muchos tipos que se alistan a continuación:

- Amenaza lógica: La que afecta a la información almacenada en los activos.
- Amenaza física: El atacante tiene diferentes tipos de acceso físico a la organización y puede ocasionar problemas [17].

Fraudes a través de medios tecnológicos.

En el libro [12] define fraude como desarrollar actos intencionales o causados por omisión para engañar a otros, con la finalidad de hacer daño a alguien y obtener una ganancia para el delincuente. Los delincuentes han encontrado en la tecnología un medio para materializar sus acciones, escudándose en la velocidad, el anonimato, el alcance de los actos y la limitada atención de las instituciones para detectar el fraude.

Aunque las instituciones en la actualidad cuentan con varios elementos de seguridad y control, al momento de hablar de Internet estos pierden su efectividad, debido a la diversidad de ambientes y configuraciones existentes que en la mayoría de los casos no siguen las buenas prácticas que se exigen para asegurar la información-.

Normas ISO para la seguridad de la información.

Una norma es un documento para uso voluntario como resultado del consenso de las partes interesadas y que debe aprobarse por un organismo de normalización reconocido [13]. Existen dos organismos a nivel mundial:

- ISO (International Organization flor Standarization, Organización Internacional para la Estandarización) organismo internacional dedicado a desarrollar reglas de normalización en diferentes campos como la informática.
- IEC (International Electrotechnical Commision) organismo que publica normas de estandarización en el ámbito de la electrónica.

Las normas ISO/IEC 27000 (SGSI) requisitos para la especificación de sistemas de gestión de la seguridad de la información, proporciona el conjunto de estandarización para la seguridad de la información en las ramas:

- Sistema de gestión de la seguridad de la información.
- Valoración de riesgos.
- Controles.

Estas normas van en un rango del 27000 al 27019 y del 27030 al 27044. La ISO 27002 que se corresponde con la ISO 17799-1, describe un código de buenas prácticas para la gestión de la seguridad de la información [13].

Políticas de Seguridad

Según [19] un Plan de Seguridad debe desarrollar los objetivos de seguridad a largo plazo, siguiendo el ciclo de vida completo desde la definición hasta la implementación y revisión. La forma adecuada para plantear la planificación de la seguridad debe partir siempre de la definición de una política de seguridad que defina el qué se quiere hacer en materia de seguridad para a partir de ella, decidir mediante un adecuado plan de implementación el cómo se alcanzarán en la práctica los objetivos fijados.

Así mismo [19] compone las Políticas de Seguridad por, conductas normas y métodos de actuación y distribución de responsabilidades y actuará como documento de requisitos para la implementación de los mecanismos de seguridad. La política debe contemplar al menos la definición de funciones de seguridad, la realización de un análisis de riesgos, la definición de normativas y procedimientos, la definición de planes de contingencia ante desastres.

A partir de la Política de Seguridad se podrá desarrollar un Plan de Implementación, que es dependiente de las decisiones tomadas en ella, en el que se contemplará: el estudio de soluciones, la selección de herramientas, la asignación de recursos y el estudio de viabilidad.

2.2.2. Actividades Académicas Virtuales

[12] asegura que las actividades académicas se desenvuelven en torno a un mundo de grandes expectativas científicas y de constantes cambios tecnológicos. Con el uso y desarrollo de las plataformas educativas, la seguridad de la Información que se almacena procesa y transmite en dichos ambientes es subestimada, se hace necesario el uso de las buenas prácticas de seguridad de la información. El objetivo de la protección de los datos debe ser el de preservar la confidencialidad, integridad y disponibilidad de los datos, tomando en cuenta que existe información muy sensible como notas del curso, del cual depende un estudiante para ser promovido al siguiente nivel.

[12] propone n campo virtual es un software de aplicación Web que permite administrar, gestionar e impartir cursos en línea. En el concepto de aula virtual confluyen dos dimensiones irrenunciables; por un lado, la selección y la organización personalizada de la tecnología que determina que se pone al servicio de la actividad instruccional del mismo modo que se pone las sillas, las mesas, la pizarra, el video y otros, en una clase convencional y, por otro lado, los instrumentos instruccionales y los documento guías que son necesarios para desarrollar una actividad virtual que promueva la construcción del conocimiento.

La Educación Superior según es un marco en el que han acontecido algunos cambios internos en casi todos sus aspectos: principales funciones, relación con la sociedad, funciones de las figuras académicas y caracterización de los estudiantes, entre otros. Tales aspectos configuran una nueva cultura centrada en el desarrollo de ciertas competencias en el estudiante que le permitan autonomía para decidir sobre su propio desarrollo tanto académico como profesional, y en un rol docente orientado a nuevas metodologías que faciliten la flexibilización del currículum, una

evaluación continua-formativa y un papel de guía y orientador de los aprendizajes [13].

Los marcos normativos en materia educativa de diferentes estados demandan, de forma palpable, la implantación de las Tecnologías de la Información y la Comunicación (TIC) en la práctica docente como medio para conseguir mejoras en el proceso de aprendizaje del alumnado. Los alumnos presentan una actitud positiva para trabajar en ambientes mixtos de aprendizaje que involucren la clase presencial apoyada por entornos virtuales [14].

Enseñanza y aprendizaje Universitario en Entornos Virtuales

Las nuevas propuestas universitarias abogan por que el estudiante sea centro y protagonista del proceso de aprendizaje, y se sustituya la importancia de la enseñanza y la adquisición de conocimientos por la importancia del aprendizaje y la adquisición de competencias. Se trata por lo tanto no solo de enseñar, sino también de hacer que los estudiantes aprendan. Saber cómo aprenden, cómo dedican su tiempo y su esfuerzo a aprender, y facilitar su aprendizaje, se convierte en prioridad de la universidad [15].

Realizar un análisis de las nuevas herramientas TIC relevantes para la educación no es tarea fácil, debido al ritmo vertiginoso con el que se producen las novedades en este ámbito. Trabajar en red con el apoyo de las TIC conlleva una nueva manera de entender y de plantear las competencias necesarias para realizar las tareas y llevar a cabo las actividades establecidas [16].

Los escenarios educativos, están constituidos por un conjunto de variables que los definen, actores particulares con roles y formatos de interacción establecidos, contenidos concretos y modalidades de organización del tiempo, el espacio y los recursos específicos, la entrada en escena de las TIC modifica cada una de estas variables y extiende los procesos educativos más allá de las paredes de los centros educativos, gracias al uso de las aulas virtuales [16].

Entorno personal de aprendizaje

El ser humano está en un proceso de continuo conocimiento apoyado siempre por un entorno desde donde aprende. Históricamente lo hizo primero en grupo, en la tribu o comunidad, luego el aprendizaje fue apoyado por los maestros, apareciendo la relación maestro-aprendiz, entorno educativo presente en muchas culturas y por muchos años. Con la invención de la imprenta, se da un momento importante de cambio en el aprendizaje, ya que los libros se conviertan en fuentes primarias de información, como fuentes incuestionables de conocimiento [25].

Con el tiempo, se institucionalizan estos espacios de aprendizaje, dando lugar a la escuela con responsabilidad directa del aprendizaje. Los entornos de aprendizaje personal siempre han estado presentes en la historia del ser humano; con la ayuda de las TIC que han ayudado con mucha información. Esto evidencia que el aprendizaje ya no está centralizado, sino más bien es influenciado por varios tipos de elementos, recursos, sujetos, contextos y demás.

Las herramientas de la Web 2.0 en el sector educativo y particularmente en el universitario es una realidad, apoyado por la disponibilidad de interconectividad y acceso a Internet. Los estudiantes en la actualidad usan diversos medios como buscadores, redes sociales, SMS, aulas virtuales, fuentes alternativas de información, entre otros que son base fundamental para su aprendizaje [25].

Es notable el aumento de herramientas virtuales de apoyo en la educación, la búsqueda de contenidos específicos y el desarrollo de habilidades sin restricciones como el tiempo, la distancia y los costos, son factores decisivos en la búsqueda de conocimiento [27].

2.3.Propuesta de solución

Se desarrolló un análisis de la herramienta Moodle que se usa en la universidad Técnica de Ambato para el desarrollo de los entornos virtuales de aprendizaje, para lo que se realizó ataques simulados sobre la plataforma y se planteó un conjunto de buenas prácticas de seguridad para la información de las actividades académicas virtuales que se desarrollan en la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la UTA, elaborada a partir de recomendaciones, normativas y estándares.

CAPITULO III

METODOLOGÍA

3.1. Modalidad de Investigación

La presente investigación es de tipo aplicada ya que se buscó la aplicación y utilización de conocimientos adquiridos durante la formación profesional para dar una solución práctica a los problemas relacionados con la seguridad de la información, con la finalidad de optimizar y mejorar las actividades académicas virtuales de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales.

En este trabajo se usó la investigación bibliográfica y de campo.

3.1.1. Investigación bibliográfica

Se utilizó la investigación bibliográfica porque es necesario detectar, ampliar y profundizar mediante teorías, conceptualizaciones y criterios de diversos autores la seguridad de la información, apoyándose de fuentes confiables como libros, documentos y publicaciones científicas que aporten el conocimiento requerido para poder alcanzar una adecuada solución del problema.

3.1.2. Investigación de campo

La presente investigación es de campo porque se lleva a cabo sistemáticamente el estudio en el lugar donde se generó el problema mediante alternativas de solución que permita el adecuado control de las actividades académicas virtuales de la Carrera de Sistemas, para lo cual se hace visitas continuas a la institución con el objetivo de identificar sus actividades y obtener información necesaria para adquirir y manejar datos que permitan desarrollar la propuesta planteada.

3.2.Población y Muestra

Para realizar la investigación se trabajó con la Carrera de Ingeniería en Sistemas Computacionales e Informáticos de la Universidad Técnica de Ambato. Se aplicó la técnica de la entrevista al Ing. Jaime Ruiz docente de la carrera, encargado de realizar el control del uso de las plataformas virtuales por parte de los docentes de la carrera.

3.3. Recolección de Información

La técnica utilizada para recolectar la información es la entrevista usando la guía de entrevista como instrumento. Estos datos permitieron un mejor análisis de la información que se requirió para el desarrollo del proyecto.

3.4. Procesamiento y análisis de datos

Una vez obtenida la información se procede a realizar los siguientes pasos:

- Revisión de la información recopilada.
- Análisis estadístico de datos, gráficas, u otras operaciones en los datos de forma apropiada.
- Selección de alternativas para dar solución al problema planteado.
- Análisis e interpretación de los resultados.

3.5.Desarrollo del Proyecto

El desarrollo del proyecto tendrá las siguientes actividades:

- Identificación de las actividades en los entornos virtuales de aprendizaje.
- Análisis de la situación actual.
- Análisis de la plataforma.
- Recolección de datos.
- Organización de los datos adquiridos.
- Análisis e interpretación de la información adquirida.
- Análisis de la seguridad de la Información.
- Ataques simulados.
- Elaboración de un conjunto de buenas prácticas de seguridad para la información de las actividades académicas virtuales.
- Elaboración del informe.

CAPITULO IV

DESARROLLO DE LA PROPUESTA

4. Antecedentes de la propuesta.

La seguridad de la información no es únicamente una cuestión técnica, se debe considerar las personas, los procesos y funciones de la naturaleza de los datos, así como la protección de todos los recursos de una institución.

Las plataformas virtuales, deben cumplir estándares de seguridad que garanticen su correcto funcionamiento, de forma que esté disponible cuando se necesite, existan garantías de que los datos se procesarán adecuadamente y que solo accederán a ella las personas autorizadas.

Los usuarios de la plataforma virtual de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI son todos los actores de la comunidad universitaria teniendo en este grupo a administradores, estudiantes, docentes, docentes y autoridades. Además de los usuarios descritos considerados como finales, tanto los desarrolladores como el personal que ofrece soporte a estas herramientas son los más preocupados en que la plataforma virtual tenga un adecuado nivel de seguridad.

En base a lo indicado se propone implementar la Seguridad de la Información en los Entornos Virtuales de aprendizaje de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la UTA, para lo cual se identificaron las actividades en los Entornos Virtuales de aprendizaje que se desarrollan en la Carrera, se analizó la Seguridad de la Información en la plataforma Moodle usada en la UTA mediante ataques virtualizados, para finalmente desarrollar un conjunto de buenas prácticas de seguridad para la información de las actividades académicas virtuales, elaboradas a partir de recomendaciones, normativas y estándares.

4.1. Identificación de las actividades en los entornos virtuales de aprendizaje.

Para realizar el análisis de las actividades de cada uno de los docentes de la Facultad accedemos a la plataforma virtual en modo administrador

Gráfico 1Vista de Moodle en Modo Administrador

Dentro de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial existen tres carreras:

- La Carrera de Ingeniería en Sistemas Computacionales e Informáticos cuenta con 59 asignaturas y 22 docentes repartidos en las mismas, los recursos que más se utilizan son archivos, foros, cuestionarios y enlaces.

- La Carrera de Ingeniería Electrónica y Telecomunicaciones cuenta con 63 asignaturas y 23 docentes asignados a sus respectivos cursos, las actividades académicas que se destacan por su uso son archivos, foros, tareas y cuestionarios.

- La Carrera de Ingeniería Industrial en Procesos de Automatización cuenta con alrededor de 63 materias y 21 docentes que han sido asignados a su respectivo curso, siendo las actividades académicas virtuales más utilizadas archivos, foros, tareas y cuestionarios.

Una vez realizados los análisis correspondientes de cada una de las actividades que se realizan en la Facultad se obtienen los siguientes resultados:

En el eje de las Y se encuentran la cantidad de recursos y actividades que los docentes utilizan en los respectivos cursos virtuales que se manejan dentro de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

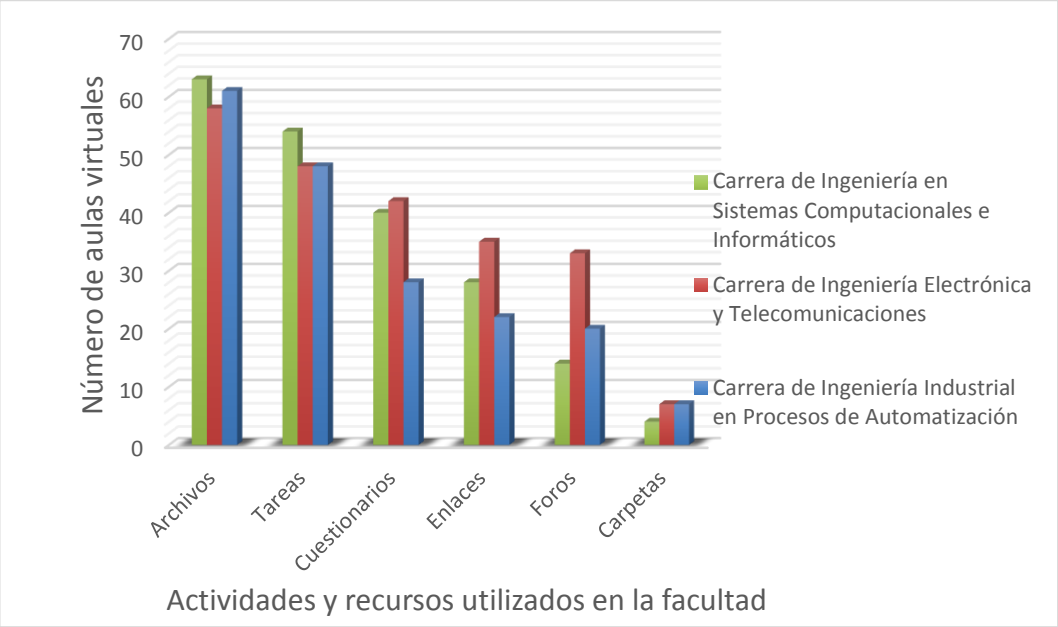


Gráfico 2 Análisis de las actividades y recursos utilizados en el Moodle de la Facultad

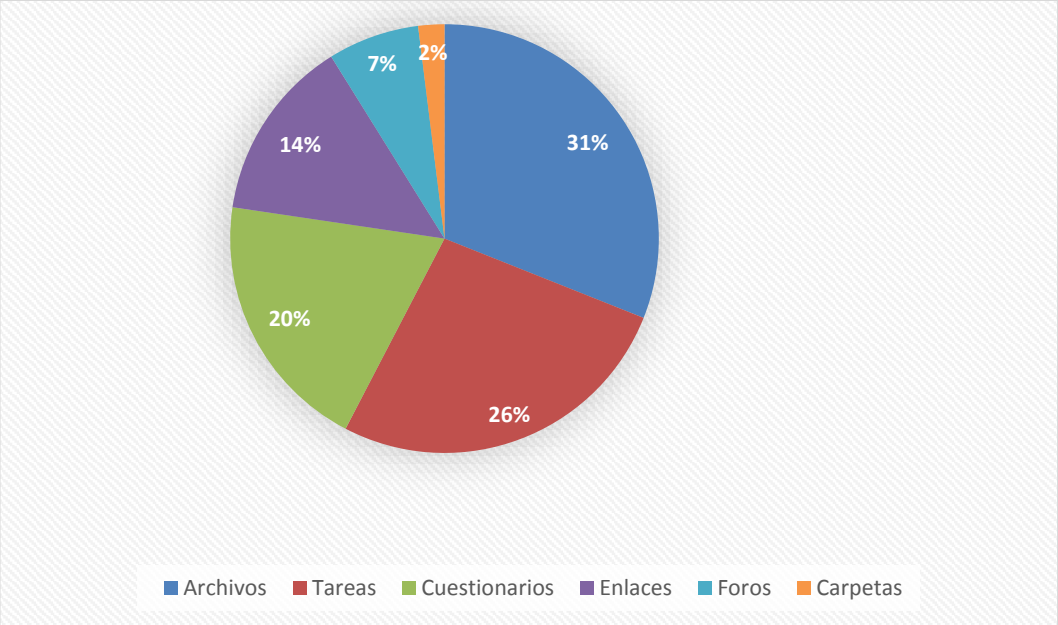


Gráfico 3 Actividades utilizadas por los docentes

Como se observa en el gráfico 2 y gráfico 3 las actividades más usadas en las tres carreras de la Facultad son:

- La actividad de tarea de Moodle proporciona un espacio en el que los estudiantes pueden enviar sus trabajos para que los docentes los califiquen y proporcionen retroalimentación. Esto ahorra papel y es más eficiente que el Email. También puede usarse para recordarles a los estudiantes sobre tareas 'de la vida real' que ellos necesitan completar fuera-de-línea, como por ejemplo actividades artísticas, y que no requieren de contenidos digitales[28]. De 66 docentes 54 de ellos utilizan esta actividad dentro de 153 aulas virtuales de la Facultad se constituye en un 26% del total de aulas virtuales.

- El módulo de actividad de Examen (Cuestionarios en Español Internacional) le permite al maestro diseñar y construir exámenes que consisten en una gran variedad de Tipos de preguntas, incluyendo preguntas de opción múltiple, falso-verdadero y respuesta corta. Estas preguntas se mantienen en el Banco de preguntas y pueden ser reutilizadas en diferentes exámenes[28]. En la Facultad 101 aulas virtuales cuentan con la actividad en estudio y 18 docentes la utilizan representando un 20% de las aulas virtuales.

- La actividad de Foro le permite a los estudiantes y docentes intercambiar ideas al publicar comentarios como parte de un 'hilo' de una discusión. Se pueden incluir archivos tales como imágenes y multimedios dentro de las publicaciones en foro. El profesor puede elegir valorar publicaciones en foros y también es posible darles permiso a los estudiantes para que valoren las publicaciones de unos a otros [28]. El gráfico también nos muestra que 70 aulas virtuales utilizan esta actividad y 10 docentes la usan, siendo el 7% del total de aulas virtuales.

Los recursos más usados en las tres carreras de la Facultad son:

- Archivos, Moodle proporciona una manera fácil para que un profesor les presente materiales a sus estudiantes. Estos materiales toman la forma de archivos, como los documentos de procesadores de texto o presentaciones de imágenes. Los materiales pueden mostrarse en la página, ya sea como ítems individuales o agrupados dentro de carpetas. Un profesor podría, por ejemplo, desear compartir solamente un documento para investigación en formato PDF; otro profesor podría tener una carpeta de exámenes antiguos a manera de ejemplos para que los descarguen los estudiantes [28]. Este es el recurso más utilizado en la Facultad, 182 aulas virtuales cuentan con este recurso y 65 docentes de la Facultad los usan en sus respectivos cursos virtuales constituyéndose el en 31% de las aulas virtuales de la Facultad.

- Enlaces, un URL (Uniform or Universal Resource Locator) es un enlace en el Internet hacia un sitio web o un canal en línea. Los maestros pueden usar el recurso URL para proporcionarles a sus estudiantes enlaces web para investigación, ahorrándole tiempo y esfuerzo a los alumnos que ya no necesitarán escribir manualmente la dirección. Los URLs pueden mostrarse en varias maneras - vea las Configuraciones del recurso URL; por ejemplo, abrir en una nueva ventana de forma que el estudiante pueda acceder y usar el URL y después cerrarlo y regresar con facilidad a su página original del curso Moodle [28]. 101 aulas virtuales tienen dentro de sus recursos los enlaces o URLS 16 docentes la utilizan para complementar sus actividades académicas siendo el 14% de las aulas virtuales.

- Carpetas, una carpeta (del inglés folder) le permite a un maestro mostrar varios recursos de curso juntos. Los recursos pueden ser de tipos diferentes y pueden subirse en una tanda, como un archivo comprimido ZIP que es expandido posteriormente, o pueden añadirse de uno a la vez hacia una carpeta vacía en la página del curso [28]. Un total de 28 aulas virtuales poseen este recurso siendo utilizados por 12 docentes y constituyéndose en el 2% del total de aulas virtuales.

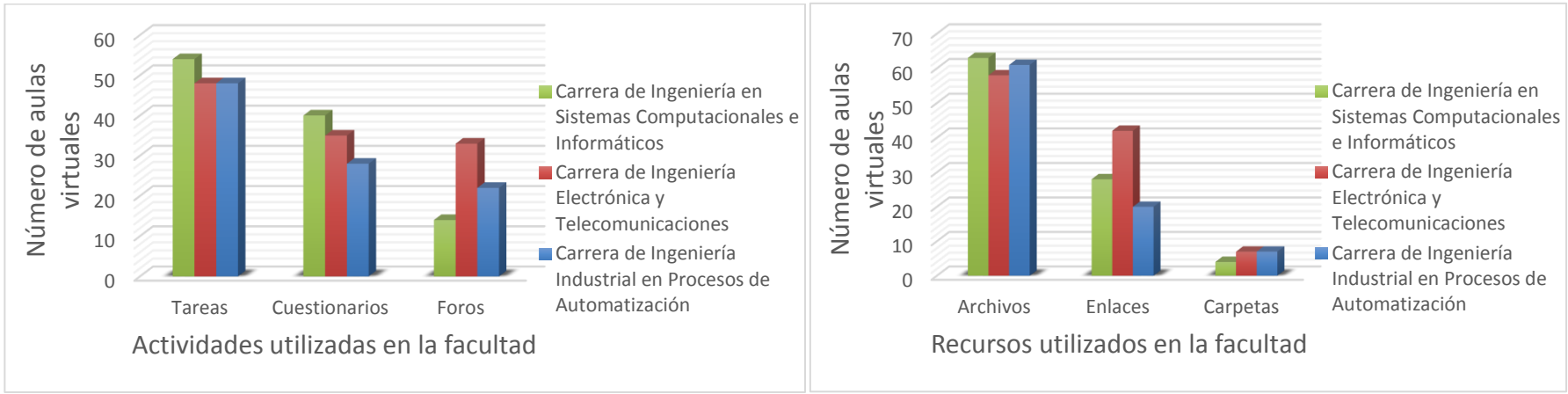


Gráfico 4 Comparación del uso de actividades y recursos dentro de la plataforma virtual

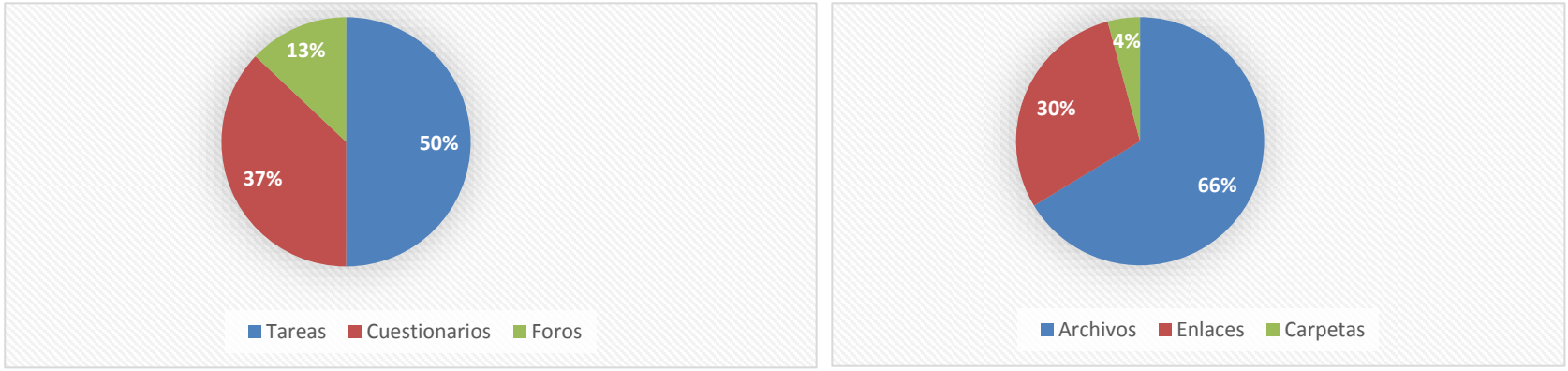


Gráfico 5 Comparación del uso entre actividades y recursos dentro de la plataforma virtual

Como muestran los gráficos 4 y 5 en la plataforma de educación virtual de la Facultad de Ingeniería en Sistemas Computacionales e Informáticos de la Universidad Técnica de Ambato, se utilizan más recursos que actividades. Siendo un 66% de las aulas virtuales en las que se utilizan los archivos como recurso principal, y las tareas con un 50% se constituye como la actividad más usada por parte de los docentes de la Facultad.

Con el presente proyecto de investigación, se pretende realizar un análisis de cada una de las vulnerabilidades que pueda surgir a partir del uso de las actividades y los recursos que mayormente utilizan los docentes de la Facultad.

Asimismo, se aplicaron entrevistas al Ing. Jaime Ruiz Mg. quien es la persona encargada de monitorear el uso de la plataforma virtual por parte de los docentes de la Carrera y al PHD. Carlos Meléndez quién es la persona encargada de la administración de los entornos virtuales de aprendizaje de la Universidad Técnica de Ambato.

A continuación, se presenta la información obtenida en las entrevistas:

ENTREVISTA

Nombre del entrevistado: PHD. Carlos Meléndez

Fecha: 01/09/2017

Cargo: Encargado del Sistema de educación a distancia de la Universidad Técnica de Ambato

Lugar: DEADV Universidad Técnica de Ambato

1. ¿Todos los docentes de la universidad utilizan la plataforma virtual de la institución?
    a. La política de la dirección es facilitar con la creación de las aulas virtuales para todos los docentes de la Universidad, pero el uso de la misma depende de las unidades académicas de cada Facultad

2. ¿Existen quejas de parte de los docentes o estudiantes sobre el uso de la plataforma virtual de la institución?
    a. Las principales quejas son en parte culpa administrativa, es decir, se les olvida las contraseñas, se cierra antes de enviar los deberes. Los principales problemas que se han reportado son de tipo eléctricos por lo que la unidad decidió almacenar la información dentro del Data Center de la universidad.

3. ¿Han existido antecedentes por sospecha de violación de la información, afectación accidental de información o afectación deliberada de información?
    a. No ha existido notificación por parte del DITIC, ni por parte de los administradores de la plataforma, aunque ha existido casos en los que los administradores han prestado sus contraseñas, así mismo exigieron casos en los que los estudiantes han prestado sus contraseñas y se ha visto afectación deliberada de información por parte de los mismos
    b. Uno de los riesgos que se han identificado, es que aulas virtuales de postgrados los usuarios que ya no se encuentran matriculados aún pueden tener acceso a la plataforma virtual

4. ¿Cuál cree que serían los motivos para que se de algún tipo de incidente en la seguridad de la plataforma virtual de la institución?
    a. Uno de los motivos sería el intentar modificar información por parte de los estudiantes en las aulas virtuales.

5. ¿Ha tenido algún tipo de afectación a la infraestructura tecnológica?

a. El control de todo tipo de ataques a la infraestructura tecnológica lo maneja el DITIC y hasta el momento no se han notificado ningún tipo de ataque.
b. Todos los problemas de infraestructura tecnológica son más de hardware y problemas de configuración del DITIC.

6. ¿Piensa que es necesario simular un test de penetración en la plataforma virtual para así determinar el nivel de seguridad de la misma?
    a. La experiencia que pueda brindar cualquier tipo de ataque y que nos permita identificar falencias del sistema a tiempo es saludable para el departamento.

7. ¿Se realizan copias de seguridad de las plataformas virtuales?
    a. Si, se realizan cuatro respaldos al día y así mismo se tienen respaldos periódicos, gracias a la experiencia que con el tiempo el departamento ha ido adquiriendo a lo largo de estos años. Así mismo se puede restaurar en poco tiempo cualquier daño que la plataforma pudiera sufrir.

8. ¿Actualiza MOODLE regularmente aplicando parches de seguridad?
    a. No, no se actualiza el MOODLE regularmente. Se espera que la versión del MOODLE esté estable. Se espera que todos los servicios que se brindan se mantengan de manera estable.
    b. Los parches de seguridad se aplican en una plataforma de pruebas y si no se presentan inconvenientes se la pone en la versión en vivo.

9. ¿El sistema sugiere a los docentes y estudiantes elegir contraseñas difíciles y a cambiarlas regularmente con una correcta implementación de políticas de contraseñas?
    a. La política del departamento nace desde la creación del usuario donde se le asigna una contraseña inicial la cual después el sistema obliga a su cambio, aplicando políticas de contraseñas.
    b. El cambio o no de esta contraseña queda a gusto del usuario, el sistema no sugiere el cambio de la misma.

10. ¿Cree que es necesario implementar un conjunto de buenas prácticas de seguridad para la información de las actividades académicas virtuales, elaborada a partir de recomendaciones, normativas y estándares?
    a. Mientras más recomendaciones existan y aumenten la documentación interna del departamento es útil

11. ¿En qué versión de PHP se ejecuta la plataforma virtual?
    a. La plataforma virtual ejecuta sobre la versión 7, porque el MOODLE se acopla en la parte de seguridad con esta versión de PHP.

12. ¿En qué versión de MySQL está en ejecución la plataforma virtual? ¿Por qué?
    a. La versión de MySQL 5.7 por ser una versión muy estable y se intenta mantener al día los parches de seguridad de la misma

13. ¿Cuál es el servidor de aplicaciones de la plataforma?
    a. Apache en su versión 2.2, se la mantiene en esta versión por los parches de seguridad que la misma brinda.

14. ¿Por qué se decidió el uso de MOODLE como plataforma virtual?
    a. Ser una plataforma de código abierto, así como el factor económico nos ha llevado a tomar la decisión de utilizarla, siempre tomando en cuenta los riesgos que esto conlleve

15. ¿En un futuro se piensa migrar la plataforma virtual a otra tecnología?
    a. Se ha pensado la migración a BlackBoard, pero primero se tendría que observar si todo queda de manera estable.

ENTREVISTA

Nombre del entrevistado: Ing. Jaime Ruiz Mg.

Fecha: 04/09/2017

Cargo: Encargado de la plataforma virtual de la Facultad de ingeniería en sistemas, electrónica e industrial

1. ¿Todos los docentes de la Facultad utilizan la plataforma virtual de la institución?

    a. Si todos los docentes de la Facultad utilizan la plataforma virtual de la institución

2. ¿Los docentes usan las aulas virtuales para el envío y recepción de Tareas? SI

    a. Si prácticamente todos los docentes la utilizan para estos fines

3. ¿Utilizan los docentes las aulas virtuales para la evaluación de los estudiantes?

    a. Aproximadamente un 50 % de docentes realizan evaluación a través de la plataforma virtual.

4. ¿Cree que es necesario que el sistema siguiera el cambio de contraseña de periódicamente, utilizando estándares de seguridad de contraseñas?

    a. Me parece que si sería necesario.

5. ¿Ha conocido casos de violación de información en la plataforma virtual de la Facultad?

    a. Casos aislados, como el que los señores estudiantes utilizan el nombre de usuario y contraseña de otro compañero para ingresar a la plataforma.

6. ¿Cree que existen Errores en el uso de la plataforma virtual por parte de docentes?

    a. Tanto como errores, no. Más bien se da una Subutilización de la misma, pues al no estar Familiarizados con dicha tecnología la utilizan de forma mínima más bien como obligación.

7. ¿Cree que es necesario implementar un conjunto de buenas prácticas de seguridad para la información de las actividades académicas virtuales, elaborada a partir de recomendaciones, normativas y estándares?

a. Por supuesto que sí, porque nos ayudaría a encontrar puntos débiles dentro de la misma y corregirlas a tiempo

8. ¿Cree que pueda existir modificación deliberada y divulgación o fuga de información que existe en las plataformas virtuales de aprendizaje?

a. No se ha conocido casos, referente a este tema

9. ¿Qué actividades realizan con mayor regularidad los docentes de la Facultad?

a. En lo que tiene que ver con utilización de recursos: proveer archivos. y en lo referente a actividades: la creación de tareas que luego revisará valorará, calificará y a la que podrá dar retroalimentación.

4.2. Análisis y Evaluación de la situación actual

Para el análisis y evaluación de la situación actual se evaluó las amenazas informáticas que pueden afectar con mayor probabilidad al entorno virtual de aprendizaje de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI de la UTA.
Se hallaron problemas con la metodología de actualización que actualmente se está tomando sobre la plataforma virtual, es decir, el no aplicar actualizaciones de la misma, igualmente un problema que se identificó es el no sugerir un cambio de contraseña después de un cierto periodo. Al mismo tiempo se hallaron fortalezas como las buenas políticas de respaldo que se manejan dentro del departamento, así como la sugerencia que nos da el sistema del uso de contraseñas difíciles una vez que la contraseña inicial es cambiada.

Asimismo, se destacan las copias de seguridad que se realizan dentro de la unidad de educación a distancia, y la adecuada capacitación de las personas encargadas del control y vigilancia de la plataforma, al ser un sistema operativo Linux no es necesario contar contra protección contra malware por lo que la protección del servidor de este tipo de intrusiones está cubierto.

Así también se obtienen resultados del análisis de las actividades académicas por parte de cada docente, obteniendo que un 99% de los docentes utilizan foros de interacción, así mismo alrededor del 80% de los mismos utilizan tareas y cuestionarios, constituyéndose todas estas actividades como las principales dentro de la plataforma de aprendizaje Moodle de la Facultad.

De acuerdo con el modelo [28], se seleccionaron las amenazas que mayor grado de afectación pueden presentar sobre el entorno virtual de aprendizaje.

Se procedió en clasificar las amenazas relacionadas con la información asociada al proceso educativo, así como también aquellas que inciden sobre los activos necesarios para utilizar esta información. Con esta información se agruparon las

relacionadas con la información por su causal en accidentales y deliberadas y las de los activos, de acuerdo con el tipo de activo afectado según sean instalaciones y servicios de infraestructura básica, infraestructura tecnológica o el personal con lo cual se definió las siguientes amenazas:

Tabla 1 Amenaza a la información

Nombre	**Descripción**
Errores en el uso del Sistema	Equivocaciones de las personas cuando usan los servicios, datos y otras situaciones comunes.
Errores de operación y mantenimiento de los sistemas	Equivocaciones de personas con responsabilidades de instalación, configuración, operación y mantenimiento de las plataformas.
Errores de monitoreo (logs)	Inadecuado registro de actividades, registros faltantes, incompletos o incorrectos.
Alteración o destrucción accidental de la información.	Alteración o pérdida accidental de la información valiosa.

Elaborado por: Aldas Falcón Christian Alejandro

Tabla 2. Afectación deliberada de información

Nombre	**Descripción**
Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
Destrucción intencional de Información	Eliminación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
Divulgación o fuga de Información	Revelación intencional de información a un tercero, con ánimo de obtener un beneficio o causar un perjuicio.
Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
Abuso de Privilegios	Se produce cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia.
Suplantación de identidad	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.

Repudio	Negación a posteriori de actos realizados en el pasado. Existen varios tipos: Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.
Afectación legal por compromiso de información	Divulgación o modificación no autorizada de información, o que se encuentre afectada por alguna legislación vigente, regulación o contratos. (ej. Datos Personales, Propiedad Intelectual)
Hacking	Ataques donde se vulneran los mecanismos de seguridad de las plataformas informáticas con el fin de lograr acceder y/o modificar información sensible.

Elaborado por: Aldas Falcón Christian Alejandro

Tipo: Amenazas a los activos

Tabla 3. Instalaciones

Nombre	**Descripción**
Desastres naturales	Eventos que pueden ocurrir sin intervención humana como causa directa o indirecta, incluyendo incendios, inundaciones, rayos, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.
Desastres industriales	Sucesos que pueden ocurrir de forma accidental o deliberada, derivados de la actividad humana de tipo industrial. Incluye incendios, inundaciones, explosiones, derrumbes, contaminación química, accidentes de tránsito, contaminación mecánica (Vibraciones, polvo en ambiente), contaminación electromagnética (interferencias de radio, campos magnéticos).
Fallas en el suministro eléctrico	Corte total del suministro eléctrico, bajas de tensión, sobrecargas.
Fallo de las comunicaciones	Corte, degradación o intermitencias en el enlace de Internet, datos o telefonía.
Condiciones inadecuadas de temperatura y humedad	Deficiencias en la climatización de los sitios, excediendo los márgenes de trabajo de los equipos, excesivo calor, excesivo frío, exceso de humedad.

Fallas en el cableado	Fallas en el sistema de distribución del cableado, cortes o daños en los cables.
Fallas en otros servicios de Infraestructura	Deficiencias de otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante.

Elaborado por: Aldas Falcón Christian Alejandro

Tabla 4. Afectación a la Infraestructura tecnológica

Nombre	**Descripción**
Falla de Equipamiento	Fallos en los equipos (hardware) que impiden su correcto funcionamiento. Puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
Falla de Software	Fallos en los programas que impiden su correcto funcionamiento. Agotamiento de recursos. Carencia de recursos de procesamiento de información suficientes que provoca la degradación o caída del sistema cuando la carga de trabajo es desmesurada.
Degradación de los soportes de almacenamiento de la información	Por defectos de fabricación o como consecuencia del paso del tiempo
Manipulación de la tecnología (configuración, programas, equipos)	Alteración intencionada del funcionamiento de los programas, del equipamiento, o de su configuración para obtener un beneficio directo o indirecto del uso de los sistemas.
Vulnerabilidades de los programas (software)	Defectos en el código que posibilitan una acción perniciosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad de operar de un sistema.
Pérdida o robo de equipamiento	La pérdida de equipos provoca la carencia de un medio para prestar los servicios, o sea indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

Ataques de Denegación de Servicio	Consumo de recursos de procesamiento más allá de la capacidad operacional de un sistema generado intencionalmente para provoca la caída del mismo.
Difusión de software malicioso	Infección y propagación de virus, espías (spyware), gusanos, troyanos, bombas lógicas y otro tipo de infecciones informáticas.

Elaborado por: Aldas Falcón Christian Alejandro

Tabla 5. Afectación a las personas

Nombre	**Descripción**
Extorsión o amenazas al Personal	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.
Indisponibilidad del Personal	Cualquier tipo de ausencia del personal como huelgas, ausentismo laboral, bajas no justificadas, bloqueo de los accesos y otros.

Elaborado por: Aldas Falcón Christian Alejandro

Definido el conjunto de amenazas a evaluar, se realizó un análisis, para así determinar las salvaguardas que mejor se apliquen.

Con esta información se clasificaron los controles en tres grupos:

- Gestión de la Seguridad.
- Protección de la Información.
- Protección de Infraestructura.

4.2.1. Gestión de la Seguridad

Políticas de Seguridad

Se debe definir un conjunto de políticas para la seguridad de la información, que estén aprobadas por las autoridades y que se comuniquen a todos los participantes del proceso, incluidos a los estudiantes. Las políticas deben enfocarse a aspectos específicos como el control de accesos, la clasificación de la información, la seguridad física y ambiental, uso aceptable de activos, dispositivos móviles, respaldo de información, protección contra malware y otros [29].

Roles y responsabilidades en Materia de Seguridad

Se deben definir y asignar claramente las responsabilidades para la seguridad de la información y segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés.

Se recomienda definir al menos la responsabilidad de los siguientes roles: Responsable de Seguridad, Responsable de Tecnología, Auditor de Seguridad, Usuarios.

Se deben desarrollar contactos con entidades externas como organizaciones educativas, proveedores de tecnología y seguridad informática y organismos públicos, con objeto de mantenerse actualizado acerca de las tendencias de la industria y la evolución de las amenazas y establecer canales de comunicación para el tratamiento de incidentes de seguridad [29].

Auditorías de Seguridad

Se realizan actividades de auditoría que involucran la verificación de los aspectos de seguridad de la plataforma tecnológica, estas se deben ejecutar periódicamente con la finalidad de revisar la efectividad de los controles implementados. Se debe examinar Gestión de Accesos, Seguridad de Infraestructura y Seguridad Física.

Concientización

Los usuarios deben recibir el entrenamiento apropiado en los temas de seguridad relevantes para su función. Se debe implementar concientizaciones de seguridad para administradores, docentes y estudiantes [29].

Gestión de Incidentes

Implementar un procedimiento donde se puedan reportar incidentes de seguridad, para que sean clasificados según su criticidad, atendidos apropiadamente y almacenados en un lugar seguro.

Recuperación

Definir planes de recuperación para contingencias asociadas a la falta de disponibilidad de la plataforma y realizar pruebas periódicas de funcionamiento de los mismos [29].

4.2.2. Protección de la Información

Según [29] clasifica la información en las siguientes estructuras:

Clasificación de Activos la Información

Los activos informáticos deben estar identificados, de acuerdo con la siguiente clasificación:

- Software (Sistema Operativo, Aplicaciones y Programas).
- Hardware de computación y comunicaciones
- Soportes de almacenamiento (discos, cinta y otros.)
- Instalaciones de Redes.

- Equipamiento de soporte (generadores, Sistemas de alimentación ininterrumpida, aire acondicionado).
- Servicios informáticos (servicios en la nube, software como servicio (SaaS),
- Web hosting
- Servicio técnico, soporte de aplicaciones.
- Servicios de comunicaciones (Enlaces de datos, Internet, enlaces telefónicos, celulares).
- Bases de datos, archivos y documentos.
- Información operacional y de configuración de sistemas.
- Contenidos educativos.

Identificación y autenticación

Controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de autenticación. Los sistemas de gestión de contraseñas deberían ser interactivos y se debe exigir a los usuarios la aplicación de buenas prácticas de seguridad para el uso de contraseñas de calidad. Es importante evitar el repudio y la suplantación de identidad, para así garantizar que el estudiante y no un tercero en su nombre es quién ha realizado las actividades educativas, incluyendo la evaluación [29].

Registro y auditoría

Producir y revisar periódicamente registros relacionados con actividad de los usuarios, excepciones, fallas y eventos de seguridad de la información. Se deben incluir tanto registros de tareas de operación y mantenimiento de los sistemas, así como también los eventos relacionados con las actividades educativas. [29]

Copias de seguridad

Implantar procedimientos de respaldo y recuperación de información. Se deben realizar pruebas regulares de las copias de la información, del software y de las imágenes del sistema para asegurar su integridad. Verificar todos los medios de almacenamiento antes de su eliminación o reutilización para garantizar que la información sensible se haya extraído o se hayan sobrescrito de manera segura [29].

4.2.3. Protección de la Infraestructura Tecnológica

Protección de la red de comunicaciones

Adoptar medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.
Se debe implementar herramientas de seguridad activas de monitoreo de red.

Protección contra malware

Implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.

Gestión de vulnerabilidades

Obtener información sobre las vulnerabilidades técnicas de la plataforma para evaluar el grado de exposición y tomar las medidas necesarias para mitigar los riesgos asociados [29].

Protección del equipamiento

Los equipos se deben proteger para reducir los riesgos de las amenazas y peligros ambientales. En este sentido deben incluirse los siguientes aspectos:

- Protección contra cortes de energía, sobrecargas y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.
- Protección del cableado eléctrico y de telecomunicaciones contra la intercepción, interferencia o posibles daños.
- Mantenimiento preventivo del equipamiento con el objeto de garantizar su disponibilidad e integridad.
- Control de ingreso y salida de equipamiento fuera de las instalaciones.

Seguridad Física

Los equipos deben ubicarse en áreas seguras, dentro de perímetros de seguridad definidos, con barreras de seguridad y controles de entrada que aseguren físicamente el acceso no autorizado, daño e interferencia. Se deben incluir los siguientes controles:
Perímetros de seguridad para la protección de las instalaciones de procesamiento de información.

- Protección de áreas seguras mediante controles de acceso físico.
- Protecciones físicas contra desastres naturales, ataques maliciosos o accidentes [29].

4.3. Análisis de vulnerabilidades

Para el análisis de vulnerabilidades se instalaron entornos virtuales simulando el entorno real del Moodle de la Universidad Técnica de Ambato.

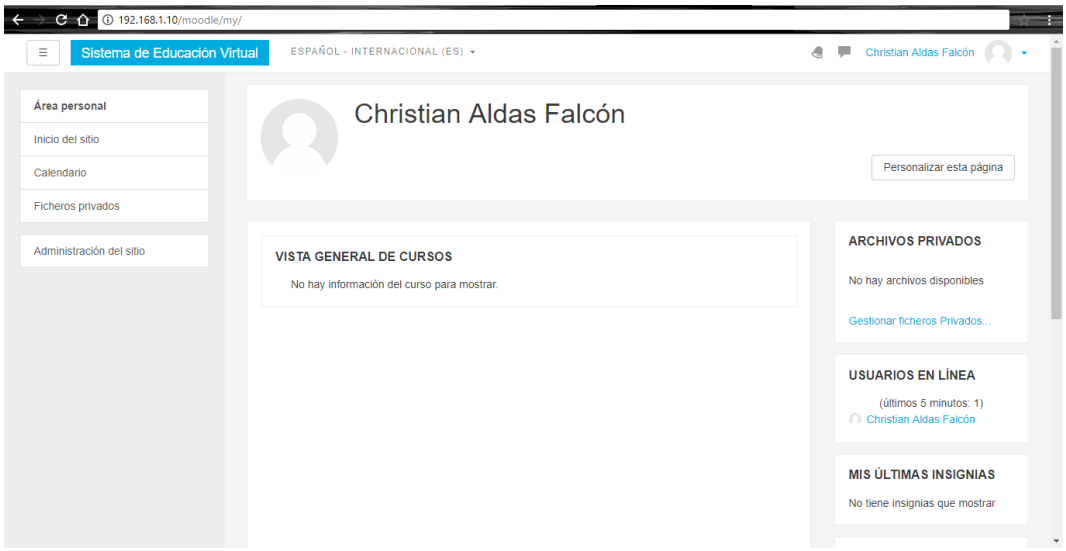


Gráfico 6 Vista de Moodle Virtualizado para realizar análisis de vulnerabilidades

Asimismo, se instaló InsightVM que es una herramienta de análisis de vulnerabilidades en su versión de prueba de 30 días, siendo una de las ventajas la gran cantidad de buenas reseñas que esta aplicación tiene, así como también su versión comunitaria NEXPOSE.

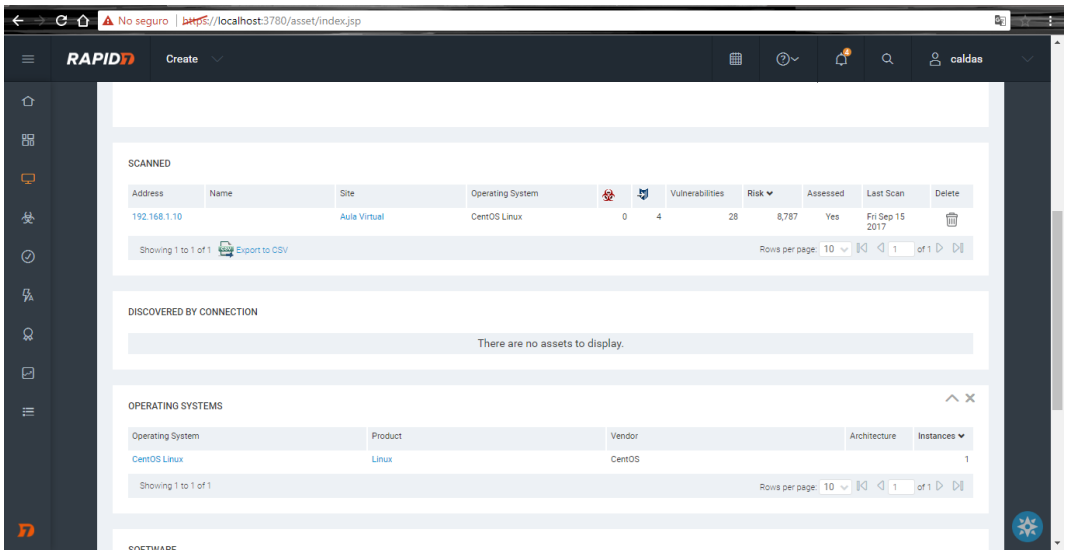


Gráfico 7 Pantalla principal donde se analizan cada una de las vulnerabilidades encontradas

Problema de seguridad	Nessus	OpenVAS	Nexpose	Nmap
Acceso FTP anónimo	✓	✓	✓	✓
VsFTPd Smiley Face Backdoor	✓	✓	✓	
Contraseñas débiles de host	✓		✓	
Man in the Middle	✓	✓		
Null Sessions	✓	✓	✓	
Configuraciones inseguras	✓			
IRCd puerta trasera	✓		✓	
Compilador distribuido	✓		✓	
Autenticación débil (PostgresSQL)	✓	✓		
Autenticación débil (VNC 5900)	✓			

Tabla 8 Tabla de comparación de herramientas de análisis de vulnerabilidades

Como se aprecia en la tabla 8 se puede apreciar la clara superioridad de NEXPOSE contra la competencia, por lo que se convierte en una de las mejores alternativas para la presente investigación.

Una vez terminado el análisis de vulnerabilidades, se encuentran los siguientes puntos de ataques:

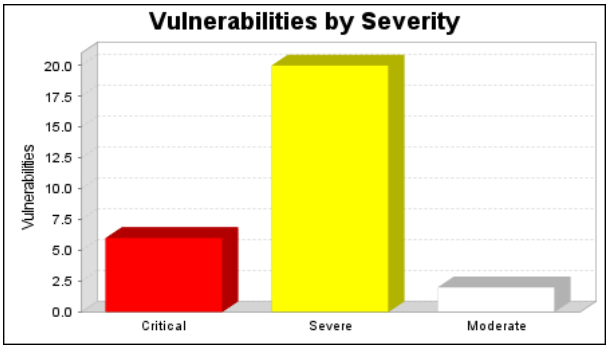


Gráfico 8 Resultados de las vulnerabilidades y su impacto a la organización

Como se aprecia en el gráfico 8 se encontraron en total 28 vulnerabilidades, de las cuales 20 son severas, 6 son vulnerabilidades críticas y 2 poseen un grado de vulnerabilidad moderado. Nos centraremos en los errores críticos y severos en los cuales encontraremos el punto de ataque.

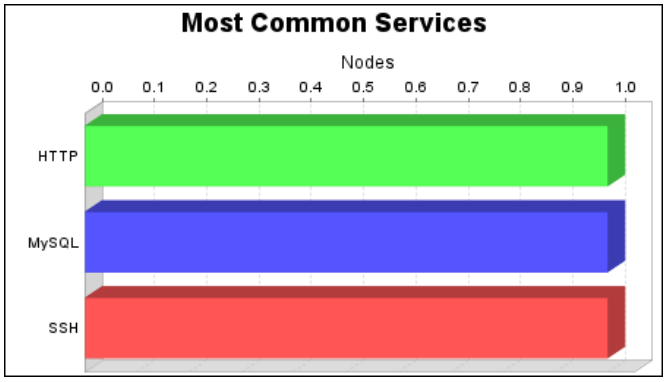


Gráfico 9 Servicios en ejecución

En el análisis de vulnerabilidades por parte de la herramienta se detectan tres servicios en ejecución, de en los cuales la herramienta busca vulnerabilidades cuyo potencial destructivo ayuden como puertas de acceso y puntos de ataque.

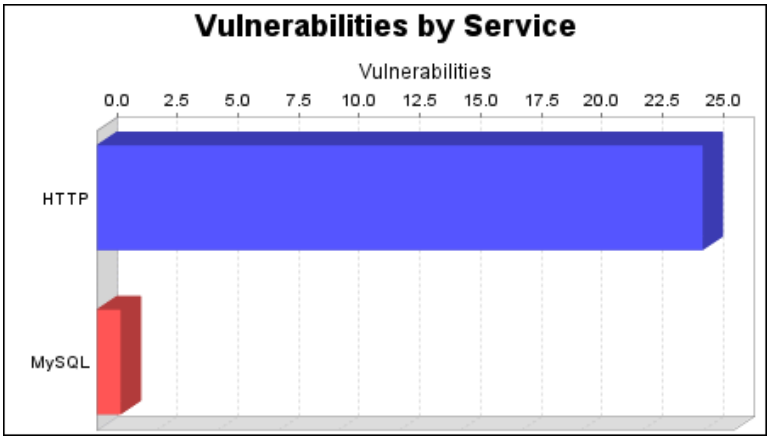


Gráfico 10 Número de vulnerabilidades por servicio

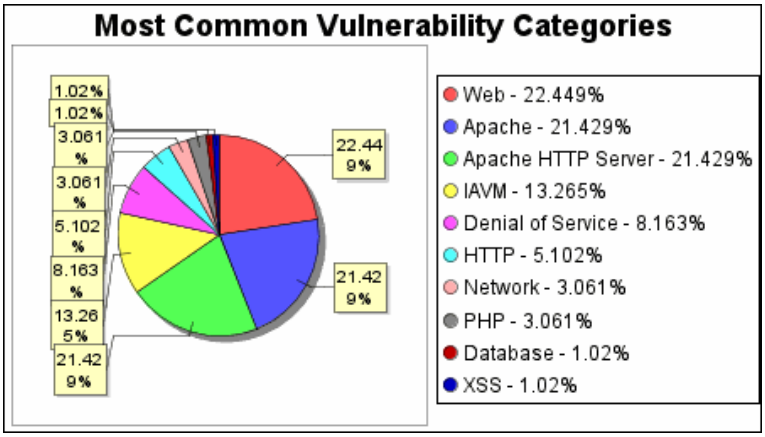


Gráfico 11 Vulnerabilidades

Durante el análisis de vulnerabilidades se encontraron 25 vulnerabilidades relacionadas con el servicio HTTP, convirtiéndose en el punto de ataque que este proyecto de investigación toma como punto vulnerable dentro de los sistemas víctimas, a continuación, se detallan las vulnerabilidades críticas que *InsightVM* descubre durante su análisis.

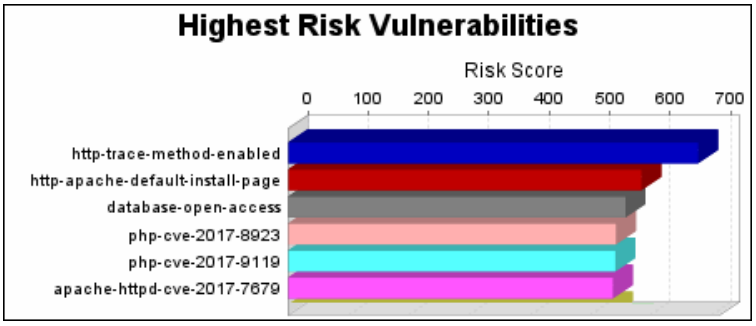


Gráfico 12 Vulnerabilidades con mayor riesgo

Como muestra el gráfico 12 que la vulnerabilidad habilitada para *http-trace-method* plantea el mayor riesgo para la organización con una puntuación de riesgo de 679. Las puntuaciones de riesgo se basan en los tipos y números de vulnerabilidades en los activos afectados.

Vulnerabilidades descubiertas y potenciales

- **Vulnerabilidades críticas**

  - *HTTP TRACE Método Habilitado (http-trace-method-enabled)*
  - Normalmente, se utiliza el método HTTP TRACE para devolver la solicitud HTTP completa al cliente solicitante para propósitos de depuración de proxy. Un atacante puede crear una página web utilizando XMLHTTP, ActiveX o XMLDOM para que un cliente emita una solicitud TRACE y capture las cookies del cliente. Esto resulta en un ataque de Cross-Site Scripting.

  Solución de Vulnerabilidad:

  - Apache HTTPD
    Deshabilitar el método HTTP TRACE para Apache
    Las versiones más recientes de Apache (1.3.34 y 2.0.55 y posteriores) proporcionan una directiva de configuración llamada TraceEnable.
    Para denegar peticiones TRACE, agregue la siguiente línea a la configuración del servidor:

    TraceEnable off

    Para versiones anteriores del servidor web Apache, utilice el módulo mod_rewrite para denegar las peticiones TRACE:

    RewriteEngine On

    RewriteCond %{REQUEST_METHOD} ^TRACE

RewriteRule. * - [F]

- *Instalación predeterminada de Apache / página de bienvenida instalada (http-apache-default-install-page)*

La instalación predeterminada de Apache o la página de "Bienvenida" está instalada en este servidor. Esto suele indicar un servidor recién instalado que todavía no se ha configurado correctamente y que puede no conocerse. En muchos casos, Apache se instala de forma predeterminada y es posible que el usuario no sepa que el servidor web se está ejecutando. Estos servidores raramente son remendados y rara vez monitoreados, proporcionando a los hackers un objetivo conveniente que no es probable que dispare ninguna alarma.

Solución de Vulnerabilidad:

El servidor web Apache debe estar deshabilitado hasta que esté configurado correctamente. Consulte la documentación del servidor HTTP de Apache para obtener instrucciones sobre cómo deshabilitar, configurar y volver a habilitar el servidor.

- *Acceso abierto a la base de datos (base de datos abierta)*

La base de datos permite a cualquier sistema remoto la posibilidad de conectarse a él. Se recomienda limitar el acceso directo a los sistemas de confianza porque las bases de datos pueden contener datos confidenciales y se descubren rutinariamente nuevas vulnerabilidades y vulnerabilidades para ellos. Por esta razón, es una violación de la sección 1.3.6 de PCI DSS tener bases de datos que escuchan en puertos accesibles desde Internet, incluso cuando están protegidos con mecanismos seguros de autenticación.

Solución de Vulnerabilidad:

Configure el servidor de base de datos para permitir únicamente el acceso a sistemas de confianza. Por ejemplo, el estándar PCI DSS requiere que coloque la base de datos
en una zona de red interna, segregada de la DMZ

- *Vulnerabilidad de PHP: CVE-2017-8923 (php-cve-2017-8923)*

La función zend_string_extend en Zend / zend_string.h en PHP a través de 7.1.5 no impide que los cambios en los objetos de cadena resulten en una longitud negativa, lo que permite a los atacantes remotos provocar una denegación de servicio (fallo de la aplicación) o posiblemente tener otro impacto no especificado por aprovechando el uso de un script de. = con una cadena larga.

Solución de Vulnerabilidad:

Descargue y aplique la actualización desde: http://www.php.net/releases/

- *Vulnerabilidad de PHP: CVE-2017-8923 (php-cve-2017-8923)*

La función i_zval_ptr_dtor en Zend / zend_variables.h en PHP 7.1.5 permite a los atacantes causar una denegación de servicio (consumo de memoria y caída de la aplicación) o posiblemente tener otro impacto no especificado al activar operaciones creadas en estructuras de datos de array.

Solución de Vulnerabilidad:

Descargue y aplique la actualización desde: http://www.php.net/releases/

- *Apache HTTPD: mod_ssl De referencia de puntero nulo (CVE-2017-3169) (apache-httpd-cve-2017-3169)*

El activo afectado es vulnerable a esta vulnerabilidad solamente si está ejecutando uno de los siguientes módulos: mod_ssl. Revise la configuración de su servidor web para su validación. mod_ssl puede dereference un puntero NULL cuando los módulos de terceros llaman ap_hook_process_connection () durante una solicitud HTTP a un puerto HTTPS.

Solución de Vulnerabilidad:

- Apache HTTPD> = 2.2 y <2.2.34

  Actualizar a Apache HTTPD versión 2.2.34

  Descargue y aplique la actualización desde: http://archive.apache.org/dist/httpd/httpd-2.2.34.tar.gz

  Muchas plataformas y distribuciones proporcionan paquetes binarios preconstruidos para el servidor HTTP de Apache. Estos paquetes preconstruidos suelen ser personalizados y optimizados para una distribución en particular, por lo que recomendamos que utilice los paquetes si están disponibles para su sistema operativo.

4.4.Test de Penetración

En primer lugar, es necesario conocer qué vulnerabilidades son las más comunes ser explotadas dentro de páginas y aplicaciones web, así como sus servidores.

La OWASP TOP 10 es una recolección de entrevistas realizadas a administradores de sitios y servidores web, en donde dan su opinión acerca de los ataques que frecuentemente suceden hacia sus dominios, en la siguiente tabla se listan los tipos de ataques más comunes en lo que va del año 2017.

Tabla 6 Ataques Metodología OWASP

Nombre	Descripción
1. Inyecciones	Todo tipo de código que no es propio de un sitio o aplicación web y puede ser ingresado sin que el administrador tenga conocimiento del mismo (SQL, OS, XXE)
2. Problemas de autenticación y Manejo de Sesiones	El manejo de sesiones puede estar implementado de manera incorrecta dentro de un sitio web lo que compromete de manera grave a las contraseñas de los usuarios, así como una autenticación no cifrada puede desencadenar robos de sesión mediante cookies vulnerables.
3. Cross Site Scripting XSS	Ocurre cuando un atacante ejecuta un código en un sitio que no posea validación de entradas, para esperar una respuesta HTTP. El código inyectado no afecta directamente a la aplicación sino a un usuario que puede abrir un link incorrecto de la página clonada, el código es incluido en esta nueva página dentro de la URL o en los parámetros HTTP
4. Control de acceso roto	Una mala implementación del control de las acciones que puede o no realizar un usuario es usada por los atacantes para ganar un mayor acceso dentro de un sitio desprotegido.
5. Configuración de seguridad deficiente.	La comunicación entre el sitio web, los servidores, y el manejo de contenidos debe estar configurado de tal manera que sean manejados aisladamente, compartiendo sólo los datos necesarios entre ellos para no comprometer la seguridad de todo el servidor del sitio y sus bases de datos.
6. Exposición de información sensible.	Muchas páginas y aplicaciones web no consideran que cierta información sea necesariamente protegida, por lo cual queda expuesta hacia atacantes que

	pueden utilizarla para realizar fraudes y suplantar la identidad de un usuario
7. Insuficiente protección contra ataques	La percepción de que "un hacker no atacaría este sitio web" es uno de los principales factores para evitar configuraciones de seguridad necesarias dentro de un sitio web, para evitar gastos en expertos o simplemente por descuido.
8. Cross-Site Request Forgery (CSRF)	Se basa en vulnerabilidades encontradas dentro de las cookies de sesión de un sitio web cuando no son cifradas, un usuario que se haya logueado no tiene conocimiento si su sesión ha sido robada y un atacante tiene acceso a toda la información disponible.
9. Usar componentes con vulnerabilidades conocidas	El evitar actualizaciones importantes de los componentes de un sitio web y sus servidores conlleva a estar vulnerables a ataques que ya se han realizado y publicado.
10. Apis desprotegidas	Esta vulnerabilidad fue incluida el presente año, cuando las aplicaciones utilizan tokens de sesión para iniciar las mismas mediante aplicaciones de terceros, usando código JavaScript, si no es bien protegido y no se transporta por canales seguros, la información puede ser robada y leída por terceros.

Al concluir el estudio de las vulnerabilidades más comunes catalogadas por la OWASP se procede con la realización de una tabla detallando qué actividades se van a realizar para la verificación de la existencia de vulnerabilidades dentro del Entorno Virtual de aprendizaje de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales de la FISEI.

Tabla 7 Análisis de metodologías a utilizar

Nombre	**Descripción**	**Riesgo**
Footprinting	Primera fase de hacking ético en donde se conoce las generalidades de un entorno a ser atacado.	----------
Google hacking	Utilización de motores de búsqueda para encontrar entradas hacia páginas web	Bajo

	restringidas de un sitio o aplicación, como por ejemplo usar Google hacking para encontrar la página de administración del sitio en cuestión.	
Escaneo de puertos	Mediante el uso de comandos basados en el mapeo de puertos se obtiene información acerca de aquellos que se encuentran abiertos con lo cual un ataque puede ser focalizado hacia un puerto en específico.	Bajo
Enumeración	Es utilizado para el conocimiento a fondo del sitio web, con los permisos adecuados de la empresa se conoce el aspecto interno de sus servidores y sitios web, manejo de usuarios y roles y procesos de registro con sus respectivas políticas.	---------
Mapa arquitectura web	El conocer a fondo el entorno al cual se va a atacar es necesario dentro de la enumeración para tener un conocimiento más amplio del sitio web.	----------
Identificación de puntos de entrada	Para verificación de puntos de entrada de un entorno web se requiere la utilización de métodos POST y GET dentro de las cabeceras de la misma, para verificar si el sitio posee vulnerabilidades en donde un atacante puede ingresar libremente sin necesitar autenticaciones.	Medio
Enumeración de interfaces de administrador	El manejo de Procesos correctamente ejecutados y políticas que toman en cuenta la seguridad son aspectos que tomar en cuenta al momento de verificar las interfaces de administradores de un entorno.	Bajo
Definición de roles en Moodle.	El tipo de usuarios existentes y las acciones que cada uno de ellos puede realizar o no es una configuración básica que debe ser analizada con la presente investigación.	Medio
Proceso de registro de nuevos usuarios.	El proceso de registro de nuevos usuarios, mediante el uso de credenciales que sean obligatoriamente cambiadas por el usuario y otros procesos de seguridad que serán especificados más adelante se considera como parte fundamental de la investigación.	Bajo

Análisis de vulnerabilidades y explotación	Previamente. habiendo estudiado las generalidades del sitio web se procede con la explotación de las vulnerabilidades más peligrosas y conocidas para poder corregirlas debidamente.	----------
Test de transporte de credenciales con canales encriptados.	Con este test se pretende analizar la existencia de protocolos SSL, principalmente el protocolo HTTPS que garantiza que los datos enviados son encriptados y así sean robados no pueden ser leídos.	Alto
Uso de credenciales por defecto y verificación políticas manejadas por los administradores	Uno de los principales problemas dentro de una institución son los usuarios finales quienes desconocen de los riesgos de usar credenciales por defecto, por lo cual son necesarias políticas de seguridad impartidas por los administradores.	Alto
Funcionalidades de contraseñas para encontrar vulnerabilidades	Las políticas de una institución para el manejo de contraseñas son buenas al principio solicitando al usuario cambiar su contraseña por defecto por una más fuerte, pero pueden existir vulnerabilidades no controladas permitiendo que el usuario cambie su contraseña por una débil en el segundo intento, a más de ello el reseteo de contraseñas debe ser verificado	Medio
Tiempos de espera en cerrar sesión	Una sesión inactiva puede ser blanco para un atacante por lo que la revisión del tiempo de espera antes de cerrarse automáticamente la sesión del usuario es necesario.	Medio
Uso de friendly URLs	Evitar el poner mucha información acerca de las herramientas de trabajo y los números de página en donde se encuentra un usuario en la URL se consigue mediante el uso de friendly URLs las cuales no permiten la observación de estos datos de primera mano.	Bajo
Detección de atacantes	En caso de existir algún ataque, ¿De qué manera puede ser detectado? ¿Y cómo es controlado si existe algún cambio?	Medio
Intrusión	Este tipo de ataques se enfoca en reemplazar directamente a un usuario o conseguir que la página web actúe de una forma que no estaba programada	----------
Ataque de fuerza bruta.	La prueba y error es utilizada para la verificación de esta vulnerabilidad. El probar usuarios y contraseñas hasta dar con uno representa que la página web no posee un	Alto

	mecanismo de cierre por lo que daría paso a un libre ataque de fuerza bruta.	
Secuestro de sesión	El manejo incorrecto de cookies de sesión permite que un usuario esté expuesto a un robo de la misma mediante virus o engaños para obtener cookies y que éstas no se encuentren cifradas es un alto riesgo dentro de una entidad	Alto
Falsificación HTTP	De la misma manera utilizando las cabeceras de un protocolo HTTP el cual no se encuentra cifrado puede ser víctima de intrusiones no deseadas al servidor	Medio
Escala de privilegios	Un atacante que haya robado la sesión de un usuario normal puede convertirse en administrador si no existen protocolos de seguridad.	Alto
XSS	La inyección de código no deseado para poder realizar acciones que no están programadas dentro de un sitio web representa uno de los principales riesgos en las páginas web según la OWASP TOP 10 por lo que es imperativo realizar test de ataques XSS para comprobar la existencia de estas vulnerabilidades.	Alto
Inyección SQL	Analizar la base de datos y los datos que pueden ser vistos dentro de la página web representa un riesgo a tomar en cuenta dentro de un escaneo de vulnerabilidades por lo que es necesario comprobar la correcta configuración de la base y del sitio web	Alto
Ataques DOS	Un servidor maneja múltiples peticiones simultáneamente, pero cuando éstas sobrepasan la cantidad soportada por el mismo se produce un fallo en los tiempos de respuesta. Este tipo de ataque es uno de los más preocupantes debido a su dificultad de detección y mitigación por lo que es necesario la comprobación del mismo y la búsqueda de posibles soluciones.	Alto

4.5. Análisis de reconocimiento de la página web por medio de Footprinting

Conocer el sitio web a donde se desea realizar las pruebas es el primer paso por seguir dentro de la metodología del hacking ético. Es necesario reconocer a dónde se pretende realizar un ataque, las URLS conocidas del sitio, así como los contactos pertenecientes a sus administradores.

Para conocer de mejor manera al sitio web que se realizará el Pentesting se inicia utilizando un motor de búsqueda.

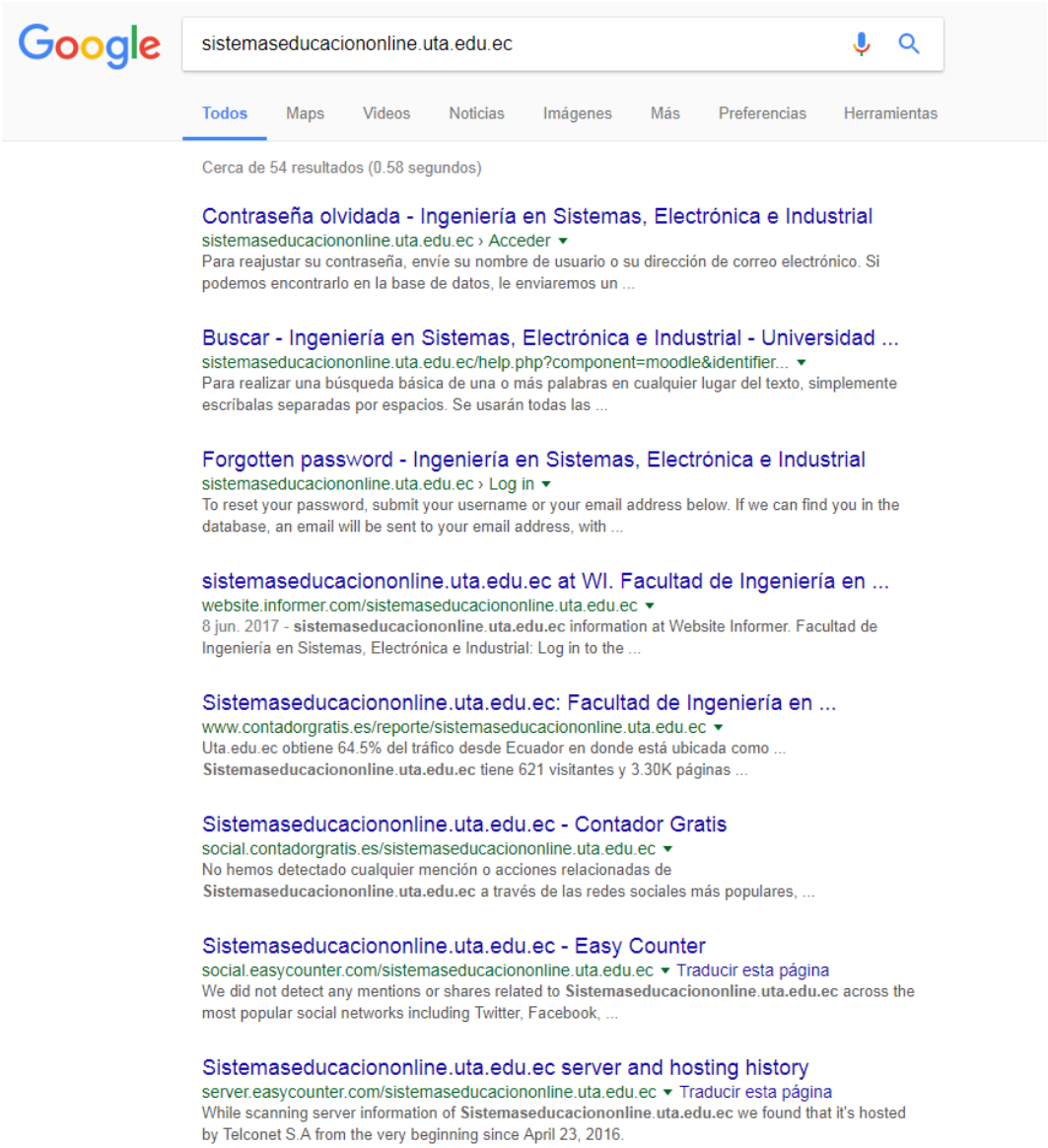
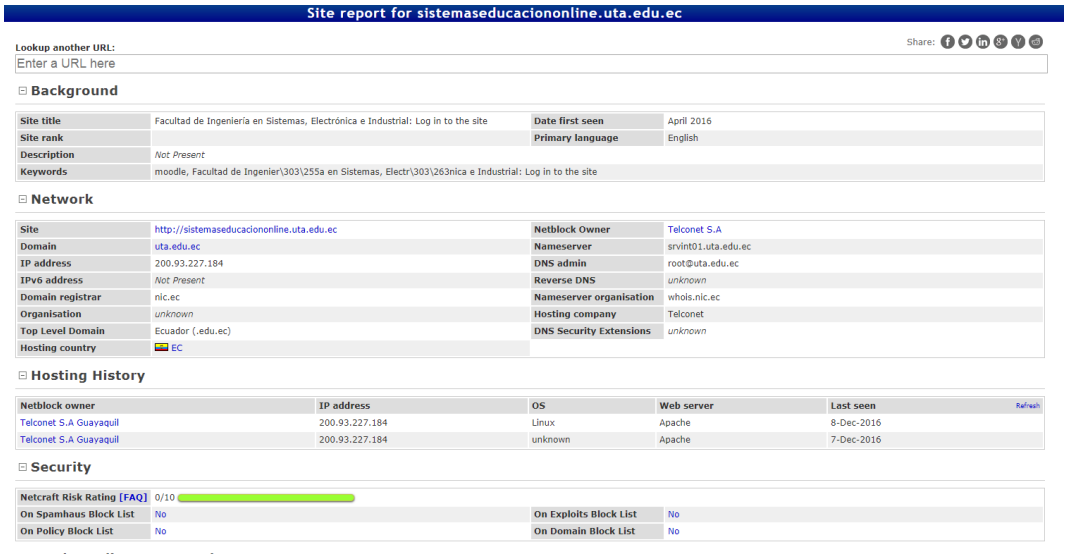


Gráfico 13 Búsqueda en Google de la página web

Los resultados de las búsquedas web nos permiten en el análisis de Footprinting visualizar en todos los dominios en los que la página web en este caso de la plataforma la virtual de la Universidad Técnica de Ambato

De igual manera conocer las herramientas con las que el sitio web está realizado y con cuáles trabaja es necesario para tener un enfoque claro acerca de vulnerabilidades existentes en las mismas. Mediante el uso de la herramienta online Netcraft se obtuvo información del sitio web y de las herramientas utilizadas para ponerlo en funcionamiento.



Site report for sistemaseducacionononline.uta.edu.ec

Lookup another URL: Enter a URL here

Share:

Background

Site title	Facultad de Ingeniería en Sistemas, Electrónica e Industrial: Log in to the site	Date first seen	April 2016
Site rank		Primary language	English
Description	*Not Present*		
Keywords	moodle, Facultad de Ingenier\303\255a en Sistemas, Electr\303\263nica e Industrial: Log in to the site		

Network

Site	http://sistemaseducacionononline.uta.edu.ec	Netblock Owner	Telconet S.A
Domain	uta.edu.ec	Nameserver	srvint01.uta.edu.ec
IP address	200.93.227.184	DNS admin	root@uta.edu.ec
IPv6 address	*Not Present*	Reverse DNS	*unknown*
Domain registrar	nic.ec	Nameserver organisation	whois.nic.ec
Organisation	*unknown*	Hosting company	Telconet
Top Level Domain	Ecuador (.edu.ec)	DNS Security Extensions	*unknown*
Hosting country	EC		

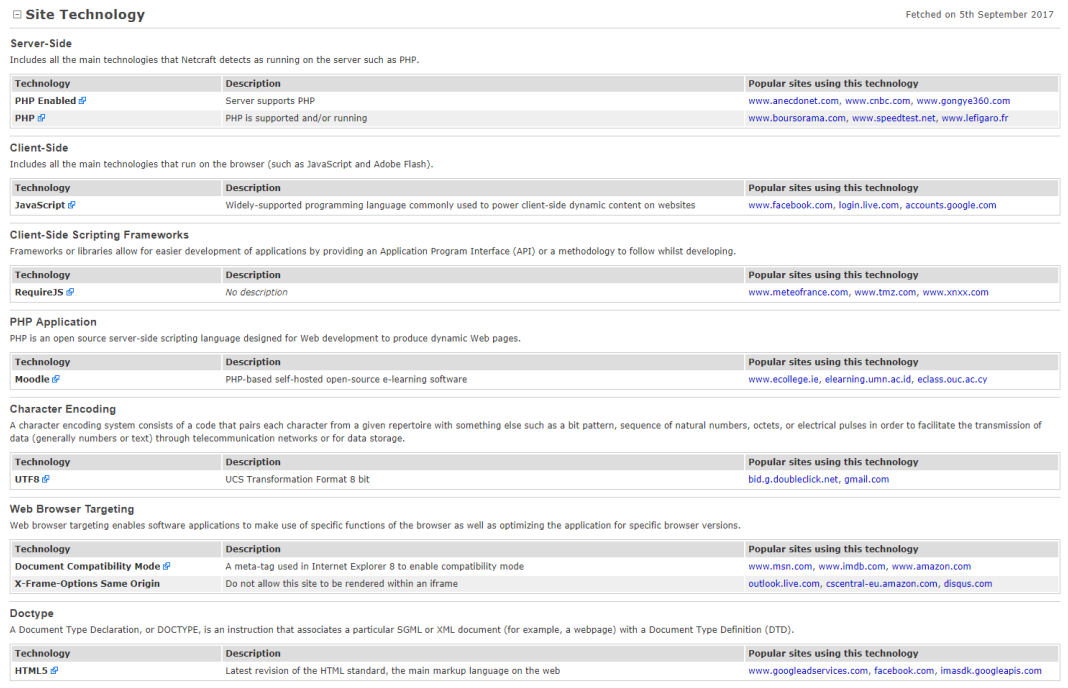
Hosting History

Netblock owner	IP address	OS	Web server	Last seen (Refresh)
Telconet S.A Guayaquil	200.93.227.184	Linux	Apache	8-Dec-2016
Telconet S.A Guayaquil	200.93.227.184	unknown	Apache	7-Dec-2016

Security

Netcraft Risk Rating [FAQ]	0/10		
On Spamhaus Block List	No	On Exploits Block List	No
On Policy Block List	No	On Domain Block List	No

Gráfico 14 Respuesta de consulta en Netcraft (1)



Site Technology Fetched on 5th September 2017

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
PHP Enabled	Server supports PHP	www.anecdonet.com, www.cnbc.com, www.gongye360.com
PHP	PHP is supported and/or running	www.boursorama.com, www.speedtest.net, www.lefigaro.fr

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.facebook.com, login.live.com, accounts.google.com

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
RequireJS	*No description*	www.meteofrance.com, www.tmz.com, www.xnxx.com

PHP Application

PHP is an open source server-side scripting language designed for Web development to produce dynamic Web pages.

Technology	Description	Popular sites using this technology
Moodle	PHP-based self-hosted open-source e-learning software	www.ecollege.ie, elearning.umn.ac.id, eclass.ouc.ac.cy

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	bid.g.doubleclick.net, gmail.com

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Document Compatibility Mode	A meta-tag used in Internet Explorer 8 to enable compatibility mode	www.msn.com, www.imdb.com, www.amazon.com
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	outlook.live.com, cscentral-eu.amazon.com, disqus.com

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	www.googleadservices.com, facebook.com, imasdk.googleapis.com

Gráfico 15 Respuesta de consulta en Netcraft (2)

Con la información adquirida se realiza también la investigación de los sitios públicos y privados de la página web. En este caso el sitio que se presenta a los usuarios y el de administración.

Gráfico 16 Vista de modo administrador del Moodle de la Facultad

Otra forma de conocer en mayor medida a un sitio web es mediante el comando whois dentro de Linux o con la herramienta online Easycounter la cual tiene la misma función.

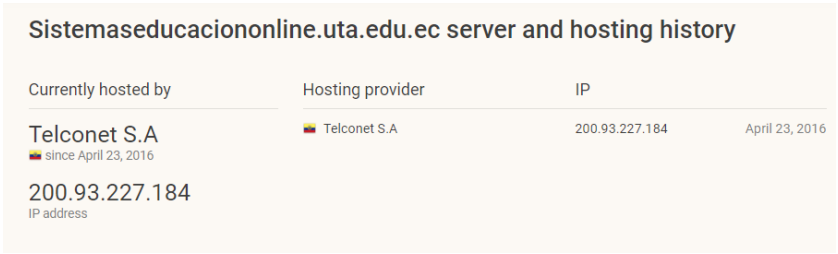


Gráfico 17 Respuesta de consulta de la página web en Easycounter (1)

```
inetnum:        200.93.224/20
status:         allocated
aut-num:        N/A
owner:          Telconet S.A
ownerid:        EC-TESA-LACNIC
responsible:    TELCONET S. A.
address:        Kennedy Norte MZ, 109,
address:        59342 - Guayaquil -
country:        EC
phone:          +593 4 2680555 [101]
owner-c:        TRS4
tech-c:         SEL
abuse-c:        SEL
inetrev:        200.93.224/21
nserver:        SRV1.TELCONET.NET
nsstat:         20170608 AA
nslastaa:       20170608
nserver:        SRV2.TELCONET.NET
nsstat:         20170608 AA
nslastaa:       20170608
created:        20040123
changed:        20040123

nic-hdl:        SEL
person:         Carlos Montero
e-mail:         networking@TELCONET.EC
address:        Kennedy Norte MZ, 109, Solar 21
address:        59342 - Guayaquil -
country:        EC
phone:          +593 42680555 [4601]
created:        20021004
changed:        20170323

nic-hdl:        TRS4
person:         Carlos Montero
e-mail:         networking@TELCONET.EC
address:        Kennedy Norte MZ 109 SL 21, ,
address:        - Guayaquil - GU
```

Gráfico 18 Respuesta de consulta de la página web en Easycounter (2)

Con los primeros pasos del Footprinting se pudo obtener una gran cantidad de información tal como:

- Direcciones IP importantes
- Nombres de dominio
- Direcciones de los proveedores y sus datos
- Correos electrónicos
- Herramientas de funcionamiento
- Nombre y sistema operativo del servidor

Finalmente se procede a realizar una búsqueda más minuciosa mediante el comando nmap hacia la página web para verificar los puertos abiertos y cómo se comunica internamente.

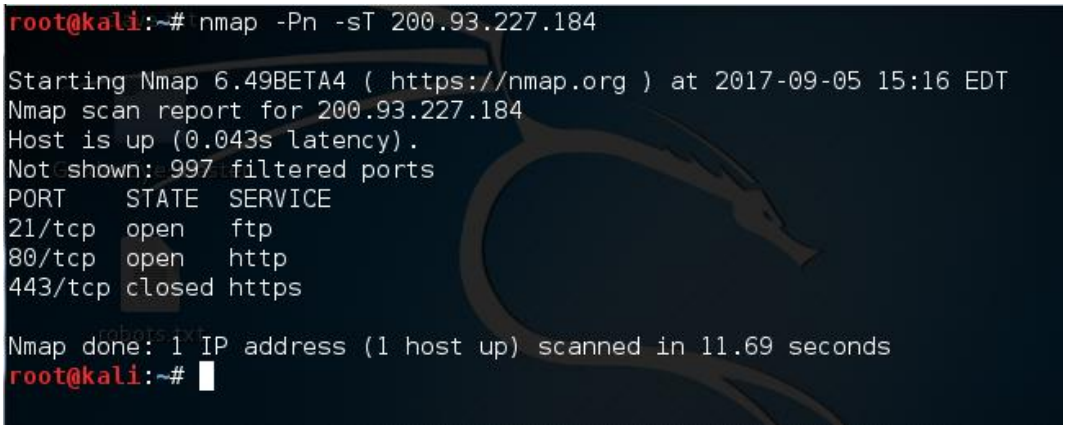


Gráfico 19 Consulta de nmap a puertos abiertos de la plataforma

Como nos muestra el gráfico anterior hay puertos los cuales pueden ser fuentes de ataque. Tenemos el puerto 21 que corresponde al puerto FTP el que nos permite descargar archivos desde el servidor hacía un equipo cliente, generalmente tiene cifrado por contraseña por lo que los ataques más comunes son de fuerza bruta, los mismos para descifrar una contraseña pueden durar días e incluso meses. Asimismo, el puerto 80 que permite al servidor HTTP escuchar una petición hecha por un cliente, es decir a cualquier computador en es específico. Por último, encontramos al puerto 443 que corresponde a HTTPS que es un protocolo de aplicación basado en HTTP, es decir, corresponde a una versión segura de éste.

Igualmente se comprueba los filtros de firewall existentes

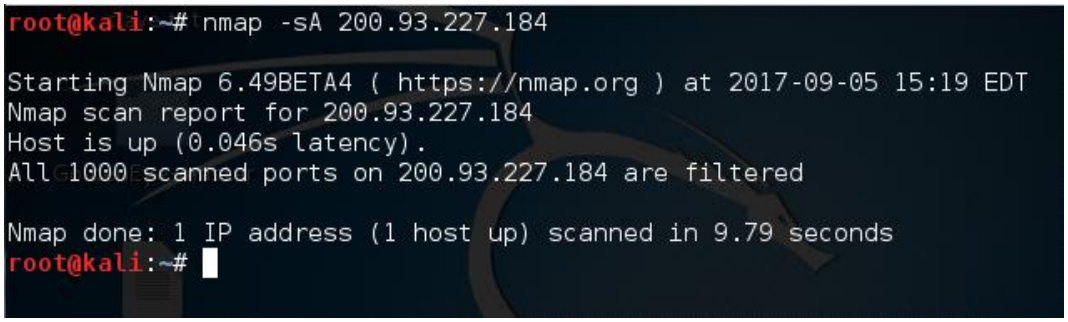


Gráfico 20 Consulta con nmap de presencia de filtrado firewall

Con la prueba anterior notamos la presencia de un filtrado firewall, que significa que todos los puertos poseen un filtrado negando el acceso por cualquiera de ello a cualquier atacante externo.

Una forma de obtener todos los datos de las herramientas utilizadas por un sitio web es mediante el comando whatweb el cual proporciona información detallada de las herramientas utilizadas y su versión.

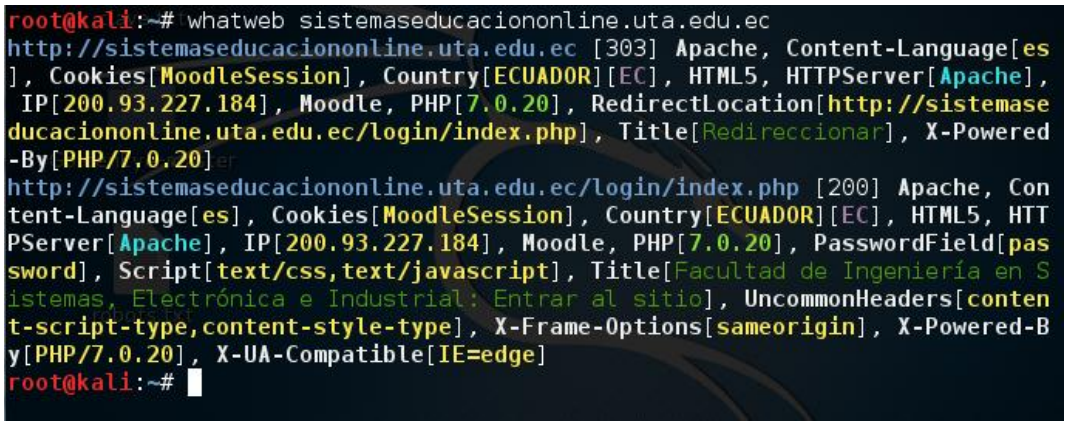


Gráfico 21 Análisis de la plataforma virtual

Con la respuesta obtenida se enfoca de mejor manera el estudio de la presente investigación teniendo en cuenta que el sitio web es manejado por PHP versión 7.0.20, así como también se identifican el uso de cookies con el nombre MoodleSession que más adelante serán sujetos de pruebas, se logra identificar también el servidor de aplicaciones Apache a quién también se atacará para probar su buen funcionamiento y configuración.

Enumeración

La enumeración dentro del Hacking no es más que la extracción de nombres de administradores, redes, arquitecturas, herramientas, recursos y servicios de un sistema. En la presente investigación se enfoca la enumeración a los primeros procesos manejados por la administración de Moodle como son sus interfaces y creación de nuevos usuarios.

En primer lugar, se realiza la investigación de la arquitectura completa de la página web, de esta forma determinar la existencia de páginas web con información sensible que no debería ser accedida fácilmente por cualquier persona.

Al realizar un análisis sin haber hecho ningún inicio de sesión se obtuvo.

Gráfico 22 Enumeración de la Plataforma Virtual

Como resultado pudo observar la presencia de ‘cookies’ al ingresar a la plataforma virtual, si realizar un login dentro de la plataforma se evidencia claras deficiencias de seguridad.

Mediante la herramienta OWASP ZAP se puede apreciar de mejor manera y en mayor profundidad esta arquitectura, al ser una herramienta de auditoría de seguridad de una página web muestra claras ventajas contra otras herramientas con similares características.

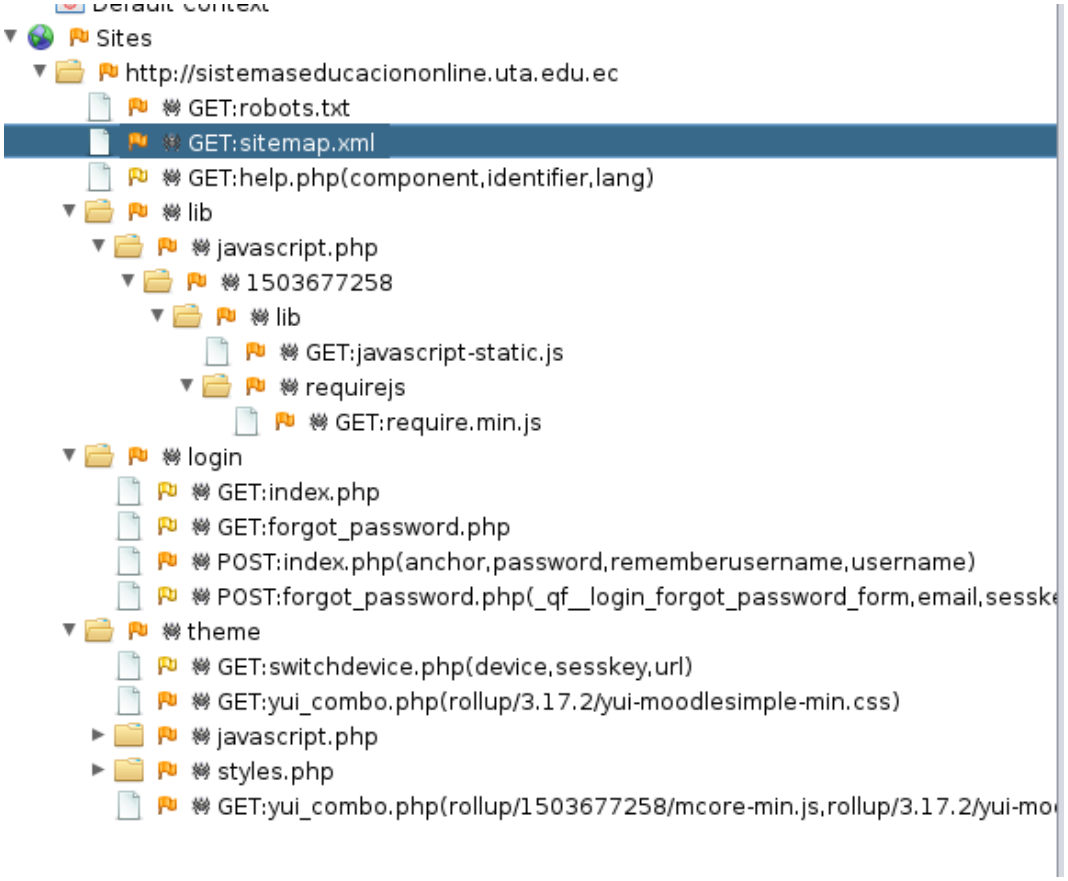


Gráfico 23 Respuesta de análisis de arquitectura usando la herramienta OWASP ZAP

En donde se encuentra páginas que la anterior herramienta no tomó en cuenta, en este caso se tratan de páginas del sitio destinadas a la recopilación de código JavaScript y de sus hojas de estilos y temas.

Gráfico 24 Resultado de ingreso a URL de código JavaScript obtenida mediante OWASP ZAP

El gráfico anterior nos muestra el código JavaScript que permite a los atacantes realizar cambios en el mismo con el fin de cambiar líneas de código como también realizar un estudio de la arquitectura de Moodle.

Mediante la utilización de la misma herramienta se pudo obtener ciertas cabeceras mediante comandos POST y GET respectivamente.

Processed	Method	URI	Flags
	GET	https://www.cedia.org.ec/britannica/	OUT_OF_SCOPE
	GET	http://pivot.cos.com/funding_main	OUT_OF_SCOPE
	GET	http://www.scielo.br/	OUT_OF_SCOPE
	GET	http://sistemaseducaciononline.uta.edu.ec/login/forgot_p...	
	GET	http://sistemaseducaciononline.uta.edu.ec/help.php?com...	
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/switch...	
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/image....	
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/yui_co...	
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/styles....	
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/yui_co...	
	GET	http://sistemaseducaciononline.uta.edu.ec/lib/javascript....	
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/javasc...	
	GET	http://sistemaseducaciononline.uta.edu.ec/lib/javascript....	
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/javasc...	
	GET	http://sistemaseducaciononline.uta.edu.ec/pluginfile.php...	
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/image....	
	POST	http://sistemaseducaciononline.uta.edu.ec/login/index.php	
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/switch...	
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/switch...	
	POST	http://sistemaseducaciononline.uta.edu.ec/login/forgot_p...	
	GET	http://docs.moodle.org/32/es/error/moodle/invalidsesskey	OUT_OF_SCOPE
	GET	http://moodle.org/	OUT_OF_SCOPE
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/switch...	
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/image....	
	GET	http://yuilibrary.com/license/	OUT_OF_SCOPE
	GET	http://www.w3.org/1999/xhtml	OUT_OF_SCOPE
	GET	http://yui.yahooapis.com/	OUT_OF_SCOPE
	GET	http://www.w3.org/TR/SVG11/feature	OUT_OF_SCOPE
	GET	http://sistemaseducaciononline.uta.edu.ec/theme/switch...	

Gráfico 25 Métodos POST y GET testeados en la página web del aula virtual

Al definir el método que un navegador web debe utilizar para enviar variables a la página especificada por su acción, se utilizan los métodos GET o POST. Ambos envían variables a través de una página, pero lo hacen de diferentes maneras.

Para entender un poco más los métodos encontrados en el gráfico anterior [31] define GET envía sus variables en la URL de los navegadores web de sus visitantes, lo que facilita ver lo que se envió. Sin embargo, también hace que sea muy fácil para los visitantes cambiar lo que se envió, y, además, normalmente hay un límite bastante bajo en el número de caracteres que se pueden enviar en una URL - normalmente menos de 250. Como resultado, si usted envía variables largas usando GET, usted es probable perder grandes cantidades de él.

POST por otro lado envía sus variables ocultas a su usuario, lo que significa que es mucho más difícil de imitar, no se puede cambiar sin un esfuerzo en nombre de sus visitantes, y tiene un límite mucho más alto (generalmente varios megabytes) en la cantidad de datos que puede ser enviado. La desventaja de usar POST es que los navegadores no reenviarán automáticamente los datos de publicación si el usuario hace clic en su botón Atrás, lo que lleva a mensajes como "Los datos de esta página deben ser reenviados", lo que a menudo confunde a los usuarios. Esto no sucede con GET, ya que los navegadores consideran que las URL de GET son las mismas que cualquier otra URL, y tan felizmente reenvían los datos según sea necesario.

```
HTTP/1.1 200 OK
Date: Mon, 11 Sep 2017 20:51:14 GMT
Server: Apache
X-Powered-By: PHP/7.0.20
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-UA-Compatible: IE=edge
X-Frame-Options: sameorigin
Set-Cookie: MoodleSession=2neu7gio0n1lg8ab878v5tc1s6; path=/
Expires:
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Content-Language: es
Accept-Ranges: none
Connection: close
Content-Type: text/html; charset=utf-8
```

Gráfico 26 Respuestas de las cabeceras de la página principal de Moodle

Con la información obtenida se puede concluir que:

- Utiliza el protocolo HTTP
- Utiliza cookies de sesión
- No tiene parámetros max-age los que serán estudiados más adelante

Debido a políticas institucionales no se pudo realizar el análisis de cabeceras mediante el comando telnet, debido a que existe un firewall controlado por el Dirección de Tecnología de la Información y Comunicación, el cual es distinto al

departamento donde se realizó el trabajo, pero se utilizó la herramienta OWASP ZAP para análisis de ciertos métodos POST y aquellas cabeceras.

Seguido de ello es necesario conocer de qué manera los administradores controlan el sitio y qué procesos son capaces de hacer. Para ello, mediante la colaboración con el director de la Dirección de Educación a Distancia y Virtual, se tuvo acceso a dichas interfaces.

Para iniciar sesión como administrador de Moodle es necesario ingresar a la página web http://sistemaseducaciononline.uta.edu.ec/admin/user.php .

Gráfico 27 Página principal de administración de Moodle

Al iniciar sesión se despliega todas las posibles acciones que puede realizar un administrador.

Gráfico 28 Interfaz de administrador de Moodle

De igual manera se encuentran definidos los usuarios de Moodle y su gestión.

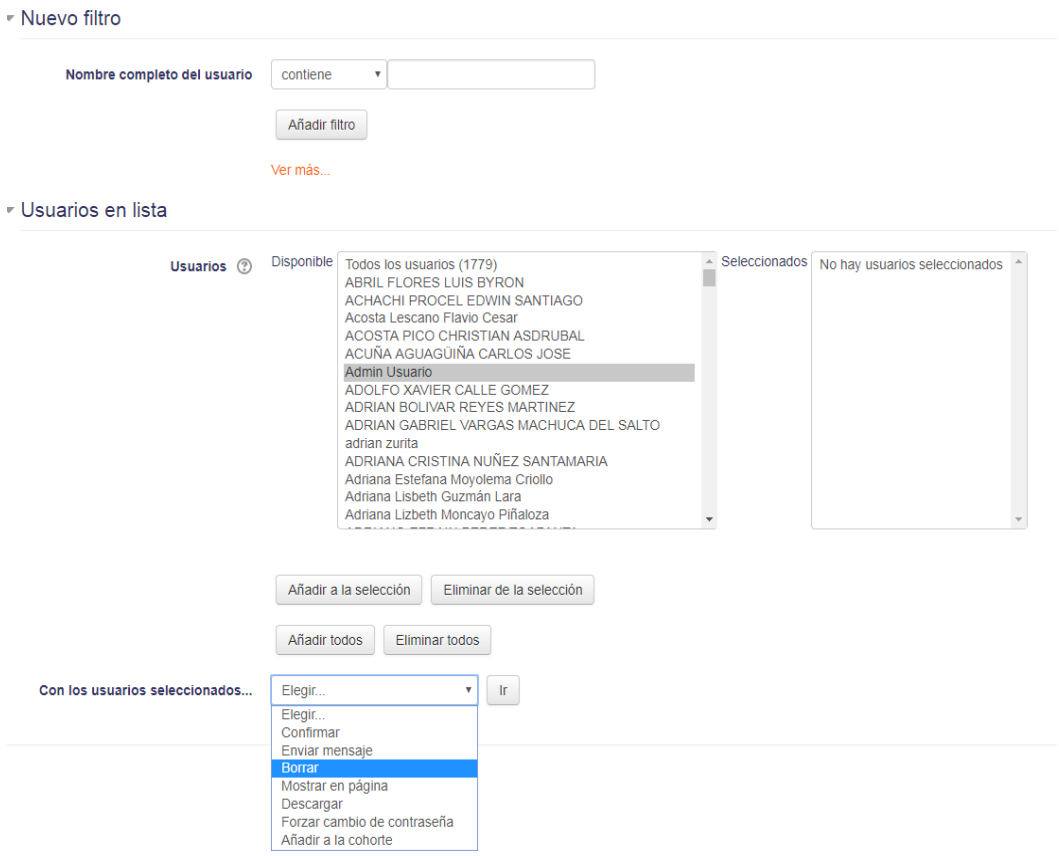


Gráfico 29 Interfaz de manejo de usuarios de Moodle

Los roles de cada usuario deben manejarse con sumo cuidado para evitar la escala de privilegios y que los usuarios estén libres de realizar acciones que no son permitidas para ellos.

Se debe tener en cuenta que los usuarios a crear pueden ser administradores, alumnos y docentes de Moodle, cada uno de ellos posee su información sensible por lo que es necesario asegurar sus datos de la mejor manera posible desde la administración.

Para la comprobación de vulnerabilidades de referencias inseguras a objetos directos se utilizará el mapeo realizado en la recolección de datos encontrando dichas referencias. Por ejemplo, la localización de entradas que usen como parámetro un nombre de tabla, nombre de una fila, lo que puede representar un error de seguridad.

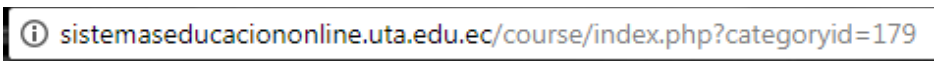


Gráfico 30 Enlace a la página principal de Moodle

En donde se puede apreciar que esta vulnerabilidad está presente siendo posible cambiar el número de la categoría para ingresar a otra página del mismo sitio. Lo cual puede provocar una vulnerabilidad de inyección que será comprobada más adelante.

4.5.1. Ataques a la plataforma virtual de la Universidad Técnica de Ambato

Después de haber estudiado los parámetros iniciales del sitio web se puede proceder al análisis de vulnerabilidades. Para este análisis se tuvo en cuenta el OWASP TOP 10 siendo enfocado en la estructura de Hacking Ético por lo cual las primeras vulnerabilidades a tratar son las que saltan a simple vista.

El cifrado de datos es necesaria debido a que un atacante puede realizar un análisis completo de la red e intervenir peticiones que son realizadas hacia una aplicación web, si las mismas no se encuentran cifradas, el atacante tiene un fácil acceso a información sensible, en el caso del presente proyecto de investigación, se pueden obtener usuarios y contraseñas del aula virtual, un riesgo muy grave en un entorno educativo.

Los datos enviados por los usuarios dentro de Moodle no se encuentran cifrados al no contar con protocolos SSL, específicamente el protocolo HTTPS el cual es utilizado para la prevención de ataques de hombre en el medio en donde el atacante intercepta las peticiones entre el usuario y el servidor y, al no estar cifradas, obtiene en texto plano la información del usuario.

```
HTTP/1.1 200 OK
Date: Mon, 11 Sep 2017 20:51:14 GMT
Server: Apache
X-Powered-By: PHP/7.0.20
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-UA-Compatible: IE=edge
X-Frame-Options: sameorigin
Set-Cookie: MoodleSession=2neu7gio0n1lg8ab878v5tc1s6; path=/
Expires:
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Content-Language: es
Accept-Ranges: none
Connection: close
Content-Type: text/html; charset=utf-8
```

Gráfico 31 Identificación de la configuración de Moodle

Al hablar de credenciales también se debe tener en cuenta a los usuarios, qué tipo de credenciales utilizan para el inicio de sesión dentro del entorno web.

Las políticas de la DEaDV otorgan una clave temporal a un usuario recién creado, el cual al momento de su primer ingreso le es solicitado que la cambie por una de su agrado que contenga ciertos parámetros de seguridad los cuales son: Una

longitud de mínimo 6 caracteres, al menos una mayúscula, al menos un dígito numérico y al menos un carácter especial, lo cual es considerado como seguro, pero es necesaria la comprobación de ésta funcionalidad al momento de cambiar la contraseña por segunda o tercera ocasión.

Gráfico 32 Identificación de políticas de contraseñas usadas por la plataforma virtual

Al momento de ingresar una contraseña débil se muestra.

Gráfico 33 Respuesta ante cambios de contraseña débiles o por defecto

Por lo cual se puede concluir que se han tomado medidas para la prevención de uso de credenciales por defecto por parte de los usuarios.

De igual manera es necesario un análisis de ataques de fuerza bruta para determinar si existe algún mecanismo de cierre automático por parte de la página web.

Intrusión

- Secuestro de sesión

Dentro de una página web, las sesiones muchas veces son guardadas en las cookies presentes en el navegador. Con una correcta configuración de las mismas, cuando existen, son cifradas o, en varios casos, se encuentran bloqueadas.

En el sitio web perteneciente al entorno virtual educativo de la Facultad de Ingeniería en Sistemas Electrónica e Industrial, manejado por la DEaDV, primero se realiza un análisis del tipo de cookies que se están utilizando mediante un método GET o POST de las cabeceras de la página web.

```
HTTP/1.1 200 OK
Date: Mon, 11 Sep 2017 20:51:14 GMT
Server: Apache
X-Powered-By: PHP/7.0.20
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-UA-Compatible: IE=edge
X-Frame-Options: sameorigin
Set-Cookie: MoodleSession=2neu7gio0n1lg8ab878v5tc1s6; path=/
Expires:
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Content-Language: es
Accept-Ranges: none
Connection: close
Content-Type: text/html; charset=utf-8
```

Gráfico 34 Análisis a las cabeceras para comprobación del tipo de sesión y cookies utilizadas

Cuando una aplicación no renueva la cookie de sesión después de la autenticación de un usuario, existe la posibilidad de encontrar la vulnerabilidad de arreglo de sesiones, que consiste en forzar al usuario a utilizar una cookie ya conocida y descifrada por un atacante. Las principales razones por la que éstos ataques pueden resultar exitosos son cuando: el sitio web vuelve a iniciar otra sesión sin previamente finalizar la sesión activa o cuando un atacante es capaz de forzar un ID de sesión ya conocida de algún usuario, por lo tanto, cuando el usuario se autentica, el atacante tiene acceso a esta sesión.

Al analizar el manejo de sesiones mediante las cabeceras de la aplicación se encontró que son manejadas por el parámetro MoodleSession que se transporta usando el protocolo HTTP.

Debido a la vulnerabilidad de no usar un cifrado de datos, con el uso de la herramienta WireShark se obtuvo la clave de sesión de un usuario.

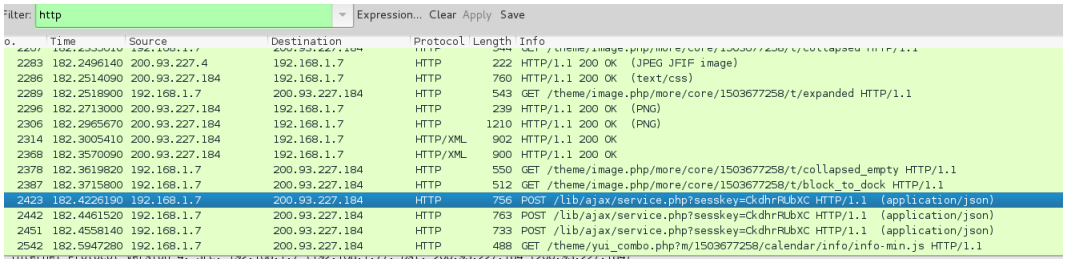


Gráfico 35 Sniffing de actividades HTTP dentro de la red que tengan que ver con Moodle

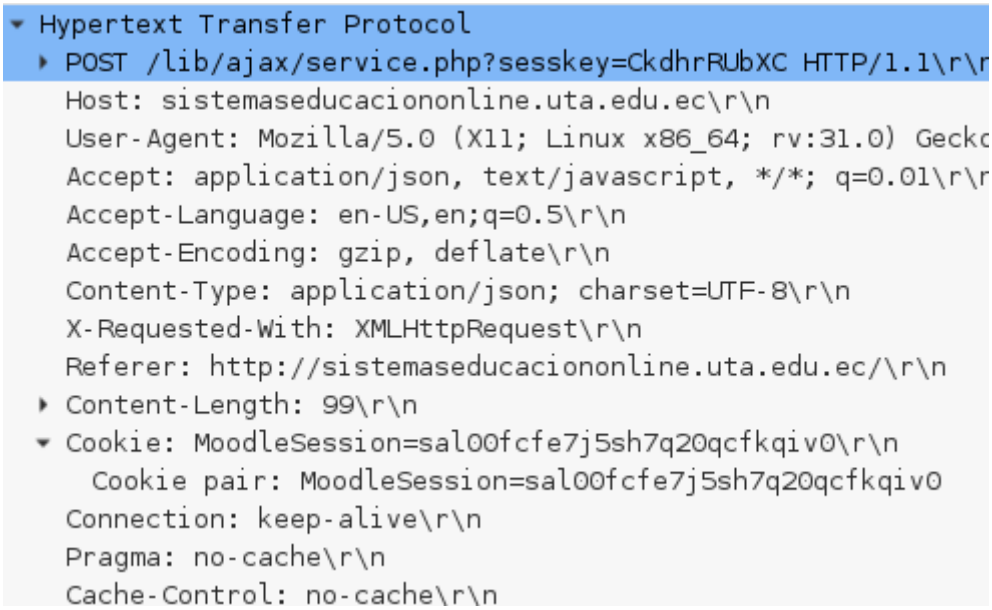


Gráfico 36 Resultado de análisis de cabeceras con el parámetro MoodleSession

Con la clave de sesión obtenida se procedió a utilizar otra máquina con un navegador Mozilla y un addon llamado firebug, el cual permite cambiar la id de sesión del navegador.

Gráfico 37 Uso del addon firebug para análisis de cookies.

El valor de la cookie es editado por el que se obtuvo con la herramienta WireShark

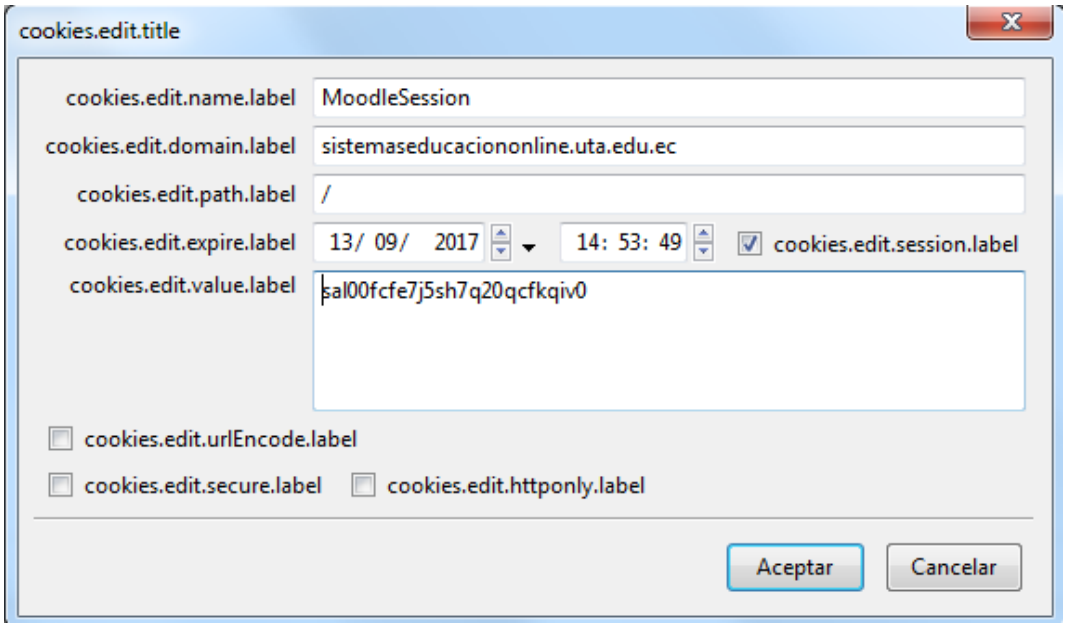


Gráfico 38 Interfaz de firebug para edición de cookies

Y se refresca la página con esta nueva cookie.

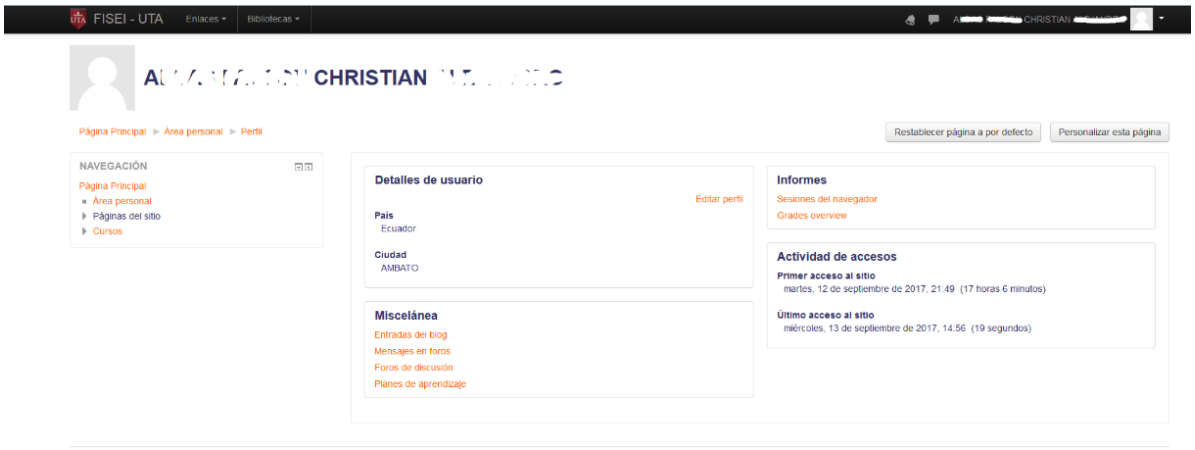


Gráfico 39 Éxito al robar una sesión de un usuario

Obteniendo acceso como un usuario sin la necesidad de conocer las credenciales del mismo, lo que representa una vulnerabilidad grave dentro de la institución.

- XSS

Ocurre cuando un atacante inyecta código ejecutable en el navegador para esperar una respuesta HTTP. El código inyectado no afecta directamente a la aplicación sino a un usuario que puede abrir un link incorrecto de la página clonada, el código es incluido en esta nueva página dentro de la URL o en los parámetros HTTP.

Al reemplazar parámetros HTTP con diferentes nombres, puede causar que una aplicación interprete los valores de maneras no anticipadas. Mediante la explotación de esta vulnerabilidad, un atacante puede sobrepasar las validaciones de atributos de entrada, activar mensajes de error o modificar variables internas.

En la URL de la página web del aula virtual se inyecta un código de una alerta en JavaScript para determinar la existencia de esta vulnerabilidad, como se demuestra en el gráfico 40 el ataque no fue exitoso, y finalmente terminamos redireccionados hacia la página principal de la plataforma virtual.

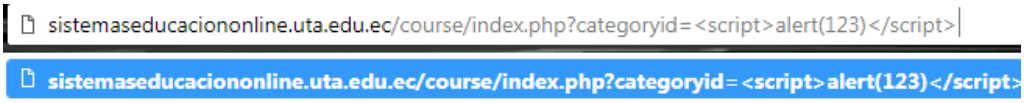


Gráfico 40 Intento de XSS a la página principal de la plataforma

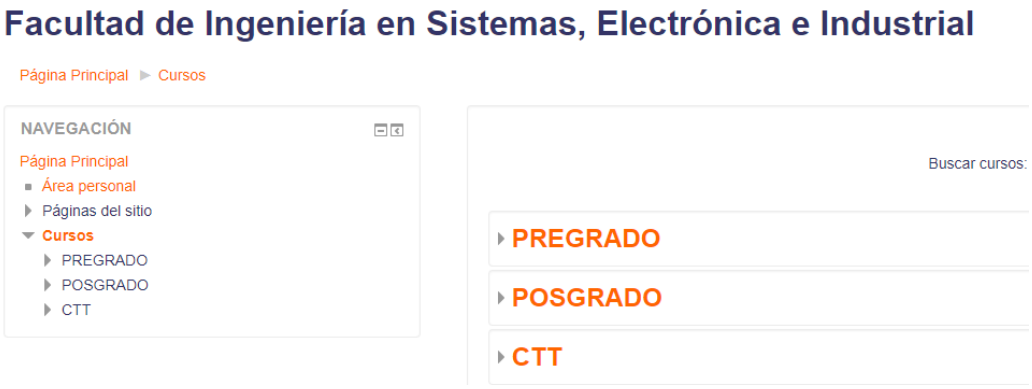


Gráfico 41 Resultado después del intento de XSS

Por lo cual se puede concluir que la inyección XSS a través de la URL no es exitosa,

existe una configuración adecuada por parte de la DEaDV.

- Inyección SQL

Una inyección SQL consiste en la inserción parcial o completa de una consulta SQL vía entrada de datos por parte del cliente hacia la aplicación, para tener un acceso a los datos manejados por el servidor. Una inyección SQL exitosa puede devolver como respuestas información sensible de la base de datos del servidor, modificar la base de datos, ejecutar operaciones administrativas y recuperar contenido de un archivo existente en la base de datos,

Existen distintas maneras de comprobar este tipo de vulnerabilidad, como se pudo comprobar en el test anteriormente realizado, los comandos y caracteres ajenos a la URL son ignorados por lo que un test a la URL queda descartado; mediante la herramienta de Kali Linux, SQLMAP se realiza un análisis de la existencia de la presente vulnerabilidad, las inyecciones de cualquier tipo de datos.

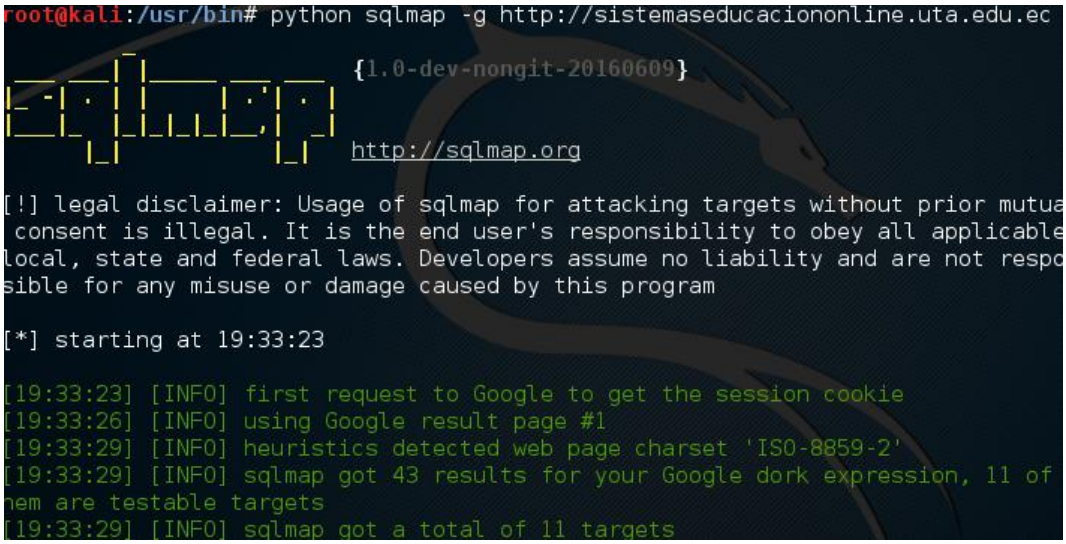


Gráfico 42 Interfaz inicial de sqlmap

Apenas empieza el análisis y da un error.

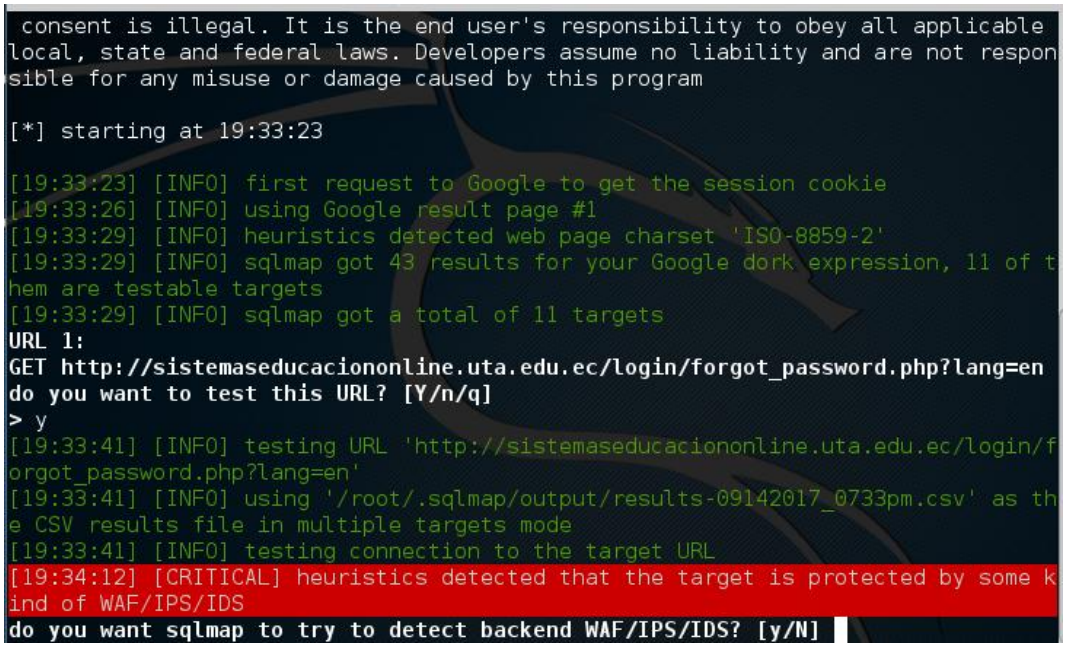


Gráfico 43 Error al detectar protección WAF, IPS o IDS

El cual expresa acerca de la protección existente dentro de Moodle por lo cual puede dificultar el análisis de inyección SQL

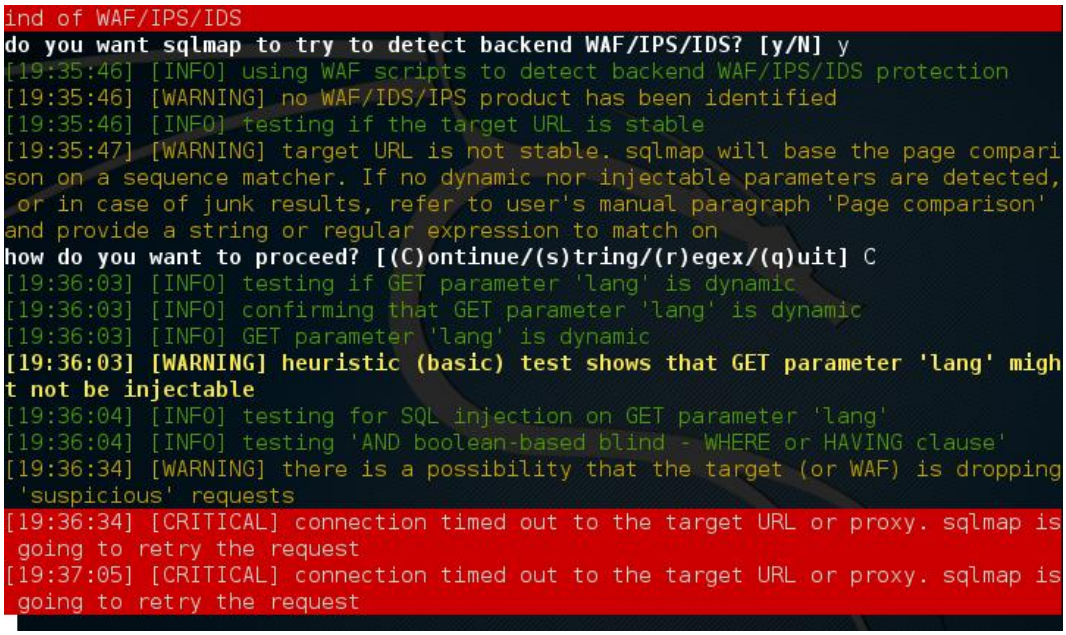


Gráfico 44 Error al estar protegido con un proxy

Finalmente aparece un error de conexión en donde el proxy existente evita el análisis por lo que se puede concluir que existe la protección en contra de inyecciones SQL dentro de Moodle.

- Inyección XML

Se produce cuando un atacante intenta inyectar un documento de tipo XML a la aplicación.

Se realiza en la URL del sitio web y se intenta ingresar un documento de este tipo con parámetros de usuario y contraseña para obtener accesos no autorizados.

El sitio web del aula virtual rechaza todo tipo de solicitudes ajenas a la URL original, es por lo que el presente test no pudo ser realizado y representa una gran seguridad por parte del manejo del sitio web, mas como ejemplo es citado a continuación un intento de inyección XML realizado como ejemplo en la guía de metodología OWASP, para detección de vulnerabilidades en aplicaciones web.

Primero se analiza un archivo XML obtenido de una base de datos

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
        <user>
                <username>gandalf</username>
                <password>!c3</password>
                <userid>0</userid>
                <mail>gandalf@middleearth.com</mail>
        </user>
        <user>
                <username>Stefan0</username>
                <password>w1s3c</password>
                <userid>500</userid>
                <mail>Stefan0@whysec.hmm</mail>
        </user>
</users>
```

Gráfico 45 Ejemplo de un archivo XML de sesión [32]

Después de inyectar un código malicioso, por ejemplo, el de credenciales distintas es generado un nuevo archivo XML.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
        <user>
                <username>gandalf</username>
                <password>!c3</password>
                <userid>0</userid>
                <mail>gandalf@middleearth.com</mail>
        </user>
        <user>
                <username>Stefan0</username>
                <password>w1s3c</password>
                <userid>500</userid>
                <mail>Stefan0@whysec.hmm</mail>
        </user>
        <user>
                <username>tony</username>
                <password>Un6R34kb!e</password>
                <userid>500</userid>
                <mail>s4tan@hell.com</mail>
        </user>
</users>
```

Gráfico 46 Ejemplo de reemplazo de sesión dentro de un archivo XML [32]

- Ataques DOS

Se trata de una de las vulnerabilidades más graves para un sistema manejado en web, no existe una forma total de prevenir estos ataques, ya que, debido a la evolución de la tecnología, de la misma manera evolucionan las maneras de vulnerar y las herramientas para el mismo.

El ataque DOS puede ser dirigido a un servicio específico de un servidor o a todas sus funcionalidades, siendo éste el más peligroso; se debe tomar en cuenta la diferencia entre DOS y DDOS, mientras que DOS es en pequeña escala y dirigido para un ataque pequeño, un DDOS (Distributed Denial of Services) está enfocado en provocar un daño más persistente y duradero.

En el test realizado se emplearon distintos enfoques de ataque.

Primero se realizarán pruebas de estrés para conocer hasta cuantas peticiones soporta el servidor sin sufrir una caída, para ello se utiliza el comando AB (***ApacheBench***) que nos ayudará a medir el rendimiento del servidor de aplicaciones Apache de la plataforma virtual.

```
root@kali:~# ab -r -n 100 -c 20 http://sistemaseducaciononline.uta.edu.ec/login/index.php
This is ApacheBench, Version 2.3 <$Revision: 1604373 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking sistemaseducaciononline.uta.edu.ec (be patient).....done


Server Software:        Apache
Server Hostname:        sistemaseducaciononline.uta.edu.ec
Server Port:            80

Document Path:          /login/index.php
Document Length:        30235 bytes

Concurrency Level:      20
Time taken for tests:   6.199 seconds
Complete requests:      100
Failed requests:        0
Total transferred:      3072500 bytes
HTML transferred:       3023500 bytes
Requests per second:    16.13 [#/sec] (mean)
Time per request:       1239.894 [ms] (mean)
Time per request:       61.995 [ms] (mean, across all concurrent requests)
Transfer rate:          483.99 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:       44  268 173.4    271    1485
Processing:   351  862 313.5    820    2242
Waiting:       84  388 177.5    344    1105
Total:        395 1130 321.0   1102    2529

Percentage of the requests served within a certain time (ms)
  50%   1102
  66%   1162
```

Gráfico 47 Comando AB ejecutado en Kali

Inicialmente se trabaja con 100 peticiones haciendo 20 peticiones concurrentes, para ir aumentando en medida para determinar cuántas peticiones soporta el servidor llegando a un límite de 10000 usuarios con 20 peticiones concurrentes

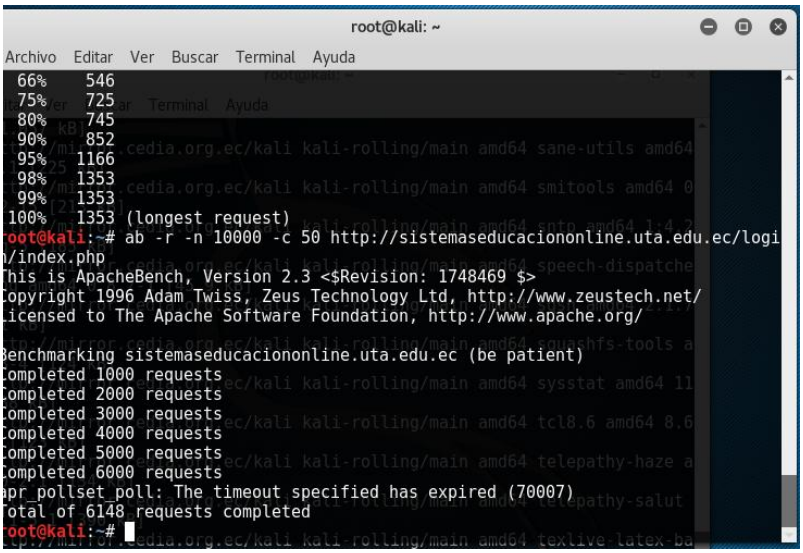


Gráfico 48 Uso del comando ab para análisis de estrés con carga alta

Una vez realizado el análisis de estrés podemos concluir que el servidor soporta cerca de 60000 peticiones con 20 peticiones simultáneas, con esta información se realizan los ataques para verificar.

En el primero es mediante la utilización del comando hping3, que es una aplicación de terminar de Linux nos permite analizar y ensamblar paquetes TCP/IP. Es diferente a un PING normal ya que nos permite el envío de paquetes TCP, UDP y RAW IP. También nos ayuda a analizar la eficacia de un firewall e incluso la protección frente a ataques DoS de un sistema o de un Firewall.

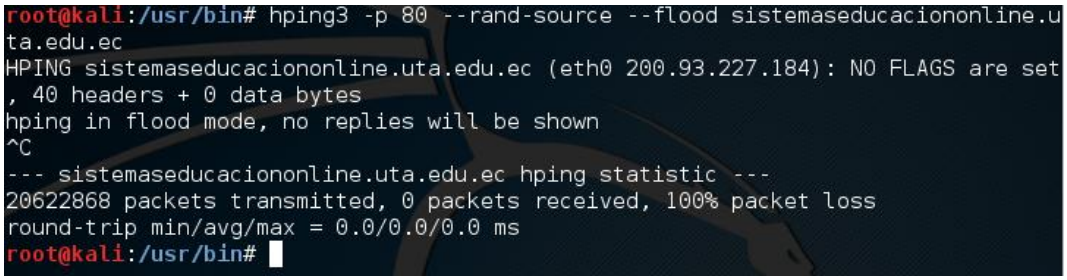


Gráfico 49 Ataque DoS con hping3

Con este tipo de ataque se pretende agotar el ancho de banda de la víctima. Se enviaron de forma continuada un número elevado de paquetes ICMP (Internet Control Message Protocol) Echo Request (Ping) de tamaño considerable, como se puede observar en el gráfico se enviaron 20622868 paquetes sin ningún éxito debido a esto nuestra intención de ICMP Flood no fue exitosa denotando una buena configuración contra este tipo de ataques por parte del DITIC.

- Detección de IPS atacantes

Después de un fallo de seguridad es necesario conocer varios aspectos del ataque, en este caso es la manera en que son manejados los accesos hacia la plataforma virtual.
Dentro de Moodle existe un rastreo de cambios realizados, informando a los usuarios desde dónde se han realizado cambios y conexiones en su perfil.

Gráfico 50 Rastreo de IPS Atacantes

Gráfico 51 IP rastreada con explorador TOR

4.6.Buenas prácticas de Seguridad.

Después de identificar las amenazas existentes de acuerdo con [13], se propone el siguiente conjunto de buenas prácticas de seguridad informáticas a partir de estándares y normas cuales se generan a partir de las vulnerabilidades identificadas actualmente en la plataforma virtual de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Al finalizar con el análisis de vulnerabilidades y valorar el riesgo que representa, es necesario presentar posibles soluciones que pueden ser incorporadas por el DEaDV para poder mitigar los riesgos de las vulnerabilidades encontradas.

Para el presente estudio se acoge a la metodología Magerit la cual presenta los pasos a seguir para la gestión de riesgos partiendo de un análisis de vulnerabilidades.

El primer paso de la gestión de riesgos de la metodología Magerit es la determinación de las salvaguardas, las cuales son pasos que seguir para mitigar los riesgos, explorando distintos enfoques de la entidad.

Identificación de las salvaguardas

Según lo analizado anteriormente las actividades más utilizadas en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial son:

- Tareas
- Cuestionarios
- Foros

Para salvaguardar todas estas actividades que se identificaron, hay que tomar en cuenta las siguientes recomendaciones que [13] y [28] plantean definiendo que la información que se manejan en estas actividades son de vital importancia para los cursos virtuales en los que se encuentran dichas actividades.

Medidas de seguridad simples

- Verificar las estrategias de respaldos de seguridad y capacitar al personal a cargo de los mismos, cuáles son los procedimientos de restauración que se deben tomar cuando la plataforma se encuentre amenazada.
- Cargar solamente el software o servicios que se va a utilizar dentro de la plataforma virtual, sin habilitar complementos que ralenticen el buen funcionamiento de la misma.
- Actualizar la plataforma virtual con regularidad, aplicando parches de seguridad.
- Diseñar diferentes capas de seguridad, exterior, intermedia e interior como mínimo.

Recomendaciones básicas

- Actualice Moodle regularmente en cada lanzamiento/versión.
- Los agujeros de seguridad publicados atraen la atención de los crakers después del lanzamiento. Cuanto más antigua sea la versión, tanto más probable es que tenga vulnerabilidades.
- Desactive Register globals (Registros globales). Esto ayudará a prevenir contra posibles problemas XSS en scripts de terceros.
- Use Contraseñas complejas seguras para el administrador y los profesores. Elegir contraseñas "difíciles" es una práctica de seguridad básica para proteger contra el cracking por "fuerza bruta" de las cuentas.
- Proporcione cuentas de profesor únicamente a usuarios dignos de confianza. Evite crear cajas de arena (sandboxes) públicas con cuentas gratuitas de profesor en servidores de producción.
- Las cuentas de profesor tienen permisos mucho más libres y es más fácil crear situaciones donde sea posible abusar de los datos o robarlos.
- Separe sus sistemas todo lo que le sea posible
- Otra técnica básica de seguridad es usar diferentes contraseñas en diferentes sistemas, usar diversas máquinas para diversos servicios, etc. Esto impedirá que el daño se extienda, incluso si una cuenta o un servidor son atacados.
- Protecciones Generales (Mecanismos de cierre, DOS, logs del sistema).

Las protecciones generales se basan en los controles de acceso, manejo de peticiones y la información que es guardada a partir de las distintas conexiones.

En primer lugar, la implementación de un mecanismo de cierre automático a partir de una equivocación del usuario en sus credenciales de acceso es necesaria para poder evitar ataques de fuerza bruta. Teniendo en cuenta que es una plataforma educativa virtual es importante tener en consideración la cantidad de veces que un usuario puede errar en su acceso, se sugiere realizarlo de la siguiente manera:

- Al quinto intento fallido bloquear el ingreso durante 5 minutos
- Después de ello dar tres intentos más, después de ello bloquear el acceso al usuario para que solicite a la administración de la Facultad que renueve su acceso.

A partir de ello y mediante el análisis realizado dando como resultado problemas con los ataques DOS se buscan métodos con los cuales se pueda mitigar el impacto del mismo.

Moodle permite distribuir la carga de acceso hacia el servidor, la cual mitiga en gran medida un ataque DOS así:

- Ingeniería en Sistemas puede encargarse de las solicitudes enviadas por las Facultades de las Ingenierías de la Universidad y del Departamento de Idiomas o la Dirección de Educación a Distancia y Virtual puede manejar las Facultades Administrativas, Contabilidad, Diseño y Ciencias Humanas, así como el manejo de los procesos de capacitaciones ofrecidos por la Universidad.

- El Departamento de Tecnologías de la Información y Comunicación puede manejar Ciencias de la Salud y las Facultades ubicadas en el Campus Querochaca.

De esta manera pueden ser mitigados los ataques DOS en dependencia de donde lleguen y siendo un ataque externo ésta carga es dividida por lo cual el impacto se vería disminuido en este tipo de ataques.

Finalmente, al manejo de un análisis forense al finalizar un ataque se debe realizar con un análisis a los logs que son guardados en los servidores para determinar posibles culpables y poder, mediante ello, tomar medidas preventivas para ataques futuros.

Los expertos en seguridad recomiendan un cortafuego (firewall) dual. Existen diferentes combinaciones hardware/software. El desactivar servicios no usados es a menudo tan efectivo como un cortafuego. Use netstat -a para revisar puertos de red abiertos. No es una garantía de protección Permita los puertos 80, 443(ssl), y 9111 (para el chat), Admin remoto: ssh 22, o rpd 3389

• Protecciones de las aplicaciones

Siguiendo con el aseguramiento de la información de las sesiones y todo lo que conlleva asegurar que la información que se sube hacia el Moodle se deben proteger las aplicaciones y mucho más con algo tan delicado como las plataformas de educación virtual.

En este caso es específicamente la protección a Moodle, tomando en cuenta la vulnerabilidad encontrada en el manejo y configuración de Cookies que

son necesarias para mantener la sesión a través del parámetro MoodleSession el cual en la presente investigación fue la principal vulnerabilidad encontrada con un riesgo alto en donde los datos sensibles de los usuarios están expuestos.

Existen diferentes maneras de disminuir el impacto del robo de sesiones a través de Cookies, uno de ellos es utilizando el transporte de seguridad estricto, específicamente en el parámetro max-age, el cual es la cantidad de milisegundos que tiene de vida una cookie antes de ser reemplazada por otra, por lo que a un atacante no le serviría para mantener una sesión permanente de existir este parámetro el cual debe ser añadido en el código PHP.

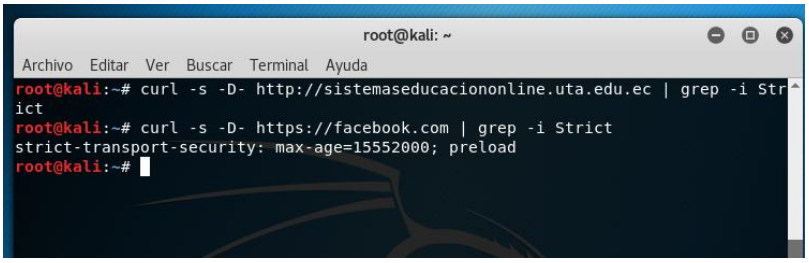


Gráfico 52 Uso del comando curl para obtener parte del código de una página web, filtrado por parámetro Strict-Transport-Security

En el gráfico 52 se observa la ejecución del comando CURL para comparar la configuración del parámetro max-age entre la página del portal de educación virtual y Facebook. Es una manera de entorpecer el ataque provocado por un sniffer, no es forma de solucionarlo completamente ya que el sniffer de igual manera seguirá tomando la nueva cookie generada por lo que el atacante tiene la capacidad de renovar la cookie y volver a iniciar sesión. Para garantizar una correcta validación de datos asegurando que no puedan ser leídos es necesario la implementación de protecciones en las comunicaciones.

- Protección de las comunicaciones

El protocolo HTTPS es una transferencia de protocolo de hipertexto seguro, por sus siglas en inglés, es basado en HTTP y utiliza protocolos criptográficos SSL los cuales garantizan la comunicación segura entre emisor y receptor, teniendo en cuenta que la información puede estar siendo monitoreada por un tercero (ataque man in the middle), pero no puede leer la información que obtiene ya que se encuentra cifrada.

En el análisis realizado hacia el entorno virtual educativo perteneciente a la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, y manejado por la DEaDV no se encontró el presente protocolo y la información es enviada en texto plano, por lo la sesión fue robada de una manera relativamente sencilla.

Es necesario la implementación de protocolos de cifrado SSL para poder evitar estas vulnerabilidades, los protocolos SSL son obtenidos a partir de un certificado de seguridad como lo usa la página web de la Universidad.

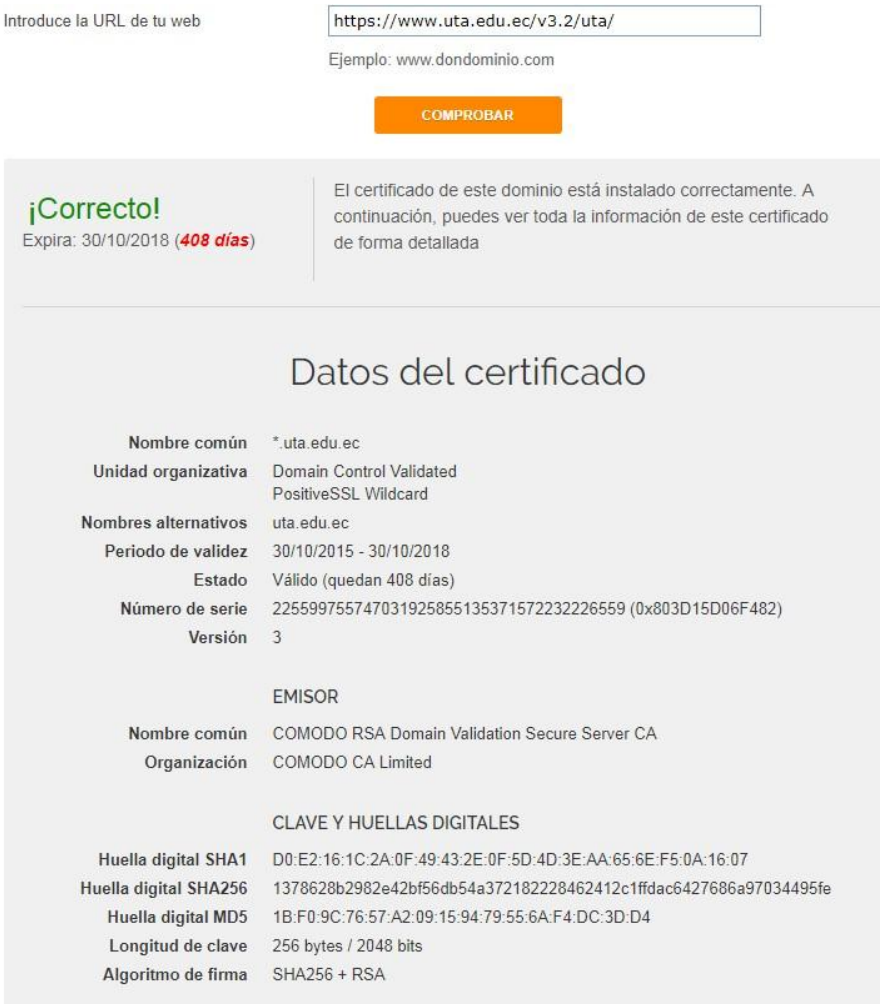


Gráfico 53 Análisis de certificado SSL de la página web de la universidad (1)

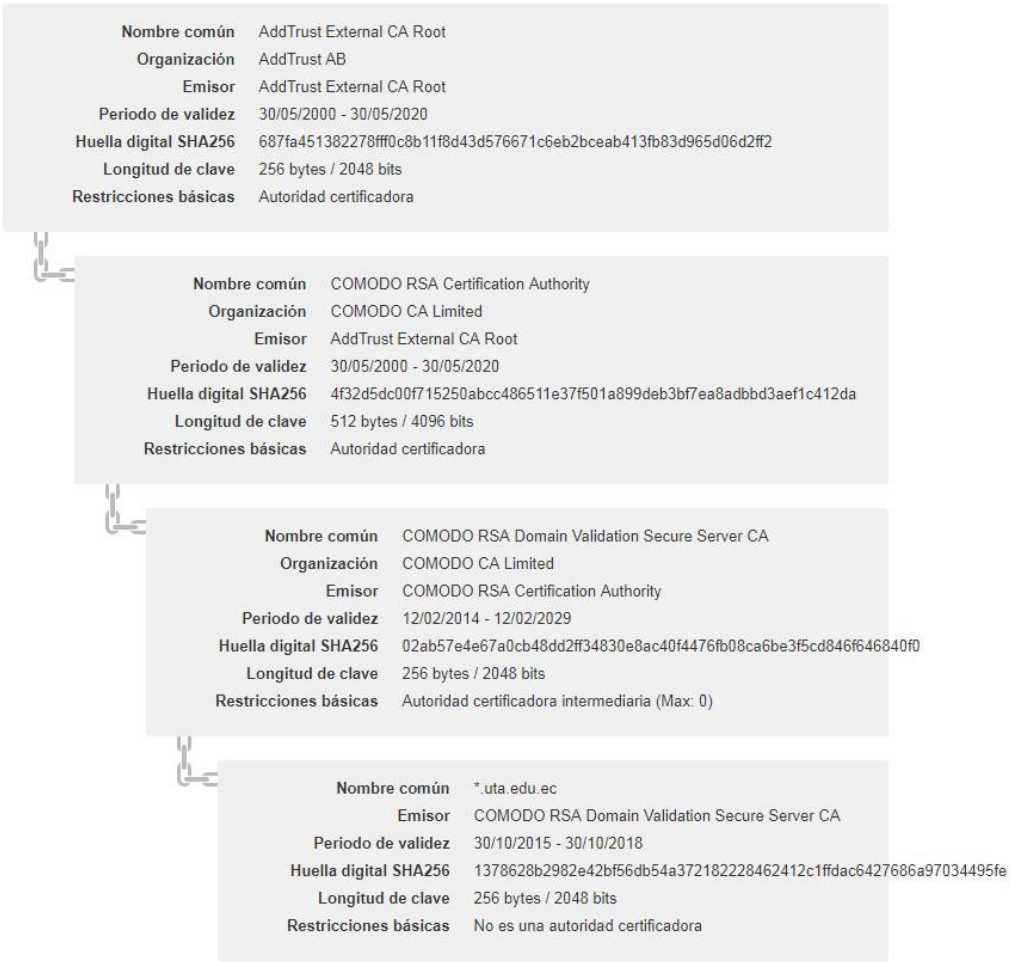


Gráfico 54 Análisis de certificado SSL de la página web de la universidad (2)

Como muestran los gráficos 53 y 54 el certificado de la página de la Universidad Técnica de Ambato www.uta.edu.ec posee un certificado cuya validez expira en el año 2018 contando aún con 406 días de validez y asegurando una conexión por HTTPS, lo cual Magerit nos recomienda utilizar así asegurando todo tipo de conexiones y de esta manera asegurando la transmisión de la información que puede llegar a ser sensible para la Facultad y Universidad.

Siendo esta la debilidad que pudiendo ser explotada con ataques de mayor envergadura, se convierte en la puerta más vulnerable dentro de la plataforma virtual.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Las actividades más comunes dentro de la Facultad de Ingeniería en Sistemas Computacionales e Informáticos son tareas en un 50%, cuestionarios en un 37% y foros en un 13% asimismo los archivos con un 66%, los enlaces con un 30% y carpetas con un 4% son los recursos más utilizados.
- La Dirección de Educación a Distancia y Virtual ha realizado cambios en sus medidas de seguridad a partir de tesis anteriores, pero aún posee ciertas falencias en su aplicación.
- No existe un mecanismo de cierre automático al ingresar credenciales incorrectas, lo que puede provocar riesgos en ataques de fuerza bruta.
- La protección a las Cookies de sesión de un usuario es ineficaz lo que provoca un alto riesgo de robo de sesiones.
- Hay riesgo de provocar la caída de los servidores mediante ataques DOS debido a que la carga de las peticiones no está distribuida.
- No se encontraron protocolos de encriptación SSL principalmente el protocolo HTTPS en el login de la página, provocando un grave riesgo ante un ataque de hombre en el medio el cual puede robar la sesión del usuario.
- Magerit V3 permite identificar vulnerabilidades y amenazas que pueden afectar a cualquier fuente de información.
- Con la aplicación de normas y estándares de seguridad de información todo tipo de amenaza puede ser mitigada.

5.1.1. Recomendaciones

- Se recomienda la realización periódica de evaluaciones de seguridad, principalmente ataques en contra de la plataforma para medir su respuesta y mitigar riesgos.
- Se sugiere que se adquiera un certificado SSL para el manejo de todas las páginas web administradas por la DEaDV.
- La DEaDV podría considerar la posibilidad de repartir el manejo de sus entornos virtuales para mitigar los ataques DOS y evitar un alto impacto en los servidores.
- Se sugiere manejar la metodología Magerit para el análisis de riesgos y la metodología de Hacking Ético para la investigación de vulnerabilidades.
- Asimismo, se sugiere el análisis de técnicas de aseguramiento de la información y la calidad de la misma.

Bibliografía

[1] Ekos, «Especial educación superior Ecuador excelencia académica,» *Ekos,* nº 253, p. 124, 2015.

[2] J. Lasheras, «Marco de trabajo de representación y reuso de requisitos de seguridad,» Universidad de Murcia. , España., 2012.

[3] V. Gámiz, «Entornos Virtuales para la formación práctica de estudiantes de educación: implementación, experimentación y evaluación de la plataforma aulaweb,» Universidad de Granada., España., 2009.

[4] E. M. Torres Núñez, «Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato,» UTA, Ambato, 2015.

[5] J. Areitio, Seguridad de la Información, Madrid: Paraninfo, 2008.

[6] W. Stallings, Fundamentos de Seguridad en Redes Aplicaciones y Estándares, Madrid: Pearson Educación, 2004.

[7] H. Condori, «Un modelo de evaluación de factores criticos de éxito en la implementación de la seguridad,» *Revista de Investigación de Sistemas e Informática,* pp. 9-22, 2012.

[8] M. Muñoz y L. Rivas, «Estado actual de equipos de respuesta a incidentes de seguridad informática,» *Risti,* pp. 1 - 15, 2015.

[9] G. Pallas, «Metodología de Implantación de un SGSI en un grupo empresaroal jerárquico.,» Instituto de Computación. Facultad de Ingenieria Universidad de la República, Montevideo, 2009.

[10] J. Cano, Inseguridad de la Información, Colombia: Alfaomega, 2013.

[11] B. Ramos Alvarez y A. Ribagorda Garnacho, Avances en Criptología y Seguridad de la Información., España: Díaz de Santos S. A., 2004.

[12] P. Aguilera, Seguridad Informática, Editex, 2010.

[13] Ministerio de Hacienda y Administraciones Públicas, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de

Información., España: Ministerio de Hacienda y Administraciones Públicas, 2012.

[14] G. Escrivá Gascó, R. Romero Serrano, D. Ramada y R. Onrubia , Seguridad Informática, Madrid: Heinemann, 2013.

[15] J. Costas, Seguridad Informática, Bogota: Rama, 2011.

[16] J. García, Y. Fernández, R. Martínez, A. Ochoa y A. Ramos, Hacking y seguridad en internet, Bogotá: Rama, 2013.

[17] J. L. Ramos Ramos, «Pruebas de Penetración o Pent Test,» *Revista de Información, Tecnología y Sociedad*, vol. 1, nº 8, pp. 31-33, 2013.

[18] Á. Carrasco Núñez, «Conceptos de seguridad informática y su reflejo en la Cámara de Cuentas de Andalucía,» *Auditoría Pública*, nº 61, pp. 111 - 117, 2013.

[19] A. Cervigón y M. Alegre, Seguridad Informática, Madrid: Paraninfo, 2011.

[20] F. Portantier, Seguridad Informática, Redusers, 2012.

[21] A. Dionicio, Intervención pedagógica con b-learning., Ayacucho Argentina.: Editorial Dunken., 2014.

[22] M. Rubio y C. Galván, «Portafolios digitales para el desarrollo de competencias transversales,» *Digital Education*, pp. 53 - 69, 2013.

[23] J. Romero, T. Martínez y J. Trujillo, «Posibilidades didácticas de las herramientas moodle para producción de cursos y materiales eductivos,» *Digital Education*, pp. 59 - 76, 2015.

[24] G. Bautista Pérez, F. Borges Sáiz y A. Forés i Miravalles, Didactica Universitaria de Entornos Virtuales de Enseñanza-Aprendizaje, Madrid: Narcea S.A. de Ediciones, 2006.

[25] C. Coll y C. Monereo, Psicología de la educación virtual, Madrid: Ediciones Morata, 2008.

[26] P. Humanante, F. García y M. Conde, «Entornos Personales de Aprendizaje y Aulas Virtuales: una Experiencia con Estudiantes Universitarios,» *VAEP-RITA*, vol. 1, nº 4, pp. 2011 - 2017, 2013.

[27] G. Ortegón Cortázar, «Optimización de sistemas de gestión académica. Una propuesta de gestión, medición y procesamiento de datos en un entorno virtual de aprendizaje para la toma de decisiones en instituciones educativas,» *Rev. esc.adm.neg.*, vol. 1, nº 79, pp. 80 - 97, 2015.

[28] «Moodle,» [En línea]. Available: https://docs.moodle.org. [Último acceso: 14 Septiembre 2017].

[29] Ministerio de Hacienda y Administraciones Públicas, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información., Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[30] J. M. K. G. B. Hernán Santiso, «Seguridad en Entornos de Educación Virtual,» vol. 1, nº 1, p. 22, 2016.

[31] P. Hudson, «hacking With PHP,» 2015. [En línea]. Available: http://www.hackingwithphp.com/7/3/1/get-and-post. [Último acceso: 17 09 2017].

[32] G. d. P. OWASP, «Open Web Application Security Project Foundation,» 2015.

Anexos y Apéndices

Anexo A

Análisis de las Actividades Virtuales de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial

Carrera de Ingeniería en Sistemas Computacionales e Informáticos:

PRIMER SEMESTRE	
CURSO	**ACTIVIDADES**
NTICS I	✓ Tareas ✓ Archivos ✓ Cuestionarios
Álgebra I	✓ Foros ✓ Archivos ✓ Tareas ✓ Enlaces
Lógica Matemática	✓ Archivos
Lenguaje y Comunicación	✓ Foros ✓ Archivos ✓ Tareas
Geometría Plana y Trigonometría	✓ Archivos
Física I	✓ Archivos ✓ Cuestionarios ✓ Tareas
Programación I	✓ Carpetas ✓ Tareas ✓ Enlaces ✓ Archivos ✓ Cuestionarios ✓ Talleres
Técnicas de Estudio	✓ Archivos ✓ Tareas ✓ Cuestionarios

SEGUNDO SEMESTRE	
CURSO	**ACTIVIDADES**
Cálculo I	✓ Archivos ✓ Cuestionarios
Geometría Analítica	✓ Archivos
Álgebra Lineal	✓ Archivos ✓ Tareas ✓ Cuestionarios
Física II	✓ Archivos ✓ Tareas ✓ Cuestionarios
Programación II	✓ Carpetas ✓ Tareas ✓ Enlaces ✓ Archivos ✓ Cuestionarios ✓ Talleres
NTICS II	✓ Archivos ✓ Enlaces ✓ Páginas ✓ Glosarios ✓ Cuestionarios ✓ Tareas
Metodología de la Investigación	✓ Foros ✓ Archivos ✓ Cuestionarios ✓ Tareas

TERCER SEMESTRE	
CURSO	**ACTIVIDADES**
Arquitectura de Computadores	✓ Archivos ✓ Tareas ✓ Enlaces ✓ Cuestionarios
Medidas Eléctricas	✓ Foros ✓ Archivos ✓ Tareas
Estadística y Probabilidad	✓ Archivos ✓ Tareas ✓ Cuestionarios
Estructura de Datos	✓ Archivos ✓ Tareas ✓ Enlaces ✓ Cuestionarios
Sistemas Operativos	✓ Tareas ✓ Enlaces ✓ Archivos ✓ Cuestionarios
Cálculo II	✓ Archivos ✓ Páginas ✓ Cuestionarios

CUARTO SEMESTRE	
Computación Visual	✓ Archivos ✓ Tareas ✓ Enlaces ✓ Cuestionarios
Redes de Computadores	✓ Enlaces ✓ Archivos ✓ Tareas
Diseño de Interfaces	✓ Archivos ✓ Chat ✓ Video Conferencias ✓ Enlaces ✓ Tareas ✓ Cuestionarios
Base de Datos I	✓ Foros ✓ Enlaces ✓ Archivos ✓ Tareas ✓ Páginas
Métodos Numéricos	✓ Archivos ✓ Enlaces ✓ Cuestionarios ✓ Tareas
Investigación Operativa	✓ Enlaces ✓ Archivos ✓ Cuestionarios ✓ Tareas

QUINTO SEMESTRE	
Optativa I (Tratamiento de Imágenes)	✓ Archivos ✓ Tareas ✓ Cuestionarios
Interredes LAN WAN	✓ Archivos ✓ Páginas ✓ Tareas ✓ Cuestionario
Desarrollo de Software I	✓ Archivos ✓ Páginas ✓ Enlaces ✓ Wikis ✓ Talleres ✓ Cuestionarios
Base de Datos II	✓ Enlaces ✓ Archivos ✓ Tareas ✓ Páginas
Modelos y Simulación	✓ Foros ✓ Archivos ✓ Enlaces ✓ Cuestionarios ✓ Tareas
Ingeniería de Software I	✓ Archivos ✓ Tareas

SEXTO SEMESTRE	
Optativa II (Robótica)	✓ Foros ✓ Archivos
Sistemas Distribuidos	✓ Foros ✓ Archivos ✓ Tareas ✓ Cuestionarios ✓ Enlaces
Desarrollo de Software II	✓ Archivos ✓ Tareas ✓ Enlaces
Realidad Nacional	✓ Foros ✓ Archivos ✓ Carpetas ✓ Tareas ✓ Cuestionarios ✓ Enlaces
Inteligencia Artificial	✓ Foros ✓ Enlaces ✓ Archivos ✓ Páginas ✓ Tareas
Base de Datos Distribuidas	✓ Foros ✓ Archivos ✓ Tareas
Sistemas de Información	✓ Archivos ✓ Tareas ✓ Páginas ✓ Cuestionarios

SÉPTIMO SEMESTRE	
Desarrollo de Software III	✓ Archivos ✓ Tareas ✓ Cuestionarios
Ingeniería de Software II	✓ Archivos ✓ Tareas ✓ Cuestionarios ✓ Enlaces
Gestión de Proyecto Socio productivos	✓ Foros ✓ Archivos ✓ Tareas ✓ Cuestionarios ✓ Enlaces
Emprendimiento	✓ Archivos ✓ Tareas ✓ Cuestionarios ✓ Enlaces
Gestión de Calidad	✓ Foros ✓ Enlaces ✓ Archivos ✓ Páginas ✓ Tareas ✓ Talleres
Inteligencia Artificial II	✓ Foros ✓ Archivos ✓ Tareas ✓ Enlaces
Sistemas de Información	✓ Archivos ✓ Tareas ✓ Páginas ✓ Cuestionarios
Diseño de Redes	✓ Archivos ✓ Carpetas ✓ Tareas ✓ Cuestionarios

OCTAVO SEMESTRE	
Optativa III (Teoría de Juegos)	✓ Archivos ✓ Tareas ✓ Cuestionarios
Administración de Base de Datos	✓ Archivos ✓ Tareas ✓ Enlaces
Planificación Informática	✓ Archivos ✓ Tareas ✓ Cuestionarios
Gerencia Administrativa	✓ Archivos ✓ Tareas ✓ Enlaces
Intranets Extranet	✓ Páginas ✓ Enlaces ✓ Archivos ✓ Tareas
Sistema de Soporte de Decisiones	✓ Archivos ✓ Tareas
Sistemas de Información	✓ Archivos ✓ Tareas ✓ Páginas ✓ Cuestionarios
Diseño de Redes	✓ Archivos ✓ Carpetas ✓ Tareas ✓ Cuestionarios

NOVENO SEMESTRE	
Diseño de Investigación	✓ Archivos ✓ Tareas ✓ Cuestionarios
Gerencia Informática	✓ Archivos ✓ Tareas ✓ Cuestionarios
Finanzas Legislación y Tributación	✓ Archivos ✓ Tareas
Administración de Sistemas Operativos y Redes	✓ Archivos ✓ Páginas ✓ Tareas ✓ Enlaces
Seguridad Informática	✓ Enlaces ✓ Archivos ✓ Tareas ✓ Cuestionarios
Solución de Negocios	✓ Archivos ✓ Tareas
Auditoría y Evaluación de Sistemas	✓ Archivos ✓ Tareas ✓ Cuestionarios ✓ Enlaces
Diseño de Redes	✓ Archivos ✓ Carpetas ✓ Tareas ✓ Cuestionarios

Carrera de Ingeniería Electrónica y Telecomunicaciones:

PRIMER SEMESTRE	
CURSO	**ACTIVIDADES**
NTICS I	✓ Foros ✓ Tareas ✓ Archivos ✓ Cuestionarios ✓ Enlaces ✓ Glosarios ✓ Páginas ✓ Videos ✓ Carpetas
Álgebra I	✓ Archivos ✓ Tareas ✓ Cuestionarios
Lógica Matemática	✓ Archivos ✓ Tareas
Lenguaje y Comunicación	✓ Foros ✓ Carpetas ✓ Enlaces ✓ Archivos ✓ Tareas ✓ Cuestionarios
Geometría Plana y Trigonometría	✓ Páginas ✓ Enlaces ✓ Archivos ✓ Tareas
Física I	✓ Archivos ✓ Enlaces ✓ Cuestionarios ✓ Tareas
Programación I	✓ Tareas ✓ Archivos ✓ Cuestionarios
Técnicas de Estudio	✓ Foros ✓ Carpetas ✓ Enlaces ✓ Archivos ✓ Tareas ✓ Cuestionarios

SEGUNDO SEMESTRE	
CURSO	**ACTIVIDADES**
Cálculo I	✓ Foros ✓ Archivos ✓ Tareas
Geometría Analítica	✓ Archivos
Álgebra Lineal	✓ Carpetas ✓ Consultas ✓ Enlaces ✓ Archivos ✓ Tareas ✓ Cuestionarios
Física II	✓ Archivos ✓ Foros ✓ Enlaces ✓ Cuestionarios ✓ Tareas
Programación II	✓ Tareas ✓ Archivos
NTICS II	✓ Tareas ✓ Enlaces ✓ Archivos ✓ Cuestionarios
Metodología de la Investigación	✓ Foros ✓ Archivos ✓ Carpetas ✓ Enlaces ✓ Tareas ✓ Cuestionarios

TERCER SEMESTRE	
CURSO	**ACTIVIDADES**
Redes de Computadores	✓ Archivos ✓ Tareas ✓ Enlaces
Medidas Eléctricas	✓ Carpetas ✓ Páginas ✓ Enlaces ✓ Talleres ✓ Archivos ✓ Tareas
Circuitos Eléctricos I	✓ Foros ✓ Archivos ✓ Tareas ✓ Enlaces
Estadística y Probabilidad	✓ Archivos ✓ Tareas
Programación III	✓ Tareas ✓ Talleres ✓ Archivos
Cálculo II	✓ Archivos ✓ Páginas ✓ Cuestionarios

CUARTO SEMESTRE	
CURSO	**ACTIVIDADES**
Interredes	✓ Enlaces ✓ Archivos ✓ Tareas
Electrónica Digital I	✓ Foros ✓ Archivos
Física de Semiconductores	✓ Archivos ✓ Páginas ✓ Enlaces ✓ Tareas ✓ Cuestionarios ✓ Talleres
Circuitos Electrónicos I	✓ Archivos ✓ Tareas
Circuitos Eléctricos II	✓ Archivos
Métodos Numéricos	✓ Foros ✓ Archivos ✓ Tareas
Cálculo Vectorial	✓ Foros ✓ Tareas ✓ Páginas ✓ Enlaces ✓ Cuestionarios ✓ Talleres

QUINTO SEMESTRE	
CURSO	**ACTIVIDADES**
Señales y Sistemas	✓ Archivos ✓ Tareas
Circuitos Electrónicos II	✓ Archivos ✓ Tareas
Electrónica Digital II	✓ Foros ✓ Archivos ✓ Enlaces ✓ Tareas ✓ Carpetas
Gestión de Calidad	✓ Archivos ✓ Enlaces ✓ Tareas ✓ Cuestionarios

Gestión de Redes	✓ Foros ✓ Archivos ✓ Páginas ✓ Enlaces ✓ Tareas ✓ Cuestionarios ✓ Glosarios
Máquinas Eléctricas	✓ Archivos ✓ Enlaces ✓ Carpetas
Teoría Electromagnética I	✓ Foros ✓ Archivos ✓ Enlaces

SEXTO SEMESTRE	
CURSO	**ACTIVIDADES**
Interfaz de PC	✓ Foros ✓ Archivos ✓ Tareas
Sistemas de Control	✓ Archivos ✓ Carpetas
Comunicación Analógica	✓ Foros ✓ Páginas ✓ Archivos ✓ Chat ✓ Videollamada ✓ Enlaces ✓ Tareas ✓ Glosarios ✓ Encuestas ✓ Cuestionarios
Microprocesadores	✓ Archivos ✓ Enlaces ✓ Tareas ✓ Cuestionarios
Instrumentación y Control de Procesos	✓ Foros ✓ Archivos ✓ Enlaces ✓ Cuestionarios ✓ Glosarios
Electrónica de Potencia	✓ Enlaces ✓ Cuestionarios ✓ Glosarios

Realidad Nacional	✓ Enlaces ✓ Archivos ✓ Foros ✓ Tareas ✓ Cuestionarios
Teoría Electromagnética II	✓ Archivos ✓ Enlaces

SÉPTIMO SEMESTRE	
CURSO	**ACTIVIDADES**
Comunicación Digital	✓ Foros ✓ Archivos ✓ Carpetas
Control Industrial y PLCS	✓ Enlaces ✓ Archivos ✓ Cuestionarios ✓ Glosarios ✓ Tareas
Redes de Comunicación	✓ Foros ✓ Páginas ✓ Archivos ✓ Chat ✓ Videoconferencia ✓ Enlaces ✓ Tareas ✓ Glosario ✓ Cuestionarios ✓ Encuestas
Optativa I (Planta Externa)	✓ Foros ✓ Archivos ✓ Cuestionarios ✓ Tareas
Emprendimiento	✓ Archivos ✓ Cuestionarios ✓ Tareas ✓ Enlaces
DSPS	✓ Foros ✓ Archivos ✓ Páginas ✓ Chat ✓ Enlaces ✓ Cuestionarios ✓ Tareas

Propagación	✓ Foros ✓ Archivos ✓ Carpetas ✓ Enlaces
Microcontroladores	✓ Enlaces ✓ Cuestionarios ✓ Glosarios

OCTAVO SEMESTRE	
CURSO	**ACTIVIDADES**
Optativa II (Microondas)	✓ Foros ✓ Archivos
Comunicación Óptica	✓ Foros ✓ Archivos ✓ Tareas
Comunicaciones Inalámbricas	✓ Foros ✓ Páginas ✓ Archivos ✓ Chat ✓ Videollamada ✓ Enlaces ✓ Glosarios ✓ Encuestas ✓ Cuestionarios
VLSI	✓ Enlaces ✓ Cuestionarios ✓ Glosarios ✓ Tareas
Antenas y Líneas de Transmisión	✓ Foros ✓ Archivos ✓ Chats ✓ Videollamada ✓ Enlaces ✓ Tareas ✓ Cuestionarios ✓ Encuestas
Comunicación Satelital	✓ Foros ✓ Páginas ✓ Archivos ✓ Chat ✓ Videollamada ✓ Enlaces ✓ Glosarios ✓ Encuestas Cuestionarios

Gestión de Proyectos Socio productivos	✓ Foros ✓ Archivos ✓ Tareas ✓ Cuestionarios ✓ Enlaces

NOVENO SEMESTRE	
CURSO	**ACTIVIDADES**
Optativa III (Redes Industriales)	✓ Foros ✓ Archivos ✓ Tareas ✓ Enlaces
Proyectos de Investigación	✓ Foros ✓ Archivos ✓ Tareas
Codificación de Señales	✓ Foros ✓ Archivos ✓ Páginas ✓ Chats ✓ Enlaces ✓ Tareas ✓ Glosarios ✓ Cuestionarios
Comunicaciones Avanzadas	✓ Foros ✓ Páginas ✓ Enlaces ✓ Wikis ✓ Tareas ✓ Cuestionarios ✓ Encuestas ✓ Archivos
Redes Banda Ancha	✓ Foros ✓ Páginas ✓ Archivos ✓ Chat ✓ Enlaces ✓ Glosarios ✓ Talleres
Proyectos de Telecomunicaciones	✓ Foros ✓ Archivos ✓ Tareas ✓ Cuestionarios ✓ Enlaces
Comunicaciones Móviles	✓ Páginas ✓ Archivos ✓ Tareas ✓ Cuestionarios

Carrera de Ingeniería Industrial en Procesos de Automatización

PRIMER SEMESTRE	
CURSO	**ACTIVIDADES**
Geometría y Trigonometría	✓ Foros ✓ Archivos ✓ Glosarios ✓ Cuestionarios ✓ Tareas ✓ Páginas
Álgebra I	✓ Foros ✓ Archivos ✓ Tareas ✓ Enlaces
Física I	✓ Foros ✓ Archivos ✓ Enlaces ✓ Cuestionarios
Lenguaje y Comunicación	✓ Foros ✓ Archivos ✓ Tareas
Lógica Matemática	✓ Archivos
Técnicas de Estudio	✓ Archivos ✓ Tareas

SEGUNDO SEMESTRE	
CURSO	**ACTIVIDADES**
Álgebra Lineal	✓ Archivos ✓ Tareas
NTICS II	✓ Foros ✓ Archivos ✓ Glosarios ✓ Páginas ✓ Tareas ✓ Cuestionarios
Geometría Analítica	✓ Archivos
Metodología de la Investigación	✓ Foros ✓ Archivos ✓ Tareas ✓ Cuestionarios ✓ Enlaces
Física II	✓ Archivos ✓ Tareas

TERCER SEMESTRE	
CURSO	**ACTIVIDADES**
Estadística y Probabilidad	✓ Archivos ✓ Tareas ✓ Enlaces
Base de Datos	✓ Archivos ✓ Carpetas ✓ Tareas ✓ Cuestionarios
Circuitos Eléctricos	✓ Archivos ✓ Tareas ✓ Enlaces
Metrología	✓ Foros ✓ Archivos ✓ Tareas
Tecnología de los Materiales	✓ Archivos ✓ Tareas
Dibujo Industrial	✓ Archivos
Cálculo II	✓ Archivos ✓ Páginas ✓ Cuestionarios ✓ Tareas

CUARTO SEMESTRE	
CURSO	**ACTIVIDADES**
Métodos Numéricos	✓ Archivos ✓ Enlaces ✓ Carpetas ✓ Tareas
Electrónica Industrial Básica	✓ Archivos
Estática	✓ Archivos
Máquinas eléctricas	✓ Archivos ✓ Enlaces ✓ Cuestionarios ✓ Tareas
Investigación Operativa	✓ Archivos
Seguridad y Mantenimiento Industrial	✓ Archivos ✓ Tareas
CAD	✓ Archivos ✓ Chats ✓ Video llamadas ✓ Enlaces ✓ Hot Pots ✓ cuestionarios

QUINTO SEMESTRE	
CURSO	**ACTIVIDADES**
Electrónica Digital	✓ Archivos ✓ Tareas ✓ Cuestionarios
Sistemas de Control	✓ Archivos ✓ Carpetas ✓ Tareas
Electrónica de Potencia	✓ Archivos ✓ Tareas ✓ Cuestionarios
Taller Industrial	✓ Archivos ✓ Foros ✓ Tareas
CAD/CAM	✓ Foros ✓ Carpetas ✓ Archivos ✓ Cuestionarios ✓ Tareas
Dinámica de Partícula	✓ Archivos
Resistencia de Materiales	✓ Archivos

SEXTO SEMESTRE	
CURSO	**ACTIVIDADES**
Realidad Nacional	✓ Foros ✓ Archivos ✓ Enlaces ✓ Tareas ✓ Cuestionarios
Ingeniería de Métodos	✓ Foros ✓ Archivos ✓ Carpetas ✓ Enlaces ✓ Tareas ✓ Cuestionarios
Mecánica de Fluidos	✓ Archivos
Diseño de Elementos I	✓ Archivos
Ingeniería Financiera	✓ Archivos ✓ Tareas
Máquinas CNC	✓ Archivos ✓ Enlaces ✓ Tareas
Instrumentación Industrial	✓ Archivos ✓ Carpetas ✓ Páginas ✓ Tareas

Optativa I Seguridad Industrial e Higiene Ocupacional	✓ Foros ✓ Archivos ✓ Carpetas ✓ Enlaces ✓ Páginas ✓ Tareas ✓ Cuestionarios

SÉPTIMO SEMESTRE	
CURSO	**ACTIVIDADES**
Emprendimiento	✓ Foros ✓ Archivos ✓ Enlaces ✓ Tareas ✓ Cuestionarios
Diseño de Elementos II	✓ Archivos ✓ Enlaces ✓ Tareas
Instrumentación Virtual	✓ Archivos ✓ Enlaces ✓ Tareas
PLCS	✓ Archivos ✓ Carpetas ✓ Cuestionarios ✓ Carpetas ✓ Tareas ✓ Enlaces
Administración de la Producción	✓ Foros ✓ Archivos ✓ Cuestionarios ✓ Tareas
Control Hidráulico y Neumático	✓ Foros ✓ Tareas ✓ Páginas ✓ Cuestionarios ✓ Archivos
OPTATIVA II Termodinámica	✓ Archivos ✓ Tareas ✓ Enlaces
Mecanismos	✓ Foros ✓ Archivos ✓ Carpetas ✓ Páginas ✓ Enlaces ✓ Tareas

OCTAVO SEMESTRE	
CURSO	**ACTIVIDADES**
Gestión de Proyectos Socio productivos	✓ Foros ✓ Archivos ✓ Enlaces ✓ Tareas ✓ Cuestionarios
Robótica Industrial	✓ Archivos ✓ Enlaces ✓ Tareas ✓ Cuestionarios
Gestión de Procesos	✓ Foros ✓ Páginas ✓ Archivos ✓ Chats ✓ Enlaces ✓ Tareas ✓ Cuestionarios
Control de Calidad	✓ Archivos ✓ Páginas ✓ Carpetas ✓ Enlaces ✓ Tareas ✓ Cuestionarios
Redes Industriales	✓ Archivos ✓ Tareas ✓ Enlaces ✓ Cuestionarios
Sistemas de Manufacturas	✓ Foros ✓ Páginas ✓ Enlaces ✓ Chats ✓ Tareas ✓ Cuestionarios ✓ Archivos
Ingeniería Económica Administrativa	✓ Archivos ✓ Tareas

NOVENO SEMESTRE	
CURSO	**ACTIVIDADES**
Mecatrónica	✓ Archivos ✓ Enlaces ✓ Tareas ✓ Cuestionarios
Diseño de Proyectos de Investigación	✓ Foros ✓ Archivos ✓ Enlaces ✓ Cuestionarios ✓ Tareas
Gerencia de Calidad y Producción	✓ Archivos
Gerencia de Servicios	✓ Archivos
Simulación de Sistemas de Manufactura	✓ Foros ✓ Archivos ✓ Tareas ✓ Cuestionarios
Planificación de Manufactura	✓ Archivos
Gerencia de Operaciones	✓ Foros ✓ Páginas ✓ Enlaces ✓ Chats ✓ Archivos ✓ Tareas ✓ Cuestionarios
Optativa III (Gestión Ambiental y Energías Alternativas)	✓ Archivos ✓ Tareas ✓ Enlaces