

GUÍA DEL COMPONENTE PRÁCTICO DEL CURSO SEGURIDAD INFORMATICA

ACTIVIDAD PRÁCTICA 2 – ESTANDARES Y NORMATIVIDAD

Autor:

MSc. Manuel Sierra Rodríguez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E
INGENIERÍA

PROGRAMA TECNOLOGIA EN DESARROLLO DE SOFTWARE

CURSO SEGURIDAD INFORMATICA 204039

JULIO DE 2016




ACTIVIDAD PRÁCTICA 2

INTRODUCCIÓN

De acuerdo con (Tarazona T., n.d.) la evolución de los sistemas de información y de la forma de hacer negocios, la información se ha convertido en uno de los activos de mayor valor para las personas y especialmente para las Organizaciones. “Los sistemas, redes y servicios de información afines, deben ser fiables seguros, dado que los participantes son cada vez más dependientes de estos”.

El crecimiento tecnológico y el auge en el uso de tecnologías informáticas y las comunicaciones ha venido en permanente evolución, pero al mismo tiempo se ha incrementado el delito informático, generando un gran impacto en la sociedad actual. La línea estudia la temática relacionada con la seguridad e inseguridad de las infraestructuras tecnológicas y de comportamientos de las mismas, buscando que se garantice la funcionalidad de las operaciones de manera segura, en disponibilidad de los servicios y recursos, la integridad de la información, la autenticidad y el no repudio de la información que es procesada y transmitida. Se plantea desarrollar estrategias para atender las necesidades de la seguridad de la información, estandarización, aplicación de técnicas de verificación y de auditoría.



Con esta práctica, se pretende abordar los conceptos y a la vez permiten afianzar los conocimientos adquiridos, realizando las prácticas propuestas.


TEMA: Estándares y Normatividad, gobierno en línea

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Reconocer por parte del estudiante los conceptos de seguridad de la información e informática, mediante un ejercicio práctico experimental, que les permita identificar la inseguridad en sistemas de información.

1.2 OBJETIVOS ESPECÍFICOS

- Revisar y definir las condiciones de cumplimiento de gobierno en línea, del sistema a revisar, seleccionar un sitio web
 - Aplicar el análisis de vulnerabilidades a un sitio web, con herramientas especializadas, en software libre.
- 

- Proponer un plan de acción para solucionar las vulnerabilidades encontradas confiabilidad del sistema de medición y reducir su variabilidad

2. FUNDAMENTACIÓN


En esta sección se exponen los elementos básicos conceptuales sobre el tema de esta práctica para la contextualización teórica de la misma. No obstante el estudiante deberá estudiar las referencias asignadas en el curso.

2.1 Seguridad, Amenazas, vulnerabilidades

Seguridad de la Información: son todas aquellas medidas preventivas, reactivas de las personas, en las organizaciones y los sistemas tecnológicos que permitan salvaguardar la información buscando mantener la Confidencialidad, Autenticidad, Disponibilidad e Integridad de la misma.

Seguridad informática es una rama de la informática que está enfocada a la protección del hardware, software, los sistemas de información y las redes de datos.

Ciberseguridad: "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". Según ISACA.




Ciberespacio: entorno virtual, no físico creado por equipos de cómputo unidos para interoperar en una red. Lo conforma todos los actores de interconexión, gestión de sistemas informáticos. Es decir los medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos, junto con los usuarios que interactúan con estos sistemas.

Amenaza: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema.

Confidencialidad: Es la identificación y la garantía del origen de la información. Corroborar de quien dice ser, sea.

2.2. CONCEPTOS BÁSICOS

Los conceptos más relevantes a considerar en relación con la variabilidad de los equipos de medición son los siguientes:

- **Criptografía:** es la disciplina que se encarga del estudio de códigos secretos o llamados también códigos cifrados (en griego kriptos significa secreto y gráhos, escritura, es decir mantener en secreto el mensaje. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje. Se derivan la Criptología y la Esteganografía. (Fernández, 2004).
- 


- **La Criptología:** Proviene del griego Krypto y logos, significa el estudio de lo oculto, lo escondido. Es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones.
- **Esteganografía:** La ciencia, denominada Esteganálisis, permite detectar información escondida en imágenes o archivos de sonido

2 Ataques a sistemas informáticos

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente

Informático; a fin de obtener un beneficio, por lo general de índole económico, causando efectos negativos en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques.



Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas.

Para realizar esta actividad es necesario que cada estudiante revise los aspectos conceptuales sobre Gobierno En Línea (GEL) y Sistema de Administración de la Seguridad (SASIGEL)

3. HERRAMIENTAS NECESARIOS PARA LA PRÁCTICA


Matriux, o Kali Linux, u otros

Pueden usar nessus versión home, para escáner de vulnerabilidades del sitio web.

4. FORMA DE TRABAJO

La actividad esta propuesta para ser desarrollada de forma individual. Aunque en los Grupos colaborativos se puede interactuar para el desarrollo de la actividad.

Fecha de inicio de la actividad: 24 de Octubre de 2016 a las 00:00 h



Fecha de finalización de la actividad: 03 de Noviembre de 2016, a las 23:55 h.

PROCEDIMIENTO

Antes de realizar la práctica deben tener en cuenta los siguientes aspectos para crear el escenario de práctica:

Descargar las aplicaciones teniendo en cuenta si deben ser a 32 bits o a 64 bits de acuerdo al hardware del equipo base que tengan.

4.1. REALIZAR LA PRACTICA

1. Elegir un portal web de un municipio capital de departamento sobre el cuál será evaluado la aplicación de gobierno en línea y el sistema de seguridad SASIGEL.
2. Explorar los menús, funcionalidad y servicios del portal web seleccionado.
3. Determinar mediante pruebas usando herramientas de software (Matriux, Kali Linux, otros) las vulnerabilidades, amenazas y riesgos de seguridad de los portales web del municipio seleccionado. No deben modificar nada en el sitio web.

4. Explorar fallas relacionadas con el cumplimiento de gobierno en línea, y de la seguridad del portal web de acuerdo al SASIGEL.
5. Presentar un informe final sobre el cumplimiento de GEL y SASIGEL de acuerdo a la normatividad vigente.

5. INFORME DE LA PRÁCTICA


Cada estudiante debe realizar el paso a paso e ir documentando el desarrollo de la actividad práctica en un documento en Word deberá presentar lo siguiente:

EL informe en Word será en letra Arial 11 a un espacio
El Informe debe contener el desarrollo de cada uno de los puntos anteriores en un solo archivo consolidado. Las pruebas realizadas sobre el portal web deben registrarse con pantallazos y una descripción de la falla encontrada (se deben recortar las imágenes, solo mostrar lo necesario).

- El archivo debe entregarse dentro de las fechas establecidas, de acuerdo a la agenda del curso, en el entorno de evaluación y seguimiento

6. RÚBRICA DE EVALUACIÓN

La rúbrica de evaluación de esta actividad se presenta en la siguiente página



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Rúbrica de Evaluación
ACTIVIDAD PRÁCTICA 2

Nombre del curso: SEGURIDAD INFORMÁTICA - 204039

Aspectos evaluados	Criterios de desempeño de la actividad individual Momento 1			P/ máxima
	Valoración alta	Valoración media	Valoración baja	
Funcionalidad de y servicios del portal web seleccionado.	El estudiante realizó de manera pertinente la revisión de servicios y cumplimiento normativo del sitio seleccionado	El estudiante realizó parcialmente la revisión de servicios y cumplimiento normativo del sitio seleccionado.	El estudiante nunca presentó sus aportes o no participó en la actividad.	6
	(Hasta 6 puntos)	(Hasta 3 puntos)	(Hasta 0 puntos)	
Pruebas de vulnerabilidades, amenazas y riesgos de seguridad de los portales web seleccionado	El estudiante realizó satisfactoriamente las pruebas de vulnerabilidades, amenazas y riesgos de seguridad del sitio web seleccionado	El estudiante realizó parcialmente las pruebas de vulnerabilidades, amenazas y riesgos de seguridad del sitio web seleccionado	El estudiante nunca presentó sus aportes o no participó en la actividad.	9
	(Hasta 9 puntos)	(Hasta 4 puntos)	(Hasta 0 puntos)	
Fallas	El estudiante realizó	El estudiante realizó	El estudiante ¹⁰	9

relacionadas con el cumplimiento de gobierno en línea	satisfactoriamente la revisión de fallas relacionadas con el cumplimiento de gobierno en línea.	parcialmente la revisión de las fallas relacionadas con el cumplimiento de gobierno en línea	nunca presentó sus aportes o no participó en la actividad.	
	(Hasta 9 puntos)	(Hasta 4 puntos)	(Hasta 0 puntos)	
Informe final sobre el cumplimiento de GEL y SASIGEL de acuerdo a la normatividad vigente	El estudiante realizó satisfactoriamente el Informe final sobre el cumplimiento de GEL y SASIGEL	El estudiante realizó parcialmente el Informe final sobre el cumplimiento de GEL y SASIGEL	El estudiante nunca presentó sus aportes o no participó en la actividad.	9
	(Hasta 9 puntos)	(Hasta 4 puntos)	(Hasta 0 puntos)	
TOTAL PUNTAJE DEL COMPONENTE PRÁCTICO				33



7. REFERENCIAS

- Fernández, S. (2004). La criptografía clásica, 119–142.
Retrieved from
http://www.hezkuntza.ejgv.euskadi.eus/r43-573/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_24/9_Criptografia_clasica.pdf
- Tarazona T., C. H. (n.d.). Amenazas Informáticas y Seguridad de la Información, 137–146.
- Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). Seguridad informática. Madrid, ES: Macmillan Iberia, S.A..
Retrieved from <http://www.ebrary.com>