**Universidad Nacional Abierta y a Distancia**

**Vicerrectoría Académica y de Investigación**

**Curso: Seguridad de la Información**

**Código: 202016905**

**Guía de actividades y rúbrica de evaluación –** Tarea 3 Modelando Amenazas

1. **Descripción de la actividad**

|  |  |
| --- | --- |
| **Tipo de actividad: En grupo colaborativo** | |
| **Momento de la evaluación: Intermedio** | |
| **Puntaje máximo de la actividad: 125 puntos** | |
| **La actividad inicia el:** lunes, 27 de septiembre de 2021 | **La actividad finaliza el:** domingo, 24 de octubre de 2021 |
| **Con esta actividad se espera conseguir los siguientes resultados de aprendizaje:**  Evaluar los riesgos de seguridad de la información en los procesos de desarrollo de software de acuerdo con estándares y la política de seguridad de la organización para garantizar la calidad de los productos de software. | |
| **La actividad consiste en:**  ***Trabajo Colaborativo***  Hacer una revisión de las lecturas correspondientes a la Unidad 2 que se encuentran en el entorno de aprendizaje. Los temas son:   * Principios de la seguridad de la información * Vulnerabilidades y clasificación de los sistemas informáticos * Amenazas a la seguridad informática * Propiedades del Software seguro   Cada estudiante elige uno de los siguientes interrogantes, se documenta y publica en el foro de la actividad la pregunta y la respuesta argumentada, con base en las lecturas realizadas y su criterio personal.  Interrogantes:   * ¿Explique al menos tres principios de la seguridad de la información? * ¿Qué son las vulnerabilidades? * ¿Cómo se clasifican las vulnerabilidades? * ¿Explique tres amenazas a la seguridad informática? * ¿Cuáles son las propiedades del software seguro, explique mínimo tres?   Cada estudiante elige uno de los interrogantes mencionados anteriormente, se documenta y publica en el foro de la actividad la pregunta y la respuesta argumentada, con base en las lecturas realizadas y su criterio personal. Adicionalmente, debe hacer un comentario por lo menos a una respuesta de un compañero, para expresar de manera respetuosa y argumentada su respaldo, complemento o desacuerdo.  Es importante citar las fuentes que soportan las opiniones en formato APA 7, con el fin de que los compañeros las puedan consultar para ampliar la información.  A partir de las participaciones realizadas en el foro, el grupo elabora una presentación electrónica en línea, presentando la información relevante de los temas desarrollados en las preguntas. La estructura es la siguiente  Diapositiva 1: Portada  Diapositiva 2: Principios de la seguridad de la información.  Diapositiva 3: Vulnerabilidades.  Diapositiva 4: Clasifican las vulnerabilidades.  Diapositiva 5: Que son amenazas en la seguridad de la información.  Diapositiva 6: Propiedades del software seguro.  Diapositiva 7. Conclusiones.  Diapositiva 8. Referencias bibliográficas  ***Trabajo Individual***   * Instalar la herramienta Threat Análisis and Modeling Tool 2016 de la compañía Microsoft. <https://www.microsoft.com/en-us/download/details.aspx?id=49168> * **Realización del diagrama de flujo de datos (DFD)**   Una vez recopilada toda la información sobre una aplicación se debe disponer a modelar con precisión la aplicación mediante el uso de Diagramas de Flujo de Datos (DFD). Estos diagramas nos permiten obtener una mejor comprensión de cómo la aplicación aceptará, procesará y manejará los datos. Hay una serie de símbolos que se utilizan en este tipo de diagramas (en la figura siguiente se muestra un resumen de los más importantes).    Figura 1. Símbolos de los diagramas de flujo de datos (DFD).  Una vez instalada la herramienta, para la realización de DFD hay que trabajar en la vista de diseño, que se obtiene al dar clic en la opcion «View → Design View» en el menú, tal y como se muestra en la figura siguiente:    Figura 2. Vista de diseño de la herramienta Threat Analysis and Modeling Tool 2016.  Se propone modelar la aplicación mediante el siguiente diagrama DFD que constituye una representación gráfica que agiliza el proceso de modelado de requerimientos. No olvidar configurar las propiedades de cada elemento del diagrama: por ejemplo, configurar autenticación y autorización en el servidor web protegerá de posibles amenazas, y la herramienta lo tendrá en cuenta a la hora de calcularlas. Además, saldrán amenazas repetidas. Es decir, se tendrán menos amenazas. El diagrama propuesto se encuentra en la figura 3, aunque el estudiante lo puede modelar de forma diferente según considere:  E:\CURSOS TRABAJO\SEGURIDAD SW Asignatura Master\TRABAJO MSI\TEMA 2\Trabajo Tema 21\Nuevo caso\reportUD2.png  Figura 3. Posible diagrama DFD de una aplicación.  Una vez en esta vista, hay que empezar a realizar el diagrama DFD, este debe estar acorde a topología lógica indicada en la figura 4:    Figura 4. Topología lógica de la aplicación.  En la aplicación donde vamos a modelar, en el cuadro de la derecha (Stencil) están los diferentes elementos que se pueden elegir para realizar el diagrama, con más opciones de lo indicado en el resumen de la figura 3.  NOTA: Incluir en el diagrama el nombre del estudiante y el grupo   * Cargar la plantilla que se encuentra en el siguiente <<[enlace](https://drive.google.com/drive/folders/1y5z6zTMbTsRhdXpVzsmaAhB2dgN8cde8?usp=sharing)>>, en la herramienta Threat Análisis and Modeling Tool 2016. Cargarla mediante el menú Aply Template, según la siguiente figura:     Figura 5. Cargar plantilla   * **Identificación de amenazas**   Una vez realizado el diagrama DFD pasamos a la vista de análisis, pulsando «View → Analysis View» en el menú. La herramienta calcula automáticamente las amenazas sugeridas para el diagrama de flujo de datos realizado. Al dar clic en cada una de ellas se verá información en detalle de las amenazas y un formulario para introducir más información, como podrían ser las salvaguardas que la mitiguen y su justificación.  La herramienta identifica las amenazas a nivel de red, *host* y aplicación, utilizando el Método STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege; en castellano: Suplantación de Identidad, Manipulación maliciosa de datos, Repudio, Divulgación de información, Denegación de servicio y Escalado de privilegios).    Figura 6. Relación entre las amenazas del método STRIDE y los elementos de un diagrama DFD.  Cuando se selecciona la vista de análisis, la herramienta mostrará las amenazas sugeridas para el diagrama de flujo de datos dibujado, donde, al clic en cada una de ellas, permite introducir las salvaguardas que se consideren y el análisis DREAD del paso de la metodología.    Figura 7. Vista análisis Threat Analysis and Modeling Tool.   * **Documentar las amenazas**   Una vez realizado el análisis automático de las amenazas, hay que documentarlas. Para ello hay que diligenciar la Tabla 1:   |  |  | | --- | --- | | **Descripción de la amenaza** |  | | **Objetivo** |  | | **Técnicas de ataque** |  |   Tabla 1. Documentación de las amenazas.  El alumno deberá rellenar una tabla con cinco (5) amenazas, obtenidas de la herramienta Threat Analysis and Modeling Tool 2016 y adicionalmente debe guardar el reporte del análisis automático de las amenazas y entregarlo junto con el documento del trabajo individual.  Procurar no identificar las mismas vulnerabilidades de sus compañeros. Recuerde que no se aceptan plagios.   * **Valorar las amenazas**   Una vez que tenemos identificada la lista de amenazas, el siguiente paso consiste en puntuarlas de acuerdo con el riesgo que suponen. Esto permitirá priorizar las actuaciones a efectuar para mitigar el riesgo.  Para ello utilizaremos el método DREAD (Damage, Reproducibility, Exploitability, Affected, DIscoverability; en castellano: Daño potencial, Reproductividad, Explotabilidad, Usuarios afectados, Descubribilidad). El riesgo se puede cuantificar como el resultado de multiplicar la probabilidad de que la amenaza se produzca por el daño potencial de esta.  Riesgo = Probabilidad x Impacto potencial= (R+E+DI) x (D+A) = PxI  Cada valor se cuantifica con un rango entre 1 y 3.  Figura 8. Significado de cada componente valoración del método DREAD.  Diligencia por cada amenaza la Tabla 2, en la que se incluye un ejemplo:   |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | **Probabilidad de Ocurrencia (P)** | | | **Impacto Potencial (I)** | | **P** | **I** | **Riesgo** | | **Amenaza** | ***R*** | ***E*** | ***DI*** | ***D*** | ***A*** | ***(R+E+DI)*** | ***(D+A)*** | ***PxI*** | | Inyección de comandos SQL | 3 | 2 | 2 | 3 | 3 | 7 | 6 | 42 | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |   Tabla 2. Calculo el riesgo.  El estudiante debe diligenciar en la tabla mínimo cinco amenazas, obtenidas de la herramienta Threat Analysis and Modeling Tool 2016.   * **Mitigación**   Frente a las amenazas se pueden dar diferentes respuestas, basándose principalmente en el riesgo asociado a cada una. Una amenaza puede ser eliminada cuando esta es opcional o cuando el riesgo que tiene asociado es tan alto que no se puede asumir. Puede decidirse no hacer nada, y aceptar el riesgo, cuando el impacto es bajo o si la mitigación es demasiado costosa comparada con el riesgo asociado. Generalmente se optará por mitigarla mediante alguna contramedida o salvaguarda. Por último, se puede transferir el riesgo a una tercera parte: por ejemplo, al usuario u a otra aplicación que interactúe con la nuestra.  Para las amenazas identificadas hay que seleccionar una serie de salvaguardas que mitiguen su riesgo asociado a la misma: restricciones arquitectónicas, técnicas criptográficas, mecanismos de autenticación, algoritmos seguros, etc., que nos permitan solucionar los problemas planteados.  Completar la Tabla 3, se deben indicar las medidas de mitigación de acuerdo con las amenazas identificadas en la tabla 1:  NOTA: En la tabla se incluye un ejemplo.   |  |  | | --- | --- | | **Descripción de la amenaza** | **Inyección de comandos SQL** | | **Medidas mitigación** | Validar la entrada, filtrando el contenido del campo usuario, utilizar un procedimiento almacenado que utilice parámetros para acceder a la base de datos. | | **Descripción de la amenaza** |  | | **Medidas mitigación** |  |   Tabla 3. Salvaguardas.  Como ayuda para seleccionar las salvaguardas a incluir en la aplicación para mitigar las amenazas, se incluye la figura 9 y la Tabla 4.  Imagen1  Figura 9. Salvaguardadas aplicación web.  También se puede usar la siguiente tabla para definir los salvaguardas:   |  |  |  | | --- | --- | --- | | **Amenazas** | **Propiedad** | **Salvaguardas** | | **Spoofing identity (Suplantación de Identidad)** | Autenticación | * Procesos de Autenticación, Autorización y Auditoría (AAA): *hash,* firma digital. * Protección de secretos. * No almacenamiento de secretos. * Single Sign On. * IPSEC. | | **Tampering with Data (Manipulación de datos)** | Integridad | * Procesos de AAA: *hash,* firma digital. * Códigos de autenticación de mensajes. * Firmas digitales. * Protocolos resistentes a la manipulación. * Listas control de acceso ACL. | | **Repudiation (Repudio)** | No Repudio | * Procesos de Autenticación: *hash,* firma digital. * Procesos de Auditoría. * Sellado de tiempo. | | **Information Disclosure (Revelación de información)** | Confidencialidad | * Procesos de AAA: *hash,* firma digital. * Protección de secretos. * No almacenamiento de secretos. * Protocolos seguros. * Encriptado. | | **Denial of Service (Denegación de servicio)** | Disponibilidad | * Procesos de AAA: *hash,* firma digital. * Listas control de acceso ACL. * Calidad de servicio. | | **Elevation of Privilege (Elevación de privilegios)** | Autorización | * Listas control de acceso ACL. * Control de acceso basado en roles. * Trabajar con el mínimo privilegio. * Validación de entradas. |   Tabla 4. Salvaguardas método STRIDE.  El estudiante debe realizar la entrega del documento del trabajo individual con la siguiente estructura: PortadaObjetivosDiagrama de flujo de datos (DFD). Nota el diagrama debe incluir el nombre del estudiante.Tabla 1 – Documentación de las amenazas.Tabla 2 – Calculo del riesgoTabla 3 – SalvaguardasReferencias bibliográficas Adicionalmente, debe incluir en la entrega el reporte de análisis automático de las amenazas generado en la aplicación Threat Análisis and Modeling Tool 2016. | |
| **Para el desarrollo de la actividad tenga en cuenta que:**  En el entorno de Información inicial debe:  Consultar la agenda del curso para revisar las fechas de entrega de la actividad  En el entorno de Aprendizaje debe:   * Leer las lecturas sugeridas para la unidad 2. * Ingresar al foro de la actividad para debatir con los compañeros sobre los temas referidos. * Compartir avances de la actividad individual.   En el entorno de Evaluación debe:  Cada estudiante envía un documento comprimido con:   * El documento (un documento Word o PDF) que contiene el trabajo final colaborativo * Trabajo final individual * Reporte de análisis automático de las amenazas generado en la aplicación Threat Análisis and Modeling Tool 2016.­­ | |
| **Evidencias de trabajo independiente:**  Las evidencias de trabajo independiente para entregar son:   * Trabajo final individual * Reporte de análisis automático * Aportes en el foro | |
| **Evidencias de trabajo grupal:**  Las evidencias de trabajo grupal a entregar son:   * Participación en el foro de la actividad. * Documento digital con el link de la presentación electrónica. | |

1. **Lineamientos generales para la elaboración de las evidencias de aprendizaje a entregar.**

|  |
| --- |
| Para evidencias elaboradas **en grupo colaborativamente**, tenga en cuenta las siguientes orientaciones Antes de construir la presentación electrónica es importante analizar y organizar la información.A medida que selecciona la información construya la bibliografía.Puede usar el software para presentaciones en línea que prefiera, algunas opciones son: canva, emaze, prezi, genially.Después de construir la presentación electrónica, copie el link de la presentación en un documento Word y envíe este documento por el entorno de evaluación. Verifique que el link funcione correctamente y no tenga restricciones de acceso. |
| Tenga en cuenta que todos los productos escritos individuales o grupales deben cumplir con las normas de ortografía y con las condiciones de presentación que se hayan definido.  En cuanto al uso de referencias considere que el producto de esta actividad debe cumplir con las normas **APA** |
| En cualquier caso, cumpla con las normas de referenciación y evite el plagio académico, para ello puede apoyarse revisando sus productos escritos mediante la herramienta Turnitin que encuentra en el campus virtual.  Considere que en el acuerdo 029 del 13 de diciembre de 2013, artículo 99, se considera como faltas que atentan contra el orden académico, entre otras, las siguientes: literal e) “El plagiar, es decir, presentar como de su propia autoría la totalidad o parte de una obra, trabajo, documento o invención realizado por otra persona. Implica también el uso de citas o referencias faltas, o proponer citad donde no haya coincidencia entre ella y la referencia” y liberal f) “El reproducir, o copiar con fines de lucro, materiales educativos o resultados de productos de investigación, que cuentan con derechos intelectuales reservados para la Universidad”  Las sanciones académicas a las que se enfrentará el estudiante son las siguientes:   1. En los casos de fraude académico demostrado en el trabajo académico o evaluación respectiva, la calificación que se impondrá será de cero puntos sin perjuicio de la sanción disciplinaria correspondiente. 2. En los casos relacionados con plagio demostrado en el trabajo académico cualquiera sea su naturaleza, la calificación que se impondrá será de cero puntos, sin perjuicio de la sanción disciplinaria correspondiente. |

**3. Formato de Rúbrica de evaluación**

|  |  |
| --- | --- |
| **Tipo de actividad: En grupo colaborativo** | |
| **Momento de la evaluación: Intermedio** | |
| **La máxima puntuación posible es de 125 puntos** | |
| **Primer criterio de evaluación:**  **Contenido:**  Apropiación los conceptos de Principios de la seguridad de la información, vulnerabilidades y amenazas, Propiedades del Software seguro.  **Este criterio representa 40 puntos del total de 125 puntos de la actividad.** | **Nivel alto:**  Apropia y argumenta los conceptos de principios de la seguridad informática, Vulnerabilidades, amenazas y Propiedades del Software seguro.  **Si su trabajo se encuentra en este nivel puede obtener entre 26 puntos y 40 puntos.**  **Nivel Medio:**  Algunas ideas que expresa en la presentación electrónica no son coherentes o no se presenta la totalidad de conceptos solicitados.  **Si su trabajo se encuentra en este nivel puede obtener entre 11 puntos y 25 puntos.**  **Nivel bajo:** Los conceptos plasmados en la presentación no presentan comprensión de los conceptos principios de la seguridad informática, Vulnerabilidades, amenazas y Propiedades del Software seguro .  **Si su trabajo se encuentra en este nivel puede obtener entre 0 puntos y 10 puntos.** |
| **Segundo criterio de evaluación:**  **Forma:**  Presentación del documento del trabajo colaborativo.  **Este criterio representa 5 puntos del total de 125 puntos de la actividad** | **Nivel alto:** La presentación se estructura de forma adecuada, se realiza mediante un software de presentaciones electrónicas en línea e incluye referencias en formato APA.  **Si su trabajo se encuentra en este nivel puede obtener entre 4 puntos y 5 puntos.**  **Nivel Medio:**  La presentación no incluye referencias, no se estructura de manera ordenada totalmente o no se realiza en un software de presentaciones electrónicas en línea.  **Si su trabajo se encuentra en este nivel puede obtener entre 2 puntos y 3 puntos.**  **Nivel bajo:** La presentación no se estructura de forma organizada.  **Si su trabajo se encuentra en este nivel puede obtener entre 0 puntos y 1 puntos.** |
| **Tercer criterio de evaluación:**  **Participación:**  Participación en el foro en el trabajo colaborativo.  **Este criterio representa 5 puntos del total de 125 puntos de la actividad** | **Nivel alto:**  Promueve la generación de diversos puntos de vista relacionados con la temática, enriqueciendo la discusión y agregando valor a la misma.  **Si su trabajo se encuentra en este nivel puede obtener entre 4 puntos y 5 puntos.**  **Nivel Medio:** Los contenido de algunos mensajes no son coherentes con la temática tratada, no todos son originales o no siempre promueven la generación de diversos puntos de vista, enriqueciendo la discusión y agregando valor a la misma.  **Si su trabajo se encuentra en este nivel puede obtener entre 2 puntos y 3 puntos.**  **Nivel bajo:**  Los contenidos de los mensajes no son coherentes con la temática tratada, no son originales o no promueven la generación de diversos puntos de vista para la discusión y agregando valor a la misma.  **Si su trabajo se encuentra en este nivel puede obtener entre 0 puntos y 1 puntos.** |
| **Cuarto criterio de evaluación:**  **Contenido:**  Realiza el modelado de las amenazas de una aplicación propuesta.  **Este criterio representa 60 puntos del total de 125 puntos de la actividad** | **Nivel alto:** Cada estudiante realiza el modelado de las amenazas de una aplicación propuestadonde incluye del diagrama de flujo de datos, la documentación de las amenazas, el cálculo del riesgo y los salvaguardas.  **Si su trabajo se encuentra en este nivel puede obtener entre 36 puntos y 60 puntos.**  **Nivel Medio:** El estudiante realiza de forma parcial el modelado de las amenazas de una aplicación propuestadonde incluye del diagrama de flujo de datos, la documentación de las amenazas, el cálculo del riesgo y los salvaguardas.  **Si su trabajo se encuentra en este nivel puede obtener entre 10 puntos y 35 puntos.**  **Nivel bajo:** Cada estudiante no realiza de forma adecuada realiza el modelado de las amenazas de una aplicación propuestadonde incluye del diagrama de flujo de datos incompleto y/o la documentación de las amenazas y/o el cálculo del riesgo y/o los salvaguardas o no realiza la entrega la actividad.  **Si su trabajo se encuentra en este nivel puede obtener entre 0 puntos y 9 puntos.** |
| **Quinto criterio de evaluación:**  **Forma:**  Presentación del documento del trabajo independiente.  **Este criterio representa 15 puntos del total de 125 puntos de la actividad** | **Nivel alto:** El estudiante presenta un documento en Word o PDF con todos los elementos: Portada, objetivos, diagrama de flujo de datos, la documentación de las amenazas, el cálculo del riesgo y los salvaguardas , e incluye referencias en formato APA y sin errores de ortografía y buena redacción.  **Si su trabajo se encuentra en este nivel puede obtener entre 11 puntos y 15 puntos.**  **Nivel Medio:**  El estudiante presenta un documento en Word o PDF con algunos los elementos solicitados e incluye referencias en formato APA y/o con errores de ortografía y/o buena redacción.  **Si su trabajo se encuentra en este nivel puede obtener entre 6 puntos y 10 puntos.**  **Nivel bajo:**  El documento no se estructura de forma organizada, tiene errores de ortografía y mala redacción, no incluye las normas APA o no fue realizada la actividad.  **Si su trabajo se encuentra en este nivel puede obtener entre 0 puntos y 5 puntos.** |

