**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 2 Atacando y Defendiendo

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, 21 de febrero de 2022 | **La actividad finaliza el:** domingo, 13 de marzo de 2022 |
| **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:**  Hacer una revisión de las lecturas correspondientes a la Unidad 1 que se encuentran en el entorno de aprendizaje.  **Trabajo colaborativo:**  Esta sección tiene por objetivo comprender los temas requeridos para el desarrollo de la actividad. Los temas de la unidad son:   * Pilares de la Seguridad Informática * Gestión de riesgos y Controles de Seguridad * Programas, procesos y políticas de seguridad de la información * Planes de Continuidad   Para ello el grupo colaborativo se organiza para consultar, abordar y debatir los siguientes interrogantes:   1. ¿Cuáles son los pilares de la seguridad informática y explicarlos? 2. ¿Qué es la gestión de riesgos en la seguridad informática? 3. ¿Qué son los controles de seguridad? 4. ¿Por qué es importante implementar una política de seguridad de la información en una organización? 5. ¿Cuál es el objetivo de realizar los planes de continuidad en una organización?   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 2,3,4,5 y 6: Desarrollo temático.  Diapositiva 7: Referencias.  Diapositiva 8. Conclusiones.  **Trabajo Individual:**  Esta actividad consta de dos partes :   * **PRIMERA PARTE – Defendiendo**   ¿Son conscientes de la información que cualquier persona puede averiguar sobre nosotros sin restricciones en Internet?. El objetivo es aprender a encontrar lo que se puede conocer de si mismos en internet, usando herramientas **OSINT (Open Source INTelligence)**, traducido como **Inteligencia de Fuentes Abiertas. H**ace referencia al conjunto de técnicas y herramientas para recopilar información pública, analizar los **datos** y correlacionarlos convirtiéndolos en **conocimiento útil**.  En Google existen operadores con capacidad de combinación que nos aportan una información muy extensa: *intitle*, *allintitle*, *inurl*, *allinurl*, *filetype*, *link*, *inanchor*, *daterange*, view/indexFrame.shtml, entre otros. Por otro lado, existen multitud de metabuscadores y otras grandes fuentes de información dentro de Internet para buscar cualquier huella o rastro digital.  Para el desarrollo de esta actividad debe documentarse y realizar búsqueda de ustedes mismos, usando los operadores mencionados anteriormente. Buscar nombre, cedula en redes sociales, en páginas web, fotos, acceder a cámaras, buscar documentos con password.  Ejemplos:   * *Intitle: “My webcamXP server!” inurl:”:8080. (Acceder a una cámara).* * view/indexFrame.shtml * *Servidores con archivos llamados password.txt: intitle “Index of” “Index of /” password.txt (Buscar en un estructura de directorios un archivo de Password)* * *Robots: site:unir.net inurl: robot.txt*   Obtener información de los Metabuscadores que se mencionan a continuación y la adjuntan al trabajo individual. En estos buscadores incluir su nombre (Realice la búsqueda al menos en tres de los buscadores mencionados):  [*www.yasni.es*](http://www.yasni.es)  [*http://es.kgbpeople.com*](http://es.kgbpeople.com)  [*https://pipl.com*](https://pipl.com)  [*http://www.spokeo.com*](http://www.spokeo.com)  [*http://webmii.com*](http://webmii.com)  Buscar su Username en los siguientes metabuscadores para observar si está o no disponible en las diferentes redes sociales:  <http://Checkusernames.com>  <http://namechk.com>  <http://knowem.com>  Por ultimo debe concluir sobre que es la capacidad delictiva de los resultados obtenidos en el ejercicio.   * **SEGUNDA PARTE Atacando:** TOR *(The Onion Router)* es una red superpuesta sobre Internet, que permite el intercambio de información entre un origen y un destino sin revelar la identidad de los usuarios. Mantiene la integridad y el secreto de la información que viaja por ella gracias a la criptografía asimétrica y el concepto de clave pública y privada. La garantía de navegar de una forma anónima y acceder a la *Deep Web* (Red Profunda) es total, accediendo a servicios que muchas veces están al otro lado de la legalidad. * El estudiante debe instalar la aplicación TOR. * Debe realizar navegación en browser TOR. * Dejar evidencias. * Concluir sobre el uso en el navegador TOR con referencia a la parte delictiva. Revisar si en Colombia hay restricciones para el uso del Navegador TOR y las consecuencias legales de su uso.   El estudiante debe realizar la entrega del documento del trabajo individual con la siguiente estructura: PortadaObjetivosEnlace de la presentación en líneaPrimera parte: Herramientas OSINTEvidenciasConcluir sobre que es la capacidad delictiva de los resultados obtenidos en el ejercicioSegunda parte: Navegador TOREvidencias de la instalaciónEvidencias de la navegaciónConcluir sobre el uso en el navegador TOR desde la parte delictiva y sus consecuenciasReferencias bibliográficas | |
| **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 1. * Ingresar al foro de la actividad para debatir con los compañeros sobre los temas referidos.   En el entorno de Evaluación debe:   * Cada estudiante envía un documento digital (un documento Word o PDF) que contiene el link de la presentación electrónica en línea y con las evidencias de su trabajo individual. | |
| **Evidencias de trabajo independiente:**  Las evidencias de trabajo independiente para entregar son:   * Participación en el foro de la actividad. * Documento digital con las evidencias de trabajo individual. | |
| **Evidencias de trabajo grupal:**  Las evidencias de trabajo grupal a entregar son:   * Participación en el foro de la actividad con aportes que contribuyan a la consolidación del trabajo en grupo. * Enlace de la presentación electrónica en línea. | |

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   1. Antes de construir la presentación electrónica es importante analizar y organizar la información. 2. A medida que selecciona la información construya la bibliografía. 3. Puede usar el software para presentaciones en línea que prefiera, algunas opciones son: canva, emaze, prezi, genially. 4. 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. 5. Para la consolidación del trabajo independiente puede usar Word o PDF. |
| 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 los pilares de la seguridad informática, gestión de riesgos y controles, la importancia de la política de seguridad y el objetivo de los planes de contingencia.  **Este criterio representa 40 puntos del total de 125 puntos de la actividad.** | **Nivel alto:**  Apropia y argumenta los conceptos de los pilares de la seguridad informática, gestión de riesgos y controles, la importancia de la política de seguridad y el objetivo de los planes de contingencia.  **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 de los pilares de la seguridad informática, gestión de riesgos y controles, la importancia de la política de seguridad y el objetivo de los planes de contingencia.  **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**  Obtención de información pública a través de herramientas y técnicas para analizar los datos.  **Este criterio representa 30 puntos del total de 125 puntos de la actividad** | **Nivel alto:** Cada estudiante realiza de forma adecuada la obtención de información de ellos mismos a través de herramientas OSINT, haciendo uso de los operadores y de los metabuscadores sugeridos y concluye de forma acertada sobre que es la capacidad delictiva de los resultados obtenidos en el ejercicio.  **Si su trabajo se encuentra en este nivel puede obtener entre 21 puntos y 30 puntos.**  **Nivel Medio:** El estudiante realiza de forma parcial la obtención de información de ellos mismos a través de herramientas OSINT, haciendo uso de los operadores y de los metabuscadores sugeridos y concluye de forma parcial sobre que es la capacidad delictiva de los resultados obtenidos en el ejercicio.  **Si su trabajo se encuentra en este nivel puede obtener entre 10 puntos y 20 puntos.**  **Nivel bajo:**  Cada estudiante no realiza de forma adecuada la obtención de información de ellos mismos a través de herramientas OSINT, y no hace uso de los operadores y de los metabuscadores sugeridos y no concluye de forma acertada sobre que es la capacidad delictiva de los resultados obtenidos en el ejercicio 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:**  **Contenido:**  Apropiación de la instalación y uso adecuado de herramientas para navegar (TOR) en la Red Profunda.  **Este criterio representa 30 puntos del total de 125 puntos de la actividad** | **Nivel alto:** Cada estudiante realiza de forma adecuada la instalación, navegación en TOR y concluye de forma acertada sobre que es la capacidad delictiva de los resultados obtenidos en el ejercicio.  **Si su trabajo se encuentra en este nivel puede obtener entre 21 puntos y 30 puntos.**  **Nivel Medio:** El estudiante realiza de forma parcial la instalación, navegación en TOR y concluye de forma parcial sobre que es la capacidad delictiva de los resultados obtenidos en el ejercicio.  **Si su trabajo se encuentra en este nivel puede obtener entre 10 puntos y 20 puntos.**  **Nivel bajo:**  Cada estudiante no realiza de forma correcta la instalación, navegación en TOR y no concluye de forma acertada sobre que es la capacidad delictiva de los resultados obtenidos en el ejercicio o no realiza la entrega la actividad.  **Si su trabajo se encuentra en este nivel puede obtener entre 0 puntos y 9 puntos.** |
| **Sexto 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, primera parte obtención de información, segunda parte con la instalación, navegación en TOR, 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.** |