
	<p style="text-align: center;">Universidad Estatal a Distancia</p> <p style="text-align: center;">Vicerrectoría Académica</p> <p style="text-align: center;">Escuela de Ciencias Exactas y Naturales</p> <p style="text-align: center;">Cátedra TIC e Ingeniería</p>	
---	--	---

03308: Soporte Técnico

Tarea No. 2

Valor: 10%

Instrucciones generales.

Los trabajos que deben presentar (tareas o proyectos), tienen que seguir las siguientes reglas:

- Todos los trabajos escritos, deberán cumplir con los “Lineamientos de trabajos escritos de la Carrera Ingeniería Informática, documento que se encuentra dentro de la plataforma.
- En el aula virtual se permite la subida de un sólo archivo, por lo que, si tiene que subir más de un documento, deberá realizar un archivo .zip o .rar, para comprimir todos los archivos que resulten del trabajo realizado.
- El trabajo se iniciará en la semana 6 y se presentará en la plataforma en la semana 7, a más tardar el domingo de dicha semana antes de las 11:55 p.m.
- El instrumento tiene que ser entregado en el apartado que se creó dentro de la plataforma de aprendizaje en línea Moodle o según especificaciones que indique la cátedra.
- No se recibirán instrumentos después de esta fecha, sólo casos muy justificados por los estudiantes y quedará a disposición del profesor recibirlos fuera de tiempo, para lo que el profesor con el entendido del estudiante podrá realizar posteriormente a la revisión del instrumento un rebajo del 30% por la entrega tardía del mismo.
- Debe leer y analizar la rúbrica de evaluación que se encuentra al final de este documento.

- Cualquier duda serán atendidos por el profesor por medio del correo interno o bien en el foro destinado a consultas.
- Nombre del archivo que envía: debe ser el nombre del estudiante + nombre del trabajo. Ejemplo: KarolCastro-proyecto1.docx.
- Antes de realizar su proyecto o tarea, revise los temas en los que se debe basar para realizar el instrumento; recuerde incluir toda la bibliografía que utilizó. Sea claro en sus investigaciones y redacte con sus propias palabras lo que allí se le pide.

El documento debe contener los siguientes apartados:

Parte del documento	Descripción	Es incluido	Valor
Portada	Incluir como mínimo el nombre, carné, nombre de la asignatura, nombre del profesor, número de grupo, título del trabajo, fecha de entrega y centro universitario. "Siguiendo el ejemplo de la página #4 del documento: Lineamientos para trabajos escritos que se encuentra disponible en la plataforma".	SI	No aplica
Índice	Debe llevar un orden numérico que identifique donde localizar cualquier tema realizado dentro del documento.	SI	No aplica
Introducción	De manera resumida se debe brindar una visión del caso de estudio que está presentando y los objetivos que se desarrollan.	SI	Ver rúbrica
Desarrollo	Es el cuerpo del trabajo, cada trabajo deberá seguir el esquema indicado en la guía del estudiante.	SI	Ver rúbrica
Conclusiones y recomendaciones	Debe señalar de manera precisa las principales conclusiones a las que llegó después de realizado el trabajo y si existe algún tipo de recomendación para mejorar el producto entregado. "Mínimo se deben de entregar tres conclusiones y tres recomendaciones, las cuales deben	SI	Ver rúbrica

Parte del documento	Descripción	Es incluido	Valor
	estar relacionadas entre sí". Se deben separar las secciones de conclusiones y recomendaciones.		
Bibliografía	Se deberá indicar claramente las fuentes consultadas para hacer el trabajo, sean estas personas, material bibliográfico o direcciones de Internet. Favor no indicar: www.monografias.com, o www.google.com; ya que esas direcciones son genéricas y no indican el lugar exacto de dónde usted tomó los datos para el documento. Los proyectos o tareas que no contemplen la bibliografía obtendrán una nota igual a "Cero". Solo se permite un porcentaje máximo al 50% de la bibliografía digital o de Internet. El otro porcentaje restante deberá ser de literatura o de libros.	SI	Ver rúbrica

Cronograma de la Tarea No. 2.

A continuación, se presentan las fechas de la tarea.

Fecha	Actividad
Semana 6	Entrega del instrumento al estudiante, en la plataforma, por parte del profesor-tutor.
Semana 7	Entrega en la plataforma de la tarea 2 por parte del estudiante.
Temas de la tarea	Gestión de Incidentes de Seguridad desde el Soporte Técnico.
Valor:	10%
Puntos	100 puntos
Modalidad	Individual

Desarrollo de la Tarea No. 2**Instrucciones que seguir, en el informe técnico:**

Investigar en artículos web, foros, revistas o investigaciones, sobre el éxito empresarial a través de un soporte técnico enfocado en la Gestión de Incidentes de Seguridad desde el Soporte Técnico.

Deberá de realizar un informe técnico de manera expositivo-argumentativo, es decir el estudiante debe de reflexionar, evaluar y analizar el tema indicado. El informe tiene un formato libre, en el que el estudiante se vale de información confiable para formular argumentos propios.

Se recomienda iniciar el proceso de elaboración de un informe técnico generando una lluvia de ideas en concordancia con el tema de investigación y siguiendo las pautas establecidas en la sección de 'Actividades por realizar' de este documento. Este enfoque facilitará la identificación de elementos clave y la creación de una estructura sólida para el informe, garantizando así la coherencia y exhaustividad en la presentación de la información técnica.

Posterior organizar el contenido de la introducción, desarrollo y conclusión de acuerdo con las ideas identificadas en el paso anterior. Elaborar el informe técnico debe de realizarse de mínimo 4 y máximo 6 páginas de desarrollo.

Tema: Gestión de Incidentes de Seguridad desde el Soporte Técnico

Objetivo: Desarrollar un informe técnico detallado sobre la gestión de incidentes de seguridad desde el soporte técnico, alineado con las mejores prácticas de NIST SP 800-61r2 e ISO 27001.

Actividades por realizar.

Proteger los activos de información y sistemas es muy importante y debemos entender cómo un equipo de soporte técnico especializado en ciberseguridad puede proteger

datos privados y sensibles, reduciendo los riesgos de una mala gestión de la información.

Como especialista, su tarea es hacer un informe técnico que explore cómo se maneja la gestión de incidentes de seguridad desde el soporte técnico. Aquí tienes los temas que debes cubrir:

1. ¿Qué es la Gestión de Incidentes de Seguridad, según las normas y estándares NIST SP 800-61r2 e ISO 27001?
2. ¿Cómo identificar y clasificar incidentes de seguridad?
3. ¿Qué pasos se deben seguir para responder a un incidente de seguridad?
4. Explicar qué es un SIEM (Security Information and Event Management) y cuál es la importancia en la gestión de incidentes de seguridad.

El estudiante puede hacer uso de imágenes, para el apoyo de la explicación de los anteriores aspectos.

La evaluación del documento se llevará a cabo mediante la entrega de un informe que refleje los puntos mencionados anteriormente. Es importante destacar que la evaluación técnica no será considerada en este proceso, por lo que se deberá hacer referencia a la rúbrica de evaluación que se presenta a continuación para garantizar una evaluación adecuada y consistente.

Rúbrica: Valor: 10%, total de puntos: 100 puntos.

Nombre del estudiante: _____

Total de puntos: 100 puntos.

Puntos obtenidos: _____ Nota: _____ Porcentaje obtenido: _____

ASPECTO POR EVALUAR	CRITERIOS			
	Excelente	Regular	Debe mejorar	No se evidencia
1. Introducción	Evidencia una introducción que cautiva la atención del lector, va directo al grano, presenta la tesis de forma satisfactoria y enlista y describe brevemente los asuntos que se van a tratar en el ensayo. Valor 4 puntos.	Evidencia una introducción que cautiva medianamente la atención del lector, va medianamente al grano, presenta la tesis de forma medianamente satisfactoria y enlista y describe brevemente los asuntos que se van a tratar en el ensayo. Valor 3 puntos.	Evidencia una introducción que cautiva escasamente la atención del lector, casi no va al grano, presenta la tesis de forma escueta y enlista y describe algunos de los asuntos que se van a tratar en el ensayo. Valor 1 puntos.	No se evidencia una introducción que cautive al lector, no va al grano, no presenta la tesis y no enlista ni describe lo que se va a tratar en el ensayo. Valor 0 puntos.
2.	Desarrollo			
2.1. Explicación de en qué es la Gestión de Incidentes de Seguridad, según las normas y estándares NIST SP 800-61r2 e ISO 27001	La respuesta está directamente relacionada con el tema central del ensayo y guía la discusión de manera efectiva, de acuerdo con lo solicitado al criterio 1. Valor 12 puntos.	La respuesta es está medianamente relacionada con el tema y guía medianamente la discusión de manera efectiva, de acuerdo con lo solicitado al criterio 1. Valor 8 puntos.	La respuesta tiene poca relación con el tema central y no proporciona una dirección adecuada para el ensayo, de acuerdo con lo solicitado al criterio 1. Valor 4 puntos.	No presenta el criterio 1, o presenta coincidencia académica. Valor 0 puntos.
2.2. Explicación concisa sobre cómo identificar y clasificar incidentes de	La respuesta está directamente relacionada con el tema central del ensayo y guía la discusión de manera efectiva,	La respuesta es está medianamente relacionada con el tema y guía medianamente la discusión de	La respuesta tiene poca relación con el tema central y no proporciona una dirección adecuada para el	No presenta el criterio 2, o presenta coincidencia académica. Valor 0 puntos.

ASPECTO POR EVALUAR	CRITERIOS			
	Excelente	Regular	Debe mejorar	No se evidencia
seguridad	de acuerdo con lo solicitado al criterio 2. Valor 20 puntos.	manera efectiva, de acuerdo con lo solicitado al criterio 2. Valor 14 puntos.	ensayo, de acuerdo con lo solicitado al criterio 2. Valor 8 puntos.	
2.3. Análisis de que pasos se deben seguir para responder a un incidente de seguridad	La respuesta está directamente relacionada con el tema central del ensayo y guía la discusión de manera efectiva, de acuerdo con lo solicitado al criterio 3. Valor 20 puntos.	La respuesta es está medianamente relacionada con el tema y guía medianamente la discusión de manera efectiva, de acuerdo con lo solicitado al criterio 3. Valor 14 puntos.	La respuesta tiene poca relación con el tema central y no proporciona una dirección adecuada para el ensayo, de acuerdo con lo solicitado al criterio 3. Valor 8 puntos.	No presenta el criterio 3, o presenta coincidencia académica. Valor 0 puntos.
2.4. Explicación sobre qué es un SIEM (Security Information and Event Management) y cuál es la importancia en la gestión de incidentes de seguridad.	La respuesta está directamente relacionada con el tema central del ensayo y guía la discusión de manera efectiva, de acuerdo con lo solicitado al criterio 4. Valor 20 puntos.	La respuesta es está medianamente relacionada con el tema y guía medianamente la discusión de manera efectiva, de acuerdo con lo solicitado al criterio 4. Valor 14 puntos.	La respuesta tiene poca relación con el tema central y no proporciona una dirección adecuada para el ensayo, de acuerdo con lo solicitado al criterio 4. Valor 8 puntos.	No presenta el criterio 4, o presenta coincidencia académica. Valor 0 puntos.
3. Argumentación	Argumenta las ideas en un orden lógico y convincente de tal manera que son fáciles e interesantes de seguir. Valor 4 puntos.	Argumenta las ideas en un orden poco secuencial pero convincente. Valor 3 puntos.	Expresa las ideas de manera secuencial, pero no hay una argumentación. Valor 1 puntos.	No se presenta la argumentación de ideas ni la presencia secuencial convincente. Se presenta coincidencia académica. Valor 0 puntos.
4. Deducciones y relaciones	Establece deducciones y	Establece deducciones y	No establece deducciones ni	No presenta deducciones y

ASPECTO POR EVALUAR	CRITERIOS			
	Excelente	Regular	Debe mejorar	No se evidencia
	relaciones entre el texto y la realidad, elabora su propia construcción crítica. Valor 4 puntos.	relaciones entre el texto y la realidad, sin elaboración propia. Valor 3 puntos.	relaciones entre el texto y la realidad, pero aporta construcción propia. Valor 1 puntos.	relaciones entre el texto y la realidad. Se presenta coincidencia académica. Valor 0 puntos.
5. Conclusiones	Presenta 3 conclusiones del proyecto, no repite ideas, incluye las experiencias de aprendizaje, hace énfasis en la idea principal y existe un hilo conductor a lo largo del texto. Valor 3 puntos.	Presenta 2 conclusiones generales que profundizan parcialmente en el tema y el hilo conductor es parcial a lo largo del texto. O presenta 3 conclusiones que podrían ser más detalladas o carecen de profundidad en ciertas áreas. Valor 2 puntos.	Presenta 1 conclusión general casi no profundizan en el tema y el hilo conductor es escaso a lo largo del texto. Valor 1 puntos.	No presenta conclusión y recomendaciones o bien la misma presenta coincidencia académica. Valor 0 puntos.
6. Recomendaciones	Presenta 3 recomendaciones claras y efectivas, y demuestran un profundo conocimiento del tema. Son altamente aplicables y ofrecen resultados sobresalientes. Valor 3 puntos.	Presenta 2 recomendaciones adecuadas y útiles, brindando buenas soluciones al problema planteado. O presenta 3 recomendaciones que podrían ser más detalladas o carecen de profundidad en ciertas áreas. Valor 2 puntos.	Presenta 1 recomendación general, que casi no profundizan en el tema y el hilo conductor es escaso a lo largo del texto. Valor 1 puntos.	No presenta conclusión y recomendaciones o bien la misma presenta coincidencia académica. Valor 0 puntos.
7. Lista de referencias	La lista de referencias presentada responde a los	La lista de referencias presentada responde a los	La lista de referencias presentada responde a los	No presenta lista de referencias. Valor 0 puntos.

ASPECTO POR EVALUAR	CRITERIOS			
	Excelente	Regular	Debe mejorar	No se evidencia
	documentos consultados y sigue adecuadamente el formato APA 7. Valor 3 puntos.	documentos consultados, pero incumple uno o dos aspectos del formato APA 7. Valor 2 puntos.	documentos consultados, pero no responde al formato APA 7. Valor 1 puntos.	
8. Redacción	El trabajo presenta una clara redacción con secuencia lógica de ideas. Valor 4 puntos.	El trabajo presenta una redacción parcialmente clara y no responde en su totalidad a una secuencia lógica de ideas. Valor 3 puntos.	El trabajo presenta una redacción confusa y poca secuencia lógica de ideas. Valor 1 puntos.	El trabajo presenta una redacción confusa sin secuencia lógica de ideas. Valor 0 puntos.
9. Ortografía y puntuación.	El trabajo no presenta errores ortográficos ni de puntuación. Valor 3 puntos.	El trabajo presenta entre 1 y 5 errores ortográficos o de puntuación. Valor 2 puntos.	El trabajo presenta entre 6 y 8 errores ortográficos o de puntuación. Valor 1 puntos.	El trabajo presenta 9 o más errores ortográficos o de puntuación. Valor 0 puntos.
TOTAL	100	70	36	0