Área Académica de Administración de Tecnologías de Información
Administración de Tecnología de Información
Instituto Tecnológico de Costa Rica
Sede Cartago

Carrera: Licenciatura en Administración de Tecnología de Información **Semestre**: I-2022
Curso: TI2402 Algoritmos y estructuras de datos **Valor:** 20%
Prof.: Ing. María José Artavia Jiménez, MAE.

PROYECTO PROGRAMADO 2
CIBERSEGURIDAD

1. Introducción

La ciberseguridad se ha convertido en una prioridad para los gobiernos de todo el mundo, ya que consideran que proteger a los activos disponibles a través de internet, y los sistemas y las redes informáticas de los hackers, es vital para el funcionamiento, la estabilidad de una nación y el sustento de su gente.

Por otro lado, las empresas más grandes y con mayores sistemas informáticos son más propensas a ser víctimas de un ataque cibernético sin embargo, nadie está libre. Además, cada vez son más frecuentes y se producen a un ritmo más acelerado.

Es por eso que la inversión es ciberseguridad es un aspecto clave que todas las empresas y gobiernos deben considerar. La tecnología se ha vuelto una pieza fundamental de todos los negocios a nivel mundial lo que hace que seamos más propensos a los ataques y es precisamente por ello que protegerlas no es algo que deba tomarse a la ligera.

2. ¿Qué se busca con este proyecto?

- Desarrollar una solución de software para practicar acerca de los conceptos de estructuras de datos no lineales.
- Mejorar las habilidades de resolución de problemas.
- Profundizar el conocimiento del lenguaje de programación C.
- Ejercitar la toma de decisiones.
- Fomentar el trabajo **grupal, el desarrollo de habilidades de liderazgo, planeamiento y comunicación efectiva.**
- Fomentar la **investigación** por parte del estudiante.

3. Contexto y las funcionalidades esperadas

La etapa de ingeniería de requerimientos estableció que el sistema debe proveer las siguientes funcionalidades:

3.1. Registro de tipo de ciberataque

En esta sección se registrarán los tipos de ciberataques que se pueden dar a nivel mundial. Por cada uno debe registrarse: código (número entero), nombre, descripción, canales por donde se puede dar el ataque.

El sistema debe permitir que se elimine o modifique información de un tipo de ciberataque, con la restricción de que no se puede eliminar tipos de ciberataques que estén asociados a un ataque en particular. Y no se puede modificar la información del código del tipo de ciberataque. Además se debe permitir mostrar la información de los tipos de ciberataques registrados.

3.2. Registro de ciberdelincuente

Este es el registro de los ciberdelincuentes. Se debe registrar la siguiente información: código de identificación (número entero), nombre del grupo ciberdelincuente, país de origen, lista de ciberataques más reconocidos que han cometido.

Se debe permitir insertar, modificar, eliminar y consultar la información de los ciberdelincuentes, la eliminación solo se puede realizar en caso que este ciberdelincuente no esté asociado a ningún ciberataque. No se puede modificar la información del código de ciberdelincuente.

3.3. Registro de información de países

Se debe permitir registrar la información de países, para cada país se debe registrar el código (el código a utilizar es el código de los teléfonos de cada país para utilizar en llamadas internacionales), nombre del país, cantidad de habitantes, continente al que pertenece.

Para consultar los códigos definidos de forma estándar para cada país, pueden consultar la siguiente página: https://country-code.cl/es/

La información de los países debe registrarse en un árbol binario de búsqueda, utilizando el código como llave para insertar en el árbol.

Se debe permitir que se inserte, modifique, elimine y consulte la información de los países registrados. La información del árbol debe visualizarse de dos formas: un listado (utilizando el recorrido en orden) y debe visualizarse la jerarquía del árbol construido.

3.4. Gestión de información de ciberataques

El sistema debe permitir que se gestione la información de un ciberataque dado, para el registro de un ciberataque se debe indicar el nombre del país de origen del ataque, el nombre del país de destino, el tipo de ciberataque dado, el ciberdelincuente que realizó el ataque, la cantidad de datos en gigabytes que fueron afectados en dichos ciberataques, el tiempo en segundos que tardó el ciberataque.

La información de los ciberataques se registrarán en un **grafo etiquetado dirigido (implementado con listas de adyacencia)**, el nodo del grafo tendrá la información del nombre del país, y en las etiquetas de las aristas se indicará el resto de información: tipo de ataque, ciberdelincuente, cantidad de datos en gigabytes que fueron afectados y el tiempo en segundos que tardó el ciberataque. Para registrar la información del ciberataque se debe crear el nodo del país de origen y de destino en caso que no exista aún en el grafo y luego crear la arista indicando el país de origen y destino del ataque para saber la dirección de la arista, y la información de la etiqueta de la arista.

En caso que el país de origen y de destino ya estén registrados en el grafo, solamente debería crearse la arista.

En el sistema debe permitirse registrar un ciberataque, editar la información de un ciberataque previamente registrado y eliminar la información de un ciberataque, o de todo un país registrado en el grafo. También debe permitir consultar toda la información registrada en el grafo.

Cada vez que se registra un ciberataque, se debe permitir registrar un mensaje de seguridad de notificación de ciberataque. El detalle de esta funcionalidad se indica en la siguiente sección del documento.

3.5. Registro de mensaje de seguridad de notificación de ciberataque

El sistema permitirá que se registre un mensaje de seguridad para notificar que se dio un ciberataque. Cuando se genera un mensaje, se debe indicar el país al que va dirigido el mensaje (país que recibe el ataque) y el detalle del mensaje. El mensaje debe encriptarse utilizando algún algoritmo de encriptación (el grupo puede seleccionar el algoritmo a utilizar).

La información de los mensajes enviados se debe registrar en una pila, y posteriormente se debe permitir consultar el mensaje, al hacer esta consulta se debe desencriptar el mensaje.
Se debe permitir consultar toda la pila visualizando los mensajes encriptados, y se debe permitir hacer pop en la pila, y al hacer esta operación se descripta el mensaje y se muestra.

3.6. Simulación de ciberataques

El sistema debe permitir que se realice una simulación de ciberataques, para esto se debe indicar el número de ciberataques que se generará en la simulación, para cada ciberataque que se registra se debe hacer lo siguiente:

1- Generar un número aleatorio en el rango de los códigos de teléfonos que tienen los países. Este código corresponde al del país de origen del ciberataque, se debe verificar que el código obtenido esté registrado dentro del árbol que contiene información de países, en caso que no exista, se debe generar otro número aleatorio hasta que se encuentre un número asociado a un país que sí esté registrado.
2- Se repite el paso 1 para generar el código del país de destino del ciberataque, el código de origen y de destino podría ser el mismo.
3- Generar un número aleatorio para indicar el nombre del tipo de ciberataque, el número generado debe estar en el rango de los códigos asociados a los tipos de ciberataques registrados en la funcionalidad 3.1
4- Generar un número aleatorio para indicar el nombre del ciberdelincuente, el número generado debe estar en el rango de los códigos asociados a los ciberdelincuentes registrados en la funcionalidad 3.2
5- Generar un número aleatorio para indicar la cantidad de datos afectados en el ciberataque.
6- Generar un número aleatorio para indicar la cantidad de tiempo que duró el ataque.
7- Registrar el ciberataque en el grafo de ciberataques
8- Repetir los pasos del 1 al 7 según la cantidad de ciberataques indicado al inicio de la simulación.

Al finalizar la simulación se debe mostrar el grafo después de la simulación, se debe resaltar de alguna forma los ciberataques resultado de la simulación.

3.7. Obtener rutas de ciberataques

En esta funcionalidad el sistema debe permitir aplicar el algoritmo de Dijkstra para obtener cuál es la ruta más corta que pueden tomar los ataques generados desde un país destino dado, para este algoritmo se toma la información del tiempo en segundos que tarda un ciberataque y se pueden tomar en cuenta todos los diferentes tipos de ciberataques que son generados desde un país en particular.

3.8. Análisis de datos

Se deben mostrar las siguientes estadísticas:

a. Cantidad total de ciberataques enviados.
b. Cantidad total de ciberataques recibidos.
c. Cantidad total de ciberataques enviados y recibidos por país.
d. Cantidad de ciberataques enviados y recibidos por tipo de ciberataque.
e. Cantidad de ciberataques enviados por ciberdelincuente.

f. Top 3 de países con mayor cantidad de ataques recibidos.
g. Top 3 de ciberdelincuentes que han enviado más cantidad de ataques.

4. Aspectos técnicos

El proyecto deberá estar escrito en el lenguaje de programación C y debe mostrar la información en consola y contar con un menú para ejecutar las diferentes funcionalidades planteadas en esta especificación

En caso de requerir librerías externas adicionales para compilar y ejecutar el programa, deberán especificarlo en la documentación, ya que de lo contrario se descontarán puntos en la evaluación.

Para las funcionalidades en que no se indicó explícitamente la estructura de datos a utilizar el grupo tiene la libertad de seleccionar la estructura que considere más apropiada.

Se recomienda utilizar la plataforma GitHub o GitLab, estas plataformas sirven para desarrollar código de forma colaborativa y control de versiones del mismo, pueden obtener información y descargar las herramientas en los siguientes sitios:

- GitHub: https://github.com/
- GitLab: https://about.gitlab.com/

5. Documentación

La documentación es un aspecto de gran importancia en el desarrollo de programas, especialmente en tareas relacionadas con el mantenimiento de los mismos.

Para la documentación interna, deberán incluir comentarios descriptivos para cada función, con sus entradas, salidas, y restricciones.

La documentación externa deberá incluir:

1. Portada.
2. Manual de usuario: requisitos (librerías utilizadas), instrucciones de uso, ejecución y compilación.
3. Descripción del problema a resolver.
4. Diseño del programa: decisiones de diseño, uso de estructuras de datos, uso de librerías. Justifique todas sus decisiones.
5. Pruebas de funcionalidad: incluir *screenshots*.
6. Análisis de resultados: objetivos alcanzados, objetivos no alcanzados, y razones por las cuales no se alcanzaron los objetivos (en caso de haberlos). Indicar la distribución de funciones entre los integrantes del grupo.
7. Aspectos relevantes y lecciones aprendidas: Debe prepararse un listado de las lecciones aprendidas producto del desarrollo de la tarea programada (al menos 3 por cada estudiante). Las lecciones aprendidas pueden ser de carácter personal y/o técnico que involucre aspectos que han logrado un aprendizaje en temas de investigación, desarrollo de habilidades técnicas y habilidades blandas como trabajo en equipo, comunicación, forma de expresar ideas, etc.
8. Evidencias de uso de Github.

6. Evaluación

1. Documentación externa 12%.
2. Registro de tipo de ciberataque 3%
3. Registro de ciberdelincuente 3%
4. Registro de información de países 10%
5. Gestión de información de ciberataques 15%
6. Registro de mensaje de seguridad de notificación de ciberataque 13%
7. Simulación de ciberataques 15%
8. Obtener rutas de ciberataques 15%
9. Análisis de datos 14%

7. Aspectos administrativos

1. Debe crear un archivo .zip ("PP2.zip") que contenga únicamente un archivo **info.txt** y 2 carpetas llamadas **documentacion** y **solucion_computacional**, en la primera deberá incluir el documento de *word* o *open office* (no pdf) solicitado y en la segunda los archivos y/o carpetas necesarias para la implementación de esta tarea. El archivo **info.txt** debe contener la siguiente información (cualidades):
    a. Nombre del curso
    b. Número de semestre y año lectivo
    c. Nombre del Estudiante x3
    d. Número de carnet x3
    e. Número de tarea programada
    f. Fecha de entrega
    g. Estatus de la entrega (definido por el responsable de la implementación de la tarea): [Deplorable|Regular|Buena|MuyBuena|Excelente|Superior]

2. Deberá subir el archivo antes mencionado al TEC Digital en el curso de ALGORITMOS Y ESTRUCTURAS DE DATOS GR 01, en la asignación llamada "Proyecto Programado 2" debajo del rubro de "Proyectos programados". El proyecto debe entregarse el **jueves 16 de junio del 2022 antes de las 11:55pm**

3. Dentro de la carpeta de **solucion_computacional,** deberá incluir un archivo .txt (**PrimerNombreMiembro1.PrimerNombreMiembro2. PrimerNombreMiembro3.txt**) que contenga todo el texto de la solución del o de los archivos presentados (las implementaciones)**.** Este archivo puede ser revisado en el sistema de Control de Plagio del TEC Digital. **Todo el código de cada proyecto debe ser 100% original, y no se va a tolerar el plagio.** Este archivo también deberá ser subido al TEC Digital en el curso de ALGORITMOS Y ESTRUCTURAS DE DATOS GR 01, en la asignación llamada "Proyecto Programado 2 (archivo TXT)" debajo del rubro de "Proyectos programados". Se deberá subir el archivo siguiendo los mismos rangos de tiempo que los descritos en el punto anterior.

4. Los proyectos deberán ser revisados con el profesor o el asistente. Todos los miembros del grupo deberán participar de la revisión, ya que de lo contrario no se les asignará el puntaje correspondiente. La nota de la revisión es individual, el resto de la nota es grupal.

5. El proyecto se hará en grupos de 3 personas, solamente.

6. La tarea vale un 20% de la nota del curso.

7. A más tardar el día martes 24 de mayo del 2022 se deben registrar en el siguiente enlace para indicar el nombre de los integrantes del grupo: TI2402 - Proyecto 2 - Grupos

   Esta información es necesaria para crear los grupos en el TEC Digital. Si no se registran en el documento NO podrán entregar el proyecto.

8. Condiciones

Este proyecto programado se rige por las siguientes condiciones:

1. El desarrollo del proyecto es estrictamente en grupos de 3 integrantes.
2. Debe cumplir con todo lo indicado en esta especificación.
3. Deberá entregarse en tiempo y forma según el plazo establecido por los profesores al momento la lectura de este documento.
4. No se recibirán proyectos fuera de la fecha/hora indicadas, tampoco se recibirán por correo electrónico ni otro medio que no sea el TECDigital. **Todo trabajo entregado después de la fecha y hora indicada tendrá una nota de cero.**
5. Si se detecta copia o plagio se procederá según lo indicado en el Reglamento del Régimen de Enseñanza Aprendizaje del ITCR.
6. Las citas de revisión del proyecto se asignarán después de la entrega del mismo.

Nota: El incumplimiento de alguna condición implicará una calificación de cero.

IMPORTANTE: CONOCIMIENTO DE LA SOLUCIÓN PRESENTADA.

En la revisión del trabajo, los estudiantes deben demostrar un completo dominio de la solución implementada, tanto desde el punto de vista técnico (uso de herramientas) como de la funcionalidad del proyecto. La revisión se puede hacer individualmente o en grupos, examinando la solución o temas específicos aplicados en el proyecto. Todos los integrantes del grupo deben tener el mismo conocimiento de la solución presentada. Recuerde que de no contestar las preguntas durante la revisión, se puede descontar hasta un 15% de la nota obtenida de forma grupal.