**EXAMEN PARCIAL**

**SISTEMAS OPERATIVOS**

1. Examen grupal.
2. Fecha de entrega del examen a los estudiantes miércoles 29 de julio a las 18:00 pm
3. Fecha de envío del examen al profesor, sábado 1 de agosto a las 23:59 pm
4. Entregar un solo documento en pdf, con todos los detalles del procedimiento

**Introducción**

Una de las funcionalidades más importantes de los sistemas operativos es la gestión de interrupciones, la gestión de interrupciones permite la gestión de eventos externos al computador que se presentan de forma asíncrona.

**Objetivo**

El objetivo de este examen es diseñar, construir, verificar y documentar un **procedimiento** que permita implementar un keylogger residente en memoria, haciendo uso del Python. No se permite el uso de otro lenguaje de programación.

Opcionalmente use las siguientes librerías:

* signal
* pyHook

**Actividades para desarrollar por el grupo**

* Crear una cuenta en github donde colocaran todos los resultados de su examen.
* Preparar la especificación funcional del **procedimiento** a construir.
* Construir el **procedimiento**.
* Probar el **procedimiento** en 2 escenarios relacionados a:

1. Usuario de un procesador de textos por ejemplo una secretaria que usa el Microsoft Word
2. Usuario de un editor de programas en Python.

* Preparar un informe conteniendo el proceso de construcción del procedimiento, según la estructura del anexo 1, separe cada sección con un salto de página, documento a doble columna.
* Enviar la cuenta de github a su profesor, con la lista de todos los integrantes del grupo.

**Funcionalidad mínima del procedimiento, este debe ser ampliado luego de leer las referencias entregadas.**

El procedimiento debe permitir:

* Captar todas las letras del abecedario en mayúscula y minúscula, incluyendo números y caracteres especiales.
* Almacenar en un archivo cada uno de los caracteres incluyendo el momento (fecha, hora) en que el usuario presiona la tecla y deja de presionar la tecla.
* Que opere residente en memoria, el programa debe de ejecutarse al momento iniciar la operación del computador.
* Operar indistintamente en Linux o en Windows.
* Capturar los datos computador: arquitectura, id del sistema operativo, nombre del computador, IP, nombre del usuario.
* Enviar los datos captados a un directorio residente en la nube, establezca una frecuencia de envío, para ello puede hacer uso de la librería flask, que permite implementar web services.
* El procedimiento no debe de ejecutar ningún calculo adicional al momento de leer los datos, estos deben ser enviados directamente a la nube.

**Referencias**

* El grupo debe de leer las siguientes referencias para desarrollar este examen.

https://drive.google.com/drive/folders/1ujd80QV8kG0IeK-uDUKsvD34bxwEhlTL?usp=sharing

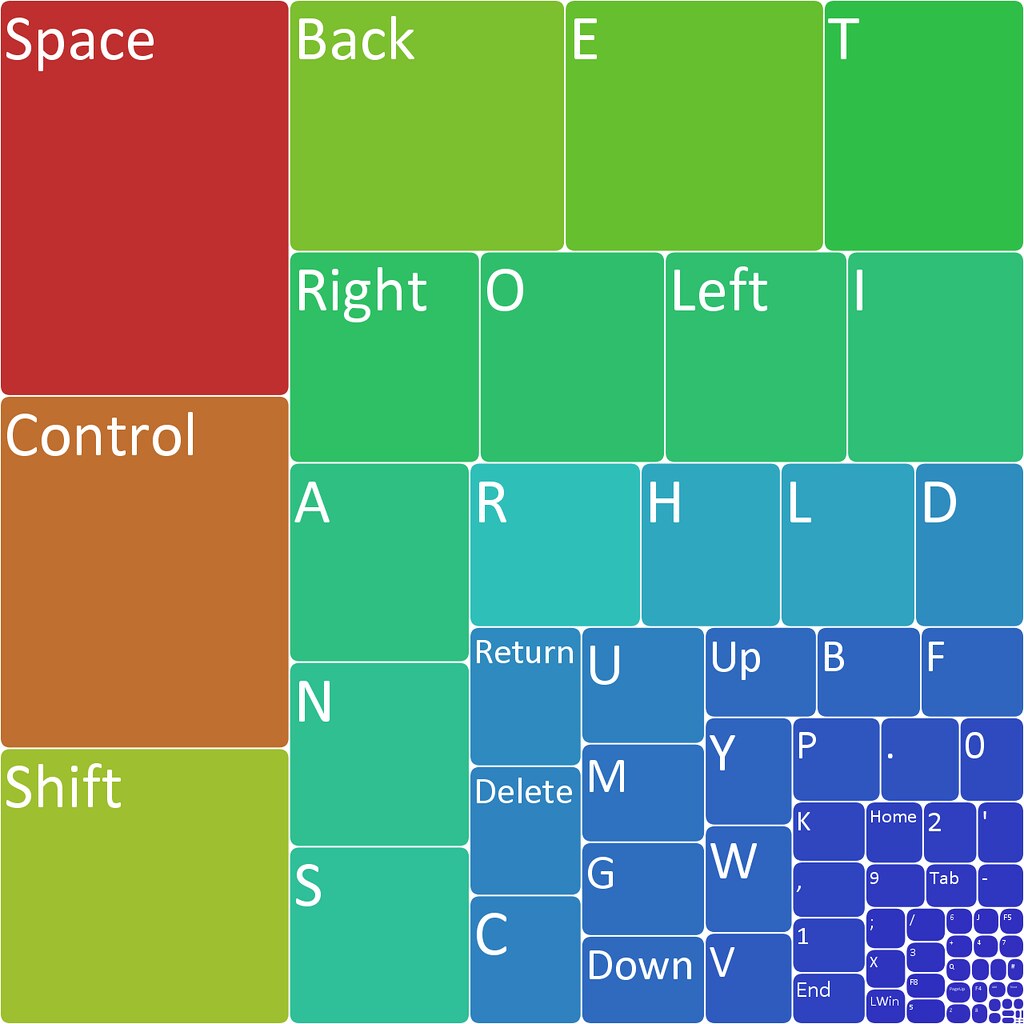
**Escenarios de prueba.**

El grupo prueba el procedimiento en 2 escenarios posibles, con esta finalidad el grupo desarrolla las siguientes actividades:

* Cada escenario implica que el usuario es una persona asume el rol de la persona que usa el programa de software indicado.
* Luego de captar los datos, el grupo extrae indicadores desde los datos captados con el fin de extraer los patrones.
* Los patrones de operación pueden ser los siguientes:

1. Teclas presionadas en un periodo de tiempo.

* El patrón se extrae calculando la distribución de frecuencias de las teclas.



**Anexo 1**

**CONTENIDO DEL INFORME EN FORMATO DE PAPER**

1. TITULO, AUTOR Y FILIACIÓN
2. Resumen
3. Introducción
4. Palabras claves
5. ENUNCIADO DEL EXAMEN
6. Colocar este documento
7. PLANTEAMIENTO DEL PROBLEMA

(use las referencias entregadas en este examen u otros que pueden identificar)

1. Interrupciones.

* Tabla de interrupciones
* Cómo se gestiona una interrupción
* Tipos de interrupciones (por ejemplo, de hardware, de software)
* Habilitación de interrupciones
* Enmascarado de interrupciones

1. Eventos asíncronos

* Gestión de eventos asíncronos en C.
* Gestión de eventos asíncronos en Python.

1. Librerías en Python.

* signal
* pyHook

1. Keyloggers.

* Tipos de keyloggers.
* Spywares
* Detección de keyloggers.

1. Estrategias para la implementación de keyloggers
2. ARQUITECTURA DEL HARDWARE (de todo el sistema)
3. Arquitectura de hardware

* Especificar los computadores involucrados en el sistema.
* Sistema operativo
* IP
* Protocolos de comunicaciones usados.
* Otros

1. ARQUITECTURA DEL SOFTWARE DE BASE (por cada computador involucrado)
2. Especificar el software de base que permite la operación del procedimiento
3. ARQUITECTURA DE LOS COMPONENTES DEL PROCEDIMIENTO (por cada computador involucrado)
4. Computador 1

* Diagrama de alto nivel (nivel 0)
* Diagramas de nivel 1.
* Diagramas de nivel 2.

1. Computador 2

* Diagrama de alto nivel (nivel 0)
* Diagramas de nivel 1.
* Diagramas de nivel 2.

La arquitectura debe ser congruente con el código fuente entregado, cada componente del procedimiento debe ser una función. El componente debe tener el mismo nombre de la función.

1. FUNCIONALIDAD DEL PROCEDIMIENTO (keylogger)

La funcionalidad debe ser congruente con los componentes del procedimiento.

1. RESULTADOS DE LAS PRUEBAS

Resultados obtenidos por cada escenario, explicar los resultados.

1. CONCLUSIONES

Extraiga conclusiones significativas.

Una conclusión es un aprendizaje logrado.

Es recomendable expresar sus conclusiones en términos numéricos.

Una conclusión no es una opinión.

Una conclusión no es la dificultad que han tenido para construir el procedimiento

1. REFERENCIAS USADAS

Bibliografía leída, incluya solo la bibliografía que ha referenciado desde su informe.

1. CÓDIGO FUENTE

* Presente el diagrama de clases del procedimiento.
* El código fuente debe ser Identado y debe ser leíble por humanos (espaciado simple, letra Currier New de tamaño 8 a una sola columna)
* Tengo cuidado en el tamaño de los tabs.
* Encuadre cada función o método en un “cuadro”.
* Hacer que el programa principal se denomine mainProcess

**No entregar archivos adjuntos, todo debe de estar en un solo pdf.**

**Nombre del archivo: apellido1.apellido2.apellido3.apellido4.exp.st324.2020i.pdf**

Coloque su código fuente como un anexo, de tal forma que sea “leíble”, asegúrese que quien lee su código lo entienda, no solo lo pegue y espere que su lector lo interprete, verifique que la letras sean de tamaño apropiado, que el tipo de letra sea Currier New, verifique el espaciado.

Los grupos de trabajo que redacte el informe final en latex tendrán 3 puntos adicionales sobre la nota del examen (máximo 19). Demostrar enviando el link de las fuentes.

<https://www.overleaf.com/>

<https://es.sharelatex.com/>