

## **1era. Olimpiada Nacional de Informática**

### **Prueba de Ejemplo**

#### **Prueba de Pericia**

##### **Objetivo**

En esta prueba se evaluarán los conocimientos prácticos sobre el hardware del computador, software e Internet. Cada equipo deberá contestar a cada una de las preguntas en la hoja de respuestas que se adjunta. En esta hoja de respuestas además se identificarán los participantes de cada equipo.

**Puntuación:** La puntuación de cada pregunta o ejercicio realizado, está indicado en cada enunciado. Las preguntas no realizadas o realizadas de forma incorrecta no puntúan. La puntuación máxima que se puede obtener en esta prueba es de 25 puntos. Con el objetivo de resolver posibles empates a puntos entre dos o más equipos, se registrará también el tiempo empleado en su resolución.

#### **Parte I (13 puntos)**

Las siguientes preguntas se refieren a la configuración del computador en el que realizan las pruebas. Puedes usar Internet para obtener información e incluso descargar herramientas siempre y cuando no sea necesario instalarlas, ya que no tendrás permiso para hacerlo.

1. (1 punto) Marca, modelo y frecuencia del procesador indicada por el sistema operativo.
2. (2 puntos) Número de versión del controlador de la tarjeta gráfica.
3. (2 puntos) Dirección IP de la puerta de enlace predeterminada.
4. (2 puntos) ¿Con qué teclas de acceso rápido, puedo cambiar a la función de múltiples escritorios?
5. (2 puntos) Valor de la variable de entorno PROCESSOR\_LEVEL.
6. (2 puntos) ¿Cuántos bytes ocupa en el disco duro la carpeta C:\ONI\_Test?
7. (1 punto) ¿Cómo se llama el jugador que logró ganarle en el cuarto juego a AlphaGo?
8. (1 punto) ¿Cómo se llama el creador del Sistema Operativo Linux?

#### **Parte II (12 puntos)**

En una empresa de tecnológica se quiere hacer un estudio del tiempo de los computadores que están inactivos durante la semana para analizar cuánto se podría ahorrar si se apagasen los equipos cuando no están utilizados. El archivo inactivos.csv recoge, para cada hora de cada día de la semana, la longitud de cada intervalo de inactividad que se ha detectado. En cada fila se indica el día de la semana y la hora en el que empiezan los intervalos y luego una lista con la duración de los intervalos en segundos.

Contestar las siguientes preguntas, utilizando como software de apoyo una hoja de cálculo o haciendo uso de un lenguaje de programación:

1. (1 punto) ¿Cuántos intervalos hay en total?
2. (2 puntos) ¿Cuál es el intervalo más largo? Dar la respuesta en días con dos decimales.
3. (2 puntos) ¿A qué hora de qué día de la semana se ha detectado el comienzo de más intervalos de inactividad? ¿Cuántos intervalos son?
4. (2 puntos) ¿A qué hora de qué día empiezan los intervalos de inactividad que dan una inactividad total mayor?
5. (1 punto) ¿En qué día de la semana hay menos intervalos?
6. (1 punto) ¿Cuánto suma la inactividad que empieza ese día? Dar la respuesta en días con dos decimales.
7. (1 punto) ¿Cuántos intervalos son menores de 20 minutos?
8. (2 puntos) Si los PCs tuviesen un temporizador que después de 20 minutos de inactividad apagara el PC, ¿cuánta inactividad se eliminaría el domingo a las 7 de la mañana? Responder en segundos.

## **Prueba “Aprender a Aprender”**

Descripción de la prueba:

La prueba consiste en tres retos que deben realizarse de manera secuencial, dado que para poder hacer uno se debe haber completado el anterior.

La solución a estos retos, así como cualquier información que se pida, deberá subirse al sistema de corrección, que validará la solución y le informará de si es correcta o no.

En caso de que lo sea, se registrará el momento en que se haya superado el reto.

En esta prueba se valorará tanto el tiempo requerido para resolver los retos como la simplicidad y elegancia de la solución ofrecida.

Cada reto correctamente solucionado obtendrá puntos según el tiempo invertido en superarlo. Al que menos tiempo haya invertido 25 puntos y luego, en orden temporal 21, 18, 15, 12, 10, 8, 6, 4, 2 y 1.

### **RETO 1 - Obtención de credenciales de acceso**

Accede a la dirección web 172.10.15.1

En esa dirección hay una zona privada, de acceso para clientes. Intenta obtener un nombre de usuario y una contraseña para acceder a dicha zona privada de la página web. Para hacerlo, tendrás que validar si hay alguna vulnerabilidad en el acceso a la zona privada.

### **RETO 2 - Obtención del listado de cuentas de la empresa.**

Una vez dentro que hayas conseguido entrar en la zona privada, hazte con el listado de cuentas de la empresa. Como la aplicación no te permite descargar nada, tendrás que copiarlo y generar un archivo de texto plano, donde deben pegarlo como respuesta. El archivo generado deberá ser subido al sistema de corrección

### RETO 3 - Código Turing

Alan Turing fue un matemático, lógico, científico de la computación, criptógrafo y filósofo británico. Fue uno de los padres de la ciencia de la computación y está considerado como uno de los personajes más importantes en la historia de la informática. Durante la segunda guerra mundial fue uno de los principales artífices de los trabajos para conseguir descifrar los códigos secretos de la máquina Enigma y permitir a los aliados anticipar los ataques y movimientos militares nazis.

Entre sus investigaciones en el campo de la criptografía, se encuentra el Código Turing, un algoritmo de cifrado que transforma un mensaje legible en un galimatías de forma que sea incompresible para toda persona que no disponga de la clave secreta para descifrarlo.

Para realizar una versión simplificada de este algoritmo, el primer paso es convertir el mensaje de texto original en un número, para poder hacer operaciones matemáticas con él. Una manera de conseguirlo es cambiar cada carácter del mensaje por su código ASCII (número decimal de 3 dígitos). A continuación, se proporciona un trozo de la tabla ASCII y un ejemplo de conversión.

065	A	097	α
066	B	098	b
067	C	099	c
068	D	100	d
069	E	101	e
070	F	102	f
071	G	103	g
072	H	104	h
073	I	105	i
074	J	106	j
075	K	107	k
076	L	108	l
077	M	109	m
078	N	110	n
079	O	111	o
080	P	112	p
081	Q	113	q
082	R	114	r
083	S	115	s
084	T	116	t
085	U	117	u
086	V	118	v
087	W	119	w
088	X	120	x
089	Y	121	y
090	Z	122	z

POR EJEMPLO:

Hola → 072111108097

El proceso de cifrado funciona de la siguiente forma.  $m$  es el mensaje sin cifrar (el que queremos que sea secreto),  $m^*$  es el mensaje cifrado (un galimatías incomprendible, que otra persona podría leer, pero no entendería a menos que disponga de la clave necesaria para descifrarlo) y  $k$  es la clave de cifrado y descifrado.

Antes de enviar cualquier mensaje, tanto el remitente como el destinatario deben conocer la clave de cifrado. Para la clave se debe utilizar un número primo, por ejemplo 11.

**Cifrado:** El remitente cifra el mensaje  $m$  calculando ( $\cdot$  representa la multiplicación):

$$m^* = m \cdot k$$

**Descifrado:** El destinatario descifra el mensaje  $m^*$  calculando:

$$m^* / k = m$$

Por ejemplo, supongamos que se quiere transmitir el mensaje  $m = \text{Hola}$  usando la clave  $k = 11$ .

$$m^* = m \cdot k = 0721111108097 \cdot 11 = 793222189067$$

Una vez cifrado el mensaje original,  $m^* = 793222189067$  puede ser transmitido sin temor a que alguien lo pueda leer.

**Pero, ¿qué sucede si se envía un segundo mensaje usando la misma clave?**

$$m_1^* = m_1 \cdot k \quad m_2^* = m_2 \cdot k$$

**El máximo común divisor de los dos mensajes cifrados,  $m_1^*$  y  $m_2^*$ , es la clave secreta  $k$ .** De este modo, si dos mensajes son interceptados, es posible recuperar la clave secreta y leer todos los mensajes.

La treceava de las cuentas de la empresa es el objetivo fundamental a obtener. Pero está encriptada con el algoritmo simplificado de Turing. Por ello, deben averiguar cuáles son las dos palabras claves de esa cuenta, descryptando la información obtenida de la lista.

Partiendo de la premisa, a continuación, los dos siguientes mensajes cifrados mediante el algoritmo descrito anteriormente, que con las palabras clave

357303324324 300333330303

Se pide descifrar ambos mensajes para saber cuáles son los mensajes originales indicando además cuál es la clave secreta.

**Nota:** Producto de las investigaciones llevadas a cabo por Alan Turing en criptografía se determinó que nunca se deben de enviar varios mensajes cifrados con la misma clave. La clave compartida por remitente y destinatario no se utiliza para cifrar, sino que se utiliza para generar nuevas claves temporales de cifrado.