



Unidad 1: BITS Y BYTES

BLOQUE I - Los fundamentos
de la Informática y
de la Seguridad

CONTENIDOS

1. Introducción.
2. Representación de la información.
3. Código binario, hexadecimal y ASCII.
4. Imágenes y gráficos.
5. ¿Qué es la criptografía?
6. Esteganografía.

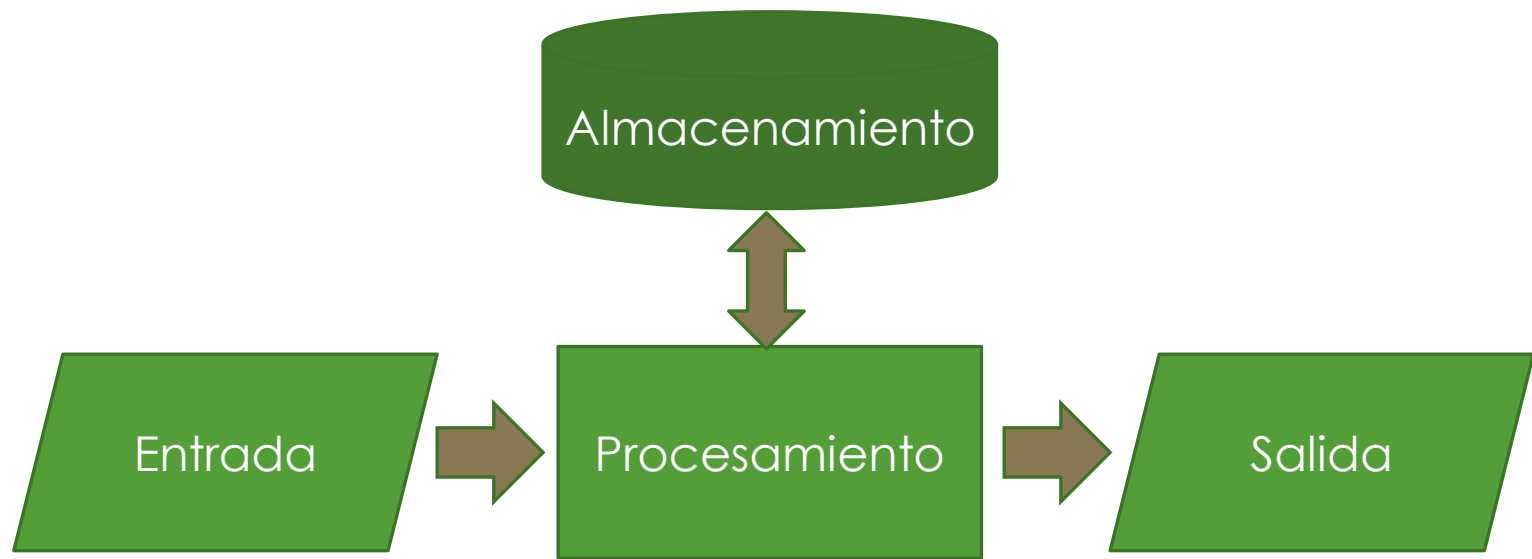
1. Introducción

◦ ¿Qué tienen en común?



IC, Beltrán 2022-2023

1. Introducción



Operaciones aritméticas y lógicas
Transformaciones y desplazamientos
Ordenaciones y búsquedas

1. Introducción

Hardware

Software

Comunicaciones

Datos/información

2. Representación de la información

Cinco aves



IIII para las culturas más antiguas

V para los romanos

5 para nosotros

Pero también 101_2 o 12_3

¿Qué significa esto? En base 2, en base 3, etc.

2. Representación de la información

- Nosotros utilizamos habitualmente el sistema decimal: sistema de numeración posicional en el que las cantidades se representan utilizando como base aritmética las potencias del número diez (unidades, decenas, centenas, millares, etc.).
- En Informática se utiliza el sistema binario: la base aritmética son las potencias del número 2.
 - Todo se representa con 0s y 1s.

Número en binario	Operaciones	Número en decimal
0	0×2^0	0
1	1×2^0	1
10	$1 \times 2^1 + 0 \times 2^0$	2
11	$1 \times 2^1 + 1 \times 2^0$	3
100	$1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$	4
101	$1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$	5
110	$1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$	6
111	$1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$	7

2. Representación de la información

- Pregunta: ¿Qué número es el 110010100_2 ?



2. Representación de la información

○ Respuesta:

$$110010100_2 =$$

$$\begin{aligned} &1 \times 2^8 + 1 \times 2^7 + 0 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + \\ &\quad 1 \times 2^2 + \\ &\quad 0 \times 2^1 + 0 \times 2^0 \\ &= 256 + 128 + 16 + 4 = 404 \end{aligned}$$



Os será muy útil saber las potencias de 2, las doce primeras: 4096, 2048, 1024, 512, 256, 128, 64, 32, 16, 8, 4, 2 y 1.

2. Representación de la información

- ¿Cómo se traducen estos 0s y 1s a algo físico dentro de un sistema informático?



No pasa corriente/pasa corriente
No se almacena carga/se almacena carga
Carga negativa/carga positiva
Agujero/elevación en un material

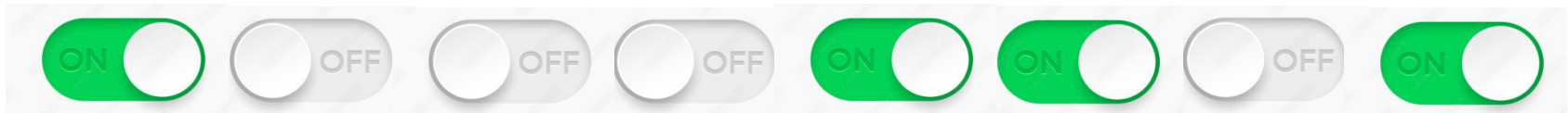
2. Representación de la información

- La unidad mínima de información en un computador es un 0 o un 1: un bit.
- Un grupo de 8 bits es denominado un Byte.



= 0, 1 bit (b)

= 1, 1 bit (b)



10001101, 1 Byte (B)

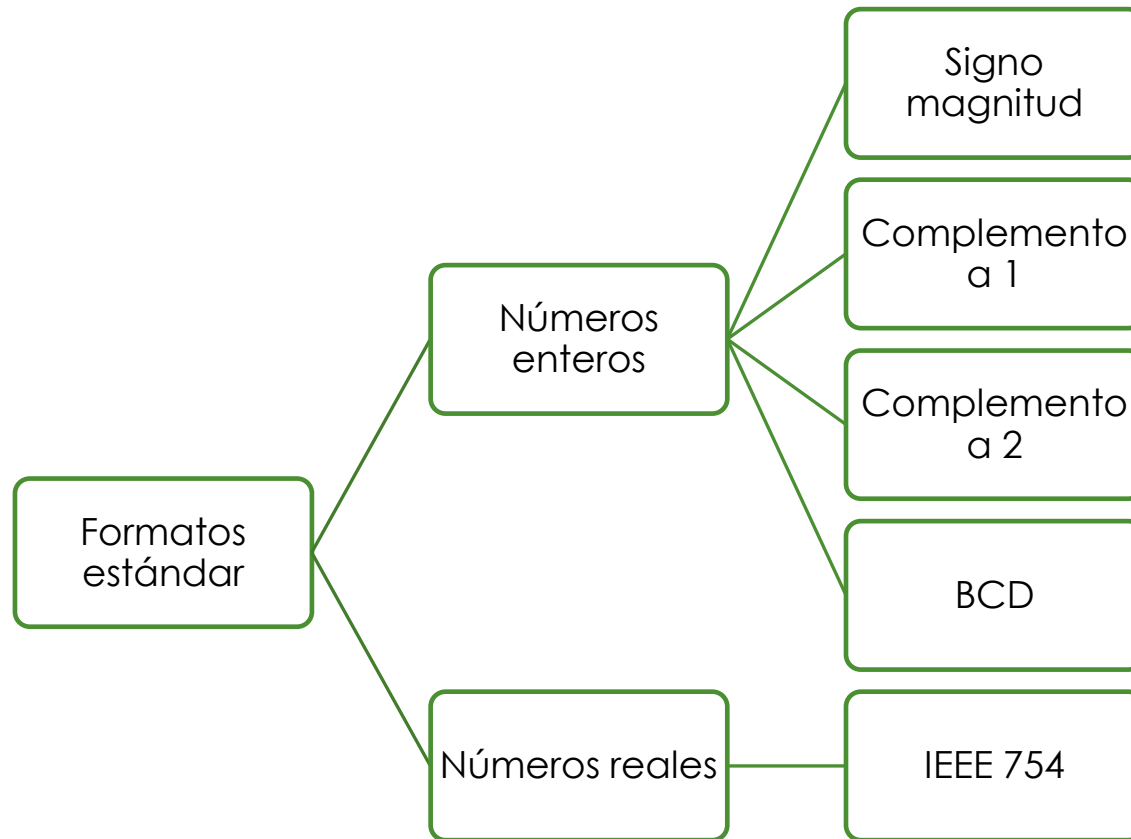
2. Representación de la información

Cantidad de información	Equivalencia	En Bytes
Byte	8 bits	1 B
Kilobyte	1024 bytes	1024 B
Megabyte	1024 KB	1.048.576 B
Gigabyte	1024 MB	1.073.741.824 B
Terabyte	1024 GB	1.099.511.627.778 B
Petabyte	1024 TB	1.125.899.906.842.624 B
Exabyte	1024 PB	1.152.921.504.606.846.976 B

3. Código binario, hexadecimal y ASCII

- Una vez que hemos comprendido cómo se procesa y almacena la información en un sistema informático mediante el sistema de numeración binario, debemos saber que es necesario definir formatos estándar para que todos trabajemos de la misma forma.
- Por ejemplo ¿cómo se representa el signo de un número entero, cómo distingo el +1 del -1? ¿cómo se representa un número con decimales?

3. Código binario, hexadecimal y ASCII



3. Código binario, hexadecimal y ASCII

- En muchos casos se manejan grupos de 64, 32 ó 16 ceros y unos (un número, una dirección de memoria, una instrucción en ensamblador).
 - Las arquitecturas actuales suelen tener este ancho, ya lo iréis comprendiendo.
- Para ahorrar espacio y simplificar la representación, se suele recurrir el sistema hexadecimal.
 - Es decir, se trabaja con base 16.

2. Representación de la información

- Pregunta: ¿Cómo representamos el número 110010100_2 en hexadecimal?



2. Representación de la información

- Respuesta:

1. Se agrupan los bits de 4 en 4, si hace falta, se rellena con ceros a la izquierda:

0001 1001 0100

2. Se pasa cada uno de estos grupos de 4 bits al sistema decimal:

1 9 4

3. Como estamos trabajando en base 16, podemos necesitar letras además de números. Por ejemplo:

2. Representación de la información

1111 0111 1101 0110

En hexadecimal sería:

F 7 D 6

Binario	Hexadecimal
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

3. Código binario, hexadecimal y ASCII

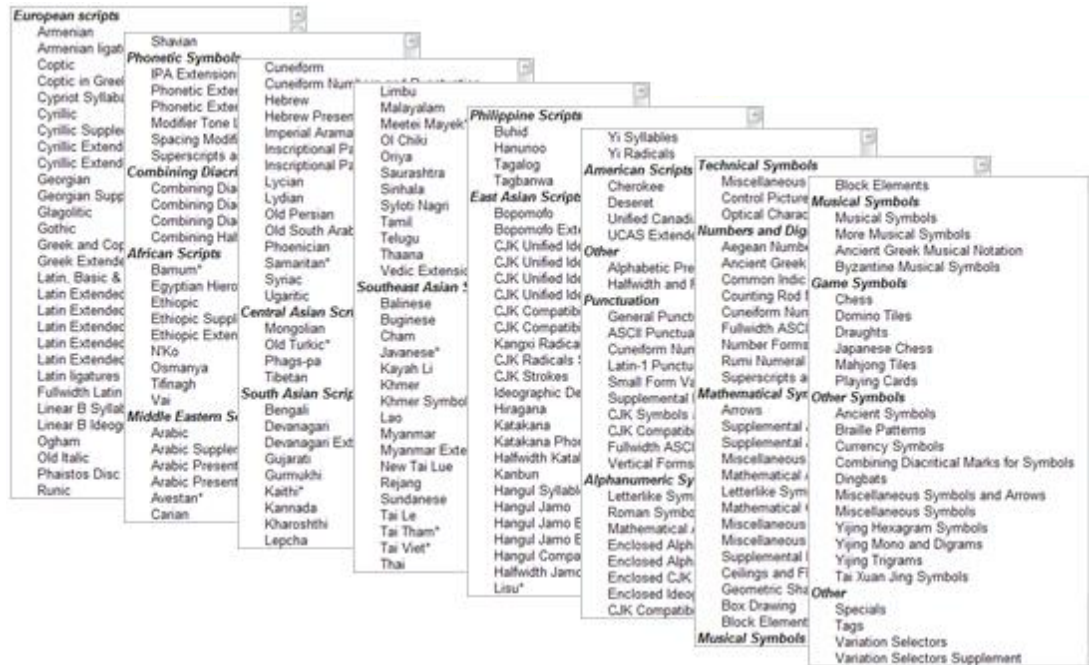
- En un sistema informático también necesitamos manejar caracteres alfabéticos, no sólo numéricos: textos.
- Uno de los códigos de caracteres más extendidos es el ASCII (American Standard Code for Information Interchange), que asigna (versión extendida) a cada carácter una secuencia única de 8 bits (ceros y unos).
- Cómo esto limitaba mucho los caracteres alfanuméricos que se podían representar, poco a poco se ha ido evolucionando hacia el formato Unicode, que puede utilizar hasta 16 dígitos binarios.

Binario	Dec	Hex	Representación
0010 0000	32	20	espacio ()
0010 0001	33	21	!
0010 0010	34	22	"
0010 0011	35	23	#
0010 0100	36	24	\$
0010 0101	37	25	%
0010 0110	38	26	&
0010 0111	39	27	'
0010 1000	40	28	(
0010 1001	41	29)
0010 1010	42	2A	*
0010 1011	43	2B	±
0010 1100	44	2C	ˆ
0010 1101	45	2D	:
0010 1110	46	2E	˙
0010 1111	47	2F	/
0011 0000	48	30	0
0011 0001	49	31	1
0011 0010	50	32	2
0011 0011	51	33	3
0011 0100	52	34	4
0011 0101	53	35	5
0011 0110	54	36	6
0011 0111	55	37	7
0011 1000	56	38	8
0011 1001	57	39	9
0011 1010	58	3A	:
0011 1011	59	3B	:
0011 1100	60	3C	≤
0011 1101	61	3D	≡
0011 1110	62	3E	≥
0011 1111	63	3F	?

Binario	Dec	Hex	Representación
0100 0000	64	40	@
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z
0101 1011	91	5B	ı
0101 1100	92	5C	\
0101 1101	93	5D]
0101 1110	94	5E	^
0101 1111	95	5F	_

Binario	Dec	Hex	Representación
0110 0000	96	60	`
0110 0001	97	61	<u>a</u>
0110 0010	98	62	<u>b</u>
0110 0011	99	63	<u>c</u>
0110 0100	100	64	<u>d</u>
0110 0101	101	65	<u>e</u>
0110 0110	102	66	<u>f</u>
0110 0111	103	67	<u>g</u>
0110 1000	104	68	<u>h</u>
0110 1001	105	69	<u>i</u>
0110 1010	106	6A	<u>j</u>
0110 1011	107	6B	<u>k</u>
0110 1100	108	6C	<u>l</u>
0110 1101	109	6D	<u>m</u>
0110 1110	110	6E	<u>n</u>
0110 1111	111	6F	<u>o</u>
0111 0000	112	70	<u>p</u>
0111 0001	113	71	<u>q</u>
0111 0010	114	72	<u>r</u>
0111 0011	115	73	<u>s</u>
0111 0100	116	74	<u>t</u>
0111 0101	117	75	<u>u</u>
0111 0110	118	76	<u>v</u>
0111 0111	119	77	<u>w</u>
0111 1000	120	78	<u>x</u>
0111 1001	121	79	<u>y</u>
0111 1010	122	7A	<u>z</u>
0111 1011	123	7B	{
0111 1100	124	7C	
0111 1101	125	7D	}
0111 1110	126	7E	~

Unicode es compatible con ASCII, simplemente añade nuevos caracteres y símbolos utilizando para ello más bits



<https://www.w3.org/International/articles/definitions-characters/index.es>

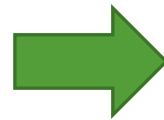
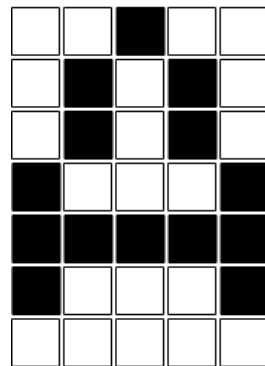
4. Imágenes y gráficos

- Las imágenes y los gráficos también deben representarse con ceros y unos dentro de un computador y también necesitan formatos estándar.
 - JPG, PNG, GIF, etc.
- Se distinguen dos tipos de imágenes:
 - Mapas de bits (producidas por el propio computador o escaneadas, tomadas con una cámara, etc.). Se caracterizan por presentar variaciones continuas en el color, las formas, las texturas, etc.
 - Objetos gráficos o imágenes vectoriales (producidas por el propio computador). Se caracterizan por estar formadas por formas geométricas puras.

4. Imágenes y gráficos

- Mapas de bits

- Se representan con una matriz de píxeles, la imagen se divide en filas y columnas.
- Para cada píxel se almacena, en binario, información sobre el color, su intensidad, transparencia, etc.



```
00100
01010
01010
10001
11111
10001
00000
```

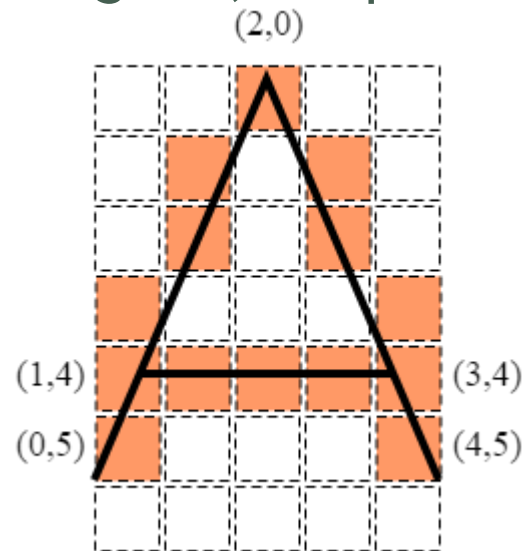
PNG
JPG
GIF

https://commons.wikimedia.org/wiki/File:Bitmap_vs_vector.png

IC, Beltrán 2022-2023

4. Imágenes y gráficos

- Objetos gráficos o imágenes vectoriales
 - En este caso lo que se representa en binario son tipos de formas geométricas, sus tamaños, sus rotaciones y ángulos, sus posiciones relativas, etc.



EPS
PDF

https://commons.wikimedia.org/wiki/File:Bitmap_vs_vector.png

IC, Beltrán 2022-2023

5. ¿Qué es la criptografía?

- La criptografía es una de las ciencias más antiguas, se utiliza desde antes de Cristo con objetivos militares y estratégicos.
- Es una de las herramientas fundamentales de la ciberseguridad actual.



Asignatura completa: **Criptografía**,
este mismo curso pero en el
segundo cuatrimestre

5. ¿Qué es la criptografía?

Criptografía: Del griego kryptós (oculto) y gráphein (escribir), es el estudio de los principios y mecanismos necesarios para establecer procesos de cifrado, descifrado y generación de claves necesarias para ellos.

Criptoanálisis: Del griego kryptós (oculto) y analýein (desatar), es el estudio de los principios y mecanismos necesarios para descifrar mensajes sin conocer las claves de cifrado

5. ¿Qué es la criptografía?

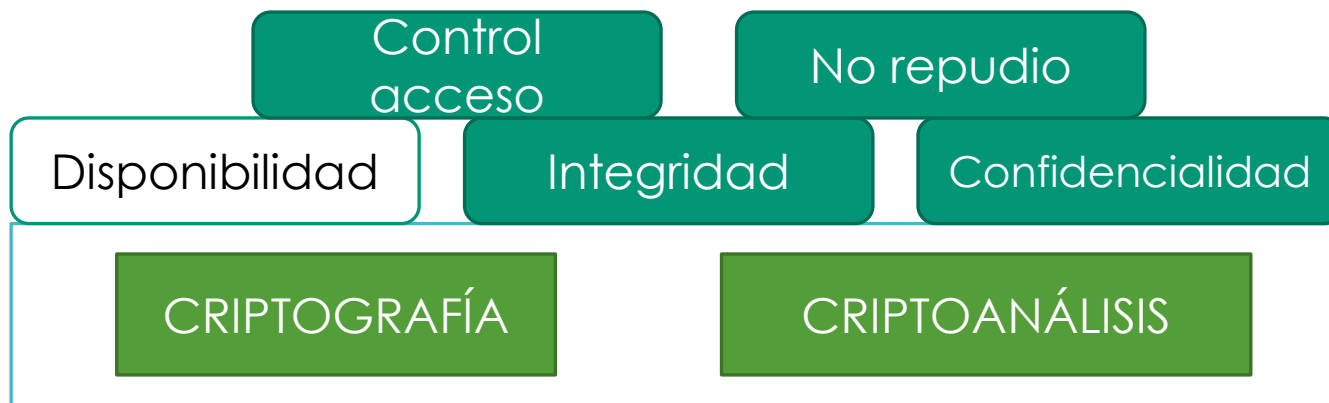
- Se puede considerar la criptografía como una rama de las Matemáticas, y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.

Datos
almacenados

Datos en
tránsito

Datos que se
están
procesando

5. ¿Qué es la criptografía?



Mecanismos clásicos/modernos
Cifrado flujo/bloque
Clave privada/pública
Protocolos, firmas, autenticación, certificados

Internet, redes sociales, métodos de pago, móviles

5. ¿Qué es la criptografía?

- Según Shannon (padre de la criptografía moderna), un buen criptosistema es el que cumple estas características:

Los recursos y esfuerzo consumido para cifrar/descifrar deben ajustarse al grado de seguridad necesario

Los mecanismos de cifrado/descifrado y generación de claves deben ser sencillos

La implementación de los algoritmos debe ser sencilla

Un error en el cifrado no debería propagarse y corromper el resto del mensaje

El tamaño del mensaje cifrado no debería superar al del mensaje original

6. Esteganografía

- La esteganografía es la ciencia que permite ocultar una información dentro de otra, que haría la función de tapadera o canal encubierto, con la intención de que no se perciba ni siquiera la existencia de dicha información.
- La “tapadera” suele denominarse estego-medio.
 - Así se habla de estego-imágenes (si se usa una imagen inofensiva para ocultar la información), estego-vídeo, estego-audio, estego-texto, etc.

6. Esteganografía

- La utilidad de un sistema esteganográfico depende de tres factores:

Capacidad (cantidad de información que puede ser ocultada)

Seguridad/invisibilidad (probabilidad de detección)

Robustez (ante alteraciones del estego-medio)



Para practicar un poco

1. Prueba a construir un “conversor” rudimentario de decimal a binario, de binario a hexadecimal, de texto a ASCII etc. No hace falta programar, inténtalo con Excel.
2. Este tutorial explica muy bien Unicode: <https://r12a.github.io/scripts/tutorial/>
3. El código/cifra de Julio César es uno de los más antiguos de la historia. Intenta comprender cómo funciona, busca un cifrador on-line (por ejemplo, <https://cryptii.com/pipes/caesar-cipher>) y juega un poco con él.
4. En este enlace tienes un listado actualizado de herramientas útiles en esteganografía, prueba alguna de ellas e investiga cómo se puede esconder información en una imagen: <https://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/#gref>

Referencias

- Fotografías
 - <https://unsplash.com>
- Iconos
 - <https://www.flaticon.es/>



**Reconocimiento-CompartirIgual 3.0
España (CC BY-SA 3.0 ES)**

©2019-2022 Marta Beltrán URJC (marta.beltran@urjc.es)
Algunos derechos reservados.

Este documento se distribuye bajo la licencia “Reconocimiento-CompartirIgual 3.0 España” de Creative Commons, disponible en
<https://creativecommons.org/licenses/by-sa/3.0/es/>