


	<p align="center">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación		
Aprobación: 2022/03/01	Código: GUIA-PRLD-001	Página: 1

GUÍA DE LABORATORIO 04

INFORMACIÓN BÁSICA					
ASIGNATURA:	<i>SEGURIDAD INFORMÁTICA</i>				
TÍTULO DE LA PRÁCTICA:	<i>CRIPTOGRAFÍA MODERNA CIFRADO POR BLOQUES</i>				
NÚMERO DE PRÁCTICA:	<i>04</i>	AÑO LECTIVO:	<i>2023</i>	NRO. SEMESTRE:	<i>A</i>
TIPO DE PRÁCTICA:	INDIVIDUAL				
	GRUPAL	MÍNIMO DE ESTUDIANTES	<i>1</i>	MÁXIMO DE ESTUDIANTES	<i>2</i>
FECHA INICIO:	<i>30/06/2023</i>	FECHA FIN:	<i>06/07/2023</i>	DURACIÓN:	<i>7 días</i>
RECURSOS Y EQUIPOS A UTILIZAR: <i>PC, IDE de Programación</i>					
DOCENTE(s): <i>Juan Carlos Zuñiga</i>					

OBJETIVOS/TEMAS Y COMPETENCIAS	
OBJETIVOS:	<ul style="list-style-type: none"> • Aplicar el algoritmo de cifrado simétrico por bloques DES • Aplicar el algoritmo de cifrado simétrico por bloques AES • Verificar las deficiencias del cifrado ECB y CBC
TEMAS:	<ul style="list-style-type: none"> • <i>DES</i> • <i>AES</i> • <i>Modos de cifrado por bloque</i>
COMPETENCIAS A ALCANZAR	<p><i>Mantiene responsablemente, software para que se adecue a las necesidades cambiantes del usuario, cliente o sociedad mediante la aplicación de técnicas y procedimientos establecidos que siguen estándares de calidad destinados a implementar la seguridad informática. (referencia C.n)</i></p> <p><i>Asegura la calidad del software mediante la aplicación de pruebas, validaciones y estándares de seguridad para garantizar el correcto funcionamiento del producto, en el marco de la seguridad informática, considerando el impacto productivo y social. (referencia C.o)</i></p> <p><i>Diseña soluciones informáticas apropiadas para proveer seguridad informática, utilizando los principios de ingeniería que integran consideraciones éticas, sociales, legales y económicas entiendo las fortalezas y limitaciones del contexto (referencia C.q)</i></p>

	<p style="text-align: center;">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
<p style="text-align: center;">Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p>Código: GUIA-PRLD-001</p>	<p>Página: 2</p>

CONTENIDO DE LA GUÍA

I. MARCO CONCEPTUAL

Modos de cifrado por bloque

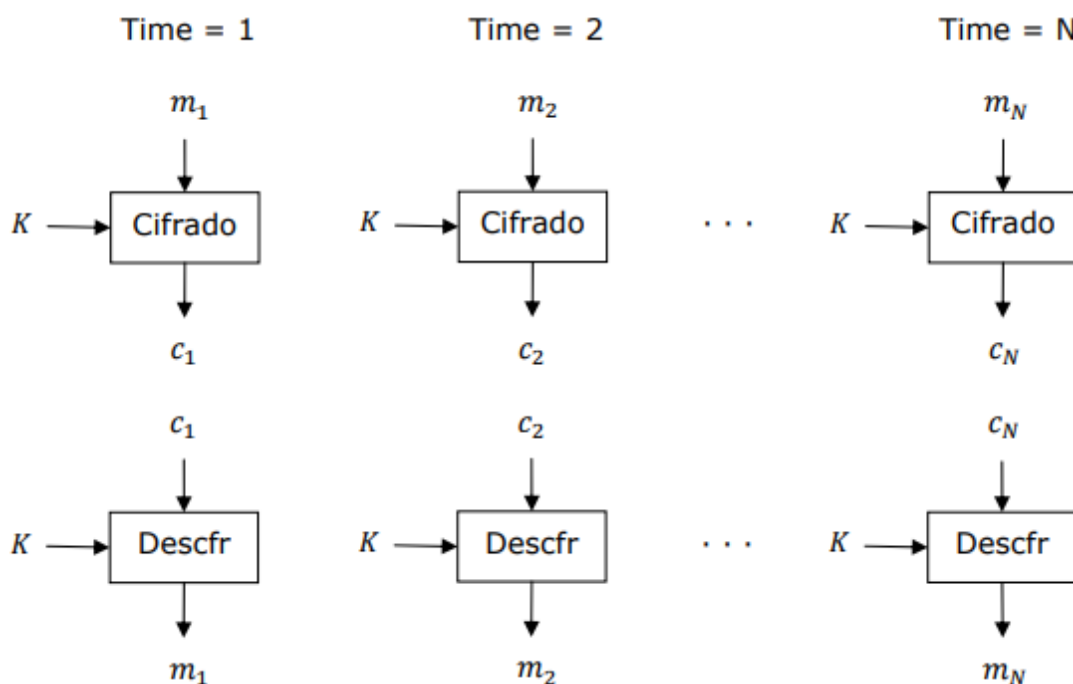
Los algoritmos de cifrado por bloque pueden ser ejecutados de diferentes modos. Sea el alfabeto del bloque a cifrar Σ y que la longitud del bloque es n , el algoritmo de cifrado es E_K , que el algoritmo de descifrado es D_K , cada bloque de texto plano es m_j y cada bloque de texto cifrado es c_j

MODO ECB. ELECTRONIC CODEBOOK MODE

En este modo, el texto plano se descompone en bloques de longitud n . Si es necesario, al texto plano se le añade un suplemento para conseguir que su longitud sea divisible por n . En este modo, cada bloque de longitud n es cifrado de forma independiente al resto de bloques: el texto cifrado es una secuencia de los bloques cifrados. Y el descifrado se realiza aplicando el algoritmo inverso a cada bloque del criptograma, también de forma independiente al resto de criptogramas.

Este modo se emplea para el envío de valores sencillos, pero es un modo que tiene ciertas debilidades:

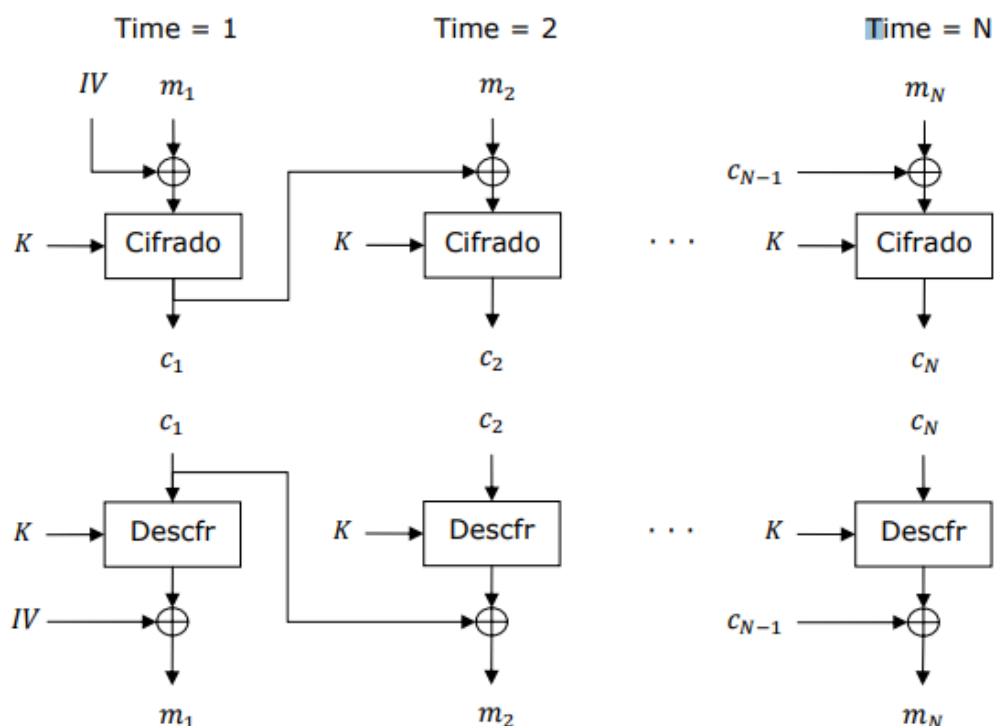
- Cuando se usa este modo, a cada bloque de texto plano le corresponde igual bloque de texto cifrado. Es así posible reconocer algunos patrones del texto plano en el texto cifrado. Eso facilita un ataque estadístico.
- Además, un atacante puede sustituir algunos bloques del texto cifrado con otros bloques cifrados que hayan sido cifrados con la misma clave. Esta manipulación es difícil de detectar en el receptor. ECB no se usa para el cifrado de textos planos largos. Se puede incrementar la seguridad de este modo de cifra es que cada bloque de texto a cifrar esté formado por un determinado número de caracteres del texto plano y otros hasta n lo ocupen caracteres aleatorios.



MODO CBC. CIPHERBLOCK CHAINING MODE.

En este modo, la entrada al algoritmo de cifrado es el resultado de la operación XOR entre el actual bloque de texto plano a cifrar y el bloque de texto cifrado precedente. Se emplea la misma clave en cada bloque.

Para descifrar, cada bloque cifrado es procesado por el algoritmo de descifrado, y el resultado es sometido a la operación XOR con el bloque cifrado precedente, para obtener así el bloque de texto plano

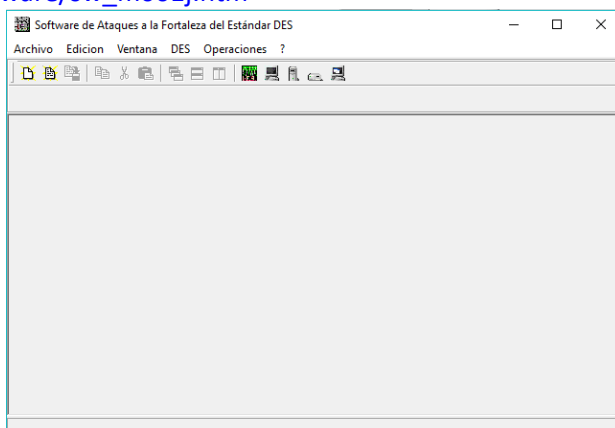


II. EJERCICIO RESUELTO

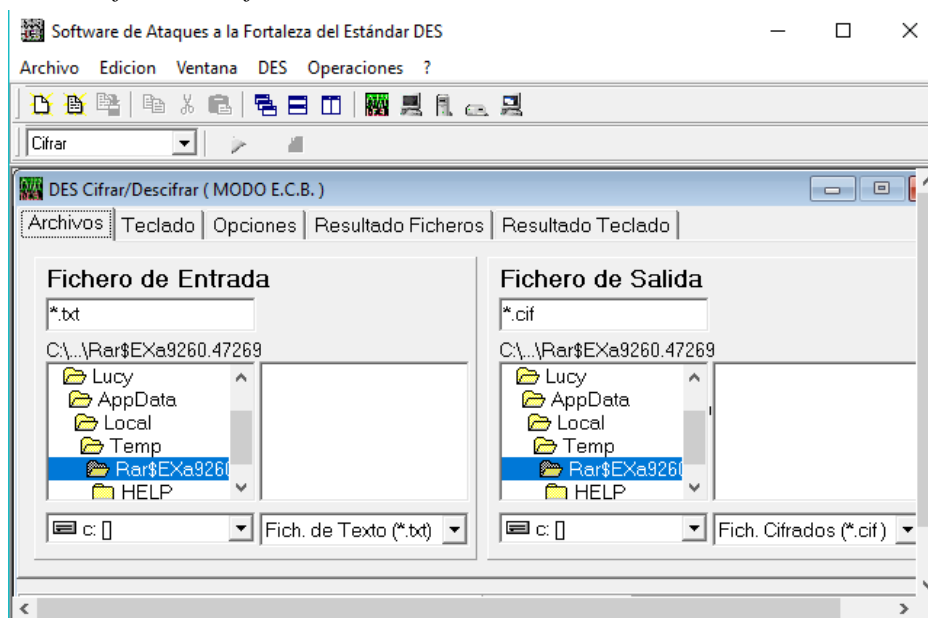
CIFRADO SIMÉTRICO DES

1. Descargue y ejecute el software libre safeDES

http://www.criptored.es/software/sw_m001j.htm



2. Seleccione *DES/ Cifrar/Descifrar*, por defecto en modo E.C.B



a) En el folder teclado, ingresa el texto claro en modo hexadecimal.

MHEX = 5656565656565656

En el folder opciones, ingresa la clave en modo hexadecimal.

KHEX = 0E439232EB6D1D62

y selecciona el *Procesar* hacia la opción *Teclado*

Seleccionar *Operaciones/Comenzar* o *play*.

b) Anote el resultado del folder *Resultado Teclado* en ASCII y hexadecimal

CHEx=6C2E1472D0CE5465

CAScII=I._rDÎTe

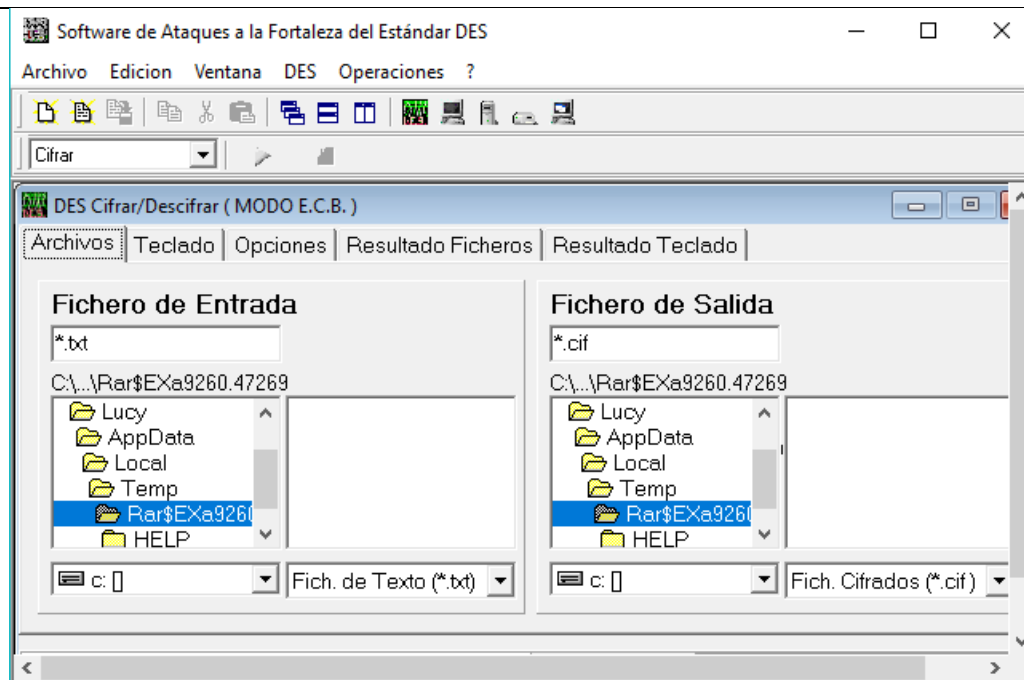
c) Descifre el resultado hexadecimal, anote la respuesta e interprete el resultado

M'HEX=5656565656565656

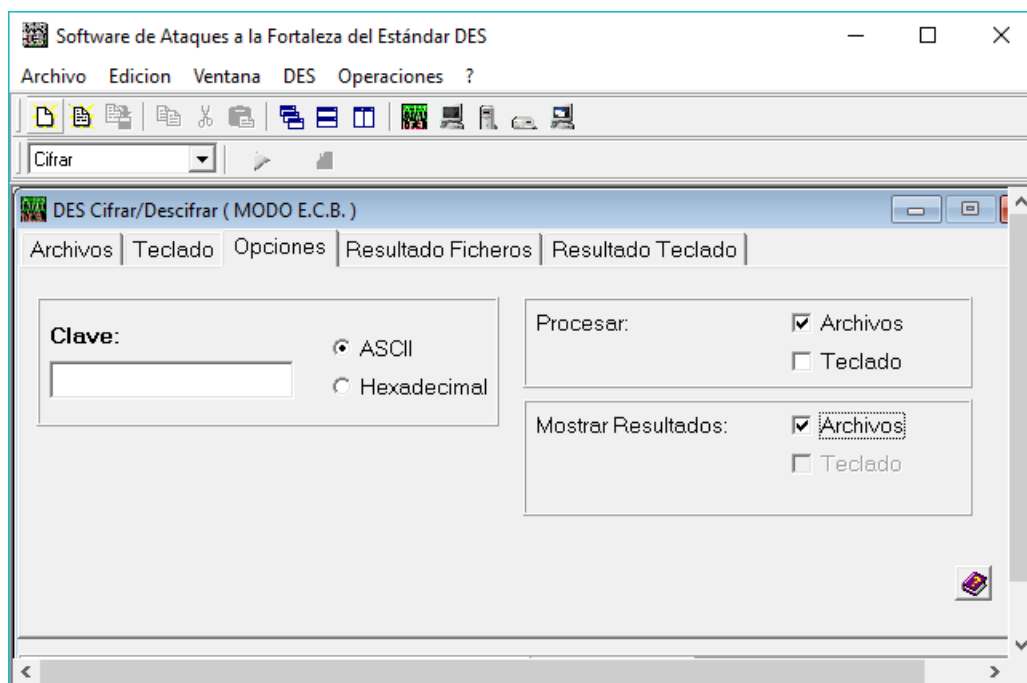
M'AScII=VVVVVVVV

ARCHIVOS DE CIFRADO SIMÉTRICO DES

Cree el archivo "prueba.txt" llenando sus apellidos, nombres y código, elija la opción *cifrar* y en el folder *Archivos* en *Fichero de Entrada* seleccione el archivo creado, en el folder *Fichero de Salida* definir el archivo "PruebaClaro.cif"





En el folder *Opciones* defina *Procesar* y *Mostrar Resultados* con la opción *Archivos*. Finalmente ingrese una clave ASCII de 8 caracteres e inicie el cifrado, guarde el resultado en el archivo “PruebaCifrado.cif”



Muestre el archivo generado a partir del block de notas

Genere el archivo “PruebaDescifrado.cif” a partir del proceso de descifrado, muestre los resultados y compare con el archivo de cifrado

	<p style="text-align: center;">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
<p style="text-align: center;">Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p>Código: GUIA-PRLD-001</p>	<p>Página: 6</p>

III. EJERCICIOS PROPUESTOS

1. Cifre considerando los valores hexadecimales. Anote los resultados y justifique los mismos:
 - a) MHEX = 6503100E95ACBDEE
 KHEX = 0123456789ABCDEF
 CHEX =
 - b) MHEX = 56CC3000E012F08B
 KHEX = 45BF3908BC3
 CHEX =
2. Cifre considerando los valores ASCII. Anote los resultados y justifique los mismos:
 - a) MASCII = CIBERSEGURIDADWEB
 KASCII = ESPECIAL
 CHEX =
 - b) MASCII = MISEGURIDAD
 KASCII = LLAVE
 CHEX =
3. Cifre considerando el texto y la clave ASCII
 - a) MASCII = "Seguridad en Redes con la clave en ASCII"
 KASCII = FFFFFFFF
 CHEX =
 - b) MASCII = "Seguridad en Redes con la clave en ASCII"
 KASCII = EEEEEEEE
 CHEX =

Compare los resultados, observando que las claves difieren en unos cuantos bits, explique los resultados.
4. Compare los resultados de cifrar el mensaje de 8 bytes MASCII = ENCRIPTO con KASCII = CLAVEDES y el mensaje de 12 bytes MASCII = ENCRIPACION usando la misma clave

CLAVES DÉBILES Y SEMIDÉBILES EN DES

ASEGÚRESE DE HACER EL INGRESO DE TEXTO Y CLAVES EN FORMATO HEXADECIMAL, AYÚDESE DEL PORTAPAPELES

5. Cifrar el mensaje M = "En este punto vamos a usar el proceso de cifrado para demostrar lo que significa el concepto de claves débiles en el algoritmo DES" utilice las siguientes claves y demuestre que se cumpla que $M=Ek[Ek(M)]$, donde EK representa el algoritmo de encriptación corrido con la clave K
 MHEX =

● K1 HEX = 0101010101010101
 CHEX K1 =
 C'HEXK1 = M'HEXK1

● K2 HEX = E0E0E0E0F1F1F1F1
 CHEX K2 =
 C'HEXK2 =

● K3 HEX = 1F1F1F1F0E0E0E0E
 CHEX K3 =

C'HEXK3 =

6. Cifrar el mensaje $M = \text{"En este punto vamos a usar el proceso de cifrado para demostrar lo que significa el concepto de claves semidébiles en el algoritmo DES"}$. utilice las siguientes claves y demuestre que se cumpla que $M = Ek1[Ek2(M)]$, donde EK representa el algoritmo de encriptación corrido con la clave K

MHEX =

• K1 HEX = 01FE01FE01FE01FE K2 HEX = FE01FE01FE01FE01

CHEX K1 =

C'HEX K2 = M'HEXK1

• K1 HEX = 1FE01FE00EF10EF1 K2 HEX = E01FE01FF10EF10E

CHEX K1 =

C'HEX K2 =

DES EN MODO CBC

7. Asumiendo un modo de cifrado CBC encriptar usando KHEX=534C68D48AEADFF2, MASCII="vamos a cifrar el mensaje usando DES en modo CBC", si IVHEX=DA5BEEF16B26983D, si lo necesita recuerde que puede usar alguna calculadora disponibles en Internet

Calculadora on-line convertidor (1)

<https://www.rapidtables.com/convert/number/ascii-to-hex.html>

Calculadora on-line operaciones (2)

<https://toolslick.com/math/bitwise/xor-calculator>

a) Convertir el mensaje a hexadecimal usando (1) y definir los bloques a cifrar, llene la segunda columna de la TABLA 1


b) Operar la función XOR usando (2), entre cada bloque del mensaje claro **Operando1** y el texto cifrado del bloque anterior **Operando2** (salvo en el primer bloque donde deberá usar el IV, llene la cuarta columna de la TABLA 1

c) Cifrar el resultado de la operación XOR, llene la quinta columna de la TABLA 1

d) Repetir hasta completar la totalidad de bloques e indicar el resultado del cifrado

Bloque	Operando1 _{XOR}	Operando 2 _{XOR}	Salida XOR	Cifrado DES
1				
2				
...				

TABLA 1

	<p style="text-align: center;">UNIVERSIDAD NACIONAL DE SAN AGUSTIN FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMA</p>	
<p style="text-align: center;">Formato: Guía de Práctica de Laboratorio / Talleres / Centros de Simulación</p>		
<p>Aprobación: 2022/03/01</p>	<p>Código: GUIA-PRLD-001</p>	<p>Página: 8</p>

IV. CUESTIONARIO

1. Visualice el video <https://www.youtube.com/watch?v=2ssaCyXRJIU>, luego responda
 - a) Describa funcionalmente los modos de cifrado por bloque, indicando en cada caso las fortalezas, debilidades y aplicaciones
 - b) Defina claramente el concepto de fortaleza de clave
2. ¿Por qué AES reemplaza a DES?

V. REFERENCIAS Y BIBLIOGRAFÍA RECOMENDADAS:

Gómez, S., Arias, J. D., & Agudelo, D. (2012). Cripto-análisis sobre métodos clásicos de cifrado. *Scientia et technica*, 2(50), 97-102.

TÉCNICAS E INSTRUMENTOS DE EVALUACIÓN	
<p>TÉCNICAS: <i>Ejercicios propuestos</i></p>	<p>INSTRUMENTOS: <i>Lista de cotejo</i></p>
<p>CRITERIOS DE EVALUACIÓN Y LOGROS ALCANZADOS <i>Niveles de logro: inicio, proceso, logro esperado, logro destacado.</i></p>	