PAC 1 (UF1)

Fecha de entrega 18 de dic en 23:59 **Puntos** 3 **Preguntas** 4
Disponible 30 de nov en 0:00 - 18 de dic en 23:59 19 días **Límite de tiempo** Ninguno

Detalles de la entrega:

Hora:	6 minutos
Puntaje actual:	3 de 3
se mantuvo el puntaje:	3 de 3

Instrucciones

Técnicas y prácticas criptográficas

INTRODUCCIÓN

En esta actividad tendrás que contestar a una serie de preguntas para evaluar los conocimientos de este módulo/asignatura.

TEMAS RECOMENDADOS:

1. Conocer los posibles fallos de seguridad al desarrollar código.
2. Distinguir el tipo de cifrado al que corresponde un algoritmo.
3. Identificar conceptos de seguridad usados en programación.
4. Conocer el proceso correspondiente a la firma digital.

Historial de intentos

	Intento	Hora	Puntaje
MÁS RECIENTE	Intento 1	6 minutos	3 de 3

Puntaje para este examen: **3** de 3
Entregado el 11 de dic en 19:07
Este intento tuvo una duración de 6 minutos.

Pregunta 1 — 0.75 / 0.75 pts

Relaciona cada concepto con su definición.

¡Correcto! se asegura de que no hayan sido modificados por terceros, es decir, que se recibe el mensaje tal y como se envió — Integridad de los datos

¡Correcto! característica por la cual los datos se encuentran a disposición de quienes deban acceder a ellos — Disponibilidad

¡Correcto! los mensajes solo podrán ser leídos por aquellas personas que han sido autorizadas para ello. De esta forma se garantiza la privacidad de los datos. — Confidencialidad

¡Correcto! característica mediante la cual el receptor conoce la identidad del emisor — Autenticidad

¡Correcto! el emisor no puede negar que ha enviado el mensaje, por lo que se evita que se culpe al canal de información de que la información no ha llegado — No repudio

Pregunta 2 — 0.75 / 0.75 pts

¿Cuál de las siguientes opciones es un fallo de seguridad a la hora de desarrollar código?

¡Correcto!
- (•) Invocar una Shell o línea de comandos.
- ( ) No invocar programas no confiables.
- ( ) Guardar datos en una base de datos protegida por contraseña.
- ( ) Asumir que los usuarios son maliciosos.

Pregunta 3 — 0.75 / 0.75 pts

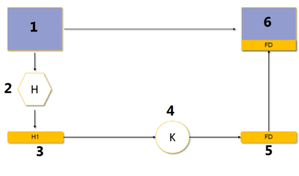
Determina cada algoritmo al tipo de cifrado según corresponda.

RSA Cifrado asimétrico
DES Cifrado simétrico
SHA-1 Función hash
MD5 Función hash
Triple DES Cifrado simétrico
AES Cifrado simétrico

Respuesta 1: ¡Correcto! Cifrado asimétrico
Respuesta 2: ¡Correcto! Cifrado simétrico
Respuesta 3: ¡Correcto! Función hash
Respuesta 4: ¡Correcto! Función hash
Respuesta 5: ¡Correcto! Cifrado simétrico
Respuesta 6: ¡Correcto! Cifrado simétrico

Pregunta 4 — 0.75 / 0.75 pts

Completa el diagrama que corresponde con la firma digital.



1) Mensaje
2) Función de una sola vía
3) Hash del mensaje
4) Clave privada del emisor
5) Firma digital del mensje
6) Mensaje firmado

Respuesta 1: ¡Correcto! Mensaje
Respuesta 2: ¡Correcto! Función de una sola vía
Respuesta 3: ¡Correcto! Hash del mensaje
Respuesta 4: ¡Correcto! Clave privada del emisor
Respuesta 5: ¡Correcto! Firma digital del mensje
Respuesta 6: ¡Correcto! Mensaje firmado

Puntaje del examen: **3** de 3

PAC 2 (UF1)

Fecha de entrega 18 de dic en 23:59 **Puntos** 2 **Preguntas** 3
Disponible 4 de dic en 0:00 - 18 de dic en 23:59 15 días **Límite de tiempo** Ninguno

Detalles de la entrega:

Hora:	4 minutos
Puntaje actual:	2 de 2
se mantuvo el puntaje:	2 de 2

Instrucciones

Control de acceso y servicios seguros

INTRODUCCIÓN

En esta actividad tendrás que contestar a una serie de preguntas para evaluar los conocimientos de este módulo/asignatura.

TEMAS RECOMENDADOS:

1. **Conocer las etapas del control de acceso.**
2. **Identificar las medidas de identificación y autenticación.**
3. **Diferenciar características ofrecidas por protocolos seguros.**

Historial de intentos

	Intento	Hora	Puntaje
MÁS RECIENTE	Intento 1	4 minutos	2 de 2

Puntaje para este examen: **2** de 2
Entregado el 11 de dic en 21:29
Este intento tuvo una duración de 4 minutos.

Pregunta 1 — 0.6 / 0.6 pts

Relaciona las siguientes etapas del control de acceso con su definición.

¡Correcto!
Identificación — el usuario indica quién es.

¡Correcto!
Autenticación — el sistema comprueba que el u:

¡Correcto!
Autorización — el sistema ofrece la informació

Pregunta 2 — 0.7 / 0.7 pts

¿Cuales de estas opciones no es una medida de identificación y autenticación?

- Biometría
- Contraseñas

¡Correcto!
- (•) Número de télefono
- Tarjeta de identificación

Pregunta 3 — 0.7 / 0.7 pts

Señala como verdadero o falso las siguientes sentencias sobre protocolos.

HTTPS, por defecto, utiliza el puerto 80. Falso
HTTPS utiliza el cifrado SSL/TLS. Verdadero
SSH utiliza las funcione hash y el cifrado asimétrico. Falso
SSH garantiza la integridad de los mensajes. [Seleccionar]
SSL garantiza la integridad de los mensajes mediante funciones hash. [Seleccionar]
Telnet es más seguro que SSH. Falso

Respuesta 1:
¡Correcto! Falso

Respuesta 2:
¡Correcto! Verdadero

Respuesta 3:
¡Correcto! Falso

Respuesta 4:
¡Correcto! Verdadero

Respuesta 5:
¡Correcto! Verdadero

Respuesta 6:
¡Correcto! Falso

Puntaje del examen: **2** de 2

PAC 3 (UF1)

Fecha de entrega 18 de dic en 23:59 **Puntos** 3 **Preguntas** 4
Disponible 9 de dic en 0:00 - 18 de dic en 23:59 10 días **Límite de tiempo** Ninguno

Detalles de la entrega:

Hora:	6 minutos
Puntaje actual:	3 de 3
se mantuvo el puntaje:	3 de 3

Instrucciones

Algoritmos de criptografía

INTRODUCCIÓN

En esta actividad tendrás que contestar a una serie de preguntas para evaluar los conocimientos de este módulo/asignatura.

TEMAS RECOMENDADOS:

1. **Saber cifrar palabras usando algoritmos.**
2. **Poder obtener la cadena resultante al cifrar una sentencia.**
3. **Conocer conceptos básicos de los algoritmos de cifrado.**
4. **Identificar la seguridad de cada algoritmo.**
5. **Conocer las clases usadas en programación de aplicaciones para cifrar datos en Java.**

Historial de intentos

	Intento	Hora	Puntaje
MÁS RECIENTE	Intento 1	6 minutos	3 de 3

Puntaje para este examen: **3** de 3
Entregado el 11 de dic en 21:35
Este intento tuvo una duración de 6 minutos.

Pregunta 1 — 0.75 / 0.75 pts

Queremos cifrar la palabra Programación con el algoritmo MD5, ¿Qué longitud tendrá la cadena resultante?

32

Respuesta 1:

¡Correcto! 32

Pregunta 2 — 0.75 / 0.75 pts

Queremos cifrar la palabra Ilerna con el algoritmo SHA-1 ¿Qué longitud tendrá la cadena resultante?

40

Respuesta 1:

¡Correcto! 40

Pregunta 3 — 0.75 / 0.75 pts

¿Cuál es el algoritmo más seguro de los siguientes?

- DES
- Triple DES

¡Correcto!
- AES

Pregunta 4 — 0.75 / 0.75 pts

Señala como verdadero o falso las siguientes sentencias.

La firma digital se basa en el algoritmo RSA. Verdadero
La clase KeyPair se utiliza en criptografía asimétrica. Verdadero
La clase Cipher se utiliza para criptografía simétrica. Verdadero

Respuesta 1:

¡Correcto! Verdadero

Respuesta 2:

¡Correcto! Verdadero

Respuesta 3:

¡Correcto! Verdadero

Puntaje del examen: **3** de 3

Test evaluable (UF1)

Fecha de entrega 18 de dic en 23:59 **Puntos** 2 **Preguntas** 5
Disponible 13 de dic en 0:00 - 18 de dic en 23:59 6 días **Límite de tiempo** 20 minutos

Detalles de la entrega:

Hora:	3 minutos
Puntaje actual:	2 de 2
se mantuvo el puntaje:	2 de 2

Instrucciones

DESCRIPCIÓN

Este ejercicio se compone de una serie de preguntas que evaluarán tus conocimientos sobre esta Unidad Formativa.

INSTRUCCIONES

- Debes completar el cuestionario en el tiempo establecido.
- No se puede abandonar la evaluación. En caso de hacerlo, el tiempo seguirá pasando igualmente hasta finalizar y no se podrá retomar el cuestionario.

Ayuda

Este examen fue bloqueado en 18 de dic en 23:59.

Historial de intentos

	Intento	Hora	Puntaje
MÁS RECIENTE	Intento 1	3 minutos	2 de 2

Puntaje para este examen: **2** de 2
Entregado el 18 de dic en 22:08
Este intento tuvo una duración de 3 minutos.

Pregunta 1 — 0.4 / 0.4 pts

Indica cuál de las siguientes opciones deben tenerse en cuanta a la hora de desarrollar una solución software:

- ¡Correcto! [x] Los usuarios serán quienes intenten buscar errores en esta aplicación
- ¡Correcto! [x] Se recomienda que los ficheros que se usen dentro de la aplicación sean solo para lectura
- [ ] Se recomienda usar rutas relativas para los ficheros con los que se trabaje dentro de la aplicación
- [ ] Toda la información sensible almacenada en una base de datos no necesita ser cifrada antes de enviarse por Internet

Pregunta 2 — 0.4 / 0.4 pts

Entre los tipos de algoritmos Hash tenemos MD5 y SHA-1 que se diferencian en el número de bits que se usan para representar la información codificada

- ¡Correcto! (•) Verdadero
- ( ) Falso

Pregunta 3 — 0.4 / 0.4 pts

Señala las normas que se han de cumplir para proteger un sistema de acceso informático:

- [ ] Redundancia
- ¡Correcto! [x] Confidencialidad
- [ ] Certificación
- ¡Correcto! [x] Disponibilidad
- ¡Correcto! [x] Integridad de los datos
- [ ] Replicación
- ¡Correcto! [x] No repudio

Pregunta 4 — 0.4 / 0.4 pts

La Autenticación es la última fase que tiene lugar en el proceso del control de acceso. Si ha resultado con éxito, el sistema ofrece la información requerida o el acceso al recurso.

- ( ) Verdadero
- ¡Correcto! (•) Falso

Pregunta 5 — 0.4 / 0.4 pts

Indica si esta afirmación es cierta o no: El protocolo HTTP es un protocolo de la capa de de la capa de aplicación que es más seguro y usa un cifrado basado en SSL/TLS.

- ( ) Verdadero
- ¡Correcto! (•) Falso

Puntaje del examen: **2** de 2

UF1. Seguridad y criptografía

Test:

1.- ¿Cuál de estas opciones no es una medida de identificación y autenticación?

a. **Firma digital**
b. Biometría
c. Contraseñas
d. Access Tokens

2.- Señala la opción que no sea una práctica en la programación segura:

a. **Todas las opciones son correctas.**
b. Informarse.
c. Utilizar listas de control de seguridad.
d. Reutilización de código.

3.- ¿Cuál de estas características se consigue con la firma digital?

a. No repudio
b. **Todas las opciones son correctas**
c. Autenticación de origen
d. Integridad del mensaje

4.- ¿De qué longitud son los resúmenes creados por el algoritmo SHA-1?

a. 128 bits
b. Ninguna de las opciones anteriores es correcta.
c. **160 bits**
d. 256 bits

5.- Señala la opción verdadera.

a. Ambas respuestas son incorrectas.
b. Ambas respuestas son correctas.
c. Cuando se realizan nuevas versiones de la aplicación, no es necesario quitar el código obsoleto.
d. **Cuando se realizan cambios en el código, debemos probar toda la aplicación.**

6.- ¿En qué fase del mecanismo de control de acceso el sistema comprueba que el usuario es quien dice ser?

a. Autorización

b. Identificación

c. Ninguna opción es correcta

d. Autenticación

7.- SHA-1 es un algoritmo de tipo

a. Función de una sola vía.

b. Ninguna de las opciones anteriores es correcta.

c. Clave asimétrica.

d. Clave simétrica.

8.- ¿Cuál de estas opciones no es un componente del control de acceso?

a. Autenticación

b. Identificación

c. Autorización

d. Biometría

UF1. Seguridad y criptografía

Test:

1.- ¿Cuál de estas opciones no es una medida de identificación y autenticación?

a. Contraseñas

b. Acces Tokens

c. Firma digital

d. Biometría

2.- Triple DES es un algoritmo de tipo

a. Función de una sola vía.

b. Clave simétrica.

c. Ninguna de las opciones anteriores es correcta.

d. Clave asimétrica.

3.- ¿De qué longitud son los resúmenes creados por el algoritmo SHA-1?

a. 160 bits

b. 256 bits

c. Ninguna de las opciones anteriores es correcta.

d. 128 bits

4.- Señala la opción que no sea una práctica en la programación segura:

a. Utilizar listas de control de seguridad.

b. Informarse.

c. Todas las opciones son correctas.

d. Reutilización de código.

5.- ¿Cuál de estas opciones no es un componente del control de acceso?

a. Identificación

b. Biometría

c. Autenticación

d. Autorización

6.- ¿En qué algoritmo se basa la firma digital?

a. RSA
b. AES
c. MD5
d. DES

7.- ¿Cuál de estos no es un punto fuerte de la criptografía simétrica?

a. Sirven como base para los sistemas criptográficos basados en hardware.
b. Permiten conseguir autenticación y no repudio.
c. Todas las opciones son puntos fuertes de la criptografía simétrica.
d. Son más rápidos que los algoritmos de clave pública.

8.- AES es un algoritmo de tipo

a. Función de una sola vía.
b. Clave simétrica.
c. Ninguna de las opciones anteriores es correcta.
d. Clave asimétrica.

UF1. Seguridad y criptografía

Test:

1.- ¿Para cuál de estos protocolos utilizamos el algoritmo RSA?

a. Todas las opciones son correctas.

b. SSL

c. Firma digital.

d. IPSec

2.- ¿De qué longitud son los resúmenes creados por el algoritmo SHA-1?

a. Ninguna de las opciones anteriores es correcta.

b. 128 bits

c. 160 bits

d. 256 bits

3.- MD5 es un algoritmo de tipo

a. Función de una sola vía.

b. Clave simétrica.

c. Clave asimétrica.

d. Ninguna de las opciones anteriores es correcta.

4.- ¿Cuál de estas opciones no es una medida de identificación y autenticación?

a. Contraseñas

b. Firma digital

c. Biometría

d. Acces Tokens

5.- Señala la opción verdadera.

a. Cuando se realizan nuevas versiones de la aplicación, no es necesario quitar el código obsoleto.

b. Ambas respuestas son correctas.

c. Ambas respuestas son incorrectas.

d. Cuando se realizan cambios en el código, debemos probar toda la aplicación.

6.- ¿Cuál de estas características se consigue con la firma digital?

a. Todas las opciones son correctas

b. Integridad del mensaje

c. Autenticación de origen

d. No repudio

7.- ¿En qué fase del mecanismo de control de acceso el sistema comprueba que el usuario es quien dice ser?

a. Ninguna opción es correcta

b. Autenticación

c. Identificación

d. Autorización

8.- ¿En qué algoritmo se basa la firma digital?

a. RSA

b. AES

c. MD5

d. DES