

EXAMEN-SEGURIDAD-DE-LA-INFORMACI...



donVito



Seguridad de la Información



3º Grado en Ingeniería Informática



**Escuela Técnica Superior de Ingeniería Informática
Universidad de Málaga**



La mejor escuela de negocios en
energía, sostenibilidad y medio
ambiente de España.

Más información
www.eoi.es

Formamos
talento para un futuro
Sostenible



100% Empleabilidad



Modalidad: Presencial u online



**Programa de Becas,
Bonificaciones y Descuentos**

EXAMEN SEGURIDAD DE LA INFORMACIÓN 2020/2021

Comenzado el	martes, 2 de febrero de 2021, 09:28
Estado	Finalizado
Finalizado en	martes, 2 de febrero de 2021, 09:58
Tiempo empleado	30 minutos
La puntuación	85,00/200,00
Calificación	4,25 de 10,00 (43%)

Pregunta 1
Correcta
Puntúa 10,00 sobre 10,00
▼ Marcar pregunta

AH ...

Selecciona una:

- ☐ a. ninguna de las respuestas son correctas
- ☐ b. asegura autenticación y disponibilidad
- ☒ c. asegura sólo autenticación e integridad
- ☐ d. asegura integridad y disponibilidad



La respuesta correcta es: asegura sólo autenticación e integridad

Pregunta 2
Correcta
Puntúa 10,00 sobre 10,00
▼ Marcar pregunta

En el protocolo TOR, ¿quién se encarga de seleccionar el camino de enrutamiento?

Selecciona una:

- ☒ a. Un servidor central
- ☐ b. El nodo destino
- ☐ c. Los vecinos del nodo origen
- ☐ d. El nodo origen



La respuesta correcta es: Un servidor central

Pregunta 3
Correcta
Puntúa 10,00 sobre 10,00
▼ Marcar pregunta

Una VPN en modo túnel ...

Selecciona una:

- ☐ a. es una herramienta que garantiza no-repudio
- ☐ b. es una herramienta que garantiza integridad
- ☒ c. es una herramienta que permite conectar subredes remotas de forma segura
- ☐ d. es una herramienta que garantiza disponibilidad



La respuesta correcta es: es una herramienta que permite conectar subredes remotas de forma segura

Pregunta 4
Correcta
Puntúa 10,00 sobre 10,00
▼ Marcar pregunta

¿Cuál de los siguientes servicios **NO** lo ofrece una PKI?

Selecciona una:

- ☒ a. Modificación de certificados
- ☐ b. Emisión de certificados
- ☐ c. Certificación cruzada
- ☐ d. Revocación y suspensión de certificados



La respuesta correcta es: Modificación de certificados

Pregunta 5
Correcta
Puntúa 10,00 sobre 10,00
▼ Marcar pregunta

El "Security Parameter Index" identifica ...

Selecciona una:

- ☐ a. la política de seguridad
- ☒ b. la asociación de seguridad
- ☐ c. la base de datos de políticas de seguridad
- ☐ d. la base de datos de asociación de seguridad



La respuesta correcta es: la asociación de seguridad

Pregunta 6
Correcta
Puntúa 10.00
sobre 10.00
✓ Marcar
pregunta

Indicar la afirmación correcta ...

Selecciona una:

- ☐ a. La principal razón de que Alice y Bob acuden a una autoridad certificadora es para que Alice y Bob puedan tener una mejor reputación dentro de un contexto de aplicación
- ☐ b. Si Alice y Bob comparten dos claves, KA y KB, y Mallory es capaz de conocer una de las claves → entonces Mallory puede descifrar las comunicaciones entre A y B, ya que el uso de criptosistemas simétricos permite de forma general deducir una clave (ej. K2) de otra (ej. K1)
- ☒ c. En un canal inseguro es posible intercambiar claves secretas entre A y B
- ☐ d. Ninguna de las respuestas anteriores son correctas

✓

La respuesta correcta es: En un canal inseguro es posible intercambiar claves secretas entre A y B

Pregunta 7
Incorrecta
Puntúa -2.50
sobre 10.00
✓ Marcar
pregunta

En SSL/TLS, DHE ...

Selecciona una:

- ☐ a. permite obtener nuevos valores secretos en cada negociación de la clave del canal WIFI inalámbrico
- ☐ b. permite obtener nuevos valores secretos en cada negociación del suite de cifrado
- ☐ c. permite obtener nuevos valores secretos en cada negociación de la clave de sesión
- ☒ d. ninguna de las anteriores

✗

La respuesta correcta es: permite obtener nuevos valores secretos en cada negociación de la clave de sesión

Pregunta 8
Incorrecta
Puntúa -2.50
sobre 10.00
✓ Marcar
pregunta

En el control de acceso MAC, un usuario con permisos Secret, ¿a qué puede acceder?

Selecciona una:

- ☐ a. Únicamente a documentos Secret
- ☐ b. A documentos Secret, Confidential, y Unclassified
- ☐ c. A documentos Top Secret, Secret, Confidential, y Unclassified
- ☒ d. A documentos Top Secret y Secret

✗

La respuesta correcta es: A documentos Secret, Confidential, y Unclassified

Pregunta 9
Sin contestar
Valor: 10.00
✓ Marcar
pregunta

Con TLS/SSL se consigue también ...

Selecciona una:

- ☐ a. autenticación mutua en todas las comunicaciones
- ☐ b. un encapsulamiento (cifrado) a nivel de transporte
- ☐ c. un encapsulamiento (cifrado) a nivel de red
- ☐ d. una protección del comprador frente al vendedor

La respuesta correcta es: un encapsulamiento (cifrado) a nivel de transporte

Pregunta 10
Correcta
Puntúa 10.00
sobre 10.00
✓ Marcar
pregunta

En DES ...

Selecciona una:

- ☒ a. se manejan bloques de texto en claro de 64 bits, una semilla de 64 bits, y subclaves de 48 bits
- ☐ b. se manejan bloques de texto en claro de 64 bits, una semilla de 64 bits, y 48 subclaves
- ☐ c. se manejan bloques de texto en claro de 64 bits, una semilla de 64 bits, y 24 subclaves
- ☐ d. se manejan bloque de texto en claro de 64 bits, una semilla de 64 bits, y 16 subclaves de 64 bits cada una

✓

La respuesta correcta es: se manejan bloques de texto en claro de 64 bits, una semilla de 64 bits, y subclaves de 48 bits

Pregunta 11
Sin contestar
Valor: 10.00
✓ Marcar
pregunta

¿Qué modos de operación permiten que el cifrado en bloque pueda utilizarse como un cifrado en flujo?

Selecciona una:

- ☐ a. CTR, CBC
- ☐ b. CTR, GCM
- ☐ c. CBC, GCM
- ☐ d. ECB, CBC

La respuesta correcta es: CTR, GCM

WUOLAH



McDonald's

**“SOY CREW DE McDONALD’S,
Y POR SUPUESTO QUE
MI TRABAJO Y MI PASIÓN
SON COMPATIBLES”**



¿TE VIENES?



My CREW

Mi trabajo. Mi pasión. Mi gente.

Seguridad de la Información



Comparte estos flyers en tu clase y consigue más dinero y recompensas



Banco de apuntes de la

WUOLAH

- 1** Imprime esta hoja
- 2** Recorta por la mitad
- 3** Coloca en un lugar visible para que tus compis puedan escanar y acceder a apuntes

- 4** Llévate dinero por cada descarga de los documentos descargados a través de tu QR



Pregunta 12
Sin contestar
Valor: 10,00
✓ Marcar pregunta

Si quiero que t usuarios de un grupo de n usuarios firmen en nombre del grupo, ¿qué esquema debería utilizar?

Selecciona una:

- ☐ a. Firma de anillo
- ☐ b. Firma ciega
- ☐ c. Firma de grupo
- ☐ d. Firma umbral

La respuesta correcta es: Firma umbral

Pregunta 13
Correcta
Puntúa 10,00 sobre 10,00
✓ Marcar pregunta

¿Cuál es la principal diferencia entre PGP y S-MIME?

Selecciona una:

- ☒ a. PGP usa una PKI en malla, y S-MIME usa una PKI híbrida
- ☐ b. PGP ofrece autenticidad y confidencialidad, y S-MIME ofrece sólo confidencialidad
- ☐ c. PGP ofrece autenticidad y confidencialidad, y S-MIME ofrece sólo autenticidad
- ☐ d. PGP usa una PKI híbrida, y S-MIME usa una PKI en malla



La respuesta correcta es: PGP usa una PKI en malla, y S-MIME usa una PKI híbrida

Pregunta 14
Correcta
Puntúa 10,00 sobre 10,00
✓ Marcar pregunta

En un certificado X.509, ¿qué es lo que firma la CA?

Selecciona una:

- ☐ a. La clave pública del dueño del certificado
- ☒ b. El valor hash del conjunto de los demás campos del certificado
- ☐ c. El conjunto de los demás campos del certificado
- ☐ d. El valor hash de la clave pública del dueño del certificado



La respuesta correcta es: El valor hash del conjunto de los demás campos del certificado

Pregunta 15
Sin contestar
Valor: 10,00
✓ Marcar pregunta

Es cierto que ...

Selecciona una:

- ☐ a. en el modo CBC, el tamaño del bloque de cifrado y del vector IV son siempre distintos
- ☐ b. en el modo CTR, el tamaño del mensaje a cifrar y del criptograma son siempre iguales
- ☐ c. en el modo CFB, el tamaño del mensaje a cifrar y del vector IV son siempre iguales
- ☐ d. Todas las respuestas anteriores son incorrectas

La respuesta correcta es: en el modo CTR, el tamaño del mensaje a cifrar y del criptograma son siempre iguales

Pregunta 16
Sin contestar
Valor: 25,00
✓ Marcar pregunta

Como experto de ciberseguridad, me gustaría que me nombrase una o varias medidas de seguridad para garantizar dentro de mi empresa un nivel aceptable de resiliencia (es decir, continuidad del negocio) frente ataques de denegación de servicio. Para ser más preciso, mi empresa ofrece diversos servicios de hosting, en el que clientes despliegan sus páginas web dentro de nuestros servidores. Por tanto, mencionar medidas de seguridad que ayuden a esta empresa a evitar o a hacer frente a ataques de DoS, justificando las razones.

Pregunta 17
Sin contestar
Valor: 25,00
✓ Marcar pregunta

Ya sabemos que Kerberos es un protocolo de autenticación ampliamente utilizado en entornos o dominios principalmente distribuidos. Sin embargo, me surgen varias dudas sobre la posibilidad o no de existir un posible ataque sobre estos tipos de sistema, así pues, como experto en ciberseguridad, me gustaría saber si usted cree: si estos sistemas pueden ser susceptibles o no a determinados ataques. Si es el caso, me gustaría, además, conocer al menos un par de medidas de seguridad para evitar o mitigar su efecto dentro de mi empresa. Razonar la respuesta.