Parcial

Teoría:

1. Tipo test
2. Definición de riesgo en un sistema de información. ¿Cómo se puede mitigar el riesgo? Indique alguna metodología de gestión de riesgos.
3. Intercambios Diffie-Hellman
4. Modo de operación de PCBC (funciones de cifrado y descifrado).
    1. L(n) = Dk [Cn] + L(n-1) + C(n-1).
    2. C(n) = Ek [Ln + C(n-1) + L(n-1)].
5. 11.2.1 ISO 27002 (¿pq e) y d) son necesarios?).
    1. Capacidad sancionadora en el caso de incumplimiento.
    2. 3 métricas: Establecer indicadores que nos permitan medir valor. EJ: Calcular tiempo que tarda 1 proceso.

Práctica VPN:

Tenemos una maquina con distribucion Ubuntu Server 22.04. Tenemos que llevar a cabo la configuración del cliente OpenVPN que conectará con el servidor VPN presente en la IP 172.31.100.100. El servdior VPN ha sido configuado con las opciones predeterminadas(protocolo udp, puerto 1196, modo tun, cifrado AES-256-CBC y clave compartida ta.key). Configurar el acceso VPN para que el cliente pueda acceder a otro equipo, el Servidor Apache, que se encuentra en la IP .109 de la Red destino. El servidor VPN ha sido configurado para que el cliente VPN pueda acceder al Servidor Apache. Arrancar el cliente y configurar su arranque automático. Después, identificar la dirección IP del servidor apache y acceder a su pagina e inicio (puede usar el cliente lynx)

APELLIDOS: Requeja Antón | FECHA: 7/11/2023 | GRUPO:

ASIGNATURA: SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS

Examen Parcial. Teoría
Sin libros ni documentación
DURACIÓN: 1 h

7B+1M → 2,0 TEORÍA: 2,0 PRÁCTICA: 2,5

1. Test de conocimientos. Marcar con una cruz la respuesta correcta. (3 puntos)
Sólo hay una respuesta válida. Cada pregunta tiene una valoración de 0.3 p. Las incorrectas descuentan 0.1 p.

1. Dentro del modelo PDCA utilizado en la ISO 27000, la revisión del SGSI y del riesgo residual se realiza en la fase:
   a) Plan
   b) Do
B c) Check
   d) Act

2. El servicio de Autentificación,
   a) Garantiza el origen y destino de la información intercambiada
   b) Evita el repudio de la información enviada
B c) Limita el acceso y uso de los recursos a los usuarios autorizados
   d) Garantiza que los usuarios autorizados tienen acceso a la información

3. Respecto al Esquema Nacional de Seguridad, indique la afirmación INCORRECTA:
   a) Es un Sistema de Gestión de la Seguridad de la Información (SGSI)
B b) Su ámbito de aplicación son las administraciones públicas y privadas
   c) Está basado en la metodología del Análisis y Gestión de Riesgos
   d) Aborda la seguridad como un proceso integral

4. En el contexto de la gestión de la seguridad, un control correctivo
   a) Intenta evitar la ocurrencia de sucesos indeseados
   b) Intenta restaurar los recursos perdidos y ayudar a la organización a recuperarse de las pérdidas
B c) Intenta identificar sucesos indeseados en el momento o después de que hayan ocurrido
   d) Intenta remediar las circunstancias que permitieron la actividad ilegítima o devolver el sistema al estado anterior a la violación

5. Para conocer la eficacia de un control de seguridad implantado se utilizan:
   a) Salvaguardas o contramedidas
B b) Métricas
   c) Vulnerabilidades
   d) Políticas

6. El principio de Minimización de Datos en el RGPD consiste en que los datos personales serán:
   a) Tratados de manera lícita, leal y transparente en relación con el interesado
   b) Recogidos con fines determinados, explícitos y legítimos
B c) Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados
   d) Exactos y actualizados si fuera necesario

7. El cifrador de Nihilist es un sistema de cifrado
   a) De flujo
   b) De suma de textos
   c) De doble transposición
   d) De sustitución polialfabética

ESCUELA POLITÉCNICA SUPERIOR UNIVERSIDAD SAN PABLO-CEU
Departamento de Tecnologías de la Información

Curso 2023-24

APELLIDOS:	NOMBRE:	DNI:	CALIFICACIÓN:
ASIGNATURA: **SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS**	FECHA: **7/11/2023**	GRUPO:	

8. En un modelo de ataque con cifrado seleccionado,
   a) se dispone exclusivamente de fragmentos o la totalidad del mensaje cifrado
   b) se cuenta con parejas de legible-cifrado
   c) se puede obtener los equivalentes cifrados de cualquier legible que desee
   d) el atacante puede cifrar y descifrar las combinaciones que desee

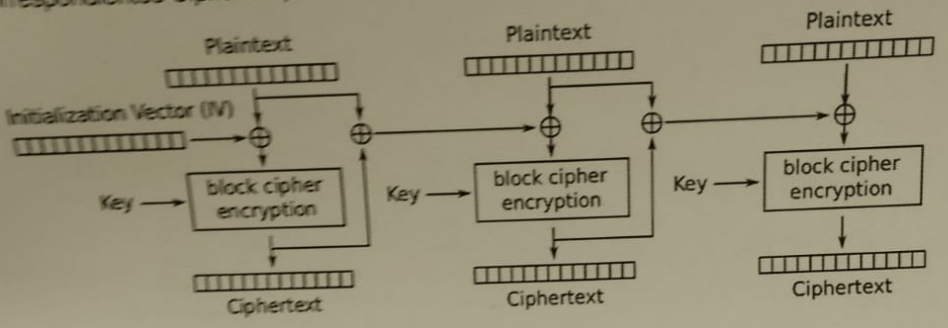
9. En un certificado digital se incluye (seleccione la opción **FALSA**):
   a) La identidad del emisor (nombre distintivo)
   b) La clave pública del titular
   c) La clave pública del emisor
   d) La fecha de caducidad

10. En TLS, los procesos de segmentación, cifrado, control de integridad y compresión (opcional) se llevan a cabo en el:
   a) Handshake protocol
   b) Record protocol
   c) Alert protocol
   d) Transfer protocol

(1 punto)

3. Ejercicio de cifrado.

En la figura adjunta se presenta el modo de operación PCBC (*Propagating cipher-block chaining*) de un sistema de cifrado de bloque (transforma las secuencias *Plaintext* de cada etapa n en sus correspondientes Ciphertext):



Considerando que L[i] y C[i] son los bloques i-ésimos de Legible y Cifrado, que el símbolo ⊕ representa la operación or-exclusiva sobre un bloque, E_K el algoritmo de cifrado con clave K, y D_K el algoritmo de descifrado inverso con la misma clave K,

A) *Expresar algebraicamente la función de cifrado de un bloque n (C[n])*

C[n] =

B) *Expresar algebraicamente la función de descifrado L[n]*

L[n] =

C) *¿Qué representa el Vector de Inicialización? ¿Quién debe conocer el valor de este IV?*

ESCUELA POLITÉCNICA SUPERIOR UNIVERSIDAD SAN PABLO-CEU
Departamento de Tecnologías de la Información

Curso 2023-2

APELLIDOS:	NOMBRE:	DNI:	CALIFICACIÓN:
ASIGNATURA: **SEGURIDAD INFORMÁTICA Y PROTECCIÓN DE DATOS**	FECHA: **7/11/2023**	GRUPO:	

(1 punto)

4. Ejercicio sobre controles

A continuación, se transcribe parte del control 11.2.1 de la ISO 27002 (Registro de usuarios)

Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario.

Guía de Implementación

Se debería controlar el acceso a los servicios de información multiusuario mediante un proceso formal de registro que debería incluir:

a) la utilización de un identificador único para cada usuario, de esta forma puede vincularse a los usuarios y responsabilizarles de sus acciones. Se debería permitir el uso de identificadores de grupo cuando sea conveniente para el desarrollo del trabajo y estos deben ser aprobados y documentados;
b) la comprobación de la autorización del usuario por el propietario del servicio para utilizar el sistema o el servicio de información. También puede ser conveniente que la gerencia apruebe por separado los derechos de acceso;
c) verificación de la adecuación del nivel de acceso asignado al propósito del negocio y su consistencia con la política de seguridad de la organización;
d) la entrega a los usuarios de una relación escrita de sus derechos de acceso;
e) la petición a los usuarios para que reconozcan con su firma la comprensión de las condiciones de acceso;
f) la eliminación inmediata de las autorizaciones de acceso a los usuarios que dejan la organización o cambien de trabajo en ella;
...

Responder a las siguientes cuestiones:

1. *Justificar la necesidad de las recomendaciones d) y e)*
2. *Indique* ***tres métricas*** *que nos permitirían evaluar el grado de implantación de este control.*