Ejercicio 1 (10 PUNTOS)

En el año 2024 un equipo de auditoría financiera solicita a la unidad de auditoría de sistemas de información de la Sindicatura de Cuentas el análisis del proceso de gestión de los ingresos por venta de entradas y abonos de la Empresa Pública Oceanográfico de Valencia, SA, del control interno y de su reflejo en la contabilidad correspondiente a 2023.

En este proceso de negocio se encuentran involucrados tres sistemas de información:

- OCEANIX: Aplicación para la venta de entradas.
- OCEABONO: Aplicación que da soporte a la venta de abonos anuales.
- OCECONTA: Sistema contable de la entidad.

OCEANIX

Es el sistema que da soporte a la venta de entradas.

El pago se realiza a través del enlace de esta aplicación con una pasarela de pago provista por una entidad financiera.

En cuanto al modelo de datos, en la siguiente tabla se muestra la estructura de la tabla de OCEANIX cuyo contenido es relevante para el proceso bajo análisis:

Nombre	**Tipo de dato**	**Descripción**
TIPO_VENTA	Numérico	Tipo de venta 1= On-line 2= Tienda física
COD_VENTA	String	Código unívoco de la venta. La estructura es la siguiente: • Indicador de si es online o física. {O,F} • Año (AAAA) • Mes (MM) • Día (DD) • Número secuencial (xxxxx) que se inicializa cada día
COD_PRODUCTO	Texto	Código del producto
FECHA_VENTA	Fecha	Fecha en que se produce la venta
IMPORTE_VENTA	Numérico	Importe de la venta >0 para las ventas <0 para las devoluciones o rectificaciones de venta

El tamaño de esta tabla, considerando únicamente el año 2023, es de 1.450.000 registros.

OCEABONO

Se trata de una aplicación utilizada exclusivamente para la venta de abonos. En esta aplicación se realiza la venta del abono y su gestión posterior (introducción de los datos necesarios para gestionar la identidad de las personas que compran un abono, control de fecha de inicio y fecha fin del abono, generar la plantilla de impresión del carné de abonado, permitir la consulta de los abonos vigentes en un determinado momento a partir del NIF del cliente, etc.).

El modelo de datos relevante para el análisis es el siguiente:

Nombre	Tipo de dato	Descripción
COD_VENTA	String	Código unívoco de la venta. Su estructura es: • "AB" • Año (AAAA) • Mes (MM) • Día (DD) • Número secuencial (xxxxx) que se inicializa cada día
COD_PRODUCTO	Texto	Código del producto
FECHA_VENTA	Fecha	Fecha en que se produce la venta
IMPORTE_VENTA	Numérico	Importe de la venta >0 para las ventas <0 para las devoluciones o rectificaciones de venta

El tamaño de esta tabla, considerando únicamente el año 2023, es de 100.250 registros.

OCECONTA

La información de la venta de entradas procedente de las aplicaciones de gestión de la venta de entradas y abonos se incorpora al sistema OCECONTA de la siguiente forma:

- La información procedente de la venta online se integra en OCECONTA a través de un webservice que, tras producirse la venta (cuando se confirma el pago correcto), registra esta información en OCECONTA.

  Se utiliza para ello la tabla *OCECONTA_WEB*.

- El personal del departamento contable, que según nos indican es el único con acceso a la aplicación, incorpora la información de las ventas realizadas en tienda a OCECONTA a través de una serie de ficheros de texto plano que extraen de la aplicación OCEANIX diariamente. Se utiliza para ello una opción de menú de la aplicación.

  Esta información queda almacenada en la tabla *OCECONTA_TIEN*.

- Las ventas correspondientes a los abonos se introducen manualmente en ambos sistemas, en OCEABONO y en OCECONTA. El personal de la tienda es quien la introduce en OCEABONO y genera unos listados de la venta de abonos realizada durante el mes para que el departamento de contabilidad lo registre en OCECONTA a mes vencido.

  La información queda registrada en la tabla *OCECONTA_AB*.

Las tres tablas citadas anteriormente (*OCECONTA_WEB*, *OCECONTA_TIEN* y *OCECONTA_AB)* comparten la siguiente estructura:

Nombre	Tipo de dato	Descripción
COD_VENTA	Numérico	Código unívoco de la venta. • Año (AAAA) • Mes (MM) • Día (DD) • Número secuencial (xxxxx) que se inicializa cada día
COD_PRODUCTO	Texto	Código del producto
FECHA_VENTA	Fecha	Fecha en que se produce la venta
IMPORTE_VENTA	Numérico	Importe de la venta >0 para las ventas <0 para las devoluciones o rectificaciones de venta

La entidad nos informa que la aplicación OCECONTA, sujeta al cumplimiento del Esquema Nacional de Seguridad y clasificada como de nivel medio, es una aplicación que se aloja en la nube privada de la entidad contratada al proveedor Kionix en modo SaaS.

Contabilización de los ingresos por venta de entradas y abonos:

- Venta de entradas:
  Diariamente la aplicación OCECONTA agrupa las ventas realizadas el día anterior y anotadas en las tablas *OCECONTA_WEB* y *OCECONTA_TIEN* para hacer un único apunte en el libro diario dependiendo del canal de venta. Para la venta online se utiliza la cuenta 70001 y para la venta en tienda la cuenta 70002.

- Venta de abonos:
  Una vez el personal de contabilidad ha introducido manualmente cada una de las ventas de abonos realizadas el mes anterior, debe ejecutar una opción de menú que agrupa todas las ventas anteriores y genera un único apunte mensual de venta de abonos en la cuenta 70003, que se registra con fecha valor correspondiente al último día del mes anterior.

- Cada apunte queda almacenado en la tabla OCECONTA_Apuntes, en la que se registran todos los apuntes realizados en contabilidad. Esta tabla tiene la siguiente información:

Nombre	**Tipo de dato**	**Descripción**
CodApunte	Numérico	Código unívoco del apunte contable.
Cuenta	Numérico	Código de la cuenta contable.
FechaApunte	Fecha	Fecha en la que se realiza el apunte contable
FechaValor	Fecha	Fecha de valor del apunte
Signo	Texto	Puede tomar los siguientes valores: "D"=Debe "H"=Haber
Importe	Numérico	Importe del apunte

Se pide:

a) Poner sendos ejemplos (no los describa con detalle, solo déjelos indicados de forma general) de procedimiento de valoración del riesgo, prueba de control y procedimiento sustantivo que se podría realizar en la auditoría de ingresos de esta entidad utilizando herramientas y técnicas automatizadas. Indique también muy sucintamente que entiende por cada uno de esos tres tipos de procedimiento. (2 puntos).

b) Finalmente, se decide utilizar el análisis de datos en este trabajo de auditoría. En concreto, para verificar la integridad del proceso de contabilización de ingresos por venta de entradas y abonos. (6,5 puntos)

   i. Haga una relación de pruebas de datos a realizar, indicando para cada una de ellas su objetivo, los riesgos asociados, qué información utilizaría y qué comprobaciones y cómo las realizaría. (5 puntos)

   ii. Describa qué tareas debería realizar en la etapa de planificación de cualquiera de las pruebas anteriores. (1,5 puntos)

c) Con respecto a la aplicación OCEOCONTA: (1,5 puntos)

   i) Indicar el modo de despliegue de la aplicación OCEOCONTA y explique las características de este. (0,5 puntos)

   ii) Indicar el tipo de servicio en nube contratado, y las características de este. (0,5 puntos)

   iii) Indicar cinco aspectos que debe tener el contrato que regule este servicio y que sean importantes para garantizar que los riesgos asociados al uso de la nube están adecuadamente gestionados. (0,5 puntos)

Ejercicio 3. (10 puntos)

Antecedentes

Su equipo de auditoría forma parte de la Sindicatura de Cuentas y le han encomendado planificar y ejecutar la auditoría de las cuentas anuales de 2022 del Organismo Autónomo XX, prestador de servicios deportivos al ciudadano en un ayuntamiento.

En estos momentos está en una fase inicial del trabajo y solo dispone de la información que se señala a continuación, pero debe hacer una planificación preliminar de la auditoría con la información disponible.

Cuentas anuales de 2022 (cifras en euros):

Balance

Activo		Pasivo	
85.000	Inmovilizado	Fondos propios	-20.000
20.000	Deudores	Préstamos a L.P.	290.000
50.000	Caja	Proveedores	35.000
150.000	Bancos		
305.000	**Total**	**Total**	**305.000**

Liquidación del presupuesto

Derechos reconocidos		Obligaciones reconocidas	
		1. Gastos personal	400.000
50.000	3. Precios públicos	2. Compras de bienes y servicios	400.000
780.000	4. Transferencias de capital de la DP	3. Gastos financieros	10.000
		6. Inversiones	20.000
830.000	**Total**	**Total**	**830.000**

Otra información

El personal consiste en 4 empleados de mantenimiento, 1 empleado de administración y 1 de informática.

El interventor municipal va cada 15 días a supervisar la marcha de la entidad.

Ha iniciado la auditoría de acuerdo con la *GPF-OCEX 1315 Revisada*, realizado un análisis preliminar e identificado y valorado una serie de posibles riesgos de incorrección material en las afirmaciones.

Ha completado una tabla (ver anexo) en la que se señala para cada tipo de transacción, saldo contable e información a revelar (TTSCIR) qué afirmaciones les afecta y la probabilidad de su riesgo inherente, que ha determinado de forma preliminar.

La entidad utiliza para su gestión contable y de compras el ERP de la entidad matriz: SAP S/4 HANA; y para la gestión del personal y nóminas la aplicación HUMAN++.

Se pide:

a) Calcular y razonar: (2 puntos)

- El nivel de importancia relativa.
- El nivel de importancia relativa para la ejecución del trabajo.
- El umbral de las incorrecciones claramente insignificantes.

b) Con la información del Anexo, debe determinar la magnitud esperada del riesgo para cada afirmación y calcular la valoración del riesgo inherente.

A continuación, despreciando los riesgos inherentes en las afirmaciones cuya valoración sea inferior a 25 (<25), los representará gráficamente en el espectro de riesgo inherente. Debe completar la tabla del anexo en el ejemplar adicional que se le entrega. Ponga los comentarios que considere pertinentes sobre ese ejemplar del anexo. (1,5 puntos)

c) Deberá señalar que riesgos considera significativos y por qué. (1,5 punto)

d) Para las afirmaciones cuyo riesgo inherente ha considerado significativo indique si va a valorar el riesgo de control y justifique las razones que sustentan esa decisión. (1,5 punto)

e) Señale:

- Qué tipos de transacciones y saldos contables se podrán considerar significativos en la auditoría y por qué. (1 punto)
- Qué aplicaciones informáticas serán significativas. (0,5 puntos)

f) A la vista de los riesgos significativos del apartado c) señale al menos un procedimiento de auditoría que responda a cada uno de ellos, para incorporarlos al programa de auditoría. (2 puntos)

Razone y justifique las respuestas.

Ejercicio 2 (11 puntos)

En este supuesto usted, como auditor de sistemas de información de la Sindicatura de Cuentas, va a ayudar al equipo de auditoría financiera en la auditoría de las cuentas anuales de 2022 que están realizando del Organismo Autónomo XX, cuyos datos básicos se han descrito en el Ejercicio 3.

Con respecto a las aplicaciones utilizadas por la entidad disponemos de la siguiente información:

SAP S/4 HANA

En la aplicación SAP S/4 HANA están dados de alta los seis empleados de la entidad más el interventor municipal. Los siete usuarios cuentan con el perfil que otorga el máximo nivel de privilegios en el sistema (SAP_ALL).

La implantación se realizó mediante un contrato adjudicado a la empresa TuSap, con la que también se tuvo un contrato de mantenimiento y evolución del sistema. No obstante, desde hace un año la entidad ha prescindido de este servicio y el sistema no se ha modificado desde entonces.

HUMAN ++

Respecto a la arquitectura del sistema, cuenta con una arquitectura de 3 capas en la que todos los roles se encuentran en la misma máquina, pese a las recomendaciones del fabricante.

El servidor se encuentra en la DMZ del organismo que está protegida por un firewall en el que se han detectado vulnerabilidades de seguridad en auditorías anteriores.

El servidor de base de datos que emplea el sistema es Oracle 10.2 y como servidor de aplicaciones utiliza WebLogic Server 6.1.

La aplicación ha sido desarrollada durante los últimos 20 años por el empleado responsable de la informática, a partir de un producto de mercado comprado en su momento. No disponen de documentación técnica de la aplicación (modelo de datos, modificaciones realizadas sobre el producto original, compatibilidades, etc.).

Se realizan muy pocas modificaciones de la aplicación, aunque es un aspecto que no podemos comprobar porque no se han activado los logs de auditoría y la documentación sobre el proceso de desarrollo es prácticamente inexistente.

Dado que hay muy pocos cambios (como mucho 2 o 3 al año), la entidad no dispone de un entorno de pruebas. Según nos indican, si hubiese que realizar cambios en los sistemas se podrían aplicar directamente en los sistemas de producción, y los cambios de la aplicación, al ser básicamente listados, se prueban también cuidadosamente en ese entorno.

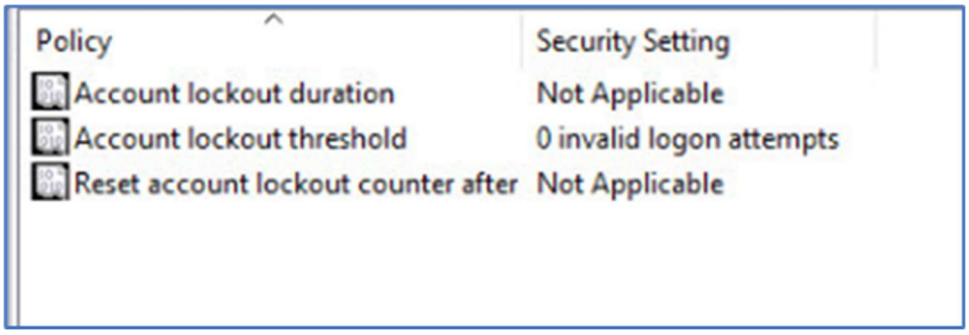
La persona de informática tiene previsto jubilarse a final de año.

El acceso a la aplicación se realiza mediante usuario y contraseña. La aplicación tiene delegada la autenticación en el Directorio Activo de Windows.

Las características de la política de autenticación son las siguientes:

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Las características de la política de la política de bloqueo de cuenta son las siguientes:



Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

Información común para ambas aplicaciones:

Las copias de seguridad se realizan mediante una herramienta específica para este propósito. Se realiza una copia semanal total del sistema los domingos y el resto de los días se hacen copias incrementales. Las copias se almacenan en una cabina de discos ubicada en el CPD de la entidad, con el objetivo de poder restablecer el sistema lo más rápido posible en caso de tener un incidente de seguridad.

El CPD se encuentra en el sótano del edificio, en una sala en la que también se almacena el material de oficina (tóneres, papel, etc.). La puerta está cerrada con llave y cuando los empleados necesitan coger algo se la piden a la persona de administración. La sala cuenta con una máquina de aire acondicionado y con un extintor de incendios.

La valoración del sistema en función de las dimensiones de seguridad es la siguiente:

- Confidencialidad: medio
- Integridad: medio
- Autenticidad: bajo
- Disponibilidad: bajo
- Trazabilidad: bajo

El análisis anterior es el único avance realizado por la entidad en materia de cumplimiento del Esquema Nacional de Seguridad.

En este ejercicio, en su calidad de auditor de sistemas, se le pide:

a) Para la preparación de la memoria de planificación, elaborar una tabla en la que se indique las áreas en las que se estructura la revisión de CGTI y los objetivos de control que están incluidos en cada área, de acuerdo con la GPF-OCEX-5330. (2 puntos)
b) Explicar la relación de los CGTI y los controles básicos de ciberseguridad. Señale cuáles son los controles básicos de ciberseguridad (CBCS), y describa una prueba de auditoría para cada CBCS que haría durante el trabajo de campo. (2 puntos)
c) A partir de los datos disponibles de los sistemas de información del organismo autónomo XX, señalar las deficiencias de control interno que haya detectado. Para cada una de ellas describa: en qué consiste la deficiencia de control interno, el riesgo asociado, la importancia relativa y la recomendación que propondría para corregirla. (7 puntos)

ANEXO

TTSCIR	Afirmación	Observaciones	Valoración del Riesgo inherente en las afirmaciones		
			Probabilidad 0<P<10	**Magnitud** 0<M<10	**Valoración**
Gastos Capítulo 1	Ocurrencia	En la entidad existe poco personal y está bien identificado y controlado por lo que los gastos reales en las obligaciones reconocidas es improbable que no se correspondan con la realidad.	2		
	Completitud	Puede darse el caso de que los gastos de seguridad social no estén contabilizados ya que las liquidaciones las hace una gestoría y se envían al banco para su cargo en cuenta. En el caso de que la entidad contabilice la nómina después del pago, el riesgo es superior.	6		
	Exactitud	Las obligaciones reconocidas, OR, se contabilizan a través de una interfaz automática generada por el programa de nóminas. Las OR de la Seguridad Social, SS, se contabilizan manualmente cuando viene el cargo bancario.	2		
	Corte de operaciones	La probabilidad de que se impute el reconocimiento de obligaciones por gastos de personal a un período al que no corresponde es posible, en particular con la SS, en caso de reclamaciones administrativas o en sede judicial de atrasos.	5		
	Clasificación	Es fácil la determinación de la cuenta del plan en la que imputar las obligaciones reconocidas por este concepto.	1		
	Presentación	No existe duda sobre la descripción de las obligaciones reconocidas como gastos de personal	2		
	Legalidad	Existe el riesgo de que pudieran reconocerse retribuciones por encima de las establecidas o de productividades, gratificaciones y horas extras que no se hayan tramitado correctamente o superen los máximos legamente establecidos.	5		
Gastos Capítulo 2	Ocurrencia	Buena parte del gasto corresponde a consumos de energía y agua que están bien medidos y han experimentado un aumento muy importante.	3		
	Completitud	Hemos observado que, aunque de pequeño importe, se ha realizado algún pago “urgente” sin crédito presupuestario y contabilizado en una cuenta no presupuestaria (no se había contabilizado la OR).	5		
	Exactitud	Es posible que la valoración de la adquisición de algún gasto o compra no se haya realizado correctamente.	4		
	Corte de operaciones	Es posible que haya facturas de proveedores que se presenten tarde y los gastos se imputen a períodos a los que no corresponden.	8		

TTSCIR	Afirmación	Observaciones	Valoración del Riesgo inherente en las afirmaciones		
			Probabilidad 0<P<10	**Magnitud** 0<M<10	**Valoración**
	Clasificación	Puede surgir alguna duda de imputación a la cuenta correspondiente de algún gasto.	4		
	Presentación	La descripción, especialmente, de algún gasto puede resultar poco clara.	4		
	Legalidad	Existe una gran probabilidad de que no se hayan seguido los procedimientos de contratación legamente establecidos para su adquisición.	9		
Ingresos Capítulo 3	Ocurrencia	El riesgo se considera bajo, porque al tratarse de ingreso directo, sin contraído previo, los derechos reconocidos coincidirán con ingresos realizados por este concepto.	2		
	Completitud	Se considera un riesgo de probabilidad alta porque al cobrarse en la taquilla es posible que determinados ingresos no se contabilicen, sobre todo si tenemos en cuenta el importe de existencias en la caja tan significativo. Se desconoce si solo cobra en la taquilla el personal de administración, porque en otro caso, aumenta la probabilidad de que no se ingrese la totalidad o que se dé mal el cambio y, por tanto, no aparecerían completamente contabilizados. Tampoco sabemos si hay taquillas automáticas o billetes prenumerados.	9		
	Exactitud	La contabilización se corresponde con el ingreso, por lo que el riesgo de inexactitud es mínimo.	2		
	Corte de operaciones	La contabilización coincidirá con el ingreso y se imputará al período correspondiente. Desconocemos si los ingresos se realizan puntualmente.	6		
	Clasificación	Es fácil la determinación de la cuenta del plan en la que imputar los derechos reconocidos por este concepto y no existe duda sobre la presentación de los ingresos reconocidos	2		
	Presentación		2		
	Legalidad	Podría darse un incumplimiento de la legalidad, por ejemplo, en la aplicación de bonificaciones o de las tarifas aplicables en función de la edad o similares. También existe el riesgo de fraude.	9		
Ingresos Capítulo 4	Ocurrencia	Se pudo haber reconocido el derecho sin que el compromiso por parte de la Diputación sea firme, o que no se cumplan los requisitos para ser beneficiario.	7		
	Completitud	Es difícil que en el caso de la transferencia de Diputación no se contabilice el total de la misma, salvo un error numérico al contabilizar.	2		
	Exactitud	La contabilización se corresponde con el ingreso, por lo que el riesgo de inexactitud es mínimo.	2		

TTSCIR	Afirmación	Observaciones	Valoración del Riesgo inherente en las afirmaciones		
			Probabilidad 0<P<10	**Magnitud** 0<M<10	**Valoración**
	Corte de operaciones	Se considera posible que se reconozca el derecho antes del cumplimiento de los requisitos para su percepción y, por tanto, se impute antes de lo que procedería, sobre todo teniendo en cuenta que está pendiente de cobro.	6		
	Clasificación	Es fácil la determinación de la cuenta del plan en la que imputar los derechos reconocidos por este concepto. No obstante, se detecta ya que ha sido contabilizada en capítulo 7 en lugar de 4	10		
	Presentación	No existe duda sobre la descripción de los ingresos reconocidos, pero en la revisión preliminar hemos visto que están mal contabilizados.	10		
	Legalidad	El riesgo de incumplimiento de la legalidad en el caso del reconocimiento de un derecho por una transferencia corriente de la Diputación es bajo porque estaría también controlado por la otra Administración.	3		
Caja	Existencia	Se determina un riesgo alto puesto que se trata de un elemento muy volátil. Existe en la entidad un único empleado de administración en el centro deportivo y el Interventor municipal va a supervisar cada 15 días. Además, el importe en caja es muy elevado.	9		
	Derechos y obligaciones	El saldo existente en la caja no es probable que sea de un tercero.	1		
	Completitud	Se valora el riesgo como alto puesto que pudiera existir dinero fuera de la caja.	9		
	Exactitud, valoración e imputación	El riesgo de un error en la valoración de las existencias de caja es medio, considerando el importante volumen existente en efectivo en caja y, previsiblemente, derivado íntegramente del cobro de los precios públicos en taquilla, por lo que existirán muchos billetes pequeños y monedas.	4		
	Clasificación	Es muy difícil equivocarse en la cuenta de contabilización en el caso de la caja	1		
	Presentación	No existe duda sobre la descripción del activo	1		

TTSCIR	Afirmación	Observaciones	Valoración del Riesgo inherente en las afirmaciones		
			Probabilidad 0<P<10	**Magnitud** 0<M<10	**Valoración**
Bancos	Existencia	Se determina un riesgo alto puesto que se trata de un elemento muy volátil. Podría darse el caso de que, por ejemplo, se utilizase la firma de los claveros fraudulentamente.	8		
	Derechos y obligaciones	El saldo ingresado en la entidad bancaria difícilmente será propiedad de un tercero.	2		
	Completitud	Se valora un riesgo medio porque pudiera darse el caso, aunque no muy probable, de que se desconociera la existencia de alguna cuenta bancaria en alguna entidad.	5		
	Exactitud, valoración e imputación	El riesgo de un error en la valoración de las existencias de bancos es prácticamente inexistente.	2		
	Clasificación	Es muy difícil equivocarse en la cuenta de contabilización en el caso de bancos, aunque un poquito superior al de la caja de la entidad, puesto que pudiera imputarse a otra cuenta bancaria.	2		
	Presentación	No existe duda sobre la descripción del activo.	2		