

Convocatoria para la provisión, mediante oposición, de dos plazas de técnico/a de grado medio en sistemas informáticos al servicio de la Cámara de Comptos de Navarra.

(Aprobada por Resolución del presidente de la Cámara de Comptos de 20 de marzo de 2025 y publicada en el Boletín Oficial de Navarra, número 72 de 10 de abril de 2025)

EJERCICIO SEGUNDO

Valoración: 65 PUNTOS

(12 de marzo de 2026)



SUPUESTO (65 PUNTOS)

En el año 2026, la Cámara de Comptos va a realizar una **auditoría financiera y de cumplimiento** sobre los principales ingresos del organismo autónomo TEATRO GAYAK de la Administración de la Comunidad Foral de Navarra del ejercicio 2025, que se corresponden con la venta de entradas y con las suscripciones al programa AMIGOS DE GAYAK.

Durante el ejercicio 2025, en este proceso de negocio se encuentran involucrados los siguientes sistemas de información:

- AMIGOS_GAYAK: gestiona las suscripciones a este programa.
- ENTRA_GAYAK 2.0: da soporte a la venta de entradas.
- CONTA_GAYAK: sistema contable del organismo autónomo.

Se anexa el modelo de datos de estos tres sistemas.

En cumplimiento de la Ley Foral reguladora de la Cámara de Comptos, TEATRO GAYAK nos ha concedido conectividad y acceso total a los sistemas de información que intervienen en el proceso.

De la reunión inicial mantenida entre el equipo de auditoría y el organismo autónomo, se ha recabado la siguiente información:

- En la segunda quincena de diciembre, TEATRO GAYAK difunde por diferentes medios (emails asociados, redes sociales, prensa escrita y su propia página web) la programación cultural prevista para el año siguiente.
- Las personas que abonen una tasa anual disfrutarán de los beneficios del programa AMIGOS DE GAYAK, que son:
 - a) Periodo preferente de compra.
 - b) Comisión “cero” en la compra de entradas.
 - c) Recepción del folleto de la programación en domicilio.

La suscripción al programa se puede realizar directamente en AMIGOS_GAYAK o físicamente en la taquilla del teatro.

El disfrute de las ventajas anteriores es efectivo a partir del día 1 del mes siguiente a la fecha de abono de la tasa.

- El abono de la tasa correspondiente, tanto si se realiza en AMIGOS_GAYAK como en la taquilla pagándose con tarjeta bancaria, se realiza a través del enlace de esta aplicación con una pasarela de pago provista por una entidad financiera. El pago de la tasa podrá realizarse también en efectivo en taquilla



- En los 10 días anteriores a la venta general de entradas, las personas suscriptoras del programa AMIGOS DE GAYAK pueden comprar, en ENTRA_GAYAK o en taquilla, las entradas que deseen.

El resto de personas que quieran acudir a los espectáculos programados podrán realizar la compra de entradas durante el periodo de venta general, que comienza un mes antes de la fecha del espectáculo.

- Los precios de las entradas de los espectáculos del TEATRO GAYAK están regulados en un decreto foral en el que consta la siguiente información:

Tipo de entrada	Importe
General	Según espectáculo
Jubilad@s	65% del precio General
Familia numerosa	85% del precio General
Grupos (más de 4 entradas)*	90% del precio General
Suscriptores AMIGOS DE GAYAK con antigüedad superior a 5 años	Descuento adicional del 5%

*El descuento por venta de más de 4 entradas es incompatible con cualquier otro descuento.

La comisión de gestión asciende a 1,5 euros por entrada adquirida.

- En 2024, se detectaron fallos en el volcado de información entre ENTRA_GAYAK 1.0 y AMIGOS_GAYAK, lo que motivó llevar a cabo un nuevo proyecto para el desarrollo de un módulo dentro de ENTRA_GAYAK para la gestión de las suscripciones al programa AMIGOS DE GAYAK. Se espera que este módulo entre en funcionamiento en el primer trimestre de 2026.
- El abono de las entradas se realiza a través del enlace de esta aplicación con una pasarela de pago provista por una entidad financiera o en efectivo en la taquilla del teatro.
- La acreditación del derecho a los distintos tipos de entradas se realiza de la siguiente forma:
 - a) Personas jubiladas: ENTRA_GAYAK llama a través del DNI a la base de datos de la Seguridad Social para verificar el cumplimiento de este requisito de manera previa a la venta de la entrada.
 - b) Familias numerosas: deberán presentar el carné acreditativo de esta condición al acceder al espectáculo. Existe una aplicación de gestión de familias numerosas para fines estadísticos.
- El teatro traslada al equipo de auditoría que durante el ejercicio 2025 recibió tres incidencias sobre el porcentaje de descuento aplicado en la venta de entradas a familias numerosas.
- El dinero en efectivo recaudado en taquilla se ingresa en el banco mensualmente.



- La información de la venta de suscripciones al programa AMIGOS DE GAYAK y de entradas procedentes de las aplicaciones de gestión se incorpora a CONTA_GAYAK de la siguiente forma:
 - a) Existen dos partidas presupuestarias para registrar estos ingresos: una para los procedentes de la suscripción al programa AMIGOS DE GAYAK y otra para los obtenidos por la venta de entradas.
 - b) Mensualmente, AMIGOS_GAYAK genera un fichero txt con los datos de la tabla ABONOS anexada. Este fichero lo recibe encriptado la persona encargada de contabilizar estos ingresos en un único apunte contable en la partida presupuestaria correspondiente.
 - c) La información procedente de la venta de entradas se integra en CONTA_GAYAK a través de un web service que, tras producirse la venta y confirmado el pago del precio, registra esta información en la partida presupuestaria correspondiente en apuntes contables individualizados.
- La aplicación CONTA_GAYAK, 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.
- A finales de 2024, el sistema ENTRA_GAYAK recibió un ataque cibernético que supuso el robo de datos de las personas que habían accedido a la venta de entradas.



SE PIDE:

- 1) Elaborar un diagrama de flujo de procesos sobre la gestión de los ingresos objeto de fiscalización. **(7 PUNTOS)**
- 2) Señalar los sistemas/aplicaciones sobre los que se deberían realizar controles generales justificando las razones para ello. **(2,5 PUNTOS)**
- 3) Describir, de acuerdo con las guías prácticas de fiscalización de los OCEX, cinco ejemplos relevantes de controles generales referidos a gestión de cambios en aplicaciones y sistemas, así como a controles de acceso a datos y programas.

(12,5 PUNTOS)

- 4) En el marco del trabajo de campo, el personal informático que forma parte del equipo de auditoría realizará las consultas necesarias a los sistemas de información para verificar los siguientes aspectos:
 - La corrección del importe de los ingresos registrados en el ejercicio fiscalizado en la partida VENTAS ENTRADAS, correspondientes a la venta de entradas a personas jubiladas no suscriptoras al programa AMIGOS DE GAYAK. **(9 PUNTOS)**
 - La adecuación de las fechas de venta de las entradas, teniendo en cuenta la existencia de un periodo preferente de compra para las personas suscriptoras del programa AMIGOS DE GAYAK. **(7 PUNTOS)**
 - La relación de personas que reúnen los requisitos para la aplicación del descuento adicional del 5 % a día de hoy. **(5 PUNTOS)**

Detallar las sentencias SQL que permitan obtener los datos requeridos.

- 5) Ante el incidente ocurrido a finales de 2024, el equipo de auditoría decide realizar una auditoría de ciberseguridad sobre el proceso continuo de identificación y remediación de vulnerabilidades según la “GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa”. Diseñar el programa de auditoría correspondiente. **(7 PUNTOS)**
- 6) El equipo de auditoría acuerda la revisión del expediente de contratación tramitado por el TEATRO GAYAK para la implantación de la aplicación de contabilidad CONTA_GAYAK.

Indicar, de acuerdo con lo establecido en la “GPF-OCEX 1403. Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios de computación en la nube”, seis ítems específicos que deben contener los pliegos en este tipo de contratación, exceptuando los referidos al tipo de servicio y al tipo de infraestructura requeridos. De los seis ítems señalados, al menos uno deberá estar directamente relacionado con la protección de datos y otro con la continuidad del servicio. **(7,5 PUNTOS)**

NOTA: No se ha previsto la subcontratación ni la cesión de datos.



CÁMARA DE
COMPTOS DE
NAVARRA
NAFARROAKO
KONTUEN
GANBERA

- 7) El equipo de auditoría decide realizar la revisión del control D1 «Uso controlado de privilegios de administración» de acuerdo con lo establecido en la “GPF-OCEX 5334. *Revisión de los CGTI del área D: Controles de acceso a datos y programas*”.

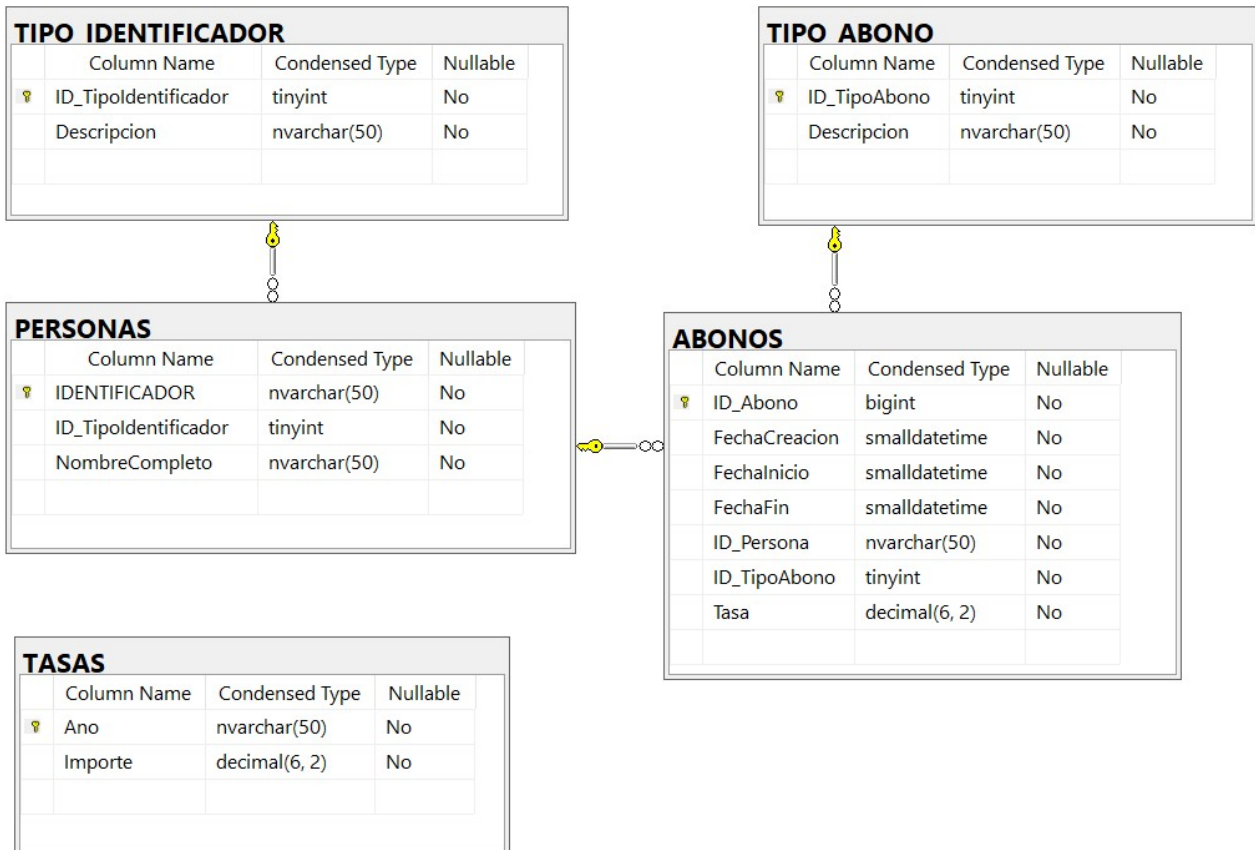
(7,5 PUNTOS)

- Indicar cuáles de los subcontroles recogidos en la guía deberían revisarse en la aplicación CONTA-GAYAK, justificando la respuesta.
- Seleccionar uno de los subcontroles anteriores e identificar tres evidencias que deberían solicitarse durante la auditoría, indicando si la solicitud debe remitirse al TEATRO GAYAK o al proveedor de servicios en la nube (Cloud Service Provider - CSP).



ANEXO. MODELO DE DATOS

AMIGOS_GAYAK



TIPO_IDENTIFICADOR

ID_Tipoidentificador	Descripcion
1	DNI
2	NIE
3	PASAPORTE
4	CIF

TIPO_ABONO

ID_TipoAbono	Descripcion
1	ON LINE
2	TAQUILLA

TASAS

Ano	Importe
2020	35,00
2021	36,00
2022	37,00
2023	38,00
2024	39,00
2025	40,00
2026	42,00



```
CREATE TABLE [dbo].[TIPO_ABONO](
    [ID_TipoAbono] [tinyint] NOT NULL,
    [Descripcion] [nvarchar](50) NOT NULL,
    CONSTRAINT [PK_TIPO_ABONO] PRIMARY KEY CLUSTERED
(
    [ID_TipoAbono] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[TIPO_IDENTIFICADOR](
    [ID_TipoIdentificador] [tinyint] NOT NULL,
    [Descripcion] [nvarchar](50) NOT NULL,
    CONSTRAINT [PK_TIPO_IDENTIFICADOR] PRIMARY KEY CLUSTERED
(
    [ID_TipoIdentificador] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[PERSONAS](
    [IDENTIFICADOR] [nvarchar](50) NOT NULL,
    [ID_TipoIdentificador] [tinyint] NOT NULL,
    [NombreCompleto] [nvarchar](50) NOT NULL,
    CONSTRAINT [PK_PERSONAS] PRIMARY KEY CLUSTERED
(
    [IDENTIFICADOR] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO

ALTER TABLE [dbo].[PERSONAS] WITH CHECK ADD CONSTRAINT
[FK_PERSONAS_TIPO_IDENTIFICADOR] FOREIGN KEY([ID_TipoIdentificador])
REFERENCES [dbo].[TIPO_IDENTIFICADOR] ([ID_TipoIdentificador])
GO

ALTER TABLE [dbo].[PERSONAS] CHECK CONSTRAINT [FK_PERSONAS_TIPO_IDENTIFICADOR]
GO

CREATE TABLE [dbo].[TASAS](
    [Ano] [nvarchar](50) NOT NULL,
    [Importe] [decimal](6, 2) NOT NULL,
    CONSTRAINT [PK_TASAS] PRIMARY KEY CLUSTERED
(
    [Ano] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO
```



CÁMARA DE
COMPTOS DE
NAVARRA
NAFARROAKO
KONTUEN
GANBERA

```
CREATE TABLE [dbo].[ABONOS](
    [ID_Abono] [bigint] NOT NULL,
    [FechaCreacion] [smalldatetime] NOT NULL,
    [FechaInicio] [smalldatetime] NOT NULL,
    [FechaFin] [smalldatetime] NOT NULL,
    [ID_Persona] [nvarchar](50) NOT NULL,
    [ID_TipoAbono] [tinyint] NOT NULL,
    [Tasa] [decimal](6, 2) NOT NULL,

CONSTRAINT [PK_ABONOS] PRIMARY KEY CLUSTERED
(
    [ID_Abono] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO

ALTER TABLE [dbo].[ABONOS] WITH CHECK ADD CONSTRAINT [FK_ABONOS_PERSONAS]
FOREIGN KEY([ID_Persona])
REFERENCES [dbo].[PERSONAS] ([IDENTIFICADOR])
GO

ALTER TABLE [dbo].[ABONOS] CHECK CONSTRAINT [FK_ABONOS_PERSONAS]
GO

ALTER TABLE [dbo].[ABONOS] WITH CHECK ADD CONSTRAINT [FK_ABONOS_TIPO_ABONO]
FOREIGN KEY([ID_TipoAbono])
REFERENCES [dbo].[TIPO_ABONO] ([ID_TipoAbono])
GO

ALTER TABLE [dbo].[ABONOS] CHECK CONSTRAINT [FK_ABONOS_TIPO_ABONO]
GO

EXEC sys.sp_addextendedproperty @name=N'MS_Description', @value=N'Fecha del
registro', @level0type=N'SHEMA',@level0name=N'dbo',
@level1type=N'TABLE',@level1name=N'ABONOS',
@level2type=N'COLUMN',@level2name=N'FechaCreacion'
GO

EXEC sys.sp_addextendedproperty @name=N'MS_Description', @value=N'Fecha de inicio
de antigüedad del abono', @level0type=N'SHEMA',@level0name=N'dbo',
@level1type=N'TABLE',@level1name=N'ABONOS',
@level2type=N'COLUMN',@level2name=N'FechaInicio'
GO
```



ENTRA_GAYAK

IMPORTE CONFIG			
Column Name	Condensed Type	Nullable	
⚡ Ano	nvarchar(50)	No	
⚡ ID_TipoImporte	tinyint	No	
Importe	decimal(6, 2)	No	

TIPO VENTA			
Column Name	Condensed Type	Nullable	
⚡ ID_TipoVenta	tinyint	No	
Descripcion	nvarchar(50)	No	

TIPO IMPORTE			
Column Name	Condensed Type	Nullable	
⚡ ID_TipoImporte	tinyint	No	
Descripcion	nvarchar(50)	No	

VENTAS			
Column Name	Condensed Type	Nullable	
⚡ ID_Venta	bigint	No	
FechaVenta	smalldatetime	No	
NumEntradas	int	No	
ID_Abono	bigint	Yes	
ID_Espectaculo	bigint	No	
ID_TipoVenta	tinyint	No	
ID_TipoImporte	tinyint	No	
Importe	decimal(6, 2)	No	

ESPECTACULOS			
Column Name	Condensed Type	Nullable	
⚡ ID_Espectaculo	bigint	No	
Titulo	nvarchar(50)	No	
Descripcion	nvarchar(50)	Yes	
Responsable	nvarchar(50)	Yes	
Duracion	real	Yes	
Edad	nvarchar(50)	Yes	
Importe	decimal(6, 2)	No	
FechaEspectaculo	smalldatetime	No	



IMPORTE_CONFIG

Ano	ID_TipoImporte	Importe
2025	1	1,00
2025	2	0,65
2025	3	0,85
2025	4	0,90
2025	5	0,05
2025	6	1,50
2026	1	1,00
2026	2	0,65
2026	3	0,85
2026	4	0,90
2026	5	0,05
2026	6	1,50

TIPO_IMPORTE

ID_TipoImporte	Descripcion
1	General
2	Jubilados
3	Familia Numerosa
4	VentaMas4
5	AbonadosMas5
6	Comision

TIPO_VENTA

ID_TipoVenta	Descripcion
1	ON LINE
2	TAQUILLA



```
CREATE TABLE [dbo].[TIPO_IMPORTE](
    [ID_TipoImporte] [tinyint] NOT NULL,
    [Descripcion] [nvarchar](50) NOT NULL,
    CONSTRAINT [PK_TIPO_IMPORTE] PRIMARY KEY CLUSTERED
(
    [ID_TipoImporte] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO
```

```
CREATE TABLE [dbo].[IMPORTES_CONFIG](
    [Ano] [nvarchar](50) NOT NULL,
    [ID_TipoImporte] [tinyint] NOT NULL,
    [Importe] [decimal](6, 2) NOT NULL,
    CONSTRAINT [PK_IMPORTES_CONFIG] PRIMARY KEY CLUSTERED
(
    [Ano] ASC,
    [ID_TipoImporte] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO
```

```
ALTER TABLE [dbo].[IMPORTES_CONFIG] WITH CHECK ADD CONSTRAINT
[FK_IMPORTES_CONFIG_TIPO_IMPORTE] FOREIGN KEY([ID_TipoImporte])
REFERENCES [dbo].[TIPO_IMPORTE] ([ID_TipoImporte])
GO
```

```
ALTER TABLE [dbo].[IMPORTES_CONFIG] CHECK CONSTRAINT
[FK_IMPORTES_CONFIG_TIPO_IMPORTE]
GO
```

```
CREATE TABLE [dbo].[ESPECTACULOS](
    [ID_Espectaculo] [bigint] NOT NULL,
    [Titulo] [nvarchar](50) NOT NULL,
    [Descripcion] [nvarchar](50) NULL,
    [Responsable] [nvarchar](50) NULL,
    [Duracion] [real] NULL,
    [Edad] [nvarchar](50) NULL,
    [Importe] [decimal](6, 2) NOT NULL,
    [FechaEspectaculo] [smalldatetime] NOT NULL,
    CONSTRAINT [PK_ESPECTACULOS] PRIMARY KEY CLUSTERED
(
    [ID_Espectaculo] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO
```

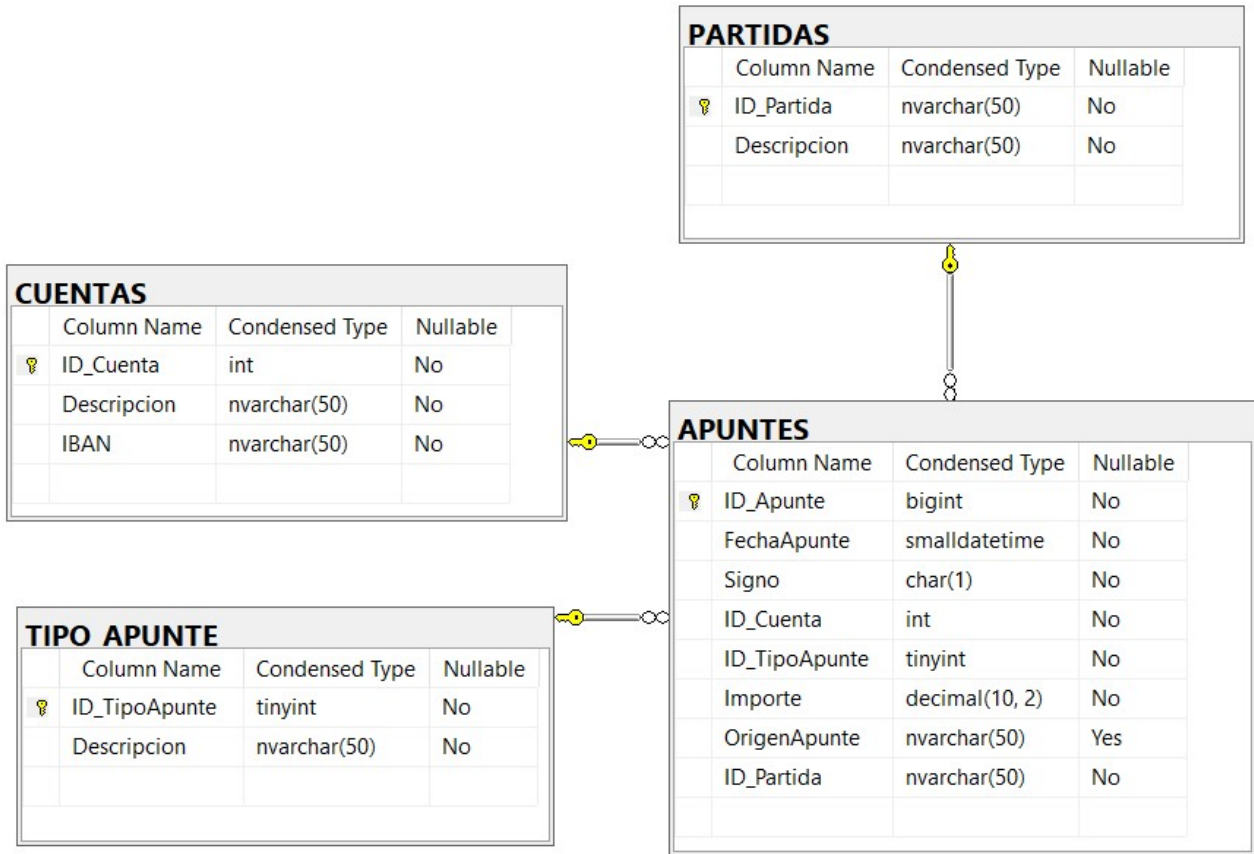
```
CREATE TABLE [dbo].[TIPO_VENTA](
    [ID_TipoVenta] [tinyint] NOT NULL,
    [Descripcion] [nvarchar](50) NOT NULL,
    CONSTRAINT [PK_TIPO_VENTA] PRIMARY KEY CLUSTERED
(
    [ID_TipoVenta] ASC
)
```



```
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,  
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]  
) ON [PRIMARY]  
GO  
  
CREATE TABLE [dbo].[VENTAS](  
    [ID_Venta] [bigint] NOT NULL,  
    [FechaVenta] [smalldatetime] NOT NULL,  
    [NumEntradas] [int] NOT NULL,  
    [ID_Abono] [bigint] NULL,  
    [ID_Espectaculo] [bigint] NOT NULL,  
    [ID_TipoVenta] [tinyint] NOT NULL,  
    [ID_TipoImporte] [tinyint] NOT NULL,  
    [Importe] [decimal](6, 2) NOT NULL,  
    CONSTRAINT [PK_VENTAS] PRIMARY KEY CLUSTERED  
(  
    [ID_Venta] ASC  
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,  
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]  
) ON [PRIMARY]  
GO  
  
ALTER TABLE [dbo].[VENTAS] WITH CHECK ADD CONSTRAINT [FK_VENTAS_ESPECTACULOS]  
FOREIGN KEY([ID_Espectaculo])  
REFERENCES [dbo].[ESPECTACULOS] ([ID_Espectaculo])  
GO  
  
ALTER TABLE [dbo].[VENTAS] CHECK CONSTRAINT [FK_VENTAS_ESPECTACULOS]  
GO  
  
ALTER TABLE [dbo].[VENTAS] WITH CHECK ADD CONSTRAINT [FK_VENTAS_TIPO_IMPORTE]  
FOREIGN KEY([ID_TipoImporte])  
REFERENCES [dbo].[TIPO_IMPORTE] ([ID_TipoImporte])  
GO  
  
ALTER TABLE [dbo].[VENTAS] CHECK CONSTRAINT [FK_VENTAS_TIPO_IMPORTE]  
GO  
  
ALTER TABLE [dbo].[VENTAS] WITH CHECK ADD CONSTRAINT [FK_VENTAS_TIPO_VENTA]  
FOREIGN KEY([ID_TipoVenta])  
REFERENCES [dbo].[TIPO_VENTA] ([ID_TipoVenta])  
GO  
  
ALTER TABLE [dbo].[VENTAS] CHECK CONSTRAINT [FK_VENTAS_TIPO_VENTA]  
GO  
  
EXEC sys.sp_addextendedproperty @name=N'MS_Description', @value=N'Solo cuando se  
trate de una abonado', @level0type=N'SHEMA',@level0name=N'dbo',  
@level1type=N'TABLE',@level1name=N'VENTAS',  
@level2type=N'COLUMN',@level2name=N'ID_Abono'  
GO  
  
EXEC sys.sp_addextendedproperty @name=N'MS_Description', @value=N'1- General, 2-  
Jubilados, 3-Fam. numerosa, 4-Venta más de 4', @level0type=N'SHEMA',@level0name=N'dbo',  
@level1type=N'TABLE',@level1name=N'VENTAS',  
@level2type=N'COLUMN',@level2name=N'ID_TipoImporte'  
GO
```



CONTA_GAYAK



TIPO_APUNTE

ID_TipoApunte	Descripcion
1	SUSCRIPCIÓN
2	ENTRADA
3	OTROS

PARTIDAS

ID_Partida	Descripcion
PARTIDA_1	ABONOS AMIGOS GAYAK
PARTIDA_2	VENTAS ENTRADAS



```
CREATE TABLE [dbo].[TIPO_APUNTE](
    [ID_TipoApunte] [tinyint] NOT NULL,
    [Descripcion] [nvarchar](50) NOT NULL,
    CONSTRAINT [PK_TIPO_APUNTE] PRIMARY KEY CLUSTERED
(
    [ID_TipoApunte] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[CUENTAS](
    [ID_Cuenta] [int] NOT NULL,
    [Descripcion] [nvarchar](50) NOT NULL,
    [IBAN] [nvarchar](50) NOT NULL,
    CONSTRAINT [PK_CUENTAS] PRIMARY KEY CLUSTERED
(
    [ID_Cuenta] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[PARTIDAS](
    [ID_Partida] [nvarchar](50) NOT NULL,
    [Descripcion] [nvarchar](50) NOT NULL,
    CONSTRAINT [PK_PARTIDAS] PRIMARY KEY CLUSTERED
(
    [ID_Partida] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO

CREATE TABLE [dbo].[APUNTES](
    [ID_Apunte] [bigint] NOT NULL,
    [FechaApunte] [smalldatetime] NOT NULL,
    [Signo] [char](1) NOT NULL,
    [ID_Cuenta] [int] NOT NULL,
    [ID_TipoApunte] [tinyint] NOT NULL,
    [Importe] [decimal](10, 2) NOT NULL,
    [OrigenApunte] [nvarchar](50) NULL,
    [ID_Partida] [nvarchar](50) NOT NULL,
    CONSTRAINT [PK_APUNTES] PRIMARY KEY CLUSTERED
(
    [ID_Apunte] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
GO

ALTER TABLE [dbo].[APUNTES] WITH CHECK ADD CONSTRAINT [FK_APUNTES_CUENTAS]
FOREIGN KEY([ID_Cuenta])
REFERENCES [dbo].[CUENTAS] ([ID_Cuenta])
GO
```



CÁMARA DE
COMPTOS DE
NAVARRA
NAFARROAKO
KONTUEN
GANBERA

```
ALTER TABLE [dbo].[APUNTES] CHECK CONSTRAINT [FK_APUNTES_CUENTAS]
GO

ALTER TABLE [dbo].[APUNTES] WITH CHECK ADD CONSTRAINT [FK_APUNTES_PARTIDAS]
FOREIGN KEY([ID_Partida])
REFERENCES [dbo].[PARTIDAS] ([ID_Partida])
GO

ALTER TABLE [dbo].[APUNTES] CHECK CONSTRAINT [FK_APUNTES_PARTIDAS]
GO

ALTER TABLE [dbo].[APUNTES] WITH CHECK ADD CONSTRAINT [FK_APUNTES_TIPO_APUNTE]
FOREIGN KEY([ID_TipoApunte])
REFERENCES [dbo].[TIPO_APUNTE] ([ID_TipoApunte])
GO

ALTER TABLE [dbo].[APUNTES] CHECK CONSTRAINT [FK_APUNTES_TIPO_APUNTE]
GO

ALTER TABLE [dbo].[APUNTES] WITH CHECK ADD CONSTRAINT [CK_APUNTES] CHECK
(((Signo)='D' OR (Signo)='H'))
GO

ALTER TABLE [dbo].[APUNTES] CHECK CONSTRAINT [CK_APUNTES]
GO

EXEC sys.sp_addextendedproperty @name=N'MS_Description', @value=N'Contiene
identificador único en el sistema de origen que da lugar al apunte, el
identificador de la venta' , @level0type=N'SHEMA',@level0name=N'dbo',
@level1type=N'TABLE',@level1name=N'APUNTES',
@level2type=N'COLUMN',@level2name=N'OrigenApunte'
GO
```

Anexo I

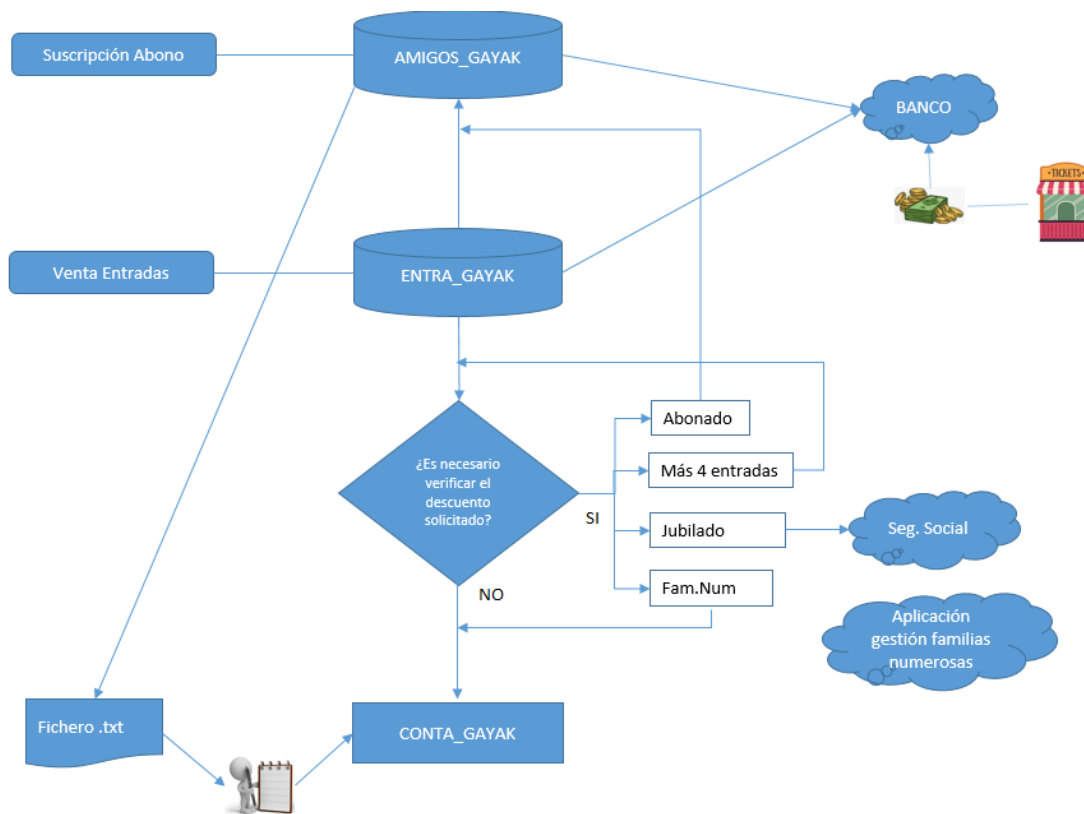
PROPUESTA DE SOLUCIÓN 2º EXAMEN

SUPUESTO (65 PUNTOS)

1) Elaborar un diagrama de flujo de procesos sobre la gestión de los ingresos objeto de fiscalización. (7 PUNTOS)

Tendrá especial relevancia en la corrección los siguientes aspectos:

- Árbol de decisión para verificación del descuento
- No existe conexión con la aplicación de familias numerosas (se acredita con la tarjeta a la entrada al espectáculo)
- La introducción del fichero .TXT en contabilidad es MANUAL
- El efectivo se introduce en el banco



2) Señalar los sistemas sobre los que se deberían realizar controles generales justificando las razones para ello. (2,5 PUNTOS)

A excepción de FAMILIA NUMEROSAS (dado que la acreditación se realiza con carnet en la entrada al espectáculo), deberán ser probados controles generales del resto de aplicaciones que intervienen en el proceso de negocio.

3) Describir cinco ejemplos relevantes de los controles generales referidos a gestión de cambios en aplicaciones y sistemas, así como a controles de acceso a datos y programas.
(12,5 PUNTOS)

GPF-OCEX 5330. Revisión de los controles generales de tecnologías de información (CGTI) en un entorno de administración electrónica. Categorías de controles

Se valorará especialmente los controles específicos referidos al cambio de versión.

B. Gestión de cambios en aplicaciones y sistemas

B.1 Adquisición de aplicaciones y sistemas

B.2 Desarrollo de aplicaciones

B.3 Gestión de cambios

- La entidad dispone de un procedimiento para la gestión de los cambios en los sistemas y aplicaciones y en sus configuraciones.
- El procedimiento de gestión de cambios aplicado contempla la autorización previa a la entrada en producción del cambio si este conlleva la introducción de un nuevo componente del sistema (equipo, aplicación, enlaces de comunicación con otros sistemas, etc.)
- Se han separado el entorno de desarrollo del de producción, realizándose el desarrollo sobre sistemas diferenciados de los productivos
- Se segregan aquellas funciones que, ante determinadas circunstancias, podrían culminar en conflicto de interés como, por ejemplo, desarrollo y operación. Se evita, siempre que sea posible, que las capacidades de desarrollo y operación recaigan en la misma persona o en el mismo equipo.
- Una vez implementados cambios en aplicaciones y sistemas, se realizan las pruebas de aceptación convenientes.

D. Controles de acceso a datos y programas

D.1 Uso controlado de privilegios de administración

D.2 Gestión de usuarios

- Está adecuadamente controlada la asignación del privilegio de administración.
- Cuando el usuario tiene diferentes roles frente al sistema (por ejemplo, usuario y administrador) se le asignan identificadores singulares para cada perfil.
- La entidad dispone de un proceso formalmente establecido de solicitud y alta de nuevos usuarios en los sistemas. La entidad dispone de un proceso formalmente establecido para la gestión de las bajas de cuentas de usuarios en el sistema que garantice que no existen cuentas no necesarias.
- Cada entidad (usuario o proceso) que accede al sistema cuenta con un identificador singular que permite reconocerlo y asignarle los derechos de acceso que le corresponden
- La política de autenticación se considera robusta y adecuada para reducir el riesgo de accesos no autorizados. Posibles mecanismos de autenticación contemplados en el ENS son:

contraseñas, certificados y certificados cualificados. Una medida que incrementa su robustez es el doble factor de autenticación.

- Los derechos de acceso de cada recurso TI se establecen según las decisiones de la persona responsable del recurso, ateniéndose a la política y/o normativa de seguridad del sistema. Se gestionan los derechos de acceso en base al principio de mínimo privilegio

4.1) La corrección del importe de los ingresos registrados en el ejercicio fiscalizado en la partida VENTAS ENTRADAS, correspondientes a la venta de entradas a personas jubiladas no suscriptoras al programa AMIGOS DE GAYAK (9 PUNTOS)

La propuesta de solución es orientativa. Se valorará otras formas de resolución no contempladas en esta propuesta.

- Supuesto que solo para los no abonados.
- Supondremos que se hace para un periodo de tiempo.

Solución:

```
/*
Segundo, el importe de la venta se corresponde con el del apunte
*/
-- no existe venta-apunte diferente, y todas las ventas tienen un apunte
select v.* from ventas v
left join apuntes a on a.OriginApunte = v.ID_Venta
where v.ID_TipoImporte = 2 -- jubilados
and v.ID_Abono is null -- no abonado
and year(a.FechaApunte) = '2025' -- ejercicio 2025
and (a.ID_Apunte is null -- no existe el apunte
or
v.importe <> a.importe ) -- importe diferente

/*
Tercero, que los apuntes están correctamente imputados a su partida
presupuestaria
*/
-- No tenemos ningún apunte para venta de entrada de jubilado que no esté en su
partida
select a.* from apuntes a
inner join ventas v on v.ID_Venta = a.OriginApunte
where v.ID_TipoImporte = 2 -- jubilados
and year(a.FechaApunte) = '2025' -- ejercicio 2025
and v.ID_Abono is null -- no abonado
and a.ID_Partida <> 'PARTIDA_2'

/*
Cuarto, el importe es correcto para la consideración de jubilado
*/
-- No existe venta a un no abonado en la que no se le haya aplicado correctamente
la reducción por jubilado
select v.ID_Venta, v.importe as venta, e.importe as precioEspectaculo, v.NumEntra
das as numeroEntradas, p.Importe as porcentaje, 0 as decuentoMas5, c.Importe as c
omisión, (v.NumEntradas * e.Importe * p.Importe) + (v.NumEntradas * c.Importe ) as
'importeCorrecto'
from ventas v
inner join ESPECTACULOS e on e.ID_Espectaculo = v.ID_Espectaculo
inner join IMPORTES_CONFIG
p on p.ID_TipoImporte = v.ID_TipoImporte and p.Ano = year(v.fechaVenta) --
porcentaje a aplicar
inner join IMPORTES_CONFIG
c on c.ID_TipoImporte = 6 and c.Ano = year(v.fechaVenta) -- comisión
where v.ID_TipoImporte = 2 -- jubilados
and year(v.FechaVenta) = '2025' -- ejercicio 2025
and ID_Abono is null -- no abonados
and v.importe <> (v.NumEntradas * e.Importe * p.Importe) + (v.NumEntradas * c.Imp
orte ) -- venta <> importe correcto
```

4.2) La adecuación de las fechas de venta de las entradas, teniendo en cuenta la existencia de un periodo preferente de compra para las personas suscriptoras del programa AMIGOS DE GAYAK.. (7 PUNTOS)

La propuesta de solución es orientativa. Se valorará otras formas de resolución no contempladas en esta propuesta.

```
-- Solo ventas anticipadas a abonados
-- Es tanto como decir que no hay ventas de entradas anticipadas a no abonados
-- Debe estar vacío
select * from ventas v
inner join espectaculos e on e.ID_Espectaculo = v.ID_Espectaculo
where year(v.FechaVenta) = '2025'
and v.ID_Abono is null -- no abonados
and v.FechaVenta < dateadd(month, -1, e.FechaEspectaculo) -- 1 mes antes

-- Además ningún abonado puede haberlas comprado antes de esos 10 días de
antelación
-- Debe estar vacío
select * from ventas v
inner join espectaculos e on e.ID_Espectaculo = v.ID_Espectaculo
where year(v.FechaVenta) = '2025'
and not v.ID_Abono is null -- abonados
and v.FechaVenta < dateadd(day, -10, dateadd(month, -1, e.FechaEspectaculo)) --
un mes y 10 días

-- las ventas para abonados tienen vigente el abono
select * from ventas v
inner join espectaculos e on e.ID_Espectaculo = v.ID_Espectaculo
inner join abonos a on a.ID_Abono = v.ID_Abono -- abonados
where year(v.FechaVenta) = '2025'
and not v.ID_Abono is null -- abonados (sobra, redundante)
and v.FechaVenta < dateadd(day, -10, dateadd(month, -1, e.FechaEspectaculo)) --
un mes y 10 días
and v.FechaVenta between a.FechaInicio and a.FechaFin -- abono vigente
```

4.3) La relación de personas que reúnen los requisitos para la aplicación del descuento adicional del 5 % a día de hoy. **(5 PUNTOS)**

La propuesta de solución es orientativa. Se valorará otras formas de resolución no contempladas en esta propuesta.

- Suponemos que se trata al día de hoy.

Solución:

```
Select p.* from abonos a
inner join personas p on p.IDENTIFICADOR = a.ID_Persona
where a.FechaFin >= getdate() -- abonos vigentes
and a.FechaInicio < dateadd(year, -5, getDate())
```

5) Ante el incidente ocurrido a finales de 2024, el equipo de auditoría decide realizar una auditoría de ciberseguridad sobre el proceso continuo de identificación y remediación de vulnerabilidades. Diseñar el programa de auditoría correspondiente. (7 PUNTOS)

GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa

CSC4-Control: Proceso continuo de identificación y remediación de vulnerabilidades

Objetivo de control: Disponer un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.

Comentarios: Su revisión se puede enfocar, de forma complementaria a los controles 1 y 2, verificando si:

- existe una política de bastionado de todos los dispositivos, aplicaciones y servicios (1,5 puntos)
- política está alineada con buenas prácticas (1,5 puntos)
- dispone de un proceso de revisión de las vulnerabilidades que retroalimente la política de bastionado. (1,5 puntos)

Otra aproximación es que el auditor escanee los dispositivos/aplicaciones utilizando herramientas automatizadas, actuando como Red Team. (1 punto)

En los comentarios de los controles 1 y 2 se indica que la revisión puede realizarse de dos formas: (1,5 punto cualquiera de las dos formas)

- Verificar que existe una gestión de inventarios hardware y software, identificando listas blancas y negras y su actualización (al ser una aproximación de “ver que existe un control”, podríamos llamarla, “de capa 2”).

- El auditor interno escanea las redes internas utilizando herramientas automáticas (actúa como Red Team, según el control 20, es decir, comportándose como lo haría un atacante), hace una “verificación técnica”, que podríamos llamar “de capa 1”. En el resto de controles también usaremos estas dos aproximaciones de revisión.

6) GPF-OCEX 1403. Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios de computación en la nube". (7,5 PUNTOS)

Hemos pedido 6 ITEMS, cada uno se valorará a 1,25. El contrato debe recoger:

- Responsabilidades del proveedor y los niveles de seguridad de la información y los servicios afectados, de forma que el proveedor aplique las medidas de seguridad oportunas.
- Acuerdos de nivel de servicio (SLA) referentes a capacidad, disponibilidad, continuidad, gestión de incidentes y gestión de cambios. De cada SLA se definirá:
 - Parámetro:
 - Responsabilidades: quién recoge y facilita los datos necesarios para realizar los cálculos
 - Fórmula para calcular el SLA
 - Periodicidad de la captura de datos, del cálculo de las métricas, y de la verificación de umbrales
 - Umbrales: valores que dispararán situaciones de aviso (hay que monitorizar) y de alarma (hay que corregir)
 - Penalizaciones.
- Mecanismos de acceso al servicio por parte de los empleados del Teatro GAYAK
- Procedimiento que coordine al Teatro GAYAK y al CSP para el mantenimiento y/o actualización de los sistemas, para prevenir paradas o errores en el servicio. Si son cambios de envergadura, el proveedor habilitará un entorno de preproducción donde Teatro GAYAK pueda verificar el correcto funcionamiento antes de la puesta en producción.
- Teatro GAYAK deberá disponer del derecho de auditoría o exigir: DA de medidas a aplicar, auditoría que verifique con evidencias el cumplimiento de las medidas del Anexo II del ENS de categoría media, auditorías de cumplimiento normativo para satisfacer requisitos de seguridad de la información, otras certificaciones en materia de seguridad.
- EL CSP deberá disponer de un procedimiento para la gestión de incidentes en el que se incluya la notificación de incidentes a Teatro GAYAK, tipos de incidentes, tiempos de respuesta y resolución, mantenimiento y gestión del registro de incidentes.
- El propietario de los datos es el Teatro GAYAK y podrá disponer de ellos solicitándolos al proveedor del servicio.
- El Teatro GAYAK tiene derecho a conocer el modelo de datos de la aplicación.
- El proveedor deberá disponer de un procedimiento de copias de seguridad que garantice la restauración de la información y deberá informar al Teatro Gayak de alcance de los respaldos, políticas de seguridad, medidas de cifrado de la información en las copias, procedimiento para solicitar restauraciones de información, realización de pruebas de restauración, traslado de copias de seguridad (si aplica).
- Para garantizar la continuidad del servicio, Teatro GAYAK deberá solicitar al CSP evidencia de la existencia de un plan de continuidad de negocio que incluya:
 - alcance con los servicios contratados
 - tiempos de recuperación identificados en el análisis de impacto y alineados con los criterios de los SLA's (RTO y RPO)

- procedimiento de coordinación ante incidentes y desastres. El proveedor deberá informar periódicamente de los incidentes que han afectado a los sistemas que soportan CONTA_GAYAK
- pruebas periódicas para validar el funcionamiento de los planes, cumplimiento de plazos y servicios mínimos prestados.
- Cláusula que recoja las condiciones, procedimientos y plazos para una terminación pactada o por incumplimiento del contrato, junto con el tiempo que tardará el proveedor en migrar los datos. Se buscará neutralidad tecnológica para facilitar la migración.
- Cláusula o establecer un procedimiento sobre el tiempo que tardará el proveedor en realizar la destrucción efectiva de los datos y mecanismos a utilizar.

7) El equipo de auditoría decide realizar la revisión del control D1 «Uso controlado de privilegios de administración», de acuerdo con lo establecido en la “GPF-OCEX 5334. Revisión de los CGTI del área D: Controles de acceso a datos y programas” (7,5 PUNTOS)

- Indicar cuáles de los subcontroles recogidos en la guía deberían revisarse en la aplicación CONTA-GAYAK, justificando la respuesta

PROPUESTA DE SOLUCIÓN (3 puntos)

Al tratarse de un entorno SaaS se tienen que revisar todos los subcontroles sobre la gestión de usuarios y privilegios de administración a nivel de la aplicación (D1.1, D1.2, D1.3 y D1.4, pero sólo en la parte de los usuarios de Teatro Gayak, es decir, no hay que revisarlos para el CSP aunque éste disponga de usuarios administradores para realizar la parte de las tareas de administración del aplicativo.

No tiene que revisarlos porque al ser usuarios que no dependen de Teatro Gayak, no procede su revisión a través de la aplicación CONTA_GAYAK, sino vía contractual, ENS, auditorías externas, etc... pero no mediante la revisión de usuarios dentro de la aplicación.

Subcontrol D11 Inventario y control de cuentas de administración

Subcontrol D12 Uso dedicado de cuentas de administración

Subcontrol D13 Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios internos

Subcontrol D14 Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios externos

- Seleccionar uno de los subcontroles anteriores e identificar tres evidencias que deberían solicitarse durante la auditoría, indicando si la solicitud debe remitirse al TEATRO GAYAK o al proveedor de servicios en la nube (Cloud Service Provider - CSP).

PROPUESTA DE SOLUCIÓN (4,5 puntos)

Todas las peticiones de evidencia irán dirigidas a Teatro Gayak

Propuestas de evidencias (a escoger subcontrol y tres evidencias del subcontrol):

Nota: se pueden proponer otras evidencias de auditoría (que pueden deducirse del programa de auditoría) ya que las listas de la guía no son listas cerradas.

Subcontrol D11 Inventario y control de cuentas de administración

EVIDENCIAS:

- Procedimiento de gestión de cuentas de administración
- Formalización de la responsabilidad de administración del sistema TI
- Inventario de cuentas de administración para CONTA_GAYAK o evidencia del listado de usuarios con privilegios de administración
- Documentación de seguridad del sistema en el que se describa el sistema de identificación utilizado
- Fichero de usuarios obtenido directamente del CONTA_GAYAK

- Evidencia del cambio de contraseña de las cuentas de administración compartidas tras el cese de uno de los administradores
- Evidencia de deshabilitación de las cuentas y su control hasta su eliminación definitiva
- Evidencia de uso de herramientas para el almacenamiento cifrado y el control de acceso a las contraseñas de uso compartido
- Evidencia de soluciones PAM para la gestión de cuentas de administración
- Evidencias sobre qué mecanismos de acceso al sistema en modo administrador ha establecido la entidad y cómo lo ha implantado.

Subcontrol D12 Uso dedicado de cuentas de administración

EVIDENCIAS:

- Listado del personal que tiene asignado el privilegio de administración
- Evidencia del uso por parte del personal que realiza labores de administración de diferentes cuentas de usuario (con privilegios de administración y sin privilegios)
- Documentación de seguridad del sistema, en el que se describa el sistema de identificación utilizado para el acceso a CONTA_GAYAK

Subcontrol D13 Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios internos

EVIDENCIAS:

- Documentación de seguridad del sistema que describa las características del mecanismo de autenticación en CONTA_GAYAK para administradores
- Evidencia de la política de autenticación implantada para los usuarios administradores
- Evidencia del proceso de entrega y aceptación de credenciales por los usuarios
- Evidencia de deshabilitación /retirada de credenciales a los usuarios
- Evidencia de que la información suministrada en los accesos está restringida al mínimo imprescindible
- Evidencia de doble factor de autenticación
- Evidencia de empleo de contraseñas de un solo uso (OTP)
- Evidencia de que los certificados empleados son cualificados
- Evidencia de que se configuran los certificados protegidos mediante un segundo factor
- Evidencias de registros de acceso
- Evidencia de que se informa al usuario del último acceso
- Evidencia de que para el acceso remoto se requiere autorización específica, se cifra su tráfico, se recogen pistas de auditoría y es deshabilitado fuera de los períodos establecidos de utilización
- Evidencia de acceso, mediante cuentas de administración, únicamente desde determinados dispositivos

Subcontrol D14 Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios externos

EVIDENCIAS:

- Documentación de seguridad del sistema que describa las características del mecanismo de autenticación en CONTA_GAYAK, para administradores
- Evidencia de la política de autenticación implantada para los usuarios administradores
- Evidencia del proceso de entrega y aceptación de credenciales por los usuarios
- Evidencia de deshabilitación /retirada de credenciales a los usuarios
- Evidencia de que la información suministrada en los accesos está restringida al mínimo imprescindible

- Evidencia de empleo de contraseñas de un solo uso (OTP)
- Evidencia de que los certificados empleados son cualificados
- Evidencia de que se configuran los certificados protegidos mediante un segundo factor
- Evidencia de empleo de certificados cualificados en soporte físico, protegidos mediante un segundo factor.
- Evidencias de registros de acceso con éxito y los fallidos
- Evidencia de que se informa al usuario del último acceso
- Evidencia de suspensión de las credenciales tras un período definitivo de no utilización