Entidad:	
Fecha de las cuentas anuales:	

Objetivos y actividades CGTI

(A) Marco organizativo

(Procedimientos para verificar los objetivos de control en la dirección y organización de las TI)

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios, o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
1. Objetivo de control: Independencia del departamento de TI , segregación de funciones y procedimientos de TI Las actividades de control que pueden conseguir este objetivo pueden incluir las siguientes:				
Obtener el organigrama de la entidad y del departamento de TI. El Departamento de TI, ¿es independiente del resto de departamentos funcionales (no tiene dependencia orgánica de otro departamento y se encuentra al mismo nivel en el organigrama)?				
¿Existe segregación entre el personal con tareas de programación y el personal con tareas de dirección y gestión de TI? (p.e. los programadores no tienen acceso a las aplicaciones en el entorno real (de producción) y a los ficheros de datos de este entorno; los operadores de gestión no tienen acceso al entorno de programación y a la documentación relacionada)				
¿Existe segregación entre el personal con tareas de control TI respecto a gestión?				
¿Existen procedimientos para las tareas relevantes del departamento de TI?				

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios, o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
2. Objetivo de control: Existencia de planes y políticas de TI Las actividades de control que pueden conseguir este objetivo pueden incluir las siguientes:				
¿Existe un plan estratégico de TI alineado con los planes estratégicos de la entidad aprobado a alto nivel directivo?				
¿Existen unas políticas de seguridad de la información aprobadas a alto nivel directivo?				
¿Existe un plan anual de proyectos de TI aprobado por la dirección gerencial?				
¿Existe dotación presupuestaria en el ejercicio para el plan anual de proyectos del ejercicio?				
¿Existe dotación presupuestaria del plan estratégico en gastos plurianuales (en su caso)?				
¿Existe un plan de formación en concienciación de seguridad TI plurianual?				
¿Cuántos empleados se formaron en seguridad TI en el último ejercicio (%)?				
3. Objetivo de control: Cumplimiento regulatorio Las actividades de control que pueden conseguir este objetivo pueden incluir las siguientes:				
¿Dispone la entidad del Documento o Documentos de Seguridad a que se refiere el artículo 88 del RD 1.720/2007, de 21 de diciembre, que desarrolla la Ley Orgánica de Protección de Datos (LOPD)?				
¿Se han inscrito los ficheros de datos personales en la Agencia Española de Protección de Datos?				

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios, o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
¿Se han realizado las auditorías bianuales previstas por la LOPD (en su caso)?				
En el caso de Administraciones públicas, ¿existe el plan de adaptación a los esquemas nacionales de seguridad e interoperabilidad y su aprobación (Disposición transitoria RD 3 y 4/2010)?				
¿Se dispone de licencias de uso (salvo para software libre) de las aplicaciones utilizadas por la entidad?				

(B) Gestión de cambios en aplicaciones y sistemas

(Procedimientos para la gestión de cambios en programas y sistemas)

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
1. Objetivo de control: Las aplicaciones y los sistemas se compran o desarrollan de forma que responden efectivamente a las necesidades de los departamentos usuarios. Las actividades de control que pueden conseguir este objetivo pueden incluir las siguientes:				
La entidad ha desarrollado un proceso de planificación y adquisición de TI que se alinea con sus objetivos organizacionales. **Verificación:** La dirección debe revisar y aprobar los proyectos para asegurar que se alinean con los requerimientos para lograr los objetivos estratégicos de la entidad y que se utilizan las tecnologías que han sido aprobadas.				
2. Objetivo de control: Los sistemas y aplicaciones se validan y prueban antes de instalarse en el				

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior* *(Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
entorno de trabajo real (producción) Las actividades de control que pueden conseguir este objetivo pueden incluir las siguientes:				
¿Existe un procedimiento definido y aprobado para realizar cambios a programas?				
¿El procedimiento de gestión de cambios exige la existencia de entornos diferentes para desarrollo de aplicaciones y producción?				
¿Se registran todos los cambios solicitados?				
¿Se aprueban las solicitudes de cambio que se van a desarrollar?				
¿Se prueban los cambios en un entorno diferente del de producción?				
¿Se aprueban las pruebas por los usuarios finales?				
¿Se aprueban los cambios antes del pase a producción?				
¿Los programadores tienen limitada la posibilidad de implantar los cambios en producción y el acceso a los datos de producción?				
¿Se documentan los cambios realizados?				
¿Existe un procedimiento de cambios de emergencia?				
¿Existe una relación de personas autorizadas para implantar los cambios en producción?				

(C) Operaciones de los sistemas de información

(Procedimientos para verificar la correcta ejecución de los servicios de TI necesarios para la entidad)

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
1. Objetivo de control: las aplicaciones y equipos que son responsabilidad del departamento de TI están identificados y controlados. Las actividades de control que pueden conseguir este objetivo pueden incluir las siguientes:				
Evidenciar la existencia de inventario de software y hardware.				
2. Objetivo de control: Los niveles de servicio de TI se encuentran definidos de forma que se satisfacen las necesidades de información financiera y existe acuerdo sobre los indicadores para medir estos niveles. Las actividades de control que pueden conseguir este objetivo pueden incluir las siguientes:				
La dirección ha definido indicadores clave para la medición de los acuerdos de niveles de servicio de TI, tanto internos como externos.				
La dirección gestiona y revisa los valores de los indicadores de los niveles de servicio de TIC. **Consejo Práctico:** Cuando se lleven a cabo walkthroughs de procesos significativos es útil preguntar a los usuarios sobre los problemas que pueden haber encontrado en materia de TI. Las respuestas nos confirmarán si se han definido o no acuerdos de nivel de servicio				
3. Objetivo de control: Los incidentes y problemas en materia TIC se comunican, registran, investigan y resuelven adecuadamente Las actividades de control que pueden conseguir este objetivo pueden incluir las siguientes:				
La dirección ha desarrollado un procedimiento para				

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
asegurar que los incidentes, errores y problemas de TIC se registran, analizan y resuelven en un plazo de tiempo adecuado.				
4. **Objetivo de control: Se ha implementado una adecuada política de protección contra el malware**				
Existen políticas y procedimientos para la protección mediante antivirus, de los sistemas de información.				
La configuración y actualización del software antivirus es adecuada para garantizar la protección, tanto en la red como en los PCs.				
Verificar la existencia y configuración del antivirus para el correo electrónico.				
5. Objetivo de control: Los datos y los informes se mantienen íntegros, válidos y exactos durante los procesos de almacenamiento y actualización Las posibles actividades de control incluyen las siguientes:				
La entidad ha desarrollado políticas y procedimientos para manejar, distribuir y retener la información y la salida de informes o datos.				
La dirección protege la información sensible, lógica y físicamente, en el almacenamiento y durante las transmisiones, contra accesos o modificaciones no autorizadas.				
La entidad tiene definidos los periodos de retención y almacenamiento para documentación, datos, programas, informes y mensajes, así como la información (claves, certificados) utilizada para la encriptación y autenticación.				
¿Se realizan pruebas sobre los interfaces entre aplicaciones para verificar que la transmisión de datos				

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
entre aplicaciones es completa, válida e íntegra?				
6. **Objetivo de control: definir y administrar medidas de seguridad física alineadas con los requerimientos de los objetivos y actividades de la entidad.** Las posibles actividades de control incluyen las siguientes:				
Existen procedimientos para la gestión de la seguridad y autorización del acceso físico de los empleados y visitantes. Los procedimientos están aplicándose y son efectivos.				
Existe un procedimiento de control para el acceso físico al Centro de Proceso de Datos (CPD). El procedimiento incluye la autorización y el registro de todos los accesos.				
El CPD dispone de medidas de protección y control ambiental y la ubicación es segura: aires acondicionados, extintores, control de temperatura y humedad, falsos suelos, …				
7. Objetivo de control: los servicios externos son seguros, exactos y están disponibles; existe control sobre la integridad del procesamiento de datos y su confidencialidad; están detallados adecuadamente y existen contratos con cláusulas de nivel de servicio. Las posibles actividades de control incluyen las siguientes:				
Se ha nombrado a una persona como responsable del seguimiento e informe sobre el logro de objetivos de acuerdo con los criterios del acuerdo de nivel de servicios.				

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
A la hora de seleccionar a los proveedores externos se aplica la política o procedimiento de gestión de compras de la entidad.				
Los contratos existen y contemplan cláusulas adecuadas para cubrir los riesgos, controles de seguridad y procedimientos para utilización de las redes y sistemas de información (confidencialidad, niveles de servicio, ..).				
La dirección lleva a cabo revisiones regulares en materia de seguridad, disponibilidad, integridad de procesamiento, y niveles de servicio de los servicios prestados por proveedores externos.				

(D) Controles de acceso a datos y programas

(Procedimientos sobre seguridad lógica y gestión de accesos)

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
1. Objetivo de Control: definir la arquitectura de red, garantizar que se utilizan técnicas de seguridad y los procedimientos de administración asociados (firewalls, segmentación de redes, detección de intrusos) y que el servicio de comunicaciones está adecuadamente soportado. Las posibles actividades de control incluyen las siguientes:				
Verificar si existe un esquema o descripción de los sistemas de comunicación con los diferentes elementos que lo componen, y de la forma en que las diferentes aplicaciones o sistemas de información se comunican entre sí.				

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
Los puntos de acceso y salida de la red local de la entidad están identificados y los servicios de comunicaciones existentes están adecuadamente soportados (verificar respaldo servicio comunicaciones).				
Existen elementos de protección de la seguridad de la red local: Firewall, detección de intrusos, DMZ, protocolos seguros de navegación ya acceso (SSL, VPN, …). Existen políticas y procedimientos para su adecuada configuración.				
El sistema está configurado para capturar los eventos y actividades clave del sistema. Existe personal encargado de revisarlos y analizarlos y se han aprobado procedimientos para la revisión.				
2. Objetivo de control: las principales aplicaciones de gestión financiera y sus subprocesos están adecuadamente asegurados para prevenir usos o accesos no autorizados, modificaciones de datos no autorizados o daño y pérdida de datos. Las actividades de control que pueden conseguir este objetivo pueden incluir las siguientes:				
Existen procedimientos y controles para identificar y autentificar a todos los usuarios que acceden a la red local. Los procedimientos y controles se aplican en la práctica (asignación de usuario y contraseña únicos, …).				
Existen políticas de seguridad definidas para la correcta configuración de usuarios y contraseñas (complejidad, +6 dígitos, …), bloqueo de cuenta por acceso no autorizado y bloqueo de pantalla de usuario por inactividad.				
Existe un procedimiento para aprobar las altas, bajas y modificaciones de los usuarios. Las altas y bajas se comunican ágilmente al departamento de TI.				

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior* *(Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
Punto de revisión: Cuando las entidades utilizan aplicaciones estándar es común que confíen en los suministradores del software para implantar y probar las aplicaciones. Para facilitar este proceso, las entidades normalmente, conceden amplios permisos de acceso al suministrador del software a los datos y otras aplicaciones. Estos accesos lógicos deben ser gestionados adecuadamente como cualquier otro permiso de acceso.				
Existe un procedimiento de revisión periódica de usuarios activos, comprobar que es adecuado. El procedimiento incluye la modificación de permisos de usuarios cuando cambian de departamento.				
El departamento de TI registra los accesos de los usuarios a los elementos críticos del sistema y realiza un seguimiento periódico. Los incidentes de seguridad por accesos o intentos de accesos no autorizados se informan a los responsables de seguridad y son investigados.				
Existen controles para garantizar una adecuada segregación de funciones en el momento de la solicitud de los permisos de acceso a sistemas. datos.(quien solicita, autoriza, ejecuta, …).				
La configuración del software y de los sistemas de almacenamiento de la información está diseñada para garantizar el acceso en base a las necesidades demostradas de ver, modificar, cambiar o borrar datos. **Punto de atención:** Cuando la entidad utiliza software comprado, es importante revisar la configuración de parámetros de acceso por defecto (p.e., permisos de acceso del "administrador" y otros usuarios privilegiados)				
3. Objetivo de Control: la configuración de los PC de los usuarios garantiza su uso seguro Las posibles actividades de control incluyen las siguientes:				

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*¿Eficaz en diseño e implementación? (Sí/No)*
La entidad sólo permite el uso de software autorizado a sus empleados al trabajar con los equipos de la entidad.				
Comprobar si los usuarios son administradores locales de sus ordenadores y/o si existe algún control sobre la instalación de software no autorizado.				
4. Objetivo de Control: garantizar la seguridad y la integridad de la información en las interfaces de los sistemas de información. Las posibles actividades de control incluyen:				
Comprobar que la información transmitida entre los diferentes SS.II. es consistente, íntegra y segura y que se utilizan protocolos seguros cuando existen riesgos sobre las comunicaciones.				

(E) Continuidad del servicio

(Procedimientos sobre los controles establecidos por la entidad para garantizar la continuidad de los servicios de TI)

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior (Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*Eficaz en diseño e implementación? (Sí/No)*
1. Control Objetivo: existen y están disponibles copias de todos los datos y programas necesarios para la recuperación de los servicios críticos de la entidad. Las actividades de control que pueden conseguir este objetivo pueden incluir las siguientes:				
Se realizan copias de seguridad planificadas y periódicas de todos los datos y programas críticos para el funcionamiento de la entidad.				

Objetivos y actividades de control	*Descripción de los CGTI*	*Cambios respecto al año anterior* *(Sin cambios o cambio significativo)*	*Procedimientos realizados/Referencia*	*Eficaz en diseño e implementación? (Sí/No)*
Existen copias de seguridad de datos y programas disponibles de los procesos críticos en ubicaciones alternativas (una ubicación externa).				
La entidad ha definido y concretado los periodos de retención de la información contenida en las copias de seguridad.				
Se realizan pruebas periódicas de recuperación de datos de las copias de seguridad y estas pruebas se documentan.				
2. Objetivo de control: desarrollar y aprobar planes de continuidad de negocio para reducir el posible impacto de una interrupción de los servicios de TI sobre los procesos críticos de gestión de la entidad. Las actividades de control que pueden conseguir este objetivo pueden incluir las siguientes:				
Existe y se ha aprobado un plan de continuidad de negocio que incluye los procesos críticos de gestión de la entidad, puntos objetivo de recuperación y plazos objetivo de recuperación.				
Se llevan a cabo pruebas periódicas del plan de continuidad y se documentan adecuadamente.				
El plan de recuperación de negocios se ha basado en un análisis de riesgos y en la determinación de los activos de TI que son críticos para la entidad.				

(F) CONCLUSIÓN

En base a los procedimientos llevados a cabo podemos afirmar que los controles establecidos por la entidad son suficientes para lograr los objetivos generales de control identificados sobre las actividades de TI y garantizan el logro de los objetivos relativos a la integridad y fiabilidad de la información financiera. Si la respuesta es "No", el auditor completará el apartado a) o b) siguientes:	☐ Sí ☐ No

a) El trabajo realizado ha puesto de manifiesto la necesidad de trabajo adicional por personal especializado de la UASI para:

- € Determinar las consecuencias de la situación de los controles de TI sobre la auditoría
- € Entender los controles implantados en materia de TI
- € Diseñar y llevara a cabo pruebas sobre los controles de TI

b) Los procedimientos llevados a cabo para evaluar el diseño e implementación de los controles generales de TI establecidos por la entidad han puesto de manifiesto las siguientes deficiencias y riesgos de errores materiales en la elaboración de las cuentas anuales:

Descripción de la deficiencia (1)	*Controles compensatorios (si existen)*	*¿Reducen adecuadamente los controles compensatorios el RIM originado por la deficiencia? (Sí/No)*	*Si la anterior columna es "NO," describir los RIM (2)*

1. *Las deficiencias de control detalladas deben ser documentadas y evaluadas.*
2. *El Riesgo de Incorrecciones Materiales (RIM) debe estar documentado y evaluado.*

El Técnico de Auditoría:		Fecha:	
El Auditor		Fecha	
El Jefe de la UASI:		Fecha:	