# GPF-OCEX 5340: Os controis de aplicación: que son e como revisalos

Referencia: ISSAI 5300, GPF-OCEX 5300 e GPF-OCEX 1315

*Documento elaborado pola Comisión Técnica dos OCEX e aprobado pola Conferencia de Presidentes de ASOCEX o 12/11/2018*



## 1. Introdución

O enfoque de auditoría baseado na análise do risco é o fundamento central da actividade auditora desenvolvida baixo as Normas Internacionais de Auditoría (NIA-ES) e as ISSAI-ES. Tal como sinala a GPF-OCEX 1315, "de acordo con este enfoque, o obxectivo do auditor é obter unha seguridade razoable de que as contas anuais no seu conxunto están libres de incorreccións materiais, debidas a fraude ou erro. Unha seguridade razoable é un grao alto de seguridade e alcánzase cando o auditor obtivo evidencia de auditoría suficiente e adecuada para reducir o risco de auditoría (é dicir, o risco de expresar unha opinión inadecuada cando as contas anuais conteñan incorreccións materiais) a un nivel aceptablemente baixo. Con todo, unha seguridade razoable non significa un grao absoluto de seguridade, debido a que existen limitacións inherentes á auditoría que fan que a maior parte da evidencia de auditoría a partir da cal o auditor alcanza as súas conclusións e na que basea a súa opinión sexa máis convincente que concluínte."

Actualmente, nunha auditoría financeira baseada na análise dos riscos realizada de acordo coa ISSAI-ES 200, o estudo e revisión dos sistemas de información nos que se sustenta a xestión dunha entidade (empresa ou fundación pública, concello, administración da comunidade autónoma, etc.) converteuse nunha actividade de importancia crecente, na medida en que esa xestión apóiase nuns sistemas de información interconectados que, coa plena implantación da administración electrónica, foron adquirindo unha complexidade cada vez maior. Esta situación xerou unha serie de novos e importantes riscos de auditoría (inherentes e de control) que deben ser considerados na estratexia de auditoría.

Para orientar e facilitar aos auditores dos OCEX a aplicación do enfoque de risco e a auditoría en contornas de administración electrónica desenvolvéronse as Guías Prácticas de Fiscalización (GPF-OCEX).

De acordo coas ISSAI-ES/NIA-ES, dentro do proceso auditor, a revisión dos controis internos implementados nas aplicacións informáticas de xestión e nas interfaces é un aspecto moi relevante, tanto máis importante canto máis complexo sexa o sistema de información que soporta o proceso de xestión incluído no alcance da auditoría.

No Anexo 2 da GPF-OCEX 1315 detállanse os pasos a seguir para analizar un sistema de información e identificar os procesos, as aplicacións de xestión significativas, e as interfaces de interese para a auditoría. O coñecemento destes elementos é unha parte esencial da planificación dunha auditoría.

Desde o punto de vista metodolóxico/cronolóxico a revisión dos controis de aplicación farase sempre tras a revisión dos controis xerais de tecnoloxías da información (véxase a GPF-OCEX 5330), respecto dos que existe unha elevada dependencia, tal como se comentará máis adiante.

Moi esquemáticamente, segundo a citada GPF-OCEX 1315, as etapas dunha auditoría executada co enfoque baseado na análise dos riscos son as mostradas na Figura 1.

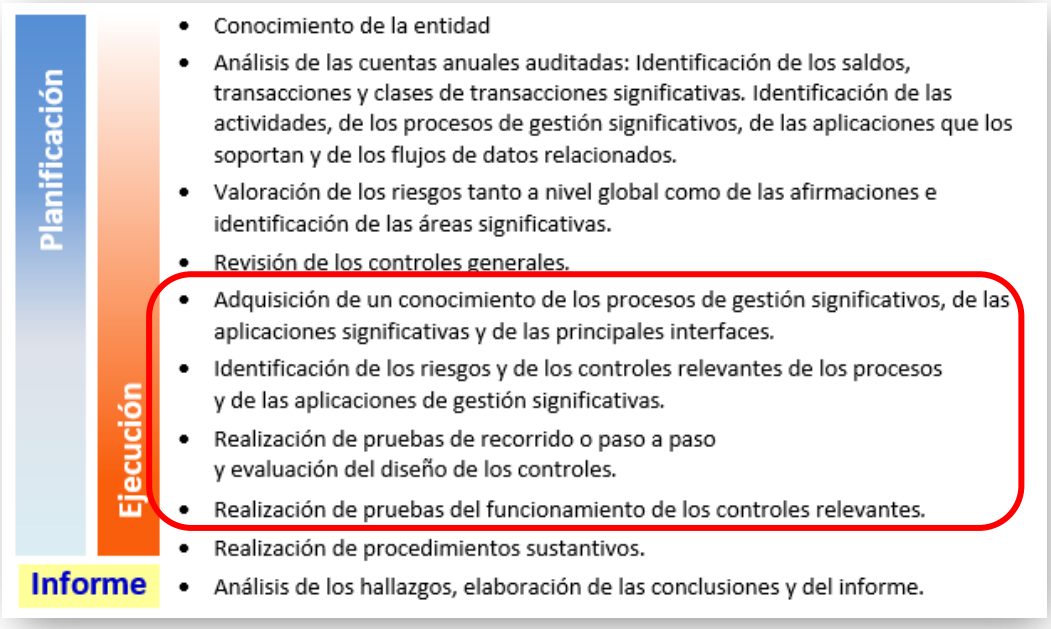



Figura 1

No Anexo 4 da GPF-OCEX 1315 inclúese un fluxograma típico dunha auditoría.

## 2. Obxectivos desta etapa da auditoría

Neste documento imos centrarnos no estudo da etapa de revisión dos controis de aplicación e dos controis sobre as interfaces, cuxa finalidade é:

- Adquirir un coñecemento profundo dos procesos de xestión revisados, dos riscos significativos existentes nas aplicacións informáticas que os soportan e nas interfaces relacionadas.
- Identificar, analizar e comprobar o adecuado funcionamento dos controis dos procesos e aplicacións de xestión e dos controis sobre as interfaces.
- Determinar a extensión dos procedementos substantivos a executar.
- Reducir o risco de auditoría a un nivel aceptable.

O **obxectivo da auditoria dos controis de aplicación** será obter unha seguridade razoable de que o sistema de control interno garante a integridade (completitude), exactitude, validez e legalidade das transaccións e datos rexistrados na aplicación de xestión revisada e a súa posterior contabilización; é dicir, se a eficacia dos controis relevantes garante a correcta execución dos procesos de xestión auditados e mitigan o risco de erros e irregularidades.

## 3. Os controis internos

3.1 Na GPF-OCEX 1315 defínese o control interno como o proceso deseñado, implementado e mantido polos responsables do goberno da entidade, a dirección e outro persoal, coa finalidade de proporcionar unha seguridade razoable sobre a consecución dos obxectivos da entidade relativos á fiabilidade da información financeira, a eficacia e eficiencia das operacións, así como sobre o cumprimento das disposicións legais e regulamentarias aplicables.

Un control é a combinación de métodos, políticas e procedementos que garanten a protección dos activos da organización, a precisión e a confiabilidade dos seus rexistros, e o cumprimento as directrices da dirección na consecución de ditos obxectivos.

As actividades de control ou controis internos poden estar totalmente automatizadas (circunstancia habitual nos actuais sistemas informáticos de xestión), poden ser manuais dependentes das TIC (bastante frecuentes tamén) ou completamente manuais (cada vez máis escasos).

**Nunha auditoría financeira considerarase que un sistema de control interno é efectivo se os controis son respectados e dan unha seguridade razoable de que non haberá erros ou irregularidades que afecten de maneira significativa aos estados financeiros.**

3.2 Por que os controis de TI son importantes para o auditor de sistemas de información?[1]

Xeralmente, o auditor de TI é solicitado para avaliar os controis relacionados coa tecnoloxía, mentres que os auditores que non auditan as TI avalían os controis financeiros, regulatorios e de cumprimento. A medida que cada vez máis organizacións dependen de TI para automatizar as súas operacións, a liña que divide a función dos auditores de TI e os auditores que non auditan as TI redúcese rapidamente. Como mínimo, requírese que todos os auditores comprendan a contorna de control da entidade auditada co fin de brindar seguridade respecto dos controis internos que operan na entidade. De conformidade cos Principios Fundamentais de Auditoría do Sector Público de ISSAI: "Os auditores deben comprender a natureza da entidade/programa a ser auditado". Isto inclúe a comprensión dos controis internos, os obxectivos, as operacións, a contorna regulatoria e os sistemas e procesos do negocio involucrados.

Cada área de control baséase nun conxunto de obxectivos de control que unha organización implementa a fin de mitigar riscos. A función do auditor é entender os riscos potenciais do negocio e de TI que enfronta a entidade auditada e, á súa vez, avaliar se os controis implementados son os adecuados para cumprir cos obxectivos de control.

3.3 Debemos facer unha primeira distinción moi importante entre[2]:

- Os **controis xerais das tecnoloxías da información (CXTI).** Afectan a todos os niveis dos sistemas de información, aínda que están relacionados con moita maior intensidade con aqueles niveis de carácter xeral que afectan a toda a organización e aos sistemas TI. Son políticas e procedementos vinculados a moitas aplicacións e favorecen un funcionamento eficaz dos controis das aplicacións. Son analizados na GPF-OCEX 5330.
- Os **controis de aplicación.** Operan ao nivel dos procesos de xestión e que se aplican ao procesamento das transaccións mediante aplicacións informáticas específicas.

3.4 Para os efectos desta guía, podemos representar o sistema de información dunha entidade mediante un modelo simplificado formado por cinco niveis ou capas tecnolóxicas superpostas, tal como se mostra na figura 2.

[1] Manual sobre auditoría TI para as Entidades Fiscalizadoras Superiores de INTOSAI.
[2] Véxase GPF-OCEX 1316; apartado 9.2.

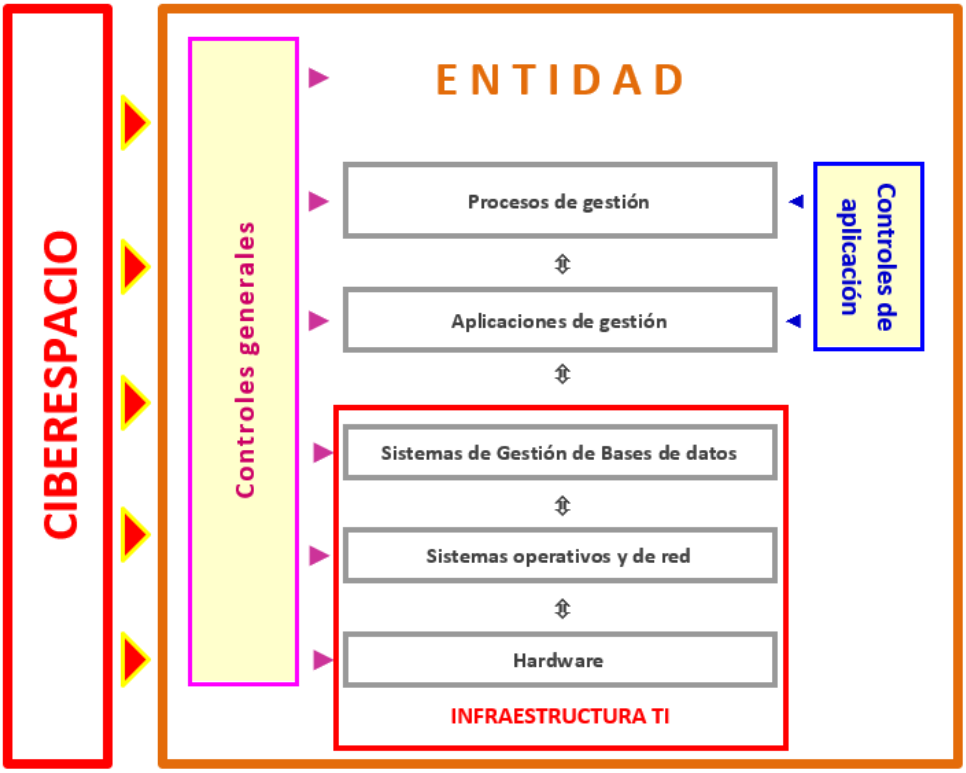



Figura 2

3.5 Ademais, os controis clasifícanse en tres tipos:

| Tipo | Características | Exemplos |
|---|---|---|
| **Preventivo** | A súa finalidade é previr que ocorra un feito que non é consistente cos obxectivos de control.<br>Detecta os problemas antes de que sucedan.<br>Monitoriza as operacións e os inputs e prevén erros, omisións ou actos malintencionados. | • Separar as funcións de aprobación dun gasto e do seu pago. Este control está deseñado para reducir o risco de pagos indebidos.<br>• Limitar o acceso aos sistemas TIC. Limitar o acceso mediante roles e passwords a cambiar programas reduce o risco de transaccións non autorizadas. |
| **Detectivo** | Detectan e informan da ocorrencia dun erro, omisión ou acto malintencionado. | • Conciliacións. Comparar por persoa independente dous conxuntos de datos relativos á mesma transacción e analizar as diferenzas permite detectar erros ou irregularidades. |
| **Compensatorio** | Se é efectivo, pode limitar ou mitigar a gravidade dunha deficiencia de control interno.<br>Limitan a gravidade dunha deficiencia e as súas consecuencias, pero non a eliminan. | • En entidades de reducida dimensión os controis de segregación de funcións poden ser difíciles de implantar e deben compensarse con controis que impliquen unha maior supervisión ou control xerencial. |

Figura 3

## 4. Concepto de control de aplicación

4.1 Os controis de aplicación son procedementos manuais ou automatizados que operan a nivel de procesos de xestión e que se aplican ao procesamento das transaccións mediante aplicacións informáticas específicas.

Estes controis esténdense sobre o conxunto do proceso de xestión ou actividade cuberto pola aplicación de xestión. **A súa comprobación proporcionará confianza unicamente sobre aquelas clases de transaccións concretas procesadas por esa aplicación, xa que son controis específicos e únicos para cada aplicación informática.**

*Exemplos de controis de aplicación inclúen a comprobación da exactitude aritmética dos rexistros, o mantemento e revisión das contas e balances de comprobación, controis automatizados tales como filtros de datos de entrada e comprobacións de secuencia numérica, e o seguimento manual dos informes de excepcións.*

4.2 A **finalidade dos controis de aplicación** nunha contorna informatizada é establecer procedementos de control específicos sobre as aplicacións de xestión co fin de asegurar razoablemente que todas as transaccións son autorizadas e rexistradas, e que son procesadas de forma completa, adecuada e oportuna, e de garantir a exactitude dos resultados. En consecuencia, os controis xogan un papel central na realización dos obxectivos da entidade, da protección do patrimonio, da exactitude e da fiabilidade da contabilidade e do respecto ás normas.

Actualmente os procesos de xestión dos entes públicos están automatizados en boa medida e a tendencia é que coa implantación da administración electrónica os controis internos estean 100% automatizados ou sexan TI dependentes; os controis 100% manuais tenden a desaparecer. Con todo, cando se revisa un proceso de xestión (nóminas, compras, recadación, etc.) analízase na súa integridade, identificando todos os riscos significativos e os controis relevantes, independentemente de se o proceso ou os controis están automatizados ou son manuais. Todos os controis internos relevantes do proceso de xestión deben auditarse, sexan manuais ou automáticos.

4.3 Desde o punto de vista do auditor, os **obxectivos xerais** dos controis das aplicacións / procesos de xestión son proporcionar unha seguridade razoable de que as transaccións e os datos son **completos, exactos, válidos e de que se cumpriu coa legalidade** na xestión das transaccións.

Estes obxectivos poden describirse así[3]:

- Os controis de **integridade**[4] (entendida como **completitude**) proporcionan unha seguridade razoable de que:
  - todas as transaccións reais son introducidas no sistema,
  - se son válidas son aceptadas no procesamento,
  - son procesadas unha soa vez, os duplicados son rexeitados,
  - as transaccións rexeitadas son identificadas, corrixidas e reprocesadas; e
  - todas as transaccións aceptadas polo sistema son procesadas completamente.

  Os controis máis usuais son: totais de lotes, control de secuencia, control de duplicados, reconciliacións, totalizadores e informes de excepción.

- Os controis de **exactitude** proporcionan unha seguridade razoable de que:

[3] Véxase FISCAM 2009, GAO, apartado 4.0.1.

[4] En galego tradúcese da mesma forma, como integridade, dous termos *integrity* e *completeness* que teñen un significado distinto no orixinal en inglés das normas de auditoría, o que provoca unha certa confusión de conceptos.

Integridade *(integrity)* é a garantía de que os datos ou información de orixe foron validados e estes non foron alterados ao ser creados, procesados, transmitidos e almacenados nos sistemas informáticos (GPF-OCEX 1500, apartado 37).

De forma similar, segundo o ENS a integridade é a propiedade da información, pola que se garante a exactitude dos datos transportados ou almacenados, asegurando que non se produciu a súa alteración, perda ou destrución, xa sexa de forma accidental ou intencionada, por erros de software ou hardware ou por condicións ambientais.

Debe distinguirse de integridade no sentido de completitude (*completeness*). Neste documento cando se utilice integridade neste sentido indicarase así: *integridade (completitude)*.

- as transaccións son rexistradas adecuadamente, coa data e importes correctos, en tempo oportuno e no período adecuado;
- os datos son procesados de forma exacta polas aplicacións, que producen resultados fiables con output exactos.

Inclúense: validacións, comprobacións automáticas de razonabilidade, de dependencia, de existencia, de formato, de rangos, de exactitude matemática, etc.

- Os controis de **validez** proporcionan unha seguridade razoable de que:
  - todas as transaccións rexistradas ocorreron realmente, corresponden á Entidade e foron adecuadamente aprobadas; e de que
  - o output contén só datos válidos.

  Unha transacción é válida cando foi debidamente autorizada e cando os datos mestres relativos a esa transacción son **fiables** (por exemplo os datos bancarios ou domicilio do acredor). A validez inclúe o concepto de **autenticidade**.

  Exemplo: comprobar unha factura co pedido e o albarán de entrada antes da súa aprobación..

- Os controis de **legalidade** proporcionan unha seguridade razoable de que na xestión das operacións cumpriuse coa legalidade vixente.

Estas características coinciden coas afirmacións implícitas na información financeira segundo a GPF-OCEX 1317.

Adicionalmente, os controis de **integridade**, de **confidencialidade** e de **dispoñibilidade** considerámolos CXTI ao nivel do proceso ou aplicación:

- Os controis de **integridade** proporcionan unha seguridade razoable de que a información procesada ou almacenada non pode ser alterada ou manipulada por persoas non autorizadas.
- Os controis de **confidencialidade** proporcionan unha seguridade razoable de que os datos, informes e outros outputs son protexidos contra accesos non autorizados.
- Os controis de **dispoñibilidade** proporcionan unha seguridade razoable dos datos e informes da aplicación están accesibles aos usuarios cando se necesitan.

Estes, principalmente son controis relacionados coa seguridade da información, as copias de seguridade e a planificación das continxencias, e en consecuencia non se consideran especificamente controis de procesos de xestión, senón CXTI ao nivel da aplicación.

4.4 Por outra banda, cada control interno ou actividade de control terá os seus **obxectivos específicos de control**. Para máis detalle ver o Anexo 3.

4.5 Cada tipo de aplicación esixe controis diferentes, xa que cada proceso de xestión ou actividade comercial, industrial, ou de servizo específica, comporta riscos diferentes, inherentes a esa actividade e susceptibles de prexudicar ou impedir alcanzar os obxectivos. Por iso, cada actividade de control está deseñada especificamente para alcanzar un ou varios destes obxectivos. A eficacia dos controis de aplicación depende de se todos estes obxectivos xerais foron alcanzados.

## 5. Interrelación dos CXTI cos controis de aplicación

5.1 Os CXTI axudan a asegurar o correcto funcionamento dos sistemas de información mediante a creación dunha contorna adecuada para o correcto funcionamento dos controis de aplicación. Sen uns controis xerais efectivos, os controis de aplicación poden deixar de ser efectivos xa que resultará moito máis fácil eludilos.

**Unha avaliación favorable dos CXTI dá confianza ao auditor sobre os controis de aplicación automatizados integrados nas aplicacións de xestión.**

*Por exemplo, a emisión e revisión manual dun informe especial de elementos non coincidentes pode ser un control de aplicación efectivo; con todo, dito control deixará de ser efectivo se os controis xerais permitisen realizar modificacións non autorizadas dos programas, de forma que determinados elementos quedasen excluídos deliberadamente de maneira indebida do informe revisado.*

Uns CXTI ineficaces poden impedir que os controis de aplicación funcionen correctamente e permitir que se dean manifestacións erróneas significativas nas contas anuais e que estas non sexan detectadas. Por tanto, **a importancia dunha deficiencia dun CXTI debe ser avaliada no que se refire ao seu efecto nos controis de aplicación**, é dicir, comprobar se os controis de aplicación dependentes son ineficientes.

*Por exemplo, garantir a seguridade das bases de datos considérase un requisito indispensable para que a información financeira sexa fiable. Sen seguridade a nivel de base de datos, as entidades estarían expostas a cambios non autorizados na información financeira*.

5.2 A NIA-ES 330 establece que ao deseñar e executar probas de controis o auditor determinará se os controis para comprobar dependen á súa vez doutros controis (controis indirectos) e, se é así, se é necesario obter evidencia adicional de auditoría que acredite o funcionamento efectivo de ditos controis indirectos.

*Por exemplo: un control consistente na revisión manual dun informe de excepción sobre vendas que excedesen os límites de crédito autorizados. A revisión do responsable e o conseguinte seguimento é o control relevante para o auditor. Os controis sobre a precisión da información incluída nos informes (por exemplo, os controis xerais) denomínanse controis indirectos e tamén hai que asegurarse que están incluídos no alcance.*

*Outro exemplo: unha entidade pode ter correctamente configurada a segregación de funcións no proceso de compras, contabilidade e pago; pero se non existe un CXTI que estableza mecanismos de identificación e autenticación dos usuarios que sexa eficaz, todo o sistema de segregación de funcións devirá á súa vez en ineficaz.*

**Se non existisen controis xerais ou non fosen efectivos, non se podería confiar nos controis de aplicación e sería necesario adoptar un enfoque de auditoría baseado exclusivamente en procedementos substantivos.**

5.3 O reto cos CXTI consiste en que estes case nunca afectan á información financeira directamente, pero teñen un efecto xeneralizado e permanente en todos os controis internos. É dicir, se un CXTI importante falla (p. ex. un control de restrición de acceso a programas e datos), ten un efecto dominante en todos os sistemas que dependen del, incluídas as aplicacións financeiras; *por exemplo, sen estar seguros de que soamente os usuarios autorizados teñen acceso ás aplicacións financeiras ou ás bases de datos subxacentes, non se pode concluír que unicamente aqueles usuarios con autorización iniciaron e aprobaron transaccións.*

Dunha forma visual, vemos que uns controis xerais débiles non protexen nin posibilitan de forma eficaz o bo funcionamento dos controis das aplicacións:


Figura 4

Con todo, uns controis xerais sólidos e eficaces, proporcionan unha contorna adecuada para o bo funcionamento dos controis das aplicacións:


Figura 5

*Outro exemplo: os controis dunha aplicación de vendas-facturación poden estar ben deseñados e correctamente implementados, pero se non hai controis sobre os accesos directos ás bases de datos que soportan e rexistran os datos e transaccións da aplicación, aqueles controis son inútiles.*

5.4 Polas razóns sinaladas ao auditar o control interno dun proceso/aplicación de xestión é necesario revisar os controis existentes en toda a "pila" do sistema de información, é dicir os controis de aplicación e os CXTI de todos os niveis do sistema de información que soportan o proceso de xestión auditado que afectan ao seu bo funcionamento, tal como se mostra gráficamente na Figura 6.

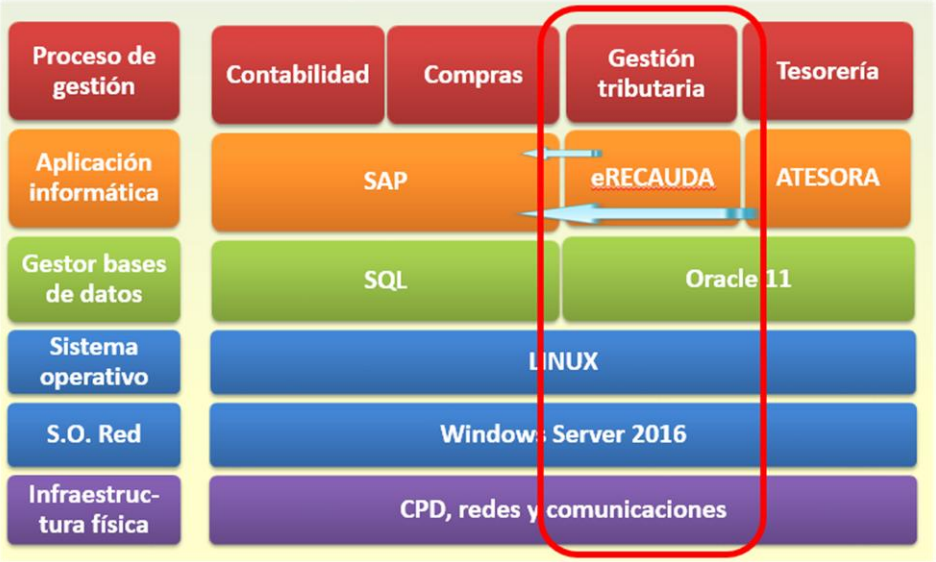



Figura 6

## 6. Adquisición dun coñecemento dos procesos de xestión significativos, das aplicacións significativas e das principais interfaces.

Estas son unhas das primeiras actividades que deben realizarse nunha auditoría financeira realizada co enfoque baseado na análise do risco, tal como pode verse na Figura 1. Na GPF-OCEX 1315 explícase a metodoloxía xeral de auditoría desa fase.

Nos anexos 1 e 2 danse unhas orientacións sobre como realizar e documentar este traballo, que se debe plasmar nun fluxograma detallado como o do exemplo de xestión de ingresos tributarios dun concello mostrado na Figura 7, complementado cunha narrativa explicativa.

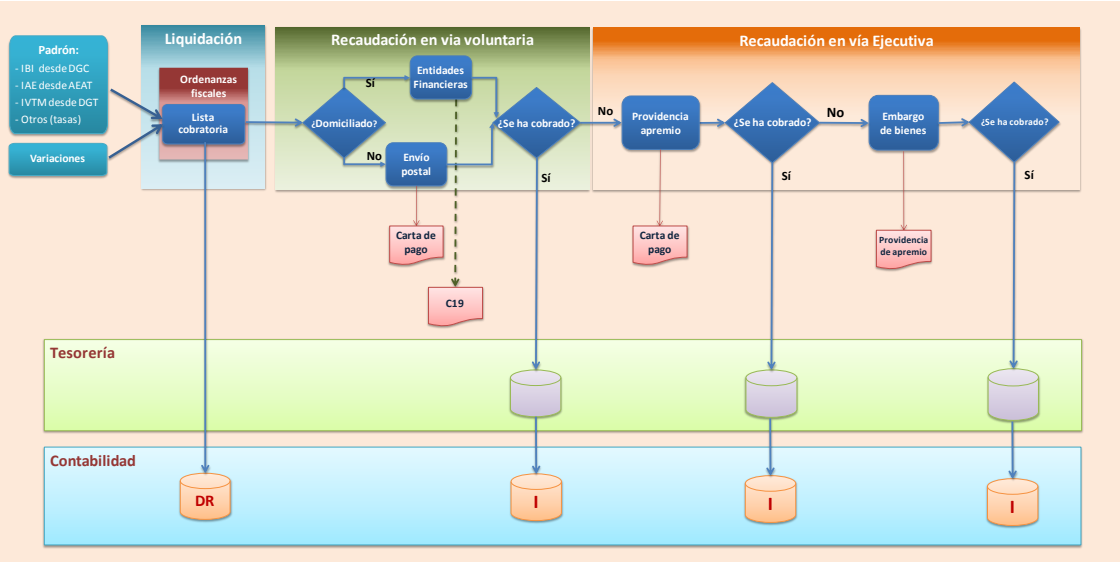



Figura 7

## 7. Identificación dos riscos e dos controis relevantes dos procesos e aplicacións de xestión significativas, e das interfaces.

7.1 Unha vez identificados os procesos e as aplicacións de xestión que teñen carácter significativo en relación coas contas anuais, que son as incluídas dentro do alcance da auditoría, e feita a revisión dos controis xerais con resultado satisfactorio (é dicir chegouse á conclusión de que son confiables), pásase á seguinte etapa da auditoría.

Se tras a revisión dos CXTI chegásese á conclusión de que non son eficaces, un auditor financeiro deberá reformularse a súa estratexia de auditoría xa que non poderá confiar nos controis de aplicación e deberá adoptar un enfoque baseado en probas substantivas para realizar a auditoría financeira[5].

Nesta etapa, o auditor TI débese delimitar o alcance detallado da auditoría para realizar sobre as aplicacións de xestión seleccionadas. Tendo en conta a complexidade dos procesos e das aplicacións de xestión nas actuais contornas de administración electrónica, é importante centrarse no esencial, por iso

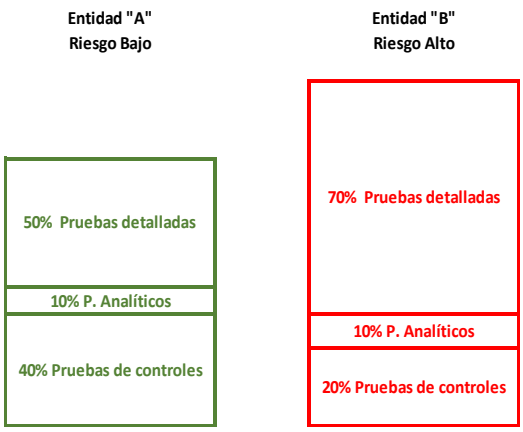
[5] A natureza, momento e alcance dos procedementos de auditoría determínanse de acordo coas circunstancias de cada traballo e deben basearse no coñecemento da actividade que realiza o ente auditado, da súa organización, dos riscos valorados así como na avaliación do control interno e da importancia relativa dos saldos nas contas anuais.

Os procedementos de auditoría financeira son as respostas aos riscos valorados e por tanto deben ser proporcionais a eses riscos. Así as áreas de risco máis alto deben recibir maior atención e esforzo de auditoría.

Os programas de auditoría deben ser adaptados a cada entidade en base á valoración do risco de incorreccións materiais, e incluirán:

- Probas de controis (se procede)
- Procedementos substantivos (incluíndo procedementos analíticos)

Podemos ver cun exemplo gráfico como pode variar a cantidade (suficiencia) de evidencia necesaria e os tipos de probas necesarias para obtela



a identificación dos riscos significativos e dos controis relevantes implantados para mitigalos constitúe a base para unha auditoría eficaz. Só avaliarase a efectividade daqueles controis que teñan relevancia a efectos da auditoría financeira, circunstancia que deberá ser definida polo auditor financeiro coa colaboración do auditor de sistemas a partir dos riscos significativos identificados.

Débense identificar os riscos existentes nos principais procesos de xestión e nos sistemas e aplicacións que as soportan, o que dará unha idea xeral dos riscos susceptibles de impedir a consecución dos obxectivos do proceso de xestión ou que poidan entrañar incorreccións materiais nas contas anuais. Esta análise dos riscos axuda a definir a estratexia de auditoría, é dicir da confianza preliminar na eficacia do control interno e do peso relativo das probas de cumprimento e dos procedementos substantivos.

Partirase do estudo realizado do proceso/aplicación a auditar (ver apartado 6 anterior) e de calquera outra documentación ou información dispoñible do proceso/aplicación, incluíndo entrevistas cos usuarios ou responsables da entidade

Normalmente, ao realizar o estudo e descrición dun proceso mediante unha narrativa e un fluxograma, inclúese unha "primeira versión" dos riscos e controis clave identificados, que serán confirmados ou modificados despois ao realizar as probas de percorrido.

7.2 A identificación dos riscos potenciais realízase consultando aos distintos usuarios ou responsables do proceso de xestión auditado e analizando os distintos pasos e compoñentes que interveñen no proceso:

- O fluxo de procesamento dos datos (ver Anexo 1)
- Os datos mestres (ver Anexo 3)
- Os permisos ou autorizacións (ver Anexo 1)
- A segregación de funcións (ver Anexo 4)
- As interfaces (datos entrantes e saíntes) (ver Anexo 2)

Ademais de identificar os riscos inherentes do proceso de xestión (manual ou automatizado) na súa integridade, nas interfaces, nos parámetros e nos datos mestres, debe adquirirse unha comprensión preliminar dos controis de aplicación que mitiguen ditos riscos.

Todos os controis importantes ligados ás aplicacións, que teñan unha influencia directa sobre o resultado do proceso, deben ser tidos en conta, **tanto os manuais como os automáticos**.

Normalmente existe unha combinación de controis automatizados e manuais que equilibran os recursos materiais e humanos requiridos polo equipo auditor e a redución do risco de auditoría.

7.3 Os **controis relevantes** son un elemento fundamental na auditoría baseada na análise do risco, xa que boa parte dos procedementos de auditoría xiran ao seu redor.

Nesta fase, de todos os controis identificados nas aplicacións revisadas, só interesan os máis importantes, os que, se están ben deseñados e implantados e funcionan con eficacia, permiten concluír ao auditor que os riscos de auditoría de que existan erros ou irregularidades non detectados polo sistema de control interno están controlados nun nivel aceptable.

É dicir, **o auditor obterá coñecemento das actividades de control relevantes para a auditoría** que, a xuízo do auditor, son[6]:

- Aquelas que é necesario coñecer, ao ser actividades de control relacionadas con riscos significativos.
- Aquelas que están relacionadas con riscos para os cales aplicar só procedementos substantivos non proporciona evidencia de auditoría suficiente e adecuada.
- As que, a xuízo do auditor, de funcionar adecuadamente, permiten mitigar o risco de incorrección material (RIM) e reducir o risco de auditoría.

[6] Véxase GPF-OCEX 1316; apartado 9.1.

O auditor debe poñer énfase na identificación e a obtención de coñecemento das actividades de control naquelas áreas nas que considera máis probable que existan riscos de incorrección material.

7.4 Unha auditoría non require o coñecemento de todas as actividades de control relacionadas con cada tipo significativo de transacción, de saldo contable e de información a revelar nos estados financeiros ou con cada afirmación correspondente a eles. Cando múltiples actividades de control alcancen individualmente o mesmo obxectivo, non é necesario obter coñecemento de cada unha das actividades de control relacionadas con dito obxectivo, bastará con verificar que un deses controis é eficaz.

7.5 Á hora de decidir se un control é relevante, debe aplicarse o xuízo profesional, e terase en conta o seguinte:

- Os controis relevantes xeralmente inclúen políticas, procedementos, prácticas e unha estrutura organizativa que son esenciais para que a dirección poida reducir os riscos significativos e alcanzar o obxectivo de control relacionado.
- Os controis relevantes a miúdo apoian máis dun obxectivo de control.
- Os controis que fan fronte directamente aos riscos significativos son con frecuencia relevantes.
- Os controis preventivos son por regra xeral máis eficientes que os detectivos. Por tanto, os controis preventivos considéranse a miúdo relevantes.
- Os controis automatizados son máis fiables que os controis manuais.

7.6 Para cada control que se identificara como relevante, o auditor debe aplicar **procedementos** para **analizar a efectividade do seu deseño para realizar a actividade de control**, considerando o risco TI e os obxectivos da auditoría. Se se conclúe que o deseño é eficaz aplicaranse procedementos de auditoría para **verificar se está implementado e en funcionamento durante todo o período auditado**.

7.7 **Os controis relevantes** (ás veces denominados controis clave)**, individualmente ou combinados entre eles, son indispensables para a redución dos riscos a un nivel aceptable**. Son os que permiten reducir os riscos de incorrección material (RIM) a un nivel aceptablemente baixo.

Constitúen o elemento fundamental do sistema de control e deben ser, pois, obxecto de comprobación prioritaria; os outros controis teñen menos importancia para o auditor. Se o auditor non se concentra sobre os controis relevantes, a auditoría corre o risco de ser demasiado xeral e ineficaz.

**7.8 Todo o traballo de auditoría posterior debe centrarse nos controis relevantes, xa que todo traballo que se realice sobre os outros controis existentes non achega satisfacción ou utilidade adicional de auditoría, e será un traballo ineficiente.**

Ver consideracións adicionais sobre os controis relevantes no apartado 6 da GPF-OCEX 5330.

## 8. Avaliación do deseño dos controis. Realización de probas de percorrido ou paso a paso.

8.1 Tras a identificación dos controis relevantes que mitigan riscos significativos (RIM se se está facendo unha auditoría financeira) o seguinte paso será avaliar o deseño dos controis para ver se son eficaces, é dicir, para determinar se cada un destes controis, individualmente ou en combinación con outros controis, é capaz de previr, detectar e corrixir de forma efectiva erros ou irregularidades materiais.

Se están ben deseñados deberase verificar que funcionaron como se esperaba, que estiveron operativos, durante todo o período auditado.

Só unha comprensión profunda do deseño dos controis permite definir unha estratexia adecuada para a avaliación do funcionamento dos controis mediante o deseño e execución de probas de cumprimento que sexan eficaces, plenamente adaptadas á actividade de control.

8.2 O deseño dos controis, especialmente a súa situación no proceso de xestión debe ser avaliado para saber se:

- Os riscos identificados son cubertos completamente.
- Os obxectivos de control definidos poden ser realmente alcanzados polos controis implantados.

- Os controis permiten realmente reducir os riscos de erros e de irregularidades.
- A cobertura dos riscos realízase de forma eficaz e económica (eficiencia).
- Outro control ou combinación de controis son máis eficaces para realizar o mesmo obxectivo de control.

Unha análise minuciosa do deseño dos controis permite:

- Identificar as lagoas, os solapamentos e os duplicados en materia de controis.
- Evitar realizar probas de controis polo auditor cando os controis son inadecuados ou ineficaces.
- Considerar se o mesmo resultado ou un mellor, pode ser obtido coa utilización ou adaptación doutros controis, especialmente con outros xa establecidos.

A evidencia probatoria da eficacia dos controis durante todo o período revisado só pode ser obtida mediante a realización de probas de controis.

8.3 Ao avaliar o deseño dos controis deben considerarse os aspectos seguintes:

- As etapas do proceso e os controis relacionados están organizados nunha orde lóxica e razoable?
- Está definida sen ambigüidade a responsabilidade da realización dos controis?
- Poden realizarse os controis de forma correcta e razoable?
- Son substituídos os controis híbridos ou manuais, na medida do posible, por controis automatizados?
- Os controis detectivos son substituídos se é posible por controis preventivos?
- Son conformes os controis ás esixencias das directivas e procedementos de traballo?
- Están dispoñibles as instrucións e informacións necesarias para a realización do control?
- Os controis son realizados por unha persoa cualificada?
- Os controis son realizados cun atraso razoable e cunha frecuencia apropiada?
- O deseño dos controis pode ser posto en marcha no marco de restricións organizativas e financeiras da entidade?

Nesta análise debe terse presente que **os controis automáticos son máis eficaces e eficientes que os controis manuais**, pois teñen un funcionamento continuo no tempo e un custo único de implementación. Ademais, a súa eficacia é máis estable en tanto non se efectúen modificacións significativas na aplicación.

Como regra xeral, unha frecuencia elevada de controis manuais ou semiautomáticos ocasiona custos e atrasos máis elevados respecto a controis automáticos cuxa frecuencia non ten practicamente influencia sobre os custos de explotación. Pola contra, unha frecuencia de execución baixa dun control manual ou semiautomático pode prexudicar a súa eficacia.

Está xeralmente admitido que **os controis preventivos permiten alcanzar máis facilmente os obxectivos de control que os controis detectivos**.

Un control que cobre varios obxectivos de control ou diferentes riscos considérase en principio máis eficaz, máis fiable e máis económico que un control centrado sobre un só risco.

En contornas ERP complexas, ao avaliar o deseño de controis de aplicación, o auditor debe clarificar as condicións técnicas requiridas para que o control se desenvolva da forma prevista. O auditor exporase principalmente as cuestións seguintes:

- Pode eludirse ou forzarse (rodeo, procedemento de excepción, superusuario) o control?
- En que medida depende o control da parametrización?
- En que medida depende o control do sistema de dereitos de acceso?
- Quen controla o sistema de dereitos de acceso?
- En que medida depende o control dos datos mestres?
- Quen controla os datos mestres?
- Pode rexistrarse o funcionamento do control para comprobacións posteriores (logs, pistas de auditoría)?

8.4 **Procedementos de auditoría aplicables.** O auditor formará a súa opinión sobre o **deseño** dos controis:

- Interrogando aos membros da dirección da empresa, aos empregados que teñan tarefas de supervisión, así como aos empregados implicados na realización do control.
- Consultando os documentos relativos ás transaccións e outros documentos importantes da empresa.
- Observando as actividades específicas de execución e de control.
- Seguindo as transaccións individuais no sistema de información (mediante as probas de percorrido).

8.5 De conformidade coas normas técnicas de auditoría, os procedementos para a avaliación do deseño dos controis deben estar **apoiados por evidencia de auditoría e adecuadamente documentados**.

Cando tras unha proba de percorrido e a análise do deseño dos controis, chégase á conclusión de que o esforzo de auditoría a efectuar para verificar un control clave é desproporcionado, débese realizar unha adaptación da selección de controis relevantes para facer un **esforzo viable**.

Tamén, ao analizar o deseño dos controis, se o auditor identifica controis relevantes que considera inoperantes, o sistema de control avaliado presenta entón unha lagoa. Para cubrila debe identificar outros controis relevantes ou **controis compensatorios** e avaliar a súa eficacia. Neste caso, o auditor debe ter presente a selección completa de controis relevantes para evitar crear redundancias custosas nos procedementos de auditoría.

## 9. Realización de probas do funcionamento dos controis relevantes

Unha vez verificada a razonabilidade e eficacia do deseño dos controis débese verificar o adecuado funcionamento operativo dos controis relevantes durante todo o período auditado.

Será aplicable a GPF-OCEX 1330.

## 10. Documentación da valoración dos riscos e da revisión dos controis relevantes

1.01 O deseño dos mapas de procesos ou fluxogramas, nos que ademais deben indicarse os principais riscos e os controis clave (representados por símbolos), debe complementarse con documentos (narrativas) nos que se describan en detalle estes aspectos.

10.2 A documentación debe permitir ao auditor comprender cales son as "regras de xestión" que deben ser garantidas polo control. Ademais, debe recoller os aspectos ligados ao deseño do control desde a perspectiva da súa implementación. Deben reflectirse os parámetros ou axustes personalizables para que o control poida funcionar conforme ás regras de xestión definidas:

| Control relevante | | Regra de xestión | Deseño do control |
|---|---|---|---|
| C001 | Tripla comprobación | Non se paga ningunha factura se non concordan o pedido, albarán e factura. | |
| C002 | Segregación de funcións | Segregación de funcións entre contabilidade, xestión de debedores e acredores, tesourería.<br>As persoas que pagan as facturas non poden crear novos provedores. | |

Figura 8 Exemplo de documentación de controis

Para a comprensión dos controis relevantes das aplicacións e, en particular, para a avaliación posterior do seu deseño, é importante efectuar unha adecuada documentación dos mesmos (aínda que non é aconsellable unha descrición excesivamente detallada dos controis, pois iso carrexaría custos e non xeraría un beneficio adicional).

10.3 Para cada proceso de xestión significativo analizado, debe cumprimentarse un formulario de análise de riscos no que debe resumirse o traballo realizado para identificar e avaliar os riscos e controis clave relacionados, como o modelo da figura seguinte.

Identificaranse os epígrafes das contas anuais (capítulo/artigo orzamentario, conta e revelación significativa da memoria), afectados por procesos de xestión (como ingresos, subvencións, compras e nóminas, etc) e as aplicacións específicas significativas que afectan a eses capítulos/artigos orzamentarios, contas e declaracións.

Un formulario proporciona unha forma práctica e útil de documentar os RIM específicos, que se deben ter en conta á hora de determinar a natureza, alcance e momento de execución dos procedementos de auditoría.

Na figura 9 pode verse un modelo de formulario deste tipo.

| **Formulario de Análise de Riscos**<br>Entidade: Concello de X Y Z | |
|---|---|
| Proceso de negocio: | *Contratación de investimentos* |
| *Subproceso:* | *Adxudicación* |
| Contas relacionadas: | Capítulo 2, 6 e acredores |
| Aplicación informática: | |

| **Risco** | **Control clave** | **Tipo de control** | **Responsable** | **Eficacia do control** | **Valoración do Risco** | **Impacto** |
|---|---|---|---|---|---|---|
| (Describir o risco e asignar un identificador secuencial) | (Describir o control e asignar un identificador secuencial. Para cada risco pode haber máis dun control) | Sinalar se é:<br>Manual/Automático<br>Detectivo/Preventivo<br>Compensatorio | (Indicar o responsable do control) | Sinalar se é:<br>Efectivo/ Non efectivo (neste caso describir a incidencia observada) | Baixo<br>Medio<br>Alto | Describir (sinalar a conta e a manifestación afectada) e cuantificar (se é posible) cal podería ser o resultado posible do mal funcionamento do control |
| R001-Descrición | C001A -Descrición | | | | | |
| R002-Descrición | C002A -Descrición | | | | | |
| | C002B -Descrición | | | | | |

Figura 9

## 11. Avaliación das incidencias detectadas

11.1 Ao revisar a situación dos controis identificados verificarase e documentarase a súa eficacia podendo atoparse cada un deles nalgunha das seguintes situacións:

Control efectivo

Control bastante efectivo

Control pouco efectivo

Control non efectivo

11.2 As deficiencias de control interno e as recomendacións que se deriven das mesmas deben estar ben soportadas nos papeis de traballo. Os achados de auditoría que as soportan deben incluír: (GPF-OCEX 1735; P9)

Criterio (de auditoría): a referencia ou norma coa que se compara ou avalía o feito observado; o que debería ser.

Nas auditorías de sistemas de información (CXTI, controis de aplicación e cibercontrois) os criterios de auditorías son os establecidos con carácter xeral na GPF-OCEX relacionadas, que están baseadas no ENS, NIA-ES, ISSAI, etc.

Feito ou condición: a situación observada e documentada na auditoría.

Están baseados en evidencia de auditoría. Poden ser deficiencias de control, problemas operacionales ou incumprimento de requirimentos legais ou administrativos.

Causa: as razóns que dan lugar ao feito observado.

Pode servir como base para propoñer accións correctoras nas recomendacións. Débese identificar a unidade ou departamento responsable da deficiencia.

As causas máis comúns inclúen políticas, procedementos ou criterios mal deseñados, ou aplicados de forma inconsistente, incompleta ou incorrecta; ou factores máis aló do control dos xestores. Os auditores poden avaliar se a evidencia proporciona un argumento razoable e convincente de por que a causa indicada é o factor clave que contribúe á diferenza entre a condición e os criterios.

Efecto: que consecuencia negativa ten lugar ou podería ter lugar, provocada pola diferenza entre o feito observado e o criterio.

Explica o impacto adverso ao obxectivo operacional ou obxectivo do control. Ao articular o impacto e o risco, o elemento do efecto real ou potencial é moi importante para axudar a convencer á administración do auditado da necesidade de tomar accións correctoras en resposta aos problemas e/ou riscos significativos identificados.

Recomendación: accións correctoras suxeridas.

As recomendacións deben redactarse de forma que se aborde a corrección das causas que orixinan o feito ou condición observado.

11.3 Ao avaliar as deficiencias de control interno detectadas débense considerar a significatividade das mesmas. Neste contexto o concepto “significativo” non pode ser definido de forma exacta, xa que unha mesma cuestión pode ser significativa, ou non, dependendo dos obxectivos da auditoría e das circunstancias. *(GPF-OCEX 1735; P10)*

11.4 As deficiencias de control interno clasifícanse en tres niveis de importancia relativa ao examinar o control interno: *(GPF-OCEX 1735; P11)*

- Unha **deficiencia de control interno** existe cando o deseño ou o funcionamento dun control non permite ao persoal da entidade ou á súa dirección, no curso ordinario das operacións, previr ou detectar erros ou irregularidades nun prazo razoable. Poden ser *deficiencia de deseño* do control (cando un control necesario para alcanzar o obxectivo de control non existe ou non está adecuadamente deseñado) ou *deficiencias de funcionamento* (cando un control adecuadamente deseñado non opera tal como foi deseñado ou a persoa que o executa non o realiza eficazmente).
- Unha **deficiencia significativa** é unha deficiencia no control interno, ou unha combinación de deficiencias, que afectan adversamente a capacidade da entidade para iniciar, autorizar, rexistrar, procesar ou reportar información financeira ou orzamentaria de forma fiable, de conformidade cos principios ou normas contables e/ou orzamentarias aplicables, e existe unha probabilidade que é máis que remota, de que unha manifestación errónea nas contas anuais, ou un incumprimento, que non é claramente trivial, non sexa previda ou detectada en prazo oportuno.
- Unha **debilidade material** é unha deficiencia significativa no control interno ou unha combinación delas, respecto das que existe unha razoable posibilidade de que unha manifestación errónea significativa nas contas anuais, incluíndo un incumprimento de carácter grave, non sexa previda ou detectada e corrixida en prazo oportuno.

11.5 A avaliación de importancia relativa ou significatividade das deficiencias inclúe consideracións sobre os seguintes factores de carácter xeral: a magnitude do impacto, a probabilidade de que ocorra e a natureza da deficiencia. *(GPF-OCEX 1735; P12)*

Implica avaliar, no contexto dos obxectivos da auditoría, os seguintes factores:

a) A magnitude do impacto refírese para o efecto probable que a deficiencia puidese ter no logro dos obxectivos da entidade e vese afectado por factores como o tamaño, o ritmo e a duración do impacto da deficiencia. Unha deficiencia pode ser máis significativa para un obxectivo que para outro.

b) A probabilidade de ocorrencia refírese á posibilidade de que unha deficiencia afecte á capacidade dunha entidade para alcanzar os seus obxectivos.

c) A natureza da deficiencia implica factores tales como o grao de subxectividade implicado coa deficiencia e se a deficiencia xorde da fraude ou dunha conduta indebida.

11.6 Para determinar se unha deficiencia de control, individualmente ou xunto con outras, constitúe unha deficiencia significativa ou unha debilidade material, o auditor considerará varios factores, incluíndo:

- Prexudica ou pode prexudicar o cumprimento dos obxectivos da entidade.
- É unha deficiencia de control interno que ocasiona un aumento significativo do risco de auditoría.
- A probabilidade de que unha persoa poida obter acceso non autorizado ou executar actividades non autorizadas ou inapropiadas en sistemas críticos da entidade ou arquivos que poidan afectar á información con impacto nas contas anuais. Isto pode incluír:
  (1) a habilidade para ter acceso a sistemas nos que residen aplicacións críticas e que posibilita a usuarios non autorizados a ler, engadir, borrar, modificar ou extraer información financeira, ben directamente ou a través da utilización de software non autorizado;
  (2) a habilidade para acceder directamente e modificar ficheiros que conteñan información financeira;
  (3) a habilidade para asignar dereitos de acceso ás aplicacións a usuarios non autorizados, coa finalidade de procesar transaccións non autorizadas.
- A natureza dos accesos non autorizados que poden conseguirse (por exemplo: limitados a programadores do sistema ou das aplicacións ou a administradores do sistema; a todos os usuarios; a alguén externo a través de acceso non autorizados por Internet) ou a natureza das actividades non autorizadas ou inadecuadas que poden levarse a cabo.
- A probabilidade de que importes das contas anuais estean afectados de forma significativa.
- A probabilidade de que outros controis poidan previr ou detectar accesos non autorizados.

- O risco de que a dirección da entidade poida burlar os controis (por exemplo, mediante dereitos de acceso excesivos).

Algunhas deficiencias de control poden ser consideradas non significativas individualmente, pero consideradas juntamente con outras similares, o efecto combinado pode ser máis significativo.

**11.7 Baseándose nas consideracións apuntadas o auditor informático determinará se as deficiencias de control son, individualmente ou en conxunto, debilidades materiais ou deficiencias significativas para o adecuado funcionamento dos sistemas de información.**

**Se as deficiencias de control constitúen debilidades materiais, o auditor financeiro, en base ao traballo do auditor informático, concluirá que os controis internos non son eficaces e deberá reformularse a súa estratexia de auditoria, é dicir, a combinación adecuada de probas de cumprimento e de probas substantivas, dando maior énfase a estas últimas para tentar minimizar o risco final de auditoría.**

11.8 Se se efectúan recomendacións, existirá unha relación directa entre o tipo de deficiencia de control (segundo a súa importancia relativa), o risco de auditoría que representa, e a prioridade que se conceda a cada recomendación.

A prioridade tamén estará matizada por consideracións custo/beneficio.

No cadro seguinte resúmese a relación existente entre os tres tipos de deficiencias de control segundo a súa significatividade ou importancia relativa, o risco que representan e a prioridade das recomendacións correspondentes: *(GPF-OCEX 1735; P13)*

| Tipo de deficiencia segundo a súa importancia relativa | Risco | Prioridade dunha recomendación | |
|---|---|---|---|
| **Debilidade material** | **Alto** | **Alta** | Requírese atención urxente da dirección para implantar controis/procedementos que mitiguen os riscos identificados. |
| **Deficiencia significativa** | **Medio** | **Media** | A dirección debería establecer un plan de acción concreto para resolver a deficiencia observada nun prazo razoable. |
| **Deficiencia de control interno** | **Baixo** | **Baixa** | |

Figura 10

11.9 As debilidades materiais deben ser incluídas no informe de auditoría como unha excepción ou como unha conclusión, segundo o tipo de informe.

## 12. Bibliografía


- Global Technology Audit Guide: Auditing Application Controls, xullo 2007, The Institute of Internal Auditors.
- COBIT and Application Controls, 2009, ISACA.
- Federal Information Systems Audit Manual (FISCAM), 2009, GAO.
- Manual IDI-WGITA sobre auditoría de TI para as Entidades Fiscalizadoras Superiores, 2013, INTOSAI. 2017 para a tradución española de OLACEFS.

## Anexo 1: Identificación das aplicacións de xestión significativas (GPF-OCEX 1315, Anexo 2)

### a) Identificación dos procesos de xestión significativos

As contas anuais dunha empresa ou entidade son o resultado da agregación de múltiples actividades que se poden agrupar en procesos, e que poden ser moi diferentes uns doutros.

Partindo das clases de transaccións significativas identificadas, o auditor debe identificar os procesos de xestión significativos que inflúen nos seus importes ou nos seus saldos contables.

Un **proceso de xestión** (ou proceso de negocio) consiste nunha serie de actividades, operacións ou funcións (manuais, semiautomáticas ou automatizadas) realizadas por unha entidade, que serven para levar a cabo a súa misión e desenvolver a súa actividade (a elaboración de produtos ou a subministración de servizos) ou o tratamento da información.

Un proceso ten un punto de inicio e outro de finalización clara e xeralmente interveñen varios departamentos da entidade. Poden clasificarse en tres grupos:

- Procesos relacionados coa **actividade principal** da entidade: xestión de subvencións, xestión de historias médicas, matriculación universitaria, compras, vendas, etc.
- Procesos **financeiros**: cobros, pagos, nóminas, etc.
- Procesos **de apoio**: agrupan todas as funcións de apoio á posta en marcha e á explotación dos procesos operativos, como xestión de recursos humanos, mantemento de inventario de inmobilizado, contabilidade, etc.

Por **procesos de xestión significativos**, para os efectos da auditoría, enténdese os principais procesos que teñen unha influencia directa sobre o fluxo de tratamento contable e a formación ou valoración de compoñentes significativos das contas anuais. O concepto de materialidade pode axudar ao auditor para determinar que compoñentes das contas e que aplicacións relacionadas son significativas para os obxectivos da auditoría.

Se existisen debilidades de control nos procesos de xestión significativos podería cuestionarse a fiabilidade das contas anuais. Por iso resulta indispensable a identificación minuciosa dos procesos de xestión significativos e dos fluxos de procesamento de datos para poder identificar e valorar os riscos no seo de cada un deles. É dicir, débese:

- Identificar os fluxos de datos. É necesario ter unha visión global da circulación dos datos ao longo de todo o proceso ou procesos analizados, desde a súa captura inicial, tratamento, ata o seu arquivo final. Isto inclúe a identificación das bases de datos que interveñen e as operacións que se realizan para transferir os datos procesados dunha base de datos a outra.
- Identificar os riscos existentes.
- Identificar os controis. Ao longo do fluxo dos datos a través do proceso establécense unha serie de controis sobre a validez, integridade, exactitude, confidencialidade e dispoñibilidade dos datos.
- Revisar pistas de auditoría (trazabilidade). A finalidade é localizar unha información ou un dato a partir doutro, resultante dunha aplicación informática lóxica e fisicamente afastada. Así, é posible por exemplo, a partir do saldo dunha conta do balance ou dun capítulo/artigo orzamentario, obter un detalle dos seus movementos, e de cada un destes o apuntamento contable realizado e a referencia aos documentos que orixinaron o movemento contable. A ausencia de pistas de auditoría é unha debilidade do control interno.

Para comprender mellor a actividade da entidade é conveniente desagregar os procesos complexos en subprocesos (un **subproceso** ou función é un subconxunto de actividades ou tarefas, realizadas por un empregado ou funcionario para levar a cabo as súas responsabilidades, que producen un resultado ou output).

Vexamos dous exemplos:

| *Proceso* | *Subprocesos* |
|---|---|
| ***Gastos de personal*** | *Orzamentación* |
| | *Xestión de postos (RPT)* |
| | *Xestión de persoas* |
| | *Elaboración da nómina* |
| | *Pago nómina* |
| | *Contabilización* |
| ***Concesión de subvencións*** | *Inicio* |
| | *Instrución* |
| | *Finalización* |
| | *Pago* |

A análise para realizar esténdese tanto ao proceso contable mesmo como ao proceso puntual de peche das contas anuais; a procesos de xestión complexos, como o de impostos-recadación ou vendas-facturación, que teñen influencia tanto no fluxo financeiro como no de mercadorías (neste caso varias contas do balance, da conta de perdas e ganancias e da liquidación do orzamento teñen o mesmo proceso como fonte ou orixe dos seus datos) e aos procesos de apoio, por exemplo os da área de recursos humanos.

Os procesos que están interrelacionados e afectan a un grupo de transaccións e contas poden agruparse en ciclos. Agrupar os procesos e aplicacións de xestión en ciclos pode axudar ao auditor a documentar a auditoría e a deseñar procedementos que sexan eficaces, eficientes e relevantes para os obxectivos da auditoría.

Os procesos poden ser representados de forma gráfica mediante fluxogramas.

Ao realizar esta análise débese aproveitar a documentación descritiva dos procesos de xestión que exista na empresa ou entidade auditada. Normalmente esta documentación céntrase nas actividades e é preciso completala para cada etapa do proceso coas entradas de datos, os tratamentos de datos e os resultados, así como os roles dos distintos axentes que interveñen.

En xeral, a documentación da entidade non sinalará os riscos dos procesos, nin os controis clave, que deberán ser identificados e documentados polo auditor nunha fase posterior, ao analizar os controis das aplicacións.

Comprender a actividade e o funcionamento da entidade e dos principais procesos de xestión, inclúe entender como se empregan as aplicacións informáticas para soportar os procesos de xestión, xa que varían dunha entidade a outra.

**b) Que é unha aplicación de xestión significativa**

Unha aplicación de xestión é unha combinación de hardware e software usada para procesar información da actividade da entidade e pode dar soporte a un ou varios procesos de xestión; esas aplicacións informáticas poden ter unha maior ou menor complexidade e grao de integración, segundo os casos.

A automatización e integración das distintas fases dos procesos de xestión e de numerosos controis internos nun sistema de información **expón riscos inherentes adicionais.** Poden presentarse, por exemplo, dificultades para implementar unha adecuada segregación de funcións; tamén, se o nivel de integración é moi elevado e os datos procésanse en tempo real ou se se aplica o principio de "entrada única de datos", xeraranse procesos e rexistros automáticos de transaccións que provocarán que poida ser imposible que existan controis humanos.

As aplicacións de xestión integradas, en particular os ERP, condicionan profundamente a maneira de traballar e determinan a forma na que se fan os intercambios entre os distintos axentes que interveñen nun proceso de xestión, contribuíndo á estruturación dos procesos.

A identificación das aplicacións de xestión significativas para os propósitos da auditoría financeira, a análise das súas características e das súas interfaces, débese facer canto antes, xa que esta información permitirá definir de forma detallada o deseño, alcance e a extensión das probas de auditoría, o grao de participación requirido do auditor informático e a elaboración dos programas de auditoría.

Polo xeral considerarase que unha aplicación é significativa, para os efectos da auditoría financeira, cando soporte un proceso de xestión significativo, se procesa transaccións agregadas superiores ao nivel de importancia relativa fixado na memoria de planificación ou se apoia un saldo contable significativo das contas anuais auditadas.

O auditor tamén pode identificar aplicacións como significativas baseándose en consideracións cualitativas. Por exemplo, sistemas que apoian a planificación financeira, os informes de xestión e actividades orzamentarias; sistemas que xestionan e proporcionan datos e información de custos; e sistemas que xestionan aspectos relacionados co cumprimento da legalidade (contratación, subvencións, etc.).

O sistema de información financeira dunha entidade pode ser visto como unha serie de agrupamentos lóxicos de transaccións e actividades relacionadas e xeralmente comprende varias aplicacións informáticas. Cada capítulo/artigo orzamentario ou conta significativa pode estar afectada ou influída por inputs dunha ou varias aplicacións (orixe de cargos e abonos).

De forma gráfica:

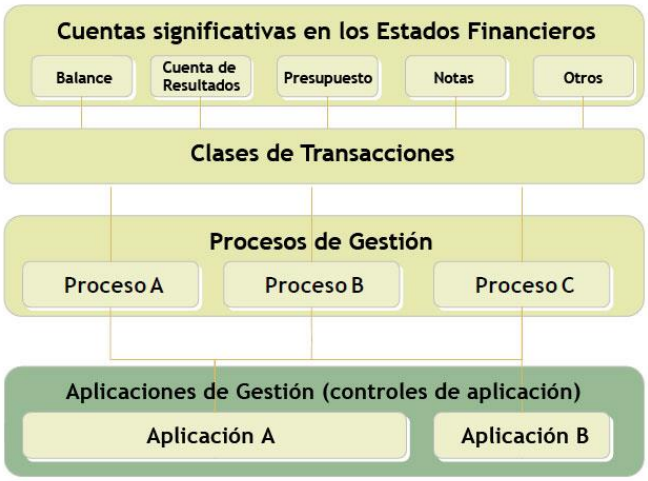



Figura 7

**c) Información a obter sobre as aplicacións de xestión**

O auditor baseándose en: a) a información obtida mediante os cuestionarios, b) entrevistas mantidas co persoal da entidade, c) experiencia de anos precedentes e d) a análise das contas anuais xunto con outra información obtida nas etapas iniciais do traballo, determinará as aplicacións informáticas que son a fonte para a formación das contas anuais.

Por exemplo, as aplicacións que conteñen rexistros auxiliares das contas para cobrar, inmobilizado e contas a pagar, polo xeral ofrecen información detallada para probas e respaldo para os saldos dos libros maiores, se se levan a cabo uns controis adecuados (por exemplo: reconciliacións).

Cando unha conta significativa ten máis dunha fonte de información financeira, o auditor debe considerar as distintas fontes e determinar cal delas é máis apropiado utilizar para os propósitos da auditoría financeira. O auditor debe avaliar a probabilidade de que se produzan incorreccións e os procedementos de auditoría que se poden aplicar ao elixir a fonte que vai utilizar.

O auditor debe obter un coñecemento suficiente dos sistemas de información relevantes para a información financeira para entender o deseño dos procesos. Debe obter e revisar documentación, como poden ser documentos de deseño, proxectos, procedementos dos procesos de xestión, manuais de usuario, etc. Debe tamén entrevistarse co persoal con coñecementos a fin de obter unha comprensión xeral de cada aplicación de xestión significativa para os obxectivos da auditoría.

Nesta táboa tentarase relacionar as principais contas ou epígrafes das contas anuais co seu correspondente proceso de xestión, coas aplicacións de xestión que o soportan e outros datos relacionados.

Será útil completar unha táboa resumen coa información que se mostra a táboa seguinte:

| Contas anuais | | Aplicacións | | | | Bases de datos | | Sistemas operativos | | Plataforma hardware |
|---|---|---|---|---|---|---|---|---|---|---|
| Epígrafe | Importe (Mill. euros) | Proceso | Aplicación utilizada | Tipo de aplicación | Respon-sable | Versión | Adminis-trador | Versión | Respon-sable | |
| | | | | | | | | | | |
| | | | | | | | | | | |

Figura 8

Despois de identificar as aplicacións significativas, debe obterse un coñecemento suficiente das mesmas e dos procedementos (incluíndo os compoñentes do control interno) mediante os cales as transaccións son iniciadas, rexistradas, procesadas e presentadas desde o momento en que acontecen ata que son incluídas nas contas anuais e **documentar** as principais características de cada aplicación significativa, por exemplo:

- Procedementos polos que se inician as transaccións, autorízanse, rexístranse, procésanse, acumúlanse e móstranse nas contas anuais, incluíndo o tipo de arquivos informáticos e a forma en que se pode acceder a eles, actualizalos e borralos.
- Natureza e tipo dos rexistros, listaxes contables, documentos fonte e contas relacionadas.
- Contorna técnica e sistemas informáticos asociados a cada aplicación.
- Procedementos para emendar o procesamento incorrecto de transaccións.
- Procesos polos que se capturan feitos e condicións diferentes dos ordinarios.
- Estimación dos volumes tratados.
- Tipo de control de acceso.
- Persoa responsable da aplicación.
- Os fluxos de transaccións (estudo detallado dos controis internos da entidade sobre unha categoría concreta de feitos que identifica todos os procedementos e controis clave relacionados co procesamento de transaccións), e
- A interacción da aplicación e software (as transaccións deixan un sistema para ser procesadas por outro, por exemplo, interfaces de tarxetas de rexistro horario de persoal co ficheiro de salarios e complementos para determinar a información da nómina.

Alcanzar unha comprensión de todo isto é fundamental para poder avaliar o risco do sistema de información, comprender os controis de aplicación, así como desenvolver os procedementos de auditoría pertinentes.

**d) Documentación do traballo**

O auditor debe preparar suficiente documentación, que describa claramente o sistema de información contable, e que inclúa evidencia sobre a implementación dos controis.

Para cada proceso ou aplicación significativa, o auditor preparará unhas notas descritivas, que poderán incluír táboas informativas e fluxogramas (ou mapas de procesos).

Unha boa descrición debe:

- Identificar o proceso de xestión e as aplicacións informáticas que o soportan.
- Describir as interfaces con outros procesos/aplicacións
- Identificar os epígrafes das contas anuais, manifestacións e contas afectadas polo proceso.
- Describir as políticas e procedementos da entidade relacionadas co proceso de xestión descrito.
- Identificar (de forma preliminar) os principais controis internos

Poderanse documentar con algunha táboa similar ás vistas nos apartados anteriores.

Será imprescindible elaborar representacións gráficas dos procesos/aplicacións, mediante fluxogramas. Tamén se poderán utilizar táboas para reflectir información relevante.

## Anexo 2 Identificación as principais interfaces *(GPF-OCEX 1315, Anexo 2, apartado 5)*

### a) Concepto de interface

Unha análise completa dun sistema de información debe ter en conta tanto as aplicacións de xestión como as interfaces.

**Unha interface é unha conexión entre dous dispositivos, aplicacións ou sistemas de orixe e destino, mediante a que se intercambia información.** Tamén se utiliza este termo para referirse á parte dun programa que interactúa co usuario (a interface de usuario), pero este aspecto non interesa neste momento.

O obxectivo desta etapa da auditoría é comprender os fluxos de información e de datos entre distintas funcións, aplicacións ou sistemas, non só electrónicos senón tamén manuais. As interfaces entre aplicacións e entre bases de datos requiren unha atención especial, en particular as relacionadas con aquelas aplicacións significativas con impacto nas contas anuais.

As contornas TI complexas xeralmente requiren interfaces complexas para integrar as súas aplicacións de xestión críticas. Incluso os sistemas ERP moi integrados a miúdo requiren complicadas interfaces para outras aplicacións distribuídas.

As interfaces adoitan ser xestionadas con tecnoloxía middleware, que actúa como un elemento central de comunicación e coordinación para as interfaces. Poden residir nos mesmos sistemas que comunican ou noutros diferentes.

Nunha interface, as intervencións do usuario poden ser moi variadas:

- integración ou exportación dun ficheiro con descrición do formato de entrada ou saída (estes casos máis que interfaces, son ficheiros de intercambio).
- Desencadenamento manual dun proceso automático.
- Simple verificación do tratamento das excepcións ou dos rexeitamentos da interface.

As interfaces como mínimo moven información dun sistema a outro, pero tamén poden ser responsables de cálculos ou de modificar datos de acordo con algún algoritmo.

**As interfaces sempre son unidireccionais, nunca bidireccionais.**

### b) Risco das interfaces

Dado que as interfaces xogan un importante papel no procesamento das transaccións, sempre deben considerarse no plan da auditoría. Debe terse presente que o seu mal funcionamento pode afectar a todo o sistema, o que representa un risco a considerar.

Débense avaliar os **riscos de interface** (perda de datos por interrupción das comunicacións, duplicación de datos no sistema de destino, actualización do sistema de destino con datos dun período incorrecto, etc.) e os controis establecidos para mitigalos.

Os **controis de interface** poden ser manuais (p.e. mediante reconciliacións manuais) ou estar automatizados (os datos de ambos sistemas concílianse automaticamente).

O **risco de interface** xorde cando as interfaces externas e internas non son adecuadamente especificadas, definidas, deseñadas, documentadas e programadas. Estes riscos de interface con frecuencia levan a unha reconciliación inconsecuente/desigual de datos enviados e recibidos, tendo como resultado erros non identificados nos datos. Unhas interfaces deseñadas de maneira efectiva previrán e detectarán estes erros da forma máis rápida posible no procesamento. Da mesma maneira facilitarán a corrección de erros e o emprego duns controis de usuario apropiados. Cando as interfaces foron adecuadamente estruturadas e documentadas, estas axudan a conseguir un mantemento rendible e unha capacidade de recuperación (de datos).

Os riscos de interface pódense xestionar asegurándose de que non se realizan cambios non autorizados nos datos; transferindo os datos a tempo/de forma periódica, precisa e completa; e levando a cabo uns procedementos de resolución de erros con exactitude e oportunamente. Ademais, o sistema de recepción dos datos debe procesalos máis dunha vez como medida preventiva ante posibles riscos de interface.

No seguinte cadro enuméranse unha serie de exemplos de obxectivos de control específicos e os riscos e controis relacionados.

| OBXECTIVO DE CONTROL | RISCO | CONTROL |
|---|---|---|
| Os controis de aplicación son adecuados para preparar ou procesar datos enviados e recibidos. | Uns controis inadecuados impiden unha dispoñibilidade da información de maneira exacta e oportuna tanto para a aplicación como para os usuarios da aplicación herdada. | ● Unha vez a aplicación recibe os datos, convértense ao formato adecuado; a continuación, a información que foi convertida entra na sesión e os erros quedan rexistrados.<br>● Os erros son emendados e reenviados, e documéntanse e son aprobadas as resolucións.<br>● Infórmase o propietario da interface dos erros que non foron emendados. |
| Os procedementos de reinicio de proceso e de recuperación de información para as sesións de interface foron adecuadamente instalados a fin de garantir que as interrupcións na transmisión de arquivos entre sistemas son resoltas a tempo. | Uns procedementos de reinicio de proceso e de recuperación de información mal deseñados poden ocasionar uns atrasos excesivos no procesamento e unha perda de tempo innecesaria e custosa do persoal. | ● As sesións de interface utilizan unha aplicación que conta co seu propio sistema de reinicio no caso de que se interrompa unha conexión.<br>● A aplicación tamén utiliza un sistema informático de control durante a transferencia de arquivos; este sistema é configurable e comproba as transferencias de datos entre as localizacións orixe e destino.<br>● As transferencias que son interrompidas ou fallan antes de que conclúan son automaticamente renovadas desde o último control. |
| Faise un seguimento da información que foi transferida entre as aplicacións e esta información é controlada a fin de asegurar que os erros son emendados de maneira adecuada. | A entrada manual de datos é vulnerable ao erro humano; sen un seguimento e un control adecuados, os erros poden pasar desapercibidos. | Uns controis de edición regulares, incluídas unhas reconciliacións, son responsables de capturar datos incorrectos antes de que se cre un arquivo de configuración da interface. |

Figura 9

Ademais, o deseño da interface debe garantir que se realiza un mapeo adecuado dos datos de orixe a unha aplicación destino ou ben a unha táboa de datos, así como unha avaliación dos datos/información no que refire ao nivel de detalle necesario a utilizar na aplicación destino.

**c) Consideracións de auditoría sobre as interfaces**

Calquera que sexan as vantaxes dun ERP e a vontade dunha entidade de implantar un sistema integrado, o sistema de información está a miúdo constituído de varias aplicacións heteroxéneas. Os procedementos de auditoría faranse sobre cada unha das aplicacións, pero tamén sobre as interfaces que posibilitan a transferencia de datos.

As interfaces deben ser descritas tendo coidado de identificar os aspectos sinalados máis adiante.

Débese indagar se existe un módulo específico para a xestión de interfaces. Xeralmente existen para as interfaces saíntes vía as funcionalidades de exportación de datos. Respecto da importación de datos, convén pescudar as funcionalidades que permiten aos usuarios seguir o bo funcionamento das interfaces, por exemplo: o seguimento dos procesos (situación, cumprimento da frecuencia prevista,…), identificación dos posibles rexeitamentos, a posibilidade de coñecer a causa dos rexeitamentos e de volver tratar os datos afectados.

É necesario identificar o tipo de interface que ten o ERP que se está revisando, en particular para as interfaces entrantes.

Pódense clasificar as interfaces segundo catro categorías principais:

- Interfaces utilizando unha linguaxe ou un módulo especificamente proposto polo fabricante do ERP. Este módulo utiliza xeralmente as funcións do ERP; os datos integrados pola interface sométense aos mesmos controis que os datos rexistrados manualmente polo usuario.
- As interfaces que utilizan a linguaxe ou un módulo proporcionado polo SGBD. Nestes casos, se os datos sométense aos controis propios do SGBD (control de coherencia de datos) non serán sometidos aos controis funcionais das aplicacións. Estes controis máis ricos poden afectar por exemplo as verificacións de cálculos (tipo de retención IRPF, tipo IVE, etc.).
- Interfaces que utilizan unha linguaxe normalizada, como no caso dos intercambios EDI.
- Outras interfaces utilizando distintos medios non previstos polo fabricante do ERP (modificación dos programas, escrituras directas nas táboas da base de datos,…).

A revisión das interfaces pasa pola comprensión do tipo de interface analizada, para identificar os tipos de controis internos aplicados e para detectar os riscos asociados. Considérase en xeral que unha interface estándar situada ao nivel da aplicación presenta poucos riscos, posto que os datos integrados que proveñan dunha aplicación externa sométense aos mesmos controis que os datos capturados directamente pola aplicación.

Outros aspectos específicos a considerar son:

- Responsable da interface.

  Quen a inicia?

- Utilización de software para xestionar interfaces.

  O software modifica os datos ou só os traslada dun sitio a outro?

- Interfase IDs: o software da interface probablemente necesitará acceder aos sistemas/aplicacións que comunica.

  Como se xestiona ese acceso?

  Utilízanse identificadores de usuario xenéricos?

  Que privilexios proporcionan eses IDs?

  Quen ten acceso e pode usar eses IDs?

- Cartafoles/directorios da interface.

  Móvense todos os datos a través dun só cartafol?

  Quen ten acceso a ese cartafol?

  Como está protexida e controlada?

  Pode algún empregado acceder a ese cartafol para depositar información para procesar? Este aspecto é especialmente crítico cando se trata de datos sobre pagos ou transferencias.

- Tipos de interface.

  Que tipo de interface se utiliza?

  É en tempo real ou de procesamento por lotes?

  Que transaccións soporta?

  Inicia o procesamento doutras transaccións?

**d) Procedementos de auditoría**

Se os métodos de revisión varían segundo o tipo de interface, o obxectivo é o mesmo en todos os casos: trátase de comprobar o funcionamento dos controis implantados pola entidade (verificación do tratamento da interface segundo a frecuencia prevista, seguimento dos controis realizados sobre os datos, dos rexeitamentos e o seu tratamento, etc.).

Os controis de interface poden ser manuais (p.e. mediante reconciliacións manuais) ou estar automatizados (os datos de ambos sistemas concílianse automaticamente).

Débense avaliar os riscos de interface (perda de datos por interrupción das comunicacións, duplicación de datos no sistema de destino, actualización do sistema de destino con datos dun período incorrecto, etc.) e os controis establecidos para mitigalos.

A interrogación de ficheiros e bases de datos utilizando CAAT é un procedemento que proporciona confianza sobre a integridade da información transmitida entre distintos sistemas.

**e) Documentación das interfaces**

Despois de identificar as aplicacións significativas e interfaces, o auditor debe obter un coñecemento suficiente das mesmas e dos procedementos (incluíndo os compoñentes do control interno) mediante os cales as transaccións son iniciadas, rexistradas, procesadas e presentadas desde o momento en que acontecen ata que son incluídas nas contas anuais, e documentar os seguintes aspectos para cada interface:

- Tipo (manual ou automática).
- Aplicacións orixe (dos datos) e destino.
- Frecuencia de uso (diario, mensual, anual).
- Controis implantados para detectar anomalías.
- Outros aspectos relevantes.

Para a súa análise inicial e documentación pode realizarse un inventario das principais interfaces mediante unha táboa:

| Nome de interface | Tipo | Aplicacións | | Tipo de fluxo | Frecuencia | Listas de erro | Avaliación dos riscos |
|---|---|---|---|---|---|---|---|
| | | Orixe | Destino | | | | |
| | | | | | | | |

Figura 10

## Anexo 3 Principais categorías de controis de aplicación ou dos procesos de xestión

Os controis dos procesos de xestión, tamén denominados controis de aplicación, son os controis automatizados e manuais aplicados no fluxo de procesamento das transaccións. Refírense á completitude, exactitude, validez e confidencialidade das transaccións e datos durante o procesamento das aplicacións. Operan a un nivel detallado de transaccións ou actividades ao longo do proceso de xestión.

As áreas específicas de controis de aplicación son:

a) Controis de entrada de datos
b) Controis sobre o procesamento de datos
c) Controis de saída
d) Controis sobre os datos mestres
e) Segregación de funcións (ver Anexo4)

Aínda que non son controis do proceso de xestión, os **controis sobre as interfaces** si que están no nivel das aplicacións e deben revisarse conxuntamente con aqueles, xa que entrañan riscos importantes de auditoría. Son aqueles controis que aseguran o procesamento ou transferencia oportuno, exacto e completo de información entre distintas aplicacións e/ou sistemas.

**a) Controis de entrada de datos**

As aplicacións poden aceptar a entrada de datos manualmente, ou automaticamente vía interfaces que procesan por lotes ou integradas en tempo real con sistemas internos ou externos. En todo caso os controis de entrada de datos son moi importantes.

Os principais ***obxectivos de control*** son os seguintes:

- A entrada de datos realízase en tempo oportuno por persoal autorizado ou procesos autorizados.
- Os datos introducidos son completos, exactos e válidos.
- Os erros e as anomalías de captura e rexistro son identificados, documentados, comunicados e corrixidos en tempo oportuno, por persoas coa adecuada autorización.
- A confidencialidade dos datos está adecuadamente protexida.

Os ***controis*** que poden establecerse para alcanzar os obxectivos de control son:

- Verificar a exactitude das correccións de erros por un servizo ou persoa independente.
- As persoas responsables da captura de datos son identificadas polo sistema.
- Os xustificantes de captura proporcionados son exhaustivos e transmitidos en tempo útil.
- Os xustificantes de captura consérvanse durante o período e na forma legalmente esixida ou poden ser reconstituidos pola organización.
- Perfís de competencias para a emisión de documentos contables (p.e. regulación das sinaturas) e posta en práctica dun control das autorizacións por sistemas de xestión de acceso.
- Segregación das funcións de creación e de validación de documentos contables.
- Visei ou sinatura sobre os xustificantes de captura de datos.
- Formularios de captura de datos comprensibles e útiles (p.e. con campos predefinidos).
- Procesos de identificación precoz e de tratamento dos erros e irregularidades.
- Arquivo sistemático dos documentos contables.
- Dixitalización dos xustificantes e conservación adecuada.
- Perfís de competencias para a captura/rexistro das transaccións e posta en práctica a través dun control das autorizacións por sistemas de xestión de accesos.
- Comparación de datos capturados con valores rexistrados.

- Máscaras de captura comprensibles e amigables con controis de formato de datos integrados (p.e. campos de data, numéricos, campos obrigatorios, etc., e lista de valores predefinidos e recorrentes).
- Control automático dos valores introducidos (p.e. superación de valores límites, control de factibilidade (credibilidade) dos contidos, sincronización cos datos arquivados).
- Despregue de etiquetas de código completas despois da gravación do código (p.e. a designación dun artigo móstrase ao gravar o número do artigo).
- Totais de control por lotes: número de documentos (p.e. facturas), suma de zonas de valores visibles nos documentos ou sumas numéricas (importes, cantidades), suma de control.
- Control secuencial de documentos contables numerados correlativamente para identificar os faltantes ou duplicados nas gravacións.
- Captura de control (chamada tamén dobre captura, control dos 4 ollos); captura dobre de valores importantes por diferentes persoas ou por unha mesma persoa.
- Control visual de valores capturados por unha segunda persoa; convén para os casos críticos e un pequeno número de transaccións.
- Proceso de identificación precoz e de tratamento de erros e de anomalías, as transaccións corrixidas deben ser enteiramente verificadas de novo.
- A exactitude, exhaustividade e a validez dos campos importantes son controlados nas pantallas ou programas superpostos ao proceso de captura.

**b) Controis sobre o procesamento dos datos**

Unha vez que os datos son introducidos no sistema e aceptados, o seu procesamento é controlado por unha serie de actividades dentro do sistema. Os pasos do procesamento son distintos para cada proceso de xestión e os requirimentos de control para mitigar os riscos inherentes son diferentes en cada caso. Unha eficaz avaliación destes controis inclúe unha comprensión das distintas fases do proceso e do fluxo dos datos, dos controis embebidos na aplicación e dos controis manuais existentes no proceso.

Os principais ***obxectivos*** dos controis de procesamento de datos son os seguintes:

- As transaccións (cálculos, totalizacións, consolidacións, análises, etc.), incluídas as que xera o propio sistema, son procesadas polo computador de forma exacta, completa e oportuna.
- As transaccións non son obxecto de perda, duplicación, manipulación ou alteración.
- A exhaustividade, exactitude e a validez do procesamento realizado son verificados segundo un procedemento de rutina.
- Os erros de procesamento son identificados rapidamente, documentados e corrixidos en tempo útil.

Os ***controis*** típicos do procesamento de datos son os seguintes:

- A aplicación está deseñada para procesar os datos coa mínima intervención manual.
- A separación de funcións está garantida incluso durante o procesamento dos datos.
- As transaccións xeradas automaticamente pola aplicación (p.e. intereses periódicos de préstamos, ordes ao exceder limiares de stocks) son obxecto dos mesmos controis de exhaustividade, exactitude e de validez que as transaccións illadas.
- As decisións importantes baseadas en cálculos automáticos son adoptadas e verificadas por persoas.
- Comparación dos datos tratados no sistema con confirmacións externas (p.e. inventarios físicos, confirmación de saldos bancarios e de saldos de clientes e provedores).

**c) Controis sobre a saída dos datos**

As saídas ou outputs son o resultado do procesamento dos datos.

Os principais ***obxectivos*** de control da saída de datos son os seguintes:

- Os resultados do procesamento son completos e exactos.
- O acceso aos datos de saída do sistema está restrinxido ao persoal autorizado.
- Os datos de saída do sistema chegan ao persoal autorizado en tempo oportuno, de conformidade cos procedementos definidos.

Os ***controis*** típicos da saída de datos son os seguintes:

- Os controis de envío e de recepción regulan as modalidades de comunicación de listaxes e outros outputs (quen, cando, que, como e cantos exemplares).
- Os sistemas de xestión de acceso garanten a trazabilidade dos accesos dos usuarios a consultas en pantalla ou a listaxes.
- Os controis de numeración e de exhaustividade garanten que a xestión, edición, restitución, recepción e destrución (p.e. en caso de copia de control) de outputs críticos (p.e. cheques, vales, etc.) efectúanse de conformidade cos procedementos.
- A exactitude e a completitude dos informes periódicos (p.e. listaxes semestrais ou anuais) son controlados mediante mostraxes.

**d) Controis sobre os datos mestres**

Os datos mestres son os datos permanentes utilizados por múltiples aplicacións e participan na correcta execución do procesamento de datos realizados polas aplicacións. O mantemento da súa integridade é un elemento crítico para a correcta execución da aplicación.

Exemplos de datos mestres:

Estrutura do plan contable
Mestre de clientes
Mestre de provedores
Mestre de empregados/nómina
Mestre de materiais (de inventario)
Mestre de bancos

Os principais ***obxectivos de control*** relativos aos datos mestres son os seguintes:

- As modificacións deben ser realizadas por persoas autorizadas, de forma exacta e completa.
- As modificacións deben ser rexistradas e arquivadas de forma que se manteña a pista de auditoría (logs).

Os ***controis*** típicos son os seguintes:

- Existen procedementos para as modificacións.
- As actualizacións realízanse de forma simultánea en todo o sistema de información.
- Só as persoas autorizadas poden modificalos.
- Mantense un ficheiro histórico con todos os cambios nos datos mestres incluíndo quen os realizou.

**e) Controis sobre as interfaces**

Raras veces unha organización utiliza un único sistema para xestionar todos os seus procesos e información. As interfaces créanse para permitir á información pasar dunha aplicación ou sistema a outro.

As características das **interfaces** afectan á avaliación do risco. As manuais presentan un maior risco de erros (de captura de datos, omisión de operacións, duplicados, etc.) que as automáticas.

Nas interfaces automáticas debe comprobarse a existencia de logs ou informes que permitan comprobar a correcta execución do procesamento (informes de anomalías, informes de execución que permitan comparar os datos que entran e saen da interface); os informes deben ser analizados e dar lugar ás accións correctoras que procedan.

A fiabilidade dunha interface analízase estudando as condicións de implementación, de funcionamento e de actualización. A priori unha interface nova, non testeada completamente, ten máis posibilidades de funcionar mal.

As interfaces de entrada e de saída dunha aplicación deben ser consideradas como fontes de risco. É moi importante identificalas e revisalas (ver Anexo 2).

Os controis de interface son aqueles deseñados para o procesamento de información oportuno, exacto e completo entre aplicacións e outros sistemas emisores e receptores de información.

Os principais **obxectivos** de control relativos ás interfaces son os seguintes:

- Implementar unha estratexia e deseño eficaces.
- A interface execútase completamente, con exactitude, só unha vez, e no período adecuado.
- Os erros da interface son rexeitados, identificados e corrixidos con prontitude.
- O acceso aos datos e procesos da interface está adecuadamente restrinxido. Os datos son fiables e obtéñense unicamente de fontes autorizadas.
- A autenticidade e a integridade das informacións provenientes de fontes externas á organización son controladas coidadosamente antes de emprender calquera acción potencialmente crítica, independentemente do medio de recepción (teléfono, fax, email, etc.).
- As informacións sensibles están protexidas durante a súa transmisión por medidas adecuadas contra accesos non autorizados, modificacións ou envío a destinatarios erróneos.

Os ***controis*** típicos ao nivel das interfaces son os seguintes:

- Existe unha estratexia e deseño para cada interface que inclúe:
  - tipo
  - campos de datos a transferir
  - controis de integridade e exactitude
  - programación temporal
  - responsable
  - requisitos de seguridade
  - corrección de erros
  - método de comunicación
- Os arquivos xerados por unha interface (entrante ou saínte) son adecuadamente protexidos contra accesos non autorizados ou modificacións.

  Un exemplo típico é o ficheiro (C34) xerado pola aplicación de pagos para a súa remisión telemática ás entidades financeiras. Tras a súa xeración arquívase nun cartafol do sistema da entidade, antes do seu envío ao banco. Un control de interface saínte consiste en protexer ese ficheiro e ese cartafol para que ninguén non autorizado poida acceder ao ficheiro editable C34 e modificalo fraudulentamente.
- Existen procedementos para asegurar que todos os arquivos enviados polo sistema orixe foron recibidos polo sistema destino.
- Os datos transmitidos son reconciliados entre as aplicacións de orixe e destino para asegurar que a interface é completa e exacta. Os totais de control coinciden e as listaxes de conciliación proporcionan suficiente información para conciliar cada transacción procesada.

**Os controis de interface poden realizarse manual ou automaticamente, de forma programada ou esporádica, electronicamente ou en papel. Os controis máis fiables son os automatizados.**

## Anexo 4 Segregación de funcións (SdF)

Ao revisar un proceso/aplicación de xestión, un aspecto fundamental é o estudo da segregación de funcións, que constitúe un dos principios máis importantes do control interno.

Significa que as funcións se distribúen entre as persoas de forma que ninguén poida controlar todas as fases do procesamento dunha transacción de modo tal que poidan pasar inadvertidas incorreccións debidas a erros ou fraudes. Teoricamente, o fluxo das actividades debería proxectarse de tal forma que o traballo dunha persoa sexa independente do doutra ou sirva para comprobación e/ou autorización deste último.

O obxectivo da segregación de funcións é alcanzado ao distribuír as actividades clave do procedemento de xestión entre varias persoas e/ou restrinxir o número de persoas con acceso a actividades que sexan incompatibles, por exemplo, autorizar unha factura e realizar o pago material.

Na práctica, este principio de segregación de funcións conciliarase con consideracións tales como o volume, a complexidade e a materialidade dos distintos tipos de operacións e a secuencia de pasos necesarios para procesalas. Os aspectos a considerar variarán amplamente dunha entidade a outra.

Nos actuais sistemas altamente automatizados, nos que os usuarios teñen acceso potencialmente a todas as funcións do sistema, a análise da segregación de funcións adquire unha importancia crítica e debe facerse unha detallada revisión dos riscos existentes na xestión dos permisos de acceso ás aplicacións e bases de datos subxacentes (ambos niveis deben analizarse de forma inseparable).

Dada a súa complexidade e "non visibilidade", nos sistemas informatizados, a análise da segregación de funcións moitas veces **só será posible realizalo** coa colaboración de persoal especializado utilizando técnicas de auditoría de sistemas.

Entre os mecanismos de control dispoñibles para axudar á hora de levar a cabo unha segregación de funcións eficaz, incluíndo controis compensatorios, inclúense:

- Pistas de auditoría/trazabilidade
- Conciliacións
- Informes sobre anomalías
- Supervisión.

Unha adecuada SdF contemplará, por exemplo:

- Ningún empregado terá responsabilidade total para modificacións nos Ficheiros Mestres de Prezos e de Condicións de Vendas. Un empregado iniciará o cambio e outro revisará e autorizará o cambio.
- Os empregados que teñan capacidade de modificar os Ficheiros Mestres non deben intervir na xestión das vendas.
- Os empregados/responsables que venden entradas non son os mesmos que están na entrada cancelando as entradas ou vixiando a entrada.
- Os empregados/responsables da xestión comercial/venda de entradas son distintos aos que supervisan as contas bancarias que recollen as vendas en efectivo ou con TPV.
- Ningún empregado terá responsabilidade total para modificacións no FME (Ficheiro Mestre de Empregados). Un empregado iniciará o cambio e outro revisará e autorizará o cambio.
- Os empregados que teñan capacidade de modificar o FME non deben intervir na elaboración da nómina.

Un aspecto que se terá sempre en conta é o custo de mantemento dos controis en relación co risco das perdas por erro ou fraude que poderían producirse en ausencia daqueles. Nas empresas e entidades de maior tamaño, as posibilidades de desagregación do traballo nos procesos de xestión son maiores, pero ás veces non é posible establecer unha adecuada segregación de tarefas, sobre todo en entidades de pequeno tamaño, xa que non se

dispón de persoal suficiente para a súa implantación, pero nestes casos deben establecerse outro tipo de controis compensatorios[7] que poden axudar a mitigar a gravidade das debilidades de control, por exemplo:

- Un supervisor que non intervén na elaboración da nómina, revisa e aproba os ficheiros da nómina antes e despois do seu cálculo definitivo.
- Utilízanse ferramentas analíticas (como ACL) para verificar a exactitude dos salarios reconciliándoos cos tc'1, Mod110 e Mod190.
- Se un empregado que participa na elaboración da nómina tamén mantén o FME, deberíase xerar un informe de todos os cambios no FME para que fosen supervisados por unha persoa independente.

Para facilitar a revisión da SdF existente nunha entidade, é conveniente utilizar un cadro como o do exemplo seguinte no que se recollan as principais situacións de falta de segregación de funcións no proceso auditado, que poden entrañar riscos de erros ou irregularidades, e por tanto riscos de auditoría.

| Función | Consideracións de control / Preguntas de auditoría | Control | Controis compensatorios |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

O procedemento de auditoría lóxico consistiría en completar a descrición dos procedementos de xestión e en cada subproceso facerse as pertinentes preguntas relacionadas coa dita xestión, documentar as respostas, a evidencia obtida sobre os posibles conflitos de SdF e as súas consecuencias na nosa avaliación do control interno e valoración do risco.

Se non é adecuada a segregación de funcións débese explicar por que e ata que punto pode afectar o risco de auditoría. Débense concretar os riscos que pode provocar a falta de segregación. Débese indagar se existen controis compensatorios que mitiguen os riscos cando non existe un control directo efectivo.

[7] Un **control compensatorio** é aquel que reduce o risco dunha debilidade, real ou potencial, non eliminada por un control directo.