Informe de Fiscalització del Compte General de la Generalitat de l'exercici de 2010

INFORME DE FISCALITZACIÓ
DEL COMPTE GENERAL DE LA
GENERALITAT DE L'EXERCICI DE 2010

VOLUM I	INTRODUCCIÓ I CONCLUSIONS GENERALS INFORME DE FISCALITZACIÓ DEL COMPTE DE L'ADMINISTRACIÓ DE LA GENERALITAT
VOLUM II	INFORMES DE FISCALITZACIÓ DE LES ENTITATS AUTÒNOMES
VOLUM III	INFORMES DE FISCALITZACIÓ DE LES EMPRESES PÚBLIQUES I D'ALTRES ENS
VOLUM IV	INFORME DE FISCALITZACIÓ DE LES FUNDACIONS DEL SECTOR PÚBLIC DE LA GENERALITAT
VOLUM V	INFORMES ESPECIALS DE FISCALITZACIÓ

Auditoria d'eficàcia dels sistemes d'informació i de control intern de la Ciutat de les Arts i de les Ciències, SA

ÍNDEX **Pàgina**

1. INTRODUCCIÓ 3

1.1 Antecedents 3

1.2 Entitat auditada 5

2. OBJECTIU I ABAST DE L'AUDITORIA 7

3. CONCLUSIÓ GENERAL 9

4. ENFOCAMENT METODOLÒGIC 11

4.1 Descripció general 11

4.2 Revisió dels controls generals de TI (CGTI) 12

4.3 Revisió dels processos i aplicacions de gestió 16

4.4 Realització de proves massives de tractament de dades 17

4.5 Criteris d'avaluació dels controls interns 18

4.6 Criteris per a la categorització de les recomanacions 18

5. RESUM GENERAL 20

5.1 Descripció de l'entorn tecnològic 20

5.2 Controls generals de TI 21

5.3 Procés de gestió dels ingressos per venda d'entrades 25

5.4 Procés de gestió de compres 28

5.5 Resultats de les proves massives de dades 30

6. RECOMANACIONS 31

6.1 Controls generals TI 31

6.2 Procés de gestió d'ingressos per venda d'entrades 33

6.3 Procés de gestió de compres 36

7. TRÀMIT D'AL·LEGACIONS 38

1. INTRODUCCIÓ

1.1 Antecedents

Entre les disposicions que regulen l'activitat de la Sindicatura de Comptes de la Comunitat Valenciana i fonamenten aquest Informe, es poden esmentar les següents:

- L'article 8.3 de la Llei de la Generalitat Valenciana 6/1985, de 11 de maig, de Sindicatura de Comptes (LSC), que estableix el següent:

  "Cal necessàriament que els informes referents als comptes generals es pronuncien sobre els punts següents:

  a) Determinar si la informació financera es presentada adequadament, d'acord amb els principis comptables que li són aplicables.

  b) Determinar si s'ha complit amb la legalitat vigent en la gestió dels fons públics.

  c) Avaluar si la gestió dels recursos humans, materials i dels fons pressupostaris s'ha desenvolupat de manera econòmica i eficient.

  d) Avaluar el grau d'eficàcia en l'assoliment dels objectius prevists."

- L'article 7 de la Llei de Sindicatura de Comptes, que assenyala que "per a desenvolupar les seues funcions, la Sindicatura de Comptes podrà utilitzar tots els mitjans adequats per a aconseguir els seus objectius, incloent-hi els de caràcter informàtic i la contractació d'experts. El Consell també podrà contractar amb empreses consultores o d'auditoria per a complir el seu programa anual d'actuació."

- L'article 11.1 de la mateixa Llei estableix expressament que:

  "En l'exercici de la seua funció fiscalitzadora, la Sindicatura de Comptes proposarà les mesures que considere que cal prendre per a la millor gestió econòmica i administrativa del sector públic valencià, i també aquelles més idònies per a aconseguir un control més eficaç d'aquest."

- L'article 58 del Reglament de Règim Interior de la Sindicatura de Comptes, en què s'estableix que "en l'exercici de la funció fiscalitzadora s'avaluarà adequadament el control intern de les institucions, organitzacions o entitats fiscalitzades".

Per complir de manera satisfactòria les seues funcions fiscalitzadores en els entorns tecnològics avançats en què actualment operen i desenvolupen la seua activitat totes les institucions públiques, singularment en l'àmbit de la gestió econòmica, financera i pressupostària, la Sindicatura de Comptes, tal com va quedar compilat en els objectius estratègics dels seus plans triennals, ha introduït en els darrers anys noves eines informàtiques d'auditoria i ha desenvolupat una metodologia de treball innovadora adaptada a les circumstàncies actuals en què ha d'acomplir la seua activitat.

L'adopció de noves eines informàtiques i metodològiques, juntament amb l'aprofundiment en l'aplicació d'un enfocament d'auditoria basat en l'anàlisi dels riscs, permet a la Sindicatura de ser més eficaç i eficient en la realització de les seues tasques fiscalitzadores; això es reflecteix, entre altres coses, en dos aspecte fonamentals:

a) Proporcionant un major grau de seguretat als equips de fiscalització, a l'auditar la informació financera en entorns informatitzats, respecte a les garanties sobre la validesa, la integritat, l'exactitud, la confidencialitat i la disponibilitat que ofereix aqueixa informació.

   Això permet, en conseqüència, d'incrementar de manera notable el nivell de qualitat dels nostres informes de fiscalització de regularitat. No obstant això, malgrat la importància que té per al pronunciament d'acord amb els apartats *a* i *b* de l'article 8.3 de la LSC, el resultat d'aquest treball no s'ha d'incloure necessàriament de manera explícita en aqueixos informes.

b) Per a atènyer la meta anterior, cal revisar exhaustivament els sistemes de gestió i de control intern de les entitats fiscalitzades, els seus procediments o processos de gestió més significatius i avaluar l'eficàcia d'aqueixos sistemes i processos —tant manuals com informatitzats— en el compliment dels seus objectius de gestió i de control.

   El resultat d'aquest treball, tot i estar subordinat a l'objectiu principal de la fiscalització derivat dels apartats *a* i *b* de l'article 8.3 de la LSC, permet d'atenir-se també al que preveuen els apartats *c* i *d* del mateix article i aportar un important valor afegit addicional al treball de fiscalització.

   Aquest treball pot ser de gran utilitat no sols als parlamentaris i els ciutadans destinataris finals de tots els informes de la Sindicatura de Comptes, sinó també, especialment, als gestors de les entitats fiscalitzades, ja que és el resultat d'un treball exhaustiu que ha dut a terme un equip pluridisciplinari i inclou recomanacions que han de contribuir sens dubte a millorar l'eficàcia i l'eficiència en la gestió i el control intern de les entitats auditades.

   Aquesta circumstància aconsella que les observacions, les conclusions i les recomanacions resultants es recopilen detalladament en un informe separat del de fiscalització de regularitat.

D'acord amb tot això, com a part de la fiscalització de l'exercici 2010 de la Ciutat de les Arts i de les Ciències, SA, (en avant, CACSA o la Societat), s'ha realitzat una auditoria d'eficàcia dels seus sistemes d'informació i de control intern.

En particular, hem revisat l'eficàcia dels controls generals dels sistemes d'informació i dels controls implantats en les aplicacions informàtiques utilitzades per a gestionar tant el procés de gestió d'ingressos per venda d'entrades com els processos de gestió de despeses i de compres, i també el procés de generació dels apunts comptables i de la informació financera.

L'adequada gestió dels entorns de tecnologies d'informació (TI) en què, per mitjà de les aplicacions informàtiques, es gestionen les principals activitats i processos de les entitats públiques, és una qüestió d'importància cabdal, atès el gran impacte que aqueixos sistemes i la seua constant actualització produeixen en una organització, en els seus processos de gestió, en la seua estructura organitzativa, en la seua cultura, en la seua presa de decisions, en la seua gestió de recursos, en la seua relació amb els usuaris, etc.

L'aplicació que gestiona els ingressos per venda d'entrades i la seua interconnexió amb l'aplicació comptable d'àmbit general, que integra la informació sobre les vendes per a elaborar la informació financera, són elements essencials en la gestió de l'activitat de CACSA.

Els processos de gestió i tramitació d'expedients de comptes i despeses també són una activitat crítica, ja que garanteixen el nucli de l'activitat de la Societat i, pel volum monetari gestionat, tenen un impacte molt significatiu en els comptes anuals.

Per això, a més de perseguir objectius d'eficiència, els sistemes informàtics s'han de dotar de controls i mesures de seguretat adequades, concordes amb la importància de la informació que s'emmagatzema, es processa i circula per aquests, minimitzant els riscs suportats fins al nivell que hom considere assumible.

Com a antecedent del treball efectuat, la Sindicatura va fer una auditoria dels controls generals dels sistemes d'informació i del procés de gestió de les despeses de CACSA en l'informe de l'exercici 2008.

1.2 Entitat auditada

La societat Ciutat de les Arts i de les Ciències, SA, es va constituir el 1991, es regeix per les normes de dret privat aplicables a les societats mercantils i té la consideració d'empresa de la Generalitat, d'acord amb l'article 5è de la Llei d'Hisenda Pública de la Generalitat Valenciana, llei que la regula en aquelles matèries que li siguen aplicables. Actualment depèn de la Conselleria de Turisme, Cultura i Esport.

La seua activitat principal se centra en la gestió del projecte Ciutat de les Arts i de les Ciències que, a l'efecte del present treball, es pot diferenciar en les àrees següents:

- Museu de les Ciències, Hemisfèric i Umbracle
- Gestió general
- Oceanogràfic
- Palau de les Arts

La gestió de les primeres activitats la porta CACSA directament, amb personal propi; la gestió de l'Oceanogràfic s'ha contractat amb l'empresa Parcs Reunits València, SA, (PRV); el Palau de les Arts és gestionat per la fundació Palau de les Arts Reina Sofia, Fundació de la Comunitat Valenciana.

Algunes dades bàsiques relacionades amb l'auditoria realitzada són els següents (no n'hi incloem cap de relacionat amb el Palau de les Arts):

		2009	2010
Venda d'entrades	(1)	22.798	23.914
D'altres ingressos	(1)	11.369	11.215
Import net de la xifra de negoci	(1)	34.167	35.129
Visites	(2)	3.421.096	3.498.757
Entrades venudes	(2)	2.102.293	2.315.814
Aprovisionaments d'altres despeses d'explotació	(1)	33.348	37.747
Despeses de personal	(1)	9.564	9.560
Nombre mitjà d'empleats		339	343
Addicions d'immobilitzats materials	(1)	70.464	19.685

(1) En milers d'euros.
(2) S'hi computen les visites sumant les dels diversos centres. Les entrades combinades poden correspondre a més d'una visita a sengles centres.
Font: Comptes anuals i informes de gestió dels exercicis de 2009 i de 2010 de CACSA

Figura 1

La Sindicatura de Comptes ha fiscalitzat els comptes anuals de l'exercici de 2010 de CACSA i l'informe resultat es pot consultar en el volum III, "Informes de fiscalització de les empreses públiques i d'altres ens", de l'Informe de Fiscalització del Compte General de la Generalitat de l'exercici de 2010. Com a annex a aqueix informe s'acompanyen els comptes anuals, l'informe de gestió de l'exercici de 2010 de CACSA i l'informe d'auditoria de comptes.[1] El conjunt d'aquests documents proporciona abundant informació complementària per a aprofundir en el coneixement de la societat.

La col·laboració dels responsables i del personal dels departaments de sistemes d'informació i d'administració dels processos de gestió auditats ha estat en tot moment completa, cosa que ha facilitat la bona marxa dels treballs d'auditoria el resultat dels quals recopila aquest Informe.

[1] Obligatori en virtut de l'article 263 del text refós de la Llei de Societats de Capital aprovat pel Reial Decret Legislatiu 1/2010, de 2 de juliol.

2. OBJECTIU I ABAST DE L'AUDITORIA

En virtut del que disposa l'article 8.3 de la Llei de la Generalitat Valenciana 6/1985, de 11 de maig, de Sindicatura de Comptes, i conformement amb el que preveu el Programa Anual d'Actuació de 2011, l'objectiu d'aquest treball ha consistit a analitzar els sistemes d'informació i de control intern de la Ciutat de les Arts i de les Ciències, SA, i a determinar si el grau d'eficàcia dels controls existents en els sistemes d'informació, tant en les aplicacions informàtiques com en els procediments manuals, aporta un nivell de confiança raonable per a garantir que s'han executat correctament els processos de gestió de les compres i despeses i dels ingressos per venda d'entrades, que s'han comptabilitzat adequadament i per a reduir el risc d'errors o irregularitats.

També hem comprovat si la informació que ha generat el sistema d'informació comptable té un grau suficient de garantia respecte a la seua validesa, integritat, exactitud, confidencialitat i disponibilitat.

Així mateix, pretenem d'oferir mesures correctores a les possibles deficiències de control intern que hem trobat en el curs de l'auditoria, per a la qual cosa formulem les recomanacions pertinents que contribuesquen a incrementar l'eficàcia del sistema de control intern i l'eficiència dels processos de gestió.

L'abast de la present auditoria ha comprès:

a) L'anàlisi del procés de gestió dels ingressos per venda d'entrades de la societat, incloent-hi el seu cobrament i la generació de la informació econòmica corresponent. Així mateix, hem revisat la interfície[2] amb l'aplicació comptable que recopila la informació subministrada per l'aplicació informàtica de venda i reserva d'entrades per a generar, juntament amb la resta d'informació econòmica, els comptes anuals de la Societat.

b) L'anàlisi del procés de gestió de les despeses, compres i inversions, des de l'aprovació de la despesa o inversió fins al pagament d'aquesta, incloent-hi la generalització de la informació econòmica relativa a aqueixos conceptes i la seua comptabilització. En el treball en aquesta àrea hem prestat especial atenció al seguiment de les recomanacions fetes en l'informe d'auditoria de sistemes d'informació de 2008 i hem revisat els controls identificats en aquella auditoria.

c) L'anàlisi dels sistemes d'informació que suporten els dos processos de gestió esmentats i dels controls generals implantats en els sistemes d'informació de la Societat.

[2] Una interfície és una utilitat que permet de transmetre informació entre dues aplicacions, sistemes o dispositius. En aquest cas, possibilita la transmissió de dades econòmiques comptables de l'aplicació informàtica de gestió de vendes a l'aplicació comptable.

Aquesta auditoria d'eficàcia dels sistemes d'informació i de control intern s'ha fet conjuntament amb la fiscalització de regularitat que la Sindicatura de Comptes acompleix anualment sobre els comptes anuals de CACSA (n'incloem l'informe en el volum III, "Informes de fiscalització de les empreses públiques i d'altres ens", de l'Informe de Fiscalització del Compte General de la Generalitat de l'exercici de 2010). Les incidències relacionades amb la revisió financera o del compliment de la legalitat, sorgides en el curs de l'auditoria, es compilen en aquell informe.

El disseny, la implantació i el bon funcionament dels controls en els processos de gestió i en els sistemes d'informació és una responsabilitat que correspon als òrgans de direcció de la Societat.

Ateses les limitacions inherents a qualsevol sistema de control intern i, en concret, dels controls implantats en la Societat, hi pot haver fets motivats per errors o irregularitats que no hagen estat detectats en la revisió efectuada.

3. CONCLUSIÓ GENERAL

La revisió que hem dut a terme ha posat de manifest que el nivell de control existent en els sistemes d'informació i de control intern relacionats amb el procés de gestió dels ingressos per venda d'entrades i amb el procés de compres i despeses aporta un grau de confiança raonable per a garantir que s'han executat correctament, que les transaccions realitzades s'han comptabilitzat adequadament, i per a reduir el risc d'errors o irregularitats sobre el procés de generació de la informació comptable corresponent, i assegura la validesa, la integritat, l'exactitud, la confidencialitat i la disponibilitat de la informació.

Així mateix, es pot concloure que els objectius de l'àrea de sistemes es troben alineats amb els objectius generals de la Societat i que els recursos TI es gestionen de manera eficient.

Durant la realització del treball de fiscalització hem identificat les àrees de millora, que assenyalem més endavant, i hem proposat recomanacions que si s'implantaven contribuirien a incrementar l'ambient de control i reduir la probabilitat que hi haja incidències. No obstant això, s'ha fet palès que les deficiències de control intern, que són l'origen de les esmentades àrees de millora i recomanacions, no s'han traduït en errors materials en els comptes anuals de l'exercici de 2010.

El gràfic següent mostra l'alt grau de compliment del conjunt de controls que s'han analitzat en aquesta auditoria (hem revisat 151 controls de totes les àrees), cosa que reflecteix l'alt nivell de control intern que hi ha en l'entitat, i l'eficàcia global del sistema de control intern de la Societat:

Àrea	**Eficàcia dels controls**			**Total de controls revisats**
	Efectius	**Parcialment efectius**	**No efectius**	
Controls generals TI	47	13	19	79
Controls de procés de vendes	26	7	6	39
Controls de procés de despeses	28	3	2	33
Total de controls avaluats	**101** *66,9%*	**23** *15,2%*	**27** *17,9%*	**151** *100,0%*

Figura 2 – Total de controls avaluats

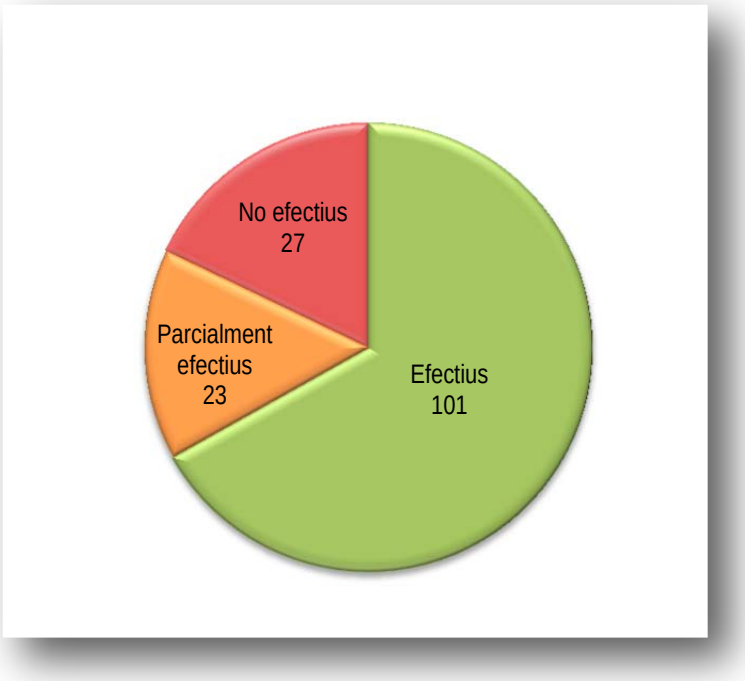

Figura 3 – Total de controls avaluats

4. ENFOCAMENT METODOLÒGIC

4.1 Descripció general

Hem estructurat el treball realitzat en tres grans blocs:

- Revisió dels controls generals establits en els sistemes d'informació que donen suport als processos de gestió revisats i a la gestió econòmica i financera.

  Puix que els sistemes d'informació generals de CACSA suporten els processos de gestió i les aplicacions informàtiques revisades, l'auditoria ha inclòs l'anàlisi dels controls generals de l'entorn de tecnologies de la informació que estableixen un marc general de confiança respecte al funcionament dels controls en els processos i les aplicacions de gestió.

  Per a poder confiar en els controls implantats en les aplicacions informàtiques és requisit fonamental que els controls generals de l'entorn de TI de l'entitat siguen efectius i, per tant, permeten de garantir el bon funcionament d'aquells, ja que altrament no es podrà confiar en els controls automàtics enclosos en aquestes.

- Revisió dels controls interns dels processos de gestió d'ingressos per venda d'entrades i de despeses i compres.

  La finalitat és determinar si el nivell de control existent en les aplicacions i l'eficàcia dels controls garanteixen la correcta execució dels processos de gestió revisats, i mitiguen el risc d'errors i irregularitats, garantint la validesa, la integritat i l'exactitud de la informació. En síntesi, el procediment que hem seguit ha consistit en el següent:

  1r. Adquirir una comprensió adequada dels processos de gestió auditats i identificar els riscs que hi ha en cada fase d'aqueixos processos i els controls que CACSA ha posat en pràctica; conèixer i entendre els sistemes informàtics concernits, els fluxos de dades que generen les operacions i com impacten en els estats financers.

  2n. Analitzar tant els controls automàtics enclosos en les aplicacions informàtiques com els controls manuals establits per a mitigar els riscs que hi haja.

  El propòsit d'aqueixa avaluació és determinar si els controls posats en pràctica en els processos són suficients i són eficaços en disseny (estan dissenyats adequadament per a cobrir els riscs d'errors en els estats financers en cadascun dels processos analitzats), identificant els controls rellevants o controls clau.

  3r. Comprovar mitjançant les proves d'auditoria oportunes si els controls clau seleccionats són eficaços en el seu funcionament operatiu.

- Realització de proves massives de **tractament de dades**, destinades a verificar la integritat i coherència de la informació associada a la gestió dels ingressos per venda d'entrades i el seu reflex en la comptabilitat.

Des del punt de vista tècnic, l'auditoria s'ha centrat especialment en l'aplicació SAP ERP (i les bases de dades i sistemes operatius subjacents), atès que és l'aplicació informàtica que dóna suport principal tant a l'execució del procés de gestió de les despeses, compres i inversions de la societat com al procés comptable; també ha estat objecte de revisió especial l'aplicació informàtica de venda i reserva d'entrades Colossus (i les bases de dades i sistemes operatius subjacents), que, juntament amb SAP, suporta el procés de gestió dels ingressos per venda d'entrades.

El treball s'ha dut a terme d'acord amb les normes tècniques d'auditoria següents:

- "Principis i normes d'auditoria del sector públic", elaborats per la Comissió de Coordinació dels Òrgans Públics de Control Extern de l'Estat Espanyol.

- "Manual de fiscalització" de la Sindicatura de Comptes.

- Els principis i les normes d'auditoria de sistemes d'informació internacionalment acceptats; en particular, els definits per l'Associació per a l'Auditoria i Control dels Sistemes d'Informació.

L'auditoria l'ha realitzada personal especialitzat de la Sindicatura de Comptes, amb la col·laboració d'experts independents externs.

Totes les deficiències de control intern observades i les recomanacions s'han comunicat íntegrament i detalladament als òrgans directius de la societat.

4.2 Revisió dels controls generals de TI (CGTI)

Els controls generals són les polítiques i els procediments que s'apliquen a la totalitat o a gran part dels sistemes d'informació de l'entitat, incloent-hi la infraestructura tecnològica del sistema d'informació auditat (que hem representat gràficament en la figura 6).

El propòsit dels controls generals en un entorn informatitzat és establir un marc conceptual de control general sobre les activitats del sistema informàtic i assegurar raonablement la consecució dels objectius generals de control intern i el correcte funcionament dels controls d'aplicació.

Els controls generals afecten tots els nivells dels sistemes d'informació, encara que estan relacionats amb molt major intensitat amb aquells nivells de caràcter general que afecten tota l'organització i els sistemes TI. És a dir que els controls generals es poden establit en els nivells següents:

- **Nivell de l'entitat**

  Els controls a aquesta escala es reflecteixen en la manera de funcionar d'una organització, i inclouen polítiques, procediments i altres pràctiques d'alt nivell que marquen les directrius de l'organització. Són un component fonamental del model COSO[3] i han de tenir en compte les operacions TI que suporten la informació financera. La identificació dels CGTI s'ha d'integrar en l'avaluació general de controls realitzada en l'àmbit d'entitat.

  Aquests controls tenen influència significativa sobre el rigor amb què el sistema de control intern és dissenyat i opera en el conjunt dels processos. L'existència d'uns CGTI rigorosos a aquesta escala, com són, per exemple, unes polítiques i procediments ben definits i comunicats, sovint suggereixen un entorn de control més eficaç i fiable. En sentit contrari, les organitzacions amb uns controls dèbils a aquesta escala és més probable que tinguen dificultats a l'hora de realitzar activitats de control regularment.

- **Nivell dels processos i aplicacions de gestió**

  Els processos de gestió són els mecanismes que utilitza una entitat per a desenvolupar la seua activitat i prestar un servei als seus destinataris o usuaris. Les entrades, el processament i les eixides són aspectes dels processos de gestió, que com més va estan més automatitzats i integrats en complexos sistemes informàtics.

  Una vegada revisats els CGTI a escala de l'entitat i dels sistemes informàtics generals, cal avaluar i comprovar la seua eficàcia en aquells processos i aplicacions que seran revisades, abans de fer treball d'auditoria sobre els seus controls d'aplicació.

  Els controls generals a aquesta escala consisteixen en les polítiques i procediments establits per a controlar determinats aspectes relacionats amb la gestió de la seguretat lògica, controls d'accés i gestió de la configuració i dels usuaris.

- **Nivell dels sistemes informàtics**

  Els serveis de tecnologia de la informació constitueixen la base de les operacions de la societat i els presta el conjunt de l'organització. Normalment inclouen la gestió de xarxes, la gestió de bases de dades, la gestió de sistemes operatius, la gestió d'emmagatzematge, la gestió de les instal·lacions i els seus serveis i l'administració de seguretat.

  Els controls a aquesta escala els formen els processos que gestionen els recursos específics dels sistema TI relacionats amb el seu suport general o amb les aplicacions principals.

[3] Committee of Sponsoring Organizations of the Treadway Commission

Aquests controls són més específics que els establits en l'àmbit d'entitat i normalment estan relacionats amb un tipus determinat de tecnologia. Aquest àmbit inclou tres àmbits tecnològics menors que cal avaluar separadament:

- Sistemes de gestió de les bases de dades
- Sistemes operatius dels servidors i de xarxa
- Infraestructura física

Tenint en consideració els diferents nivells que conformen el sistema d'informació de CACSA, la revisió dels CGTI s'ha estructurat en les àrees que detallem tot seguit i s'ha concretat en l'anàlisi dels aspectes següents, que inclouen 79 controls rellevants identificats:

A Marc organitzatiu

A.1 Organització i personal d'àrea TI

- Anàlisi de l'estructura organitzativa
- Descripció formal de funcions i responsabilitats

A.2 Planificació, polítiques i procediments

- Planificació i gestió de projectes TI significatius
- Identificació de tasques crítiques
- Polítiques i procediments de seguretat establits per al control de la infraestructura TI

A.3 Compliment normatiu (LOPD)

- Document de seguretat
- Fitxers notificats a l'Agència Espanyola de Protecció de Dades
- Informe de l'última auditoria biennal del Reglament de Mesures de Seguretat

B Gestió de canvis en aplicacions i sistemes

B.1 Adquisició d'aplicacions i sistemes

B.2 Desenvolupament i manteniment d'aplicacions

- Segregació de funcions
- Procediment d'aprovació final i traspàs a producció de canvis

- Personal amb accés a l'entorn de producció

C Operacions dels sistemes d'informació

C.1 Operacions de TI

- Procediment de gestió de rendiment operatiu i capacitat dels equips
- Planificació i gestió de processos programats
- Procediment de gestió d'incidències (Help-Desk)
- Aplicacions d'antivirus
- Inventari de maquinari i programari. Control d'instal·lacions

C.2 Seguretat física

- Mesures de protecció mediambiental: protecció física d'equips, sistemes antiincendis, controls de temperatura, revisions periòdiques, etc.
- Controls d'accés: gestió i control d'accés físic a las instal·lacions

C.3 Serveis externs

- Contractes de manteniment establits en l'àmbit informàtic
- Gestió de proveïdors (aplicacions)

D Accés a dades i programes (seguretat lògica)

D.1 Protecció de xarxes i comunicacions

- Entorn de xarxa i seguretat perimetral
- Avaluació de les mesures de seguretat de la xarxa perimetral

D.2 Procediments de gestió de drets d'accés a les aplicacions

- Gestió d'altes/baixes/modificació d'usuaris
- Directives de contrasenyes
- Directives d'auditoria
- Perfils d'usuari

D.3 Procediments de gestió de drets d'accés als sistemes i SGBD

- Gestió i control de accessos de usuaris privilegiats en l'entorn de producció dels servidors i bases de dades que donen suport a las aplicacions

E Continuïtat del servei

E.1 Còpies de seguretat

- Planificació de còpies de seguretat i monitoració
- Procediments formalitzats per a realitzar i restaurar còpies de seguretat
- Custòdia interna/externa de suports de còpia

E.2 Plans de continuïtat

- Pla de contingències

4.3 Revisió dels processos i aplicacions de gestió

Com ja hem indicat, l'objectiu de la revisió ha consistit a avaluar els procediments de gestió i de control intern, tant manuals com automatitzats, establits sobre les aplicacions corporatives (SAP ERP i Colossus) com a procés, analitzant l'alineament dels controls establits amb els riscs identificats, és a dir l'eficàcia dels controls per a mitigar aquests riscs.

Basant-nos en això, hem fet una anàlisi de l'entorn de control, dels riscs identificats, dels procediments de gestió, de les activitats de control i dels controls establits. També hem analitzat els mecanismes de monitoració dels controls.

El treball d'anàlisi i avaluació de controls establits en els processos de gestió l'hem focalitzat especialment en el procés d'ingressos. Del procés de gestió de despeses n'hem fet una actualització del coneixement d'aquest i dels controls associats i també un seguiment de les incidències i recomanacions que es feien en l'auditoria de sistemes anterior, corresponent a l'exercici de 2008.

Les principals activitats executades en aquesta fase són les següents:

- Anàlisi de processos, subprocessos i les seues funcionalitats.
- Avaluació de requeriments i identificació de riscs.
- Establiment d'objectius de control.
- Identificació de controls.
- Elaboració de matrius de riscs i controls incloent-hi els detalls de les activitats de control.
- Seguiment de transaccions.

- Prova de controls (automàtics i manuals) i de rutines mitjançant tècniques d'auditoria assistida per ordenador.
- Anàlisi de la traçabilitat d'esdeveniments (*log*, registres d'esdeveniments, etc.).
- Gestió d'incidències.
- Integritat de la informació.
- Anàlisi de la segregació de funcions.

4.4 Realització de proves massives de tractament de dades

Són destinades a verificar la integritat i la coherència entre la informació associada a la gestió dels ingressos per venda d'entrades i el seu reflex en la comptabilitat.

Inclouen l'anàlisi de la interfície (processos d'enviament i recepció d'informació) entre Colossus i SAP.

4.5 Criteris d'avaluació dels controls interns

Per tal de facilitar la comprensió de l'eficàcia dels controls, els hem categoritzats en tres nivells: efectiu, parcialment efectiu i no efectiu.

Aquests nivells de compliment són representats pels símbols següents, per a visualitzar l'eficàcia del control d'una manera més intuïtiva i fàcil:

Simbologia	Estat	Descripció
	Efectiu	El control s'ha implantat totalment i no presenta cap mena de debilitat.
	Parcialment efectiu	El control no s'ha implantat del tot o presenta alguna debilitat.
	No efectiu	El control no s'ha arribat a implantar o es fa un control irregular de l'activitat.

Figura 4

4.6 Criteris per a la categorització de les recomanacions

Les recomanacions emeses com a resultat del treball es basen en les deficiències de control intern detectades. Les hem categoritzades d'acord amb els criteris de risc i cost d'implantació del control.

El principal criteri de priorització suggerit per a abordar la implantació de les recomanacions es basa en el risc potencial que representa la incidència[4] detectada. Les primeres actuacions que caldrà portar a cap seran aquelles que mitiguen els riscs de

[4] Segons la secció 850 del Manual de fiscalització de la Sindicatura de Comptes:

7. Avaluació de les incidències detectades

Les incidències detectades en la revisió dels CGTI es classifiquen de la manera següent:

- Hi ha una **deficiència de control intern** quan el disseny o el funcionament d'un control no permet al personal de l'entitat o a la direcció d'aquesta, en el curs ordinari de les operacions, de prevenir o detectar errors o irregularitats en un termini raonable. Es pot tractar d'una *deficiència de disseny* (quan un control necessari per a assolir l'objectiu de control manca o no s'ha dissenyat adequadament) o de *deficiències de funcionament* (quan un control adequadament dissenyat no opera com deuria o la persona que l'executa no ho fa eficaçment).
- Una **deficiència significativa** és una deficiència en el control intern, o una combinació de deficiències, que afecten adversament la capacitat de l'entitat per a iniciar, autoritzar, registrar, processar o reportar informació financera o pressupostària de manera fiable, conformement als principis o normes comptables i pressupostàries aplicables. Hi ha una probabilitat més que remota que una manifestació errònia en els comptes anuals, que no és clarament trivial, no siga previnguda o detectada.
- Una **debilitat material** és una deficiència significativa en el control intern o una combinació de més d'una, respecte a les quals hi ha una possibilitat raonable que una manifestació errònia significativa en els comptes anuals no siga previnguda o detectada i corregida en el termini oportú.

nivell alt; seguidament, caldria actuar sobre les accions que mitiguen riscs de nivell mitjà, i, en darrera instància, s'abordaran aquelles accions que mitiguen riscs de nivell baix.

També s'assenyala una indicació del cost o complexitat d'implantació del control suggerit, de manera que es puga fer una avaluació cost/benefici de cadascuna de les recomanacions proposades.

Detallem tot seguit el criteri de categorització emprat:

Criteri	Descripció	Nivell	
Risc	Probabilitat de contingència o vulnerabilitat d'acord amb l'impacte potencial de la incidència detectada	**Alt**	Aspectes de control o **debilitats materials** que poden arribar a afectar de manera molt significativa el control intern o la integritat de la informació.
		Mitjà	Aspectes de control o **deficiències significatives** que no representen una bona pràctica i que podrien repercutir en el sistema de control intern o en la integritat de les dades.
		Baix	**Deficiències de control intern** que no afecten significativament el control intern, però que, al nostre entendre, la direcció de la societat les ha de tenir en compte.
Cost	Valoració aproximada o estimativa dels recursos que l'organització ha de destinar a l'execució de l'acció recomanada	**Alt**	Aspecte de control o deficiència que té una solució complexa, que requereix un temps d'implantació més llarg o un cost alt.
		Mitjà	Aspecte de control o deficiència que té una solució intermèdia en duració i en dificultat.
		Baix	Aspecte de control o deficiència que té una solució fàcil i ràpida de resoldre.

Figura 5

5. RESUM GENERAL

5.1 Descripció de l'entorn tecnològic

Els principals sistemes que suporten els processos de gestió objecte de revisió són l'aplicació SAP ERP i l'aplicació de venda i reserva d'entrades Colossus:

SAP ERP: CACSA disposa dels mòduls relatius a Finances i Comptabilitat (FI/CO), Vendes (SD), Compres (MM), Gestió de Projectes (PS) i Manteniment (PM).

També s'ha començat a utilitzar el mòdul SAP CRM per a gestionar les relacions amb els clients.

L'aplicació disposa d'Oracle 10*g* com a sistema gestor de base de dades i d'AIX com a sistema operatiu.

Els sistema operatiu de la xarxa és Windows Server 2003.

Colossus: És l'aplicació informàtica emprada per a gestionar la reserva i la venda d'entrades; és de desenvolupament propi i està en funcionament des del 31 de desembre de 2008.

L'aplicació disposa d'Oracle 10g com a sistema gestor de base de dades i d'AIX com a sistema operatiu.

Visualment, l'entorn auditat ha estat el següent:

Figura 6

Amb relació a la seguretat lògica de la xarxa corporativa, hi ha implantades mesures per a prevenir i detectar amenaces tant internes com externes. Internament s'ha segmentat la xarxa en diverses VLAN, aïllant els servidors i serveis sensibles de la Societat i també diferents xarxes d'usuari segons les necessitats i l'ús. Heus ací algunes de les característiques de la xarxa:

- Xarxes redundades: l'entitat disposa de línies de comunicació redundades mitjançant radioenllaç.

- Accessos remots: són controlats mitjançant protocols de comunicació segurs.

- Arquitectura de seguretat: es disposa d'elements de seguretat perimetral utilitzats per a filtrar i controlar tràfic entrant/sortint de l'entitat. Aquests elements de xarxa realitzen funcions de tallafoc, de filtre antiinundació, de protecció contra programari maliciós, de control de continguts i de control de connexions de xarxa privada virtual.

La Societat assenyala en el seu informe de gestió de l'exercici de 2010 que des del Departament de Sistemes s'ha treballat bàsicament a desenvolupar i optimitzar el sistema de virtualització emprat per a consolidar la major part d'aplicacions i sistemes informàtics. Aquesta virtualització dels sistemes està permetent de reduir els costs d'espai d'emmagatzemament i recursos necessaris per a millorar el rendiment de les aplicacions. De més a més, permet de gestionar el centre del procés de dades com un conjunt de recursos o agrupació de tota la capacitat de processament, memòria, xarxa i emmagatzematge disponible en la infraestructura.

CACSA ha formalitzat una política de seguretat de la informació aplicable a tot el personal de l'organització i ha establit un Comitè de Seguretat d'Informació encarregat de revisar i fer el seguiment dels esdeveniments relacionats amb la seguretat de la informació.

Hem observat un alt grau de conscienciació i orientació al control intern dels sistemes d'informació. Es manté vigent la certificació del SGSI ISO 27001.

5.2 Controls generals de TI

L'objectiu principal de la revisió ha estat obtenir una visió del grau d'eficàcia dels CGTI que hi ha en CACSA. El treball realitzat en l'auditoria de sistemes d'informació anterior ha constituït una font d'informació important en aquesta fase. Hem analitzat i fet el seguiment de les recomanacions efectuades en l'informe de l'exercici de 2008 i hem analitzat en profunditat els canvis realitzats en els processos i procediments de control des d'aquella revisió.

El gràfic següent mostra l'alt grau de compliment dels 79 controls generals que hem revisat en l'auditoria, cosa que indica que hi ha un satisfactori entorn general de control en l'entitat:

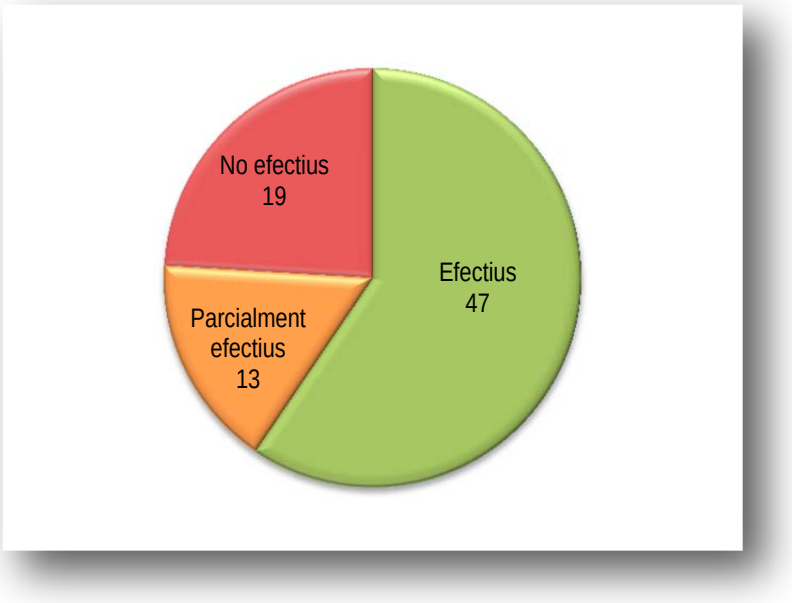

Figura 7 – Eficàcia dels CGTI

Àrea	Eficàcia dels controls			Total de controls revisats
	Efectius	Parcialment efectius	No efectius	
Marc organitzatiu	7	2	0	9
Gestió de canvis	4	0	2	6
Operacions TI	17	2	2	21
Seguretat lògica	16	7	13	36
Continuïtat de servei	3	2	2	7
Total de CGTI	**47** *59,5%*	**13** *16,5%*	**19** *24,0%*	**79** *100,0%*

Figura 8 – Eficàcia dels CGTI

Sense perjudici del satisfactori entorn general de control que hi ha en els sistemes d'informació, els principals aspectes susceptibles de millora que hem identificat després de fer la revisió es poden sintetitzar en els quinze punts següents:

Marc organitzatiu

1r. L'entitat disposa d'un Pla Estratègic de Sistemes de Tecnologies de la Informació i Telecomunicacions, elaborat per l'Àrea de Sistemes de la Informació, en el qual s'especifiquen els objectius estratègics de l'Àrea i les accions que cal abordar a mitjà termini per a atènyer-los. Ara bé, la direcció no ha aprovat formalment aquest pla.

2n. CACSA ha emprès accions encaminades al compliment de la Llei Orgànica de Protecció de Dades 15/1999. Tanmateix, no ha portat a cap l'adequació a les mesures tècniques, legals i organitzatives establides en el reglament que la desplega (RD 1720/2007); per tant, no ha complit amb tots els requisits que estableix aquesta normativa. Així mateix, hem observat que les auditories biennals obligatòries que s'han fet fins ara no són prou completes.

Referent a això, val a dir que l'entitat ha iniciat el 2011 un projecte, en col·laboració amb un proveïdor extern, per a completar l'adequació a la normativa vigent.

Gestió de canvis en aplicacions i sistemes

3r. La documentació i el seguiment dels canvis efectuats en les aplicacions analitzades (Colossus i SAP) són registrats i gestionats mitjançant l'eina eMas. Amb relació a la documentació registrada, hem pogut verificar que no es disposa de cap formulari o registre estàndard per a recopilar l'acceptació formal dels usuaris sol·licitants.

D'altra part, la documentació de les proves efectuades sobre els canvis abans del seu traspàs a producció no és prou detallada ni formalitzada.

4t. El transport a producció dels canvis efectuats en les aplicacions el fan els usuaris desenvolupadors, cosa que no garanteix una adequada segregació de funcions.

Operacions dels sistemes d'informació

5è. La sala que conté els servidors de l'entitat (CPD) disposa d'una sèrie de mesures de control mediambiental establides per a minimitzar el risc de contingències en l'emplaçament. Amb tot, hem observat que no hi ha sistemes automàtics d'extinció d'incendis ni sensors de fum. De més a més, hem advertit que hi ha material obsolet i inflamable en la sala contigua a la sala de servidors, cosa que representa un risc potencial.

Amb relació al control d'accés a la sala, hi ha mesures de control per a evitar que hi entre personal no autoritzat, si bé hem pogut verificar que les portes d'accés, tant la principal de vidre com la secundària de fusta, a causa de la poca robustesa que tenen, no garanteixen completament l'estanquitat de la sala i la restricció d'accés.

Accés a dades i programes (seguretat lògica)

6è. El procediment existent relatiu a les altes, les baixes i les modificacions d'usuaris no segueix un flux clar d'autoritzacions.

Amb relació a la gestió d'usuaris del directori actiu, hem pogut verificar que hi ha un nombre significatiu d'usuaris amb un període d'inactivitat superior a tres mesos.

També hem observat que hi ha usuaris en SAP amb un període d'inactivitat superior a tres mesos.

7è. Les polítiques de contrasenyes, amb caràcter general, no són tan robustes com recomanen les millors pràctiques en la matèria.

Es poden optimitzar en el directori actiu establint un historial de contrasenyes. Per altra banda, la directiva de bloqueig no és completament efectiva, ja que el compte es desbloqueja automàticament al cap de cinc minuts.

En els sistemes AIX que contenen les bases de dades de Colossus i de SAP, tot i ser entorns a què accedeix exclusivament personal del departament TI, no s'han establit paràmetres de contrasenyes com ara caducitat, longitud mínima, història o llindar de bloqueig.

Els sistemes gestors de bases de dades Oracle que contenen les dades de les aplicacions SAP i Colossus no disposen tampoc d'una directiva de contrasenyes robusta. Per altra banda, hem verificat que no es monitoren esdeveniments i que no s'han configurat els paràmetres relatius a les directives d'auditoria.

8è. No s'han restringit adequadament les possibilitats d'accés remot a ERP SAP. Recomanem de delimitar els usuaris que tenen aquesta mena d'accés als sistemes de gestió.

9è. Respecte a la gestió d'usuaris en SAP, hem observat que hi ha usuaris finals amb accés a diverses transaccions crítiques del sistema.

10è. Hem detectat alguns usuaris amb conflicte de segregació de funcions en el sistema SAP.

11è. Amb relació a la configuració de seguretat de SAP, hi ha punts de millora relatius a la parametrització de seguretat, com ara la restricció del nombre de començaments de sessió per usuari (o terminal), el període de caducitat de contrasenyes i el tancament automàtic de sessió per inactivitat.

Continuïtat del servei

12è. Hi ha procediments operatius per a fer còpies de seguretat i restaurar-les, encara que no s'ha documentat un pla detallat que reflectesca l'estratègia que l'entitat segueix pel que fa a les còpies de seguretat.

13è. La custòdia dels suports de còpies de seguretat es fa de manera interna i les còpies s'emmagatzemen en el robot de còpies del CPD. Amb periodicitat mensual s'extrau un joc de còpies i s'emmagatzema en una caixa de seguretat situada en el mateix edifici que el CPD. En cas de contingència, en la sala de servidors hi ha el risc de pèrdua d'informació de fins a un mes.

14è. De més a més, com que no es fa una custòdia externa de les còpies de seguretat, en cas de contingència greu es podria veure seriosament afectada l'estratègia de recuperació i continuïtat del servei.

15è. El pla de recuperació en cas de desastres no conté de manera detallada i completa l'estratègia de recuperació que l'entitat ha de seguir d'acord amb les necessitats de gestió ni tampoc una anàlisi dels riscs financers, operacionals, legals o d'imatge pública derivats de la interrupció del servei.

En l'apartat 6.1 formulem quinze recomanacions correlacionades amb els punts anteriors.

5.3 Procés de gestió dels ingressos per venda d'entrades

En aquesta auditoria hem posat èmfasi en l'anàlisi del procés de gestió dels ingressos per venda d'entrades en els centres de la Ciutat de les Arts i de les Ciències (el Museu de les Ciències, l'Hemisfèric i l'Oceanogràfic) per mitjà dels diversos canals, el seu cobrament i la seua comptabilització, i han estat objecte d'anàlisi detallada els riscs que hi pogués haver en el procés de gestió i els controls clau establits per a mitigar-los.

S'han establit diferents canals de venda d'entrades en els diversos centres de CACSA, que presenten lleugeres diferències en els seus processos:

Canal intern: Venda en taquilla
Venda en línia
Venda telefònica

Intermediari: Plataformes bancàries (Serviticket, ServiCAM i ServiCaixa)
Agències de viatges
Hotels/empreses

La venda d'entrades i tota l'operativa relacionada es gestiona per mitjà de l'aplicació informàtica Colossus. Aquesta aplicació està implantada des del 31 de desembre de 2008 i ha estat desenvolupada internament amb la col·laboració de diversos proveïdors externs.

Independentment del canal de venda, tots els operadors interactuen amb l'aplicació Colossus, que registra totes les transaccions efectuades.

L'aplicació Colossus disposa d'unes quantes interfícies d'entrada i eixida de dades:

Entrada: El canal de venda en línia i les plataformes bancàries es connecten directament a l'aplicació per a gestionar les operacions de venda.

Eixida: Les dades de les vendes generades en l'aplicació es traspassen diàriament a l'aplicació comptable SAP.

Diàriament s'executa un procés programat en Colossus que genera un fitxer de text pla amb les vendes, els cobraments i la facturació diària. Aquest fitxer s'integra manualment en SAP per al registrar comptablement les operacions efectuades.

En addició a això, el sistema Colossus genera un fitxer de text amb les altes, les baixes o les modificacions de clients a fi de traspassar aquesta informació a l'entorn SAP.

El gràfic següent mostra el grau de compliment dels 39 controls interns que hem revisat en el procés de gestió de venda d'entrades, el nivell de control del qual es pot considerar satisfactori:

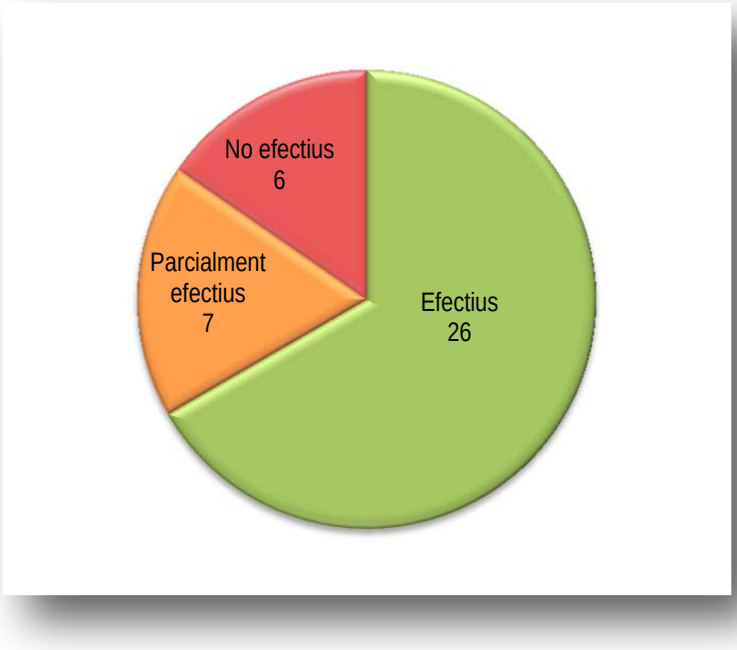

Figura 9 - Eficàcia dels controls interns
del procés de venda d'entrades

Els principals aspectes susceptibles de millora en el procés de gestió de venda d'entrades i en l'aplicació informàtica Colossus que hem identificat en la revisió efectuada els sintetitzem en els punts següents:

1r. Les funcionalitats relatives a l'edició o modificació dels fitxers mestres principals en el sistema de reserva i venda d'entrades Colossus no s'han restringit exclusivament als usuaris o grups encarregats de gestionar-los.

2n. Amb relació a la gestió dels clients, tant en SAP com en Colossus hem observat que no hi ha un control eficaç que permeta d'assegurar el registre únic de clients pels motius següents:

- El sistema Colossus no permet de registrar un client amb un codi d'identificació fiscal (CIF), però permet de donar-hi d'alta clients sense introduir-ne el CIF.

- En SAP el sistema avisa en cas que ja tinga registrat un CIF, però permet de continuar donant-hi d'alta el client.

- No hi ha un control que garantesca el registre únic de clients (en SAP i Colossus), ja que és possible que un client estiga donat d'alta amb un identificador de Colossus i al seu torn registrat en SAP amb un identificador propi i distint del de Colossus.

3r. Amb relació als processos d'autorització i aprovació de clients, hem observat que hi ha diversos procediments per a donar d'alta clients segons la tipologia d'aquests; el procés d'aprovació està molt distribuït per tal com hi ha diversos aprovadors o autoritzadors. No s'han establit controls periòdics per a revisar les altes i les modificacions de clients efectuades, tant en SAP com en Colossus, que permeten de garantir que el procés d'altes s'ha fet segons el que hi ha establit.

Pel que fa a fitxers mestres clau de Colossus relatius a tarifes, descomptes, tipus de client i ràpels, són gestionats per diverses àrees funcionals. Les dades disponibles en aqueixos fitxers mestres els ha d'aprovar prèviament la direcció. Hem advertit que no s'ha establit cap procediment per a revisar periòdicament les dades dels fitxers mestres que garantesca que la informació que hi ha en el sistema es correspon amb les dades que la direcció ha aprovat.

4t. En l'aplicació Colossus no es monitoren els canvis efectuats sobre els fitxers mestres principals, ja que no hi cap control sobre quin usuari ni en quin moment ha fet un canvi sobre un fitxer mestre.

5è. En els mètodes de pagament establits per als clients definits com de prepagament, hem detectat que el sistema Colossus permet d'establir la forma de pagament de crèdit en el moment de fer l'ordre de venda, amb el risc de fer vendes a crèdit a clients per als quals no s'ha negociat el pagament ajornat; aqueix saldo per cobrar, doncs, és susceptible d'impagament.

6è. El sistema Colossus permet de fer la devolució parcial o íntegra d'una venda realitzada. En el cas de les vendes a crèdit, el sistema fa automàticament la devolució en aqueixa modalitat; en el cas de les vendes per prepagament, però, el sistema permet de seleccionar la forma de reintegrament. Malgrat que el sistema Colossus selecciona per defecte la forma de pagament utilitzada en la venda permet fer devolucions en una forma de pagament altra que l'emprada en la venda (al comptat o a crèdit).

7è. Diàriament l'aplicació Colossus genera un fitxer amb la facturació per a ser traspassat a SAP. El procés d'importació en SAP es fa manualment, seleccionant el fitxer i carregant-lo. S'ha establit una sèrie de controls per a garantir la completesa, l'exactitud i la integritat de les dades carregades. Hem observat que el sistema SAP no disposa d'un control automàtic per a evitar que es carreguen fitxers duplicats.

5.4 Procés de gestió de compres

En l'informe de fiscalització de 2008 vàrem fer una revisió exhaustiva d'aquest procés de gestió. Com que des de llavors no hi ha hagut modificacions rellevants, en aquesta auditoria hem actualitzat el coneixement i hem revisat l'efectivitat dels controls clau analitzats aleshores.

La gestió de les compres i inversions es fa íntegrament en el sistema SAP ERP de CACSA.

El procés de compres difereix segons l'entitat encarregada de fer la comanda de compra:

CACSA Per a totes les compres de CACSA, fora de les de l'Oceanogràfic, és el personal de la Societat qui inicia tots els procediments de gestió i els executa.

Amb aquesta finalitat hi ha definit formalment, i aprovat per la Direcció, un procediment en el qual s'estableix el procés d'autorització i els requeriments necessaris per a fer obres, adquirir béns i contractar serveis.

PRV La gestió de les compres de l'Oceanogràfic la realitza autònomament PRV, que n'és l'operador encarregat, el qual ha de notificar i sol·licitar autorització per a fer les compres. Paral·lelament, PRV ha de registrar en SAP les comandes corresponents, que han d'autoritzar i alliberar uns interlocutors determinats de CACSA.

Des de CACSA es fa un seguiment de les comandes i les factures autoritzades a PRV verificant les possibles desviacions respecte als pressuposts acordats. Per tant, el procediment de gestió de les compres, amb algunes diferències respecte al procediment habitual de CACSA, concerneix persones clau de totes dues organitzacions.

Aquest procediment no es troba formalitzat.

Com a resum del treball realitzat sobre aquest procés de gestió, en el qual s'han revisat 33 controls interns, els gràfics següents mostren l'alt grau d'eficàcia dels controls, que es pot considerar satisfactori.

Com que hi ha dos procediments diferenciats per a gestionar les compres, un de general i un altre per a les compres de l'Oceanogràfic, gestionades per PRV, mostrem separadament l'eficàcia operativa dels controls en cada cas:

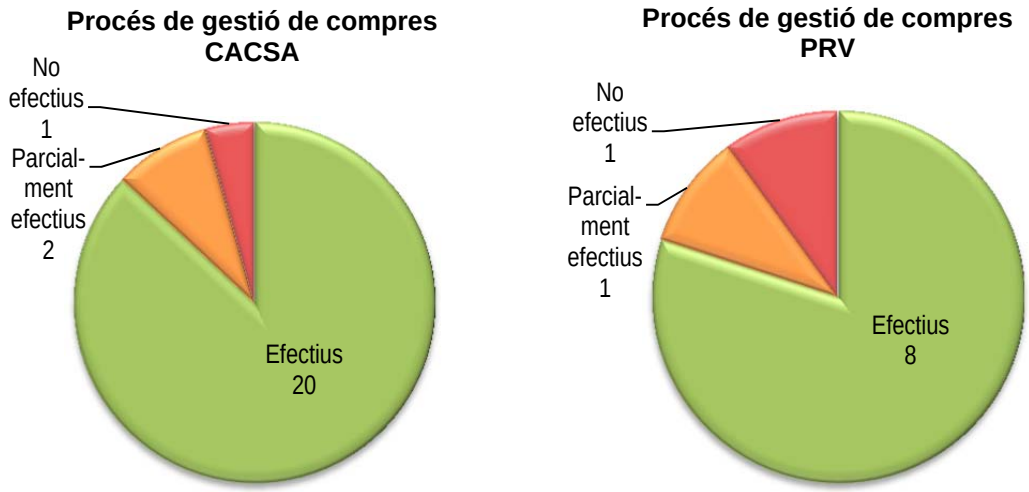

Figura 10 - Eficàcia dels controls interns del procés de compres

Els principals aspectes susceptibles de millora en el procés de gestió de compres i en l'aplicació informàtica que hem identificat en la revisió efectuada són els següents:

1r. El Departament de Compres controla manualment que les compres de cada departament no superen el pressupost que tinga assignat. Com que l'aplicació no fa automàticament aquest control, hi ha una certa possibilitat d'error humà.

2n. Una vegada conciliades les factures i els pagaments que calga tramitar, es genera per mitjà de SAP un fitxer de transferències, amb el format establit, per a enviar-lo a l'entitat bancària perquè faça el pagament. Hem comprovat que el fitxer generat per SAP és editable i podria ser modificat abans d'enviar-lo a l'entitat financera, cosa que representa un risc sobre la integritat i autenticitat de la informació.

3r. El procediment per a gestionar les compres de l'Oceanogràfic (PRV) no ha estat aprovat formalment.

4t. En tots dos processos (CACSA i PRV), el sistema permet de modificar els imports de les comandes de compres una vegada alliberades (aprovades) sense necessitat de tornar a passar de nou pel procés d'alliberament.

5.5 Resultats de les proves massives de dades

Hem analitzat la interfície entre Colossus i SAP i hem fet una sèrie de proves destinades a verificar la integritat i la coherència de la informació associada a la gestió dels ingressos per venda d'entrades i el seu reflex en la comptabilitat.

Els resultats de les proves han estat satisfactoris, i hem comprovat que la informació registrada en comptabilitat es correspon amb la informació processada per Colossus sense que hi hàgem detectat incoherències o diferències.

6. RECOMANACIONS

A conseqüència dels controls no efectius o parcialment efectius que s'han observat en el curs de la revisió, es dedueix una sèrie de recomanacions encaminades a resoldre les deficiències de control intern detectades.

6.1 Controls generals TI

Resumim en el quadre següent les recomanacions més rellevants resultants de la revisió dels CGTI en la present auditoria i les que continuen vigents de l'auditoria anterior. Hem plantejat aquestes recomanacions a partir de les deficiències assenyalades en l'apartat 5.2, incloent una avaluació del risc que representen (segons els criteris exposats en l'apartat 4.6) i del cost o de la complexitat d'implantació de la recomanació. Seguint aquesta classificació, proposem les accions següents:

ID	Àrea CGTI	Recomanació	Risc	Cost
1	Marc organitzatiu	Atesa la importància del Pla Estratègic de Sistemes, cal que l'aprove la Direcció de CACSA.	Mitjà	Mitjà
2	Marc organitzatiu	CACSA ha de completar l'adequació a l'LOPD d'aquells aspectes que n'estan pendents.	Alt	Mitjà
3	Gestió de canvis	Cal documentar detalladament el registre dels canvis en SAP incloent l'aprovació del sol·licitant.	Mitjà	Baix
4	Gestió de canvis	S'ha de garantir una adequada segregació de funcions en els traspassos a l'entorn productiu SAP dels canvis en les aplicacions.	Mitjà	Mitjà
5	Operacions TI	Cal augmentar els controls ambientals i de seguretat del CPD.	Mitjà	Mitjà
6	Seguretat lògica	Cal millorar el procediment per a la gestió d'usuaris en els diversos entorns informàtics i fer que incloga un recurs per a revisar periòdicament els usuaris.	Mitjà	Mitjà
7	Seguretat lògica	Cal millorar la configuració de les contrasenyes posant en pràctica una política de contrasenyes robustes en tots els entorns informàtics de CACSA.	Mitjà	Mitjà
8	Seguretat lògica	Cal millorar aspectes de seguretat en serveis telemàtics i definir els usuaris amb accés remot mitjançant FTP al sistema AIX que suporta SAP.	Mitjà	Baix
9	Seguretat lògica	Cal revisar i restringir els usuaris amb accés a transaccions crítiques de SAP.	Mitjà	Mitjà
10	Seguretat lògica	Cal revisar els usuaris amb conflicte de segregació de funcions en SAP i adoptar les mesures correctores oportunes.	Alt	Alt
11	Seguretat lògica	Cal enfortir la configuració de determinats aspectes de seguretat de l'entorn SAP.	Baix	Baix
12	Continuïtat del servei	Cal millorar i completar els procediments de còpies de seguretat.	Baix	Baix
13	Continuïtat del servei	Cal millorar el procediment de custòdia interna de suports de les còpies de seguretat.	Alt	Baix
14	Continuïtat del servei	Cal establir un procediment de custòdia externa dels suports de les còpies de seguretat.	Mitjà	Mitjà
15	Continuïtat del servei	Cal completar el Pla de Contingències Informàtiques i documentar detalladament les proves que s'han fet.	Mitjà	Mitjà

Figura 11

El gràfic següent mostra la classificació de les recomanacions segons els criteris combinats de risc potencial que cal mitigar i cost de l'implantament de la mesura, assenyalats en l'apartat 4.6:

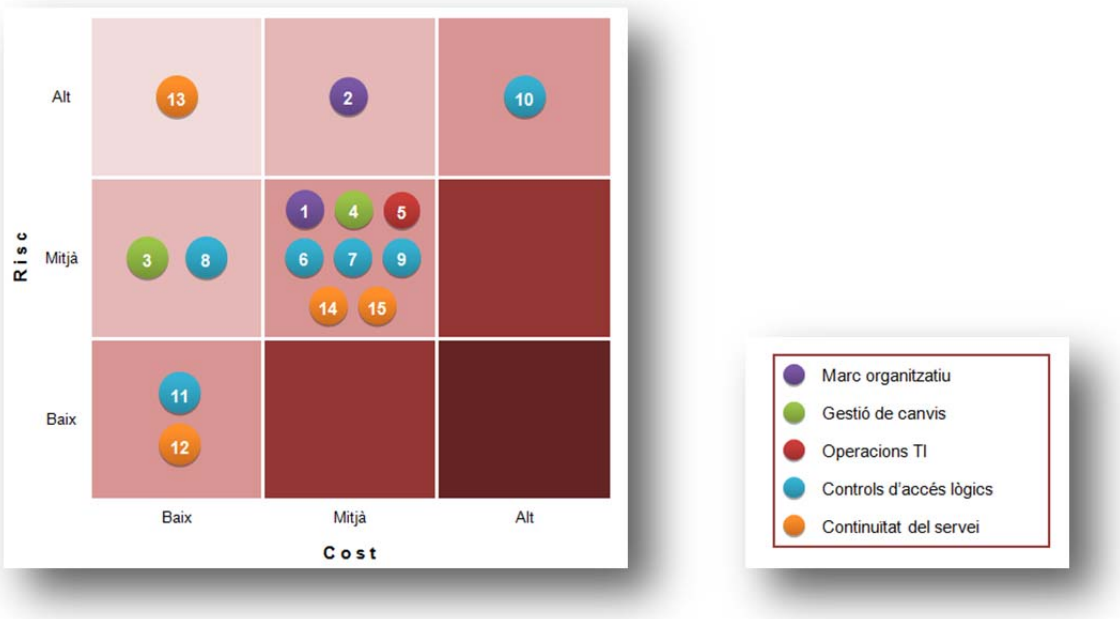

Figura 12 – Recomanacions CGTI prioritzades

Aquesta figura conté tant les recomanacions detectades durant l'exercici de 2008 que continuen vigents com les detectades en la present auditoria.

6.2 Procés de gestió d'ingressos per venda d'entrades

Resumim en el quadre següent les recomanacions més rellevants resultants de la revisió del procés de gestió d'ingressos per venda d'entrades. Aquestes recomanacions han estat elaborades a partir de les deficiències assenyalades en l'apartat 5.3, amb inclusió d'una avaluació del risc que representen (segons els criteris que hem exposat en l'apartat 4.6) i del cost o la complexitat d'implantar la recomanació. Seguint aquesta classificació, proposem les accions següents:

ID	Recomanació	Risc	Cost
1	Cal restringir els permisos d'edició dels fitxers mestres clau en Colossus relatius a clients, tarifes, descomptes, ràpels i tipus de client.	**Alt**	**Baix**
2	Cal establir un registre únic de clients per a SAP i Colossus o, alternativament, implantar controls automàtics que impedesquen discrepàncies entre els fitxers mestres de tots dos sistemes.	**Mitjà**	**Baix**
3	Cal formalitzar un procediment per a revisar periòdicament els fitxers mestres claus tant en SAP com en Colossus.	**Mitjà**	**Baix**
4	Cal formalitzar un registre d'auditoria per a monitorar les modificacions efectuades sobre els fitxes mestres clau de Colossus (clients, tarifes, descomptes, tipus de client i ràpels).	**Mitjà**	**Baix**
5	Cal restringir les formes de pagament per a clients de prepagament no permetent de pagar a crèdit.	**Mitjà**	**Mitjà**
6	Cal restringir la forma de pagament en devolucions a la mateixa utilitzada en la venda.	**Baix**	**Baix**
7	Cal establir un control per a eliminar la possibilitat de càrrega duplicada del fitxer de vendes general per Colossus.	**Mitjà**	**Alt**

Figura 13

El gràfic següent mostra la classificació de les recomanacions segons els criteris combinats de risc potencial i cost de la implantació de la mesura, assenyalats en l'apartat 3.5:

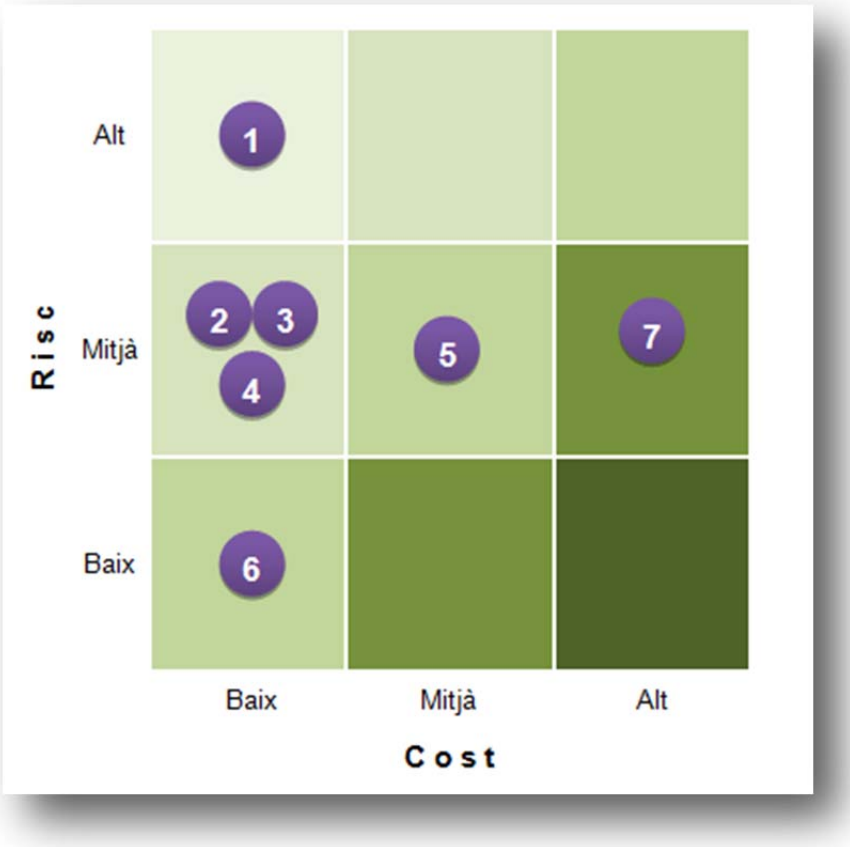

Figura 14 – Recomanacions prioritzades del procés de gestió de venda d'entrades

6.3 Procés de gestió de compres

Resumim en el quadre següent les recomanacions més rellevants resultants de la revisió del procés de gestió de compres. Aquestes recomanacions han estat elaborades a partir de les deficiències assenyalades en l'apartat 5.3, amb inclusió d'una avaluació del risc que representen (segons els criteris que hem exposat en l'apartat 4.6) i del cost o la complexitat d'implantar la recomanació. Seguint aquesta classificació, proposem les accinos següents:

ID	Recomanació	Risc	Cost
1	Cal posar en pràctica un control de límit pressupostari dins el sistema SAP per al control pressupostari de CACSA.	**Mitjà**	**Baix**
2	Cal establir un control de conciliació del detall dels pagaments tramitats per l'entitat financera i els remesos per CACSA.	**Baix**	**Baix**
3	Cal formalitzar el procediment de compres per a PRV.	**Baix**	**Baix**
4	Cal garantir el compliment de l'estratègia d'alliberament en cas de modificació de comandes ja alliberades (CACSA i PRV).	**Baix**	**Mitjà**

Figura 15

Com l'entitat ens ha informat, en el moment d'elaborar aquest Informe està en procés d'implantació la primera recomanació.

El gràfic següent mostra la classificació de les recomanacions segons els criteris combinats de risc potencial i cost d'implantació de la mesura, assenyalats en l'apartat 3.5:

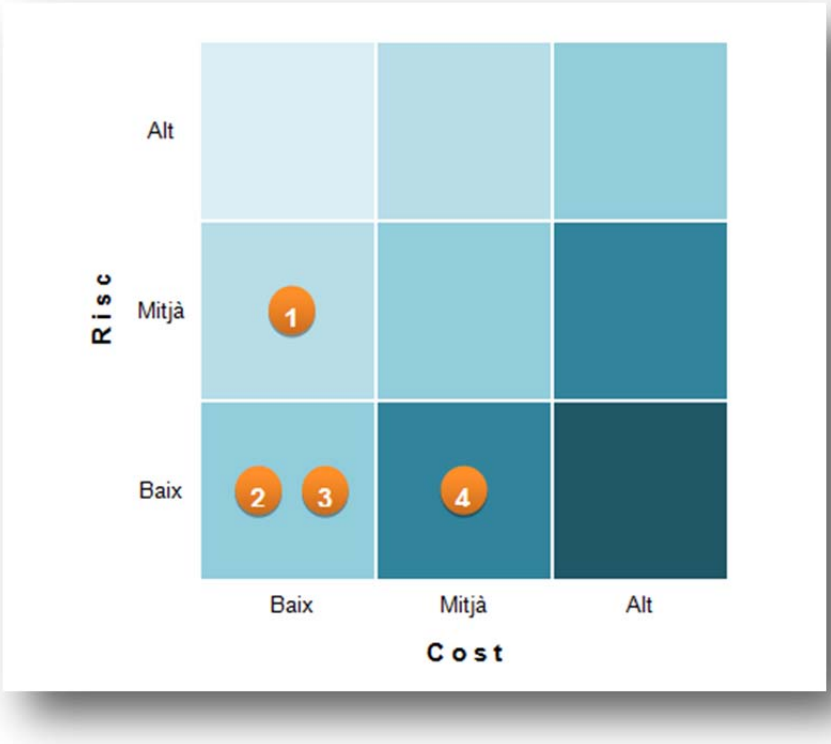

Figura 16 – Recomanacions prioritzades del procés de gestió de compres

7. TRÀMIT D'AL·LEGACIONS

En compliment del que es va acordar en el Ple de les Corts del dia 22 de desembre de 1986 i també de l'Acord del Consell d'aquesta Sindicatura de Comptes per mitjà del qual tingué coneixement de l'esborrany de l'informe sobre l'auditoria d'eficàcia dels sistemes d'informació i de control intern de la Ciutat de les Arts i de les Ciències, SA, l'esborrany esmentat es va trametre als gestors perquè, en el termini concedit, hi formulassen al·legacions.

Una vegada transcorregut aquest termini, no s'han rebut al·legacions.

INFORME DE FISCALITZACIÓ DEL COMPTE GENERAL DE LA GENERALITAT DE L'EXERCICI DE 2010

- Volum I	Compte de l'Administració de la Generalitat
- Volum II	Entitats autònomes
- Volum III	Empreses públiques i d'altres ens
- Volum IV	Fundacions del sector públic de la Generalitat
- Volum V	Informes especials de fiscalització
- Annexos:	Annex I: Comptes anuals dels comptedants
	Annex II: Al·legacions dels comptedants i informes sobre les dites al·legacions

Aquest volum, amb els informes que hi conté, va ser aprovat pel Consell de la Sindicatura de Comptes de la Comunitat Valenciana en la seua reunió del dia 12 de desembre de 2011.

València, 12 de desembre de 2011

EL SÍNDIC MAJOR

Rafael Vicente Queralt