Auditoria i Programari Lliure

Joan Puig i Sergi Blanco

Juny de 2007

Resum

Actualment les noves tecnologies i la informació que aquestes gestionen representen un element clau dins les organitzacions. La necessitat de millorar l'eficiència i eficàcia dels processos tecnològics fa imprescindible l'establiment de mecanismes de control intern. En aquest document s'analitzen els avantatges i els inconvenients de l'ús de programari lliure des de la perspectiva d'auditoria i control.

1 Introducció

En l'àmbit empresarial, durant els darrers anys, hem viscut un augment significatiu de normatives i regulacions que exigeixen i/o fomenten l'ús de pautes de bon govern, incloent mecanismes de validació i millora contínua de les activitats de les empreses (és a dir, maneres per assegurar que les coses es fan correctament i cada cop millor), com són la Sarbannes-Oxley Act, Basilea II o el reglament de la LOPD[1].

Aquest fet ha generat unes fortes necessitats de control dels processos de negoci interns, principalment amb una orientació cap als següents objectius:

- Assegurar el bon govern de l'organització, protegint els interessats en el bon funcionament d'aquesta (clients, accionistes, empleats, etc.)
- Garantir el compliment de les normatives del sector on actua l'organització.
- Millorar l'eficàcia i eficiència de les activitats de l'organització.
- Control intern.

Donada la forta dependència que tenen les organitzacions dels sistemes d'informació, junt amb la complexitat creixent d'aquests, l'establiment de controls sobre els processos tecnològics ha pres un paper protagonista entre les mesures de control intern.

És sota aquestes circumstàncies que l'*auditoria informàtica* (tant interna com externa) esdevé una eina imprescindible, que ha anat evolucionant i ampliant el seu abast en els últims anys.

Inicialment, l'auditor informàtic donava suport als auditors financers per a l'extracció de dades dels sistemes i el seu posterior tractament (p.ex.: comprovacions de coherència i integritat de les dades, replicacions de càlculs d'amortitzacions, etc.).

[1] Llei Oficial de Protecció de Dades

A mesura que els sistemes van anar integrant la totalitat de les tasques de gestió comptable i s'entrellaçaven amb altres processos de negoci, l'auditor informàtic va haver d'anar un pas més enllà i va començar a qüestionar una altra sèrie d'objectius controls:

- Qui accedeix a la informació? Qui en gestiona les autoritzacions?

- Els mecanismes de registre d'esdeveniments proporcionen traçabilitat? (p.ex.: hem de saber quin empleat ha obert un compte corrent o des de quina IP s'ha ordenat una transferència a les illes Caiman)

- S'assegura la disponibilitat de la informació vital i dels sistemes crítics? (p.ex.: moltes empreses poden quedar-se sense web durant una setmana però no poden aguantar tres dies sense l'inventari del magatzem)

- La informació té sentit des d'un punt de vista de negoci? (p. ex: no és coherent comprar 2,37 cadires o vendre per un import negatiu)

A partir d'aquest moment l'auditor informàtic no només necessita conèixer els sistemes d'informació, sinó també el negoci, i cal que s'especialitzi en definir processos de control intern per l'àrea de sistemes.

En aquesta situació, es va definir un conjunt de controls sobre les tecnologies i sistemes d'informació que pretén ser la referència per a qualsevol empresa. Es tracta de l'estàndard *CobIT*[2], definit per la ISACA[3], l'organització que l'actualitza i promociona.

Aquesta ponència parteix de l'estàndard CobIT i analitza per quins controls l'ús de *programari lliure* pot comportar un avantatge respecte a alternatives privatives.

Amb aquesta finalitat s'han analitzat cadascun dels controls proposats per l'estàndard, repartits en els quatre grups següents:

- Planificació i organització
- Adquisició i implementació
- Entrega i suport
- Supervisió i avaluació

2 Estructura del document

Després d'introduir cadascun dels quatre grups analitzats, es presenten aquells controls en què l'ús de programari lliure representa un avantatge o un inconvenient. Han quedat fora de l'abast d'aquesta anàlisi els controls pels quals és indiferent l'ús d'aplicacions lliures o privatives.

Per a cadascun dels controls, es proporciona la següent informació:

- Nom del control

[2] Control Objectives for Information and related Technology

[3] Information System Audit and Control Association

- Breu presentació del control
- Avantatges del programari lliure
- Inconvenients del programari lliure

L'única excepció serà el primer domini (Planificació i organització), ja que per la seva naturalesa estratègica i organitzativa, s'ha analitzat de forma global sense detallar punt per punt.

3 Planificació i organització

El primer grup de control proposa controls que permetin definir el paper de les tecnologies dins de l'organització en funció dels objectius de negoci.

La Direcció de l'organització ha de decidir l'estratègia a seguir en l'àmbit dels sistemes d'informació, de manera que es puguin proporcionar els serveis informàtics que requereixen les diferents àrees de negoci. L'anàlisi dels recursos humans i tècnics necessaris i disponibles resulta indispensable per garantir la qualitat de servei que el negoci necessita (p.ex.: temps de resposta davant d'incidències, costos, etc.).

La definició d'un pla estratègic per l'àrea de sistemes és una eina que permet detectar desviacions respecte als objectius del negoci (p.ex.: una petita botiga de barri no requereix la implantació d'un ERP integral). Per altra banda, l'existència d'aquests documents formalitza i dóna a conèixer internament la tàctica a seguir, i estableix l'abast de l'àrea de sistemes (p.ex.: quin nivell de servei pot cobrir).

Una de les decisions estratègiques que pot tenir gran rellevància és la conveniència d'utilitzar programari lliure o propietari en l'organització. Per prendre una postura determinada, convé tenir en compte les diferències entre aplicacions horitzontals i verticals:

- Les aplicacions horitzontals són aquelles que cobreixen una sèrie de funcionalitats comunes a qualsevol organització. Els sistemes operatius, les aplicacions ofimàtiques, els servidors web i les bases de dades són exemples clars d'aplicacions horitzontals.

  Les organitzacions disposen d'una multitud d'aplicacions lliures que cobreixen aquests aspectes, amb la garantia addicional de representar unes solucions robustes, àmpliament utilitzades a nivell professional i particular. Consegüentment, l'adquisició d'aquest tipus de programari pot representar un avantatge en termes de costos (com analitzarem en els apartats posteriors) o de seguretat tecnològica.

- Les aplicacions verticals són aquelles que cobreixen funcionalitats molt especialitzades i poden representar un valor afegit pel negoci. El terminal financer d'una entitat bancària concreta, o un sistema de gestió de les relacions amb clients (CRM) serien clars exemple d'aplicacions verticals.

  No és freqüent l'alliberació d'aplicacions molt especialitzades donats els problemes de divulgació de propietat intel·lectual i els dubtosos beneficis que es podrien obtenir. Per tant, per segons quins tipus de necessitats especifiques del negoci, no és podran trobar aplicacions lliures que les cobreixin.

Així doncs, l'elecció d'utilitzar programari lliure no és bipolar i és possible la convivència d'aplicacions lliures i privatives en un entorn heterogeni.

Finalment, l'ús d'eines que compleixin els estàndards internacionals o sectorials representa una altra decisió estratègica rellevant. Les possibilitats d'emmagatzemament i d'intercanvi d'informació tant dins com fora de l'organització, depenen fortament de la interoperabilitat dels sistemes tecnològics.

4 Adquisició i implementació

El segon grup de control cobreix la identificació de requeriments tecnològics dels sistemes d'informació, l'adquisició o desenvolupament de nous sistemes i la seva implementació alineada amb els processos de negoci. Paral·lelament, aquestes tasques es veuen complementades per les tasques de manteniment (de programari o bé de maquinari) que permetin prolongar la vida dels actius tecnològics adquirits.

Per dur a terme les tasques presentades, l'estàndard CobIT defineix 7 controls generals en els quals l'ús de programari lliure pot jugar un paper important.

4.1 Identificació de solucions

L'adquisició de programari ha de passar necessàriament per un primer procés d'anàlisi que permeti identificar les necessitats exactes dels processos de negoci que s'han de cobrir. A partir d'aquests requeriments, serà possible prendre la decisió de comprar o desenvolupar una aplicació en funció de:

- Les solucions existents al mercat.
- La relació entre el cost i el benefici que proporcionen les solucions.
- Les característiques i incompatibilitats amb els sistemes ja existents.

Avantatges

- Habitualment el programari lliure pot ser adquirit de forma gratuïta, sent opcional la possibilitat de contractar un proveïdor que ofereixi suport i garanties. Addicionalment, per una única aplicació lliure es possible trobar diverses empreses oferint suport i competint entre elles.

  Aquesta absència d'obligatorietat de contractar un proveïdor junt amb la competència darrera d'una mateixa aplicació ofereixen una gran flexibilitat en l'anàlisi cost – benefici.

- Adquirir programari lliure no genera un vincle indissoluble amb la decisió de prescindir de desenvolupar una solució pròpia. Donades les característiques que ofereix aquest tipus de programari, l'organització té la llibertat de corregir la decisió i reprendre la idea de desenvolupar una nova solució basada en l'aplicació escollida.

- El programari lliure no vincula el suport a un únic proveïdor, per tant si aquest desaparegués o no oferís un servei òptim, sempre pot ser substituït per un altre. D'aquesta forma es garanteix que el cicle de vida de l'aplicació contempli un període considerablement llarg de temps.

- La interoperabilitat i compatibilitat ha sigut tradicionalment un dels objectius del programari lliure, facilitant així la integració amb sistemes ja existents.

Inconvenients

- El programari lliure té una rica varietat d'aplicacions horitzontals, es a dir, aquelles que cobreixen les necessitats bàsiques de gaire bé totes les organitzacions. No obstant, en quant a aplicacions verticals (especialitzades), les possibilitats d'elecció es troben més limitades.

4.2 Adquisició i manteniment de les aplicacions

Un cop escollida la solució tecnològica que es vol adquirir, es necessari establir controls per assegurar que els requeriments inicials es trobaran coberts.

En cas de que es requereixi realitzar alguna adaptació (o si es tracta d'un desenvolupament nou), s'han de traduir els requeriments de negoci a especificacions de disseny sense perdre de vista les següents consideracions:

- L'aplicació ha d'incorporar controls per facilitar la seva auditabilitat.
- L'aplicació ha de garantir la seguretat i la disponibilitat.

Avantatges

- Les solucions basades en programari lliure permeten un accés complet al codi font, oferint una adaptabilitat màxima. Per tant, en base als requeriments, serà possible afegir aquelles funcionalitats i/o controls necessaris.

Inconvenients

- Generalment les aplicacions lliures no disposen d'informació funcional com per exemple diagrames de disseny d'alt nivell. L'estructura de l'aplicació ha de ser entesa a partir del codi font. No obstant, l'activa comunitat que es troba darrera d'aquestes aplicacions (empreses, desenvolupadors, usuaris, etc.) es troba oberta i accessible per ajudar a entendre el funcionament del codi.

4.3 Adquisició i manteniment la infraestructura tecnològica

Entenem per infraestructura tecnològica tot aquell maquinari que permet l'execució i comunicació de les diferents aplicacions (tant en entorns de producció com de desenvolupament). La incorporació de nou programari pot requerir l'adquisició o ampliació de la infraestructura actual i per tant, s'han d'establir controls per tal d'assegurar el nivell de servei adequat al negoci.

Avantatges

- Tradicionalment el programari lliure ha gaudit d'una optimització envejable que permet la seva execució en maquinari amb prestacions limitades. Aquest fet comporta que:
    - Les aplicacions aprofitaran eficientment els recursos tecnològics i tindran uns requeriments de capacitat inferiors per realitzar les mateixes tasques.

- La vida del sistemes tecnològics es pot prolongar, sense obligar a comprar nous equipaments per cada versió nova de l'aplicació (p.ex.: cada nova versió del sistema operatiu GNU/Linux no suposa fortes variacions dels requeriments mínims de capacitat).

Inconvenients

- Un dels inconvenients més significatius que ha arrossegat el programari lliure és l'absència de controladors per a determinats dispositius. Afortunadament, durant els darrers anys i en base a l'èxit creixent d'aquest tipus d'aplicacions, els proveïdors de maquinari estan oferint cada cop més suport pel desenvolupament de controladors.

4.4 Facilitat d'ús

El coneixement de les aplicacions adquirides necessita materialitzar-se en documentació tant pels usuaris com pel personal de suport (p.ex.: HelpDesk). Aquesta ha de representar la base per la formació del personal encarregat de mantenir o interaccionar amb els sistemes.

Avantatges

- L'obtenció o elaboració de la documentació dels sistemes es pot basar en les següents fonts d'informació:
  - Empreses que ofereixen suport i disposen de la seva pròpia documentació.
  - Documentació pública a Internet (articles, HOWTOs, etc.).
  - Comunitats a Internet disposades a resoldre qualsevol dubte i/o problema que es pugui tenir.

Inconvenients

- Tot i que existeixen una bona quantitat de llibres sobre aplicacions lliures, hi ha determinat programari que no disposa de documentació formal i la única font d'informació és la comunitat d'usuaris a Internet.

4.5 Obtenció de recursos tecnològics

Els processos de l'àrea de sistemes sempre requereixen disposar del personal, maquinari, aplicacions i/o serveis adequats. Per tant, convé establir procediments per la selecció de proveïdors i per l'elaboració d'acords contractuals. L'objectiu és poder garantir que els recursos necessaris per l'organització estaran disponibles.

Avantatges

- Per una mateixa solució basada en programari lliure poden existir diverses empreses competint entre si, per tant la selecció de proveïdors es veu enriquida per l'àmplia varietat.

- Entre els acords contractuals no s'hauran d'establir clàusules per definir:

- Qui és el propietari del codi.
- Què ocorreria si el proveïdor desaparegués.

Per la pròpia naturalesa del programari lliure, el codi es trobarà a disposició del client i aquest tindrà la llibertat de canviar de proveïdor si ho considera oportú. Conseqüentment, els acords es simplifiquen significativament.

Inconvenients

- En funció de la llicència de l'aplicació, poden haver-hi problemes si l'organització requereix la implementació d'adaptacions confidencials. Algunes llicències lliures obliguen a publicar les modificacions, tant si es distribueix l'aplicació com si és per ús intern (p.ex.: Affero GPL). Afortunadament aquest tipus de llicències no són les més habituals i només cal publicar les modificacions si la nova aplicació és distribuïda fora de l'organització.

4.6 Gestió de canvis

Tant en la fase de desenvolupament i implantació com en la fase de manteniment, serà necessària la incorporació de canvis al programari (p.ex.: adaptacions, correccions, etc...). Per tant, caldrà establir controls per gestionar procediments d'autorització i prioritzacions, historial de canvis i seguiment de modificacions.

Avantatges

- Els canvis realitzats per empreses o programadors de la comunitat són públicament accessibles per Internet i es gestionen mitjançant sistemes de control de versions (p.ex.: subversion, CVS, etc.), permetent gestionar la traçabilitat dels canvis i la recuperació de versions antigues.
- Habitualment cada aplicació i/o comunitat acostuma a disposar d'un sistema gestor de bugs i correccions (p.ex.: bugzilla, launchpad, etc.) al qual també es pot accedir públicament.
- Existeixen eines lliures complementaries que permetrien a l'empresa instaurar un sistema intern de seguiment de modificacions (p.ex.: bugzilla, subversion, trac, etc.).

Inconvenients

- L'organització no pot exercir un control directe sobre els canvis i modificacions procedents de l'exterior (altres empreses, programadors independents, etc.).

4.7 Instal·lació i acreditació de les solucions/modificacions

Per tal que les aplicacions desenvolupades o adquirides puguin passar a producció i ser utilitzades com a eines de negoci, cal definir:

- Metodologia de proves.
- Planificació de noves versions.
- Sistema d'avaluació i aprovació per part de la direcció.

- Mecanismes per la revisió i validació del resultat després de la implantació.

Avantatges

- El programari lliure compta amb una gran base d'usuaris, fet que repercuteix positivament en la ràpida identificació / correcció d'errors i millora de la robustesa.

5 Entrega i suport

El tercer grup de control es centralitza en l'execució d'aplicacions que ofereixen serveis a les diferents àrees de negoci. Així doncs, els processos de suport que asseguren l'eficàcia i eficiència dels sistemes d'informació (formació d'usuaris, monitorització de sistemes i aspectes de seguretat inclosos) es converteixen en el centre d'atencio d'aquest apartat.

En aquest grup es presentaran 5 dels 13 controls definits a l'estàndard CobIT, ja que només en aquests impacta la decisió d'utilitzar programari lliure o privatiu.

5.1 Gestió del rendiment i la capacitat

Per tal de garantir els nivells de servei acordats, caldrà revisar periòdicament el rendiment i les capacitats dels recursos tecnològics. Addicionalment serà necessari realitzar prediccions a futur que mostrin l'increment de les necessitats en funció de la càrrega de treball, la capacitat d'emmagatzematge i els requeriments de contingència.

Avantatges

- Tal i com ja s'ha indicat en punts anteriors, el programari lliure ha centralitzat molts esforços en optimitzar el rendiment (fins i tot en maquinari obsolet). Addicionalment, moltes aplicacions han sigut dissenyades per a escalar correctament en entorns de forta demanda.

5.2 Garantir la seguretat dels sistemes

La integritat i confidencialitat de la informació són un element clau de qualsevol sistema tecnològic. Per tal de minimitzar riscs, s'han d'establir i mantenir unes polítiques de seguretat tecnològica que permetin identificar rols d'ús, responsabilitats i procediments.

Addicionalment es requerirà la realització de tasques de supervisió periòdiques per identificar debilitats o incidències. L'objectiu que es persegueix inclou la reducció de la probabilitat de patir incidències de seguretat i la mitigació de l'impacte en cas de que els riscos es materialitzin.

Avantatges

- La seguretat és un del punts forts del programari lliure. La gran base d'usuaris existents que proven i reporten errors funcionals, i el gran nombre de programadors arreu del món que verifiquen la qualitat del codi generat, permet assolir una robustesa i confiabilitat difícil d'aconseguir per altres mitjans.

Inconvenients

- Els projectes de programari lliure es gestionen de forma independent per tots els membres que els conformen (empreses, programadors independents, etc.), de manera que l'empresa no pot definir mesures de control sobre el desenvolupament. De tota manera, els responsables dels projectes sí que estableixen mesures de control que són adequades per la majoria d'empreses.

5.3 Formació d'usuaris

Amb la finalitat de reduir errors, problemes de productivitat i incompliments amb els aspectes clau de seguretat, cal establir un procés que identifiqui les necessitats de formació en funció de la tipologia d'usuaris.

Addicionalment serà necessari la definició i execució d'una estratègia per la formació efectiva i la supervisió dels resultats.

Avantatges

- Tal i com s'ha indicat en el punt "Facilitat d'ús", el programari lliure disposa de diverses fonts d'informació que permeten l'elaboració de documentació o fins i tot, l'auto-formació d'usuaris.

5.4 Gestió de la configuració

Les diferents configuracions dels sistemes físics i del programari han de ser gestionats mitjançant un repositori auditable que permeti la recuperació d'estats anteriors. Per tal d'aconseguir aquest objectiu cal establir un procés encarregat d'identificar les configuracions i gestionar la seva actualització, incloent la revisió i supervisió de llicències d'ús de les aplicacions privatives.

Avantatges

- Les configuracions del sistemes basats en programari lliure acostumen a ser transparent, i per tant faciliten la gestió.

- Existeixen eines lliures que permeten mantenir historial de fitxers de configuracions (p.ex.: subversion).

- Donada la naturalesa del programari lliure, no és necessari gestionar i controlar el nombre de llicencies d'ús comprades ja que aquestes pertanyen exclusivament a l'àmbit del programari privatiu.

5.5 Gestió de dades

Amb la finalitat de garantir la qualitat i disponibilitat de les dades de negoci és necessari establir procediments per gestionar la realització de copies de seguretat i la seva recuperació.

Per tal de poder portar a terme aquestes tasques, existeixen eines lliures que permeten la realització de còpies de seguretat de forma periòdica i centralitzada.

6 Supervisió i avaluació

El quart i últim grup de control es focalitza en la supervisió del sistemes tecnològics per tal de:

- Garantir la seva alineació amb l'estratègia del negoci
- Verificar desviacions en base als acords de nivell de servei
- Validar el compliment del requeriments regulatoris (p.ex.: LOPD).

Aquesta supervisió implica paral·lelament la verificació dels processos de control per part dels auditors, que poden oferir una visió objectiva del la situació real, a diferència de la persona que s'encarrega d'operar el procés de control.

En aquest grup es presentaran 3 dels 4 controls definits per l'estàndard CobiT, donat que només en aquests impacta la decisió d'utilitzar programari lliure o privatiu.

6.1 Supervisió i avaluació del rendiment dels sistemes

Donada la necessitat de garantir la màxima eficàcia i eficiència del sistema, es requereix establir processos de supervisió que reportin i controlin de forma sistemàtica els indicadors clau de rendiment.

Aquesta informació podrà ser comparada amb els acords i les politiques establertes en alineació amb l'estratègia del negoci.

Per tal de poder portar a terme aquestes tasques, existeixen eines lliures de supervisió remota d'equips i serveis que permeten verificar el correcte funcionament dels servidors.

6.2 Supervisió i avaluació del control intern

La informació dels sistemes tecnològics representen un dels valors més importants de l'organització, per aquest motiu es requereix establir controls que validin tots els tractaments de dades. Si es detecten excepcions, aquestes hauran de ser reportades i revisades per tal de garantir la màxima integritat i coherència de la informació.

Avantatges

- L'accés al codi font de les aplicacions lliures facilita la implantació de controls a mida (en funció dels requeriments del negoci).

- Existeixen eines lliures que permeten als auditors desenvolupar part del seu treball.

6.3 Garantir el compliment regulatori

En funció de l'activitat de l'organització es requerirà validar el compliment de lleis i regulacions del sector. S'haurà de definir un procés que prengui com a objectius:

- Identificar requeriments legals i regulatoris relacionats amb les tecnologies.
- Avaluar l'impacte del requeriments regulatoris.
- Supervisar periòdicament el compliment del requeriments regulatoris.

Avantatges

- Tradicionalment, per tal de garantir interoperabilitat i transparència, el programari lliure ha basat el seu desenvolupament i les seves funcionalitats en estàndards i regulacions definides per organismes independents. (p.ex.: la Llei de Serveis de la Societat de la Informació i de Comerç Electrònic requereix que les pàgines web de l'administració siguin accessibles i compleixin els estàndards del W3C[4])

7 Conclusions

Les aplicacions informàtiques d'una organització poden ser catalogades en dos grans grups:

- Aplicacions horitzontals: Programari de base que suporta el negoci però no li aporta cap valor afegit. Inclou els sistemes operatius, les aplicacions ofimàtiques, els servidors web i les bases de dades entre altres.

- Aplicacions verticals: Programari especialitzat en funció del tipus de negoci (p.ex.: terminal financer d'una entitat bancària).

El programari lliure disposa d'un ampli ventall de productes que poden cobrir bona part de les aplicacions horitzontals, presentant aspectes que repercuteixen positivament en el control intern de les empreses, afavorint l'opinió de l'auditor. El seu caràcter obert facilita la interoperabilitat, el seguiment dels canvis i la detecció d'errors, proporcionant eines per la millora de l'eficàcia i eficiència dels processos de les organitzacions.

D'altra banda, les aplicacions verticals poden ser cobertes mitjançant l'ús d'aplicacions privatives o desenvolupaments a mida. Els avantatges associats a l'ús de programari lliure habitualment no compensen la divulgació de propietat intel·lectual que es dóna al publicar aplicacions especialitzades de valor afegit per al negoci.

Així doncs, l'elecció d'utilitzar/desenvolupar programari lliure no és una qüestió dicotòmica i és possible la configuració d'entorns heterogenis en què convisquin aplicacions lliures i privatives, aprofitant els avantatges que ofereixen cadascuna de les alternatives i minimitzant els possibles inconvenients.

8 Bibliografia

[1] Fernando Pons Ortega (Soci de Deloitte). *Auditoría Informática, una aproximación a la mejora del Control Interno*. 2007.

[2] ISACA. *CobiT framework 4.0*. 2005.

[4] World Wide Web Consortium