Operacions de serveis de SI/TI

Dídac López
Ferran Martí

PID_00207654

Universitat Oberta de Catalunya

Índex

Introducció

En aquest mòdul d'operacions del servei de SI/TI descriurem un conjunt de processos (gestió d'incidències, gestió de configuració i gestió de seguretat) i les activitats relacionades amb l'arquitectura tecnològica (maquinari, programari, xarxes, dades, etc.) que formen part del dia a dia de les operacions del servei, orientats a proporcionar el lliurament i l'ús del servei.

Els serveis de TI dels entorns de producció disposen d'activitats operacionals per a assegurar que la tecnologia està alineada globalment amb el servei i amb els objectius dels processos. Les activitats que esmentarem són descrites de vegades com a processos, però en realitat es tracta d'activitats tècniques especialitzades.

Les activitats operacionals tenen l'objectiu principal d'assegurar que la tecnologia requerida per al lliurament i suport de serveis operi de manera eficaç i eficient.

És important tenir en compte que el conjunt d'activitats d'operació de servei no tenen l'objectiu de gestionar la tecnologia per a disposar d'un bon rendiment, sinó aconseguir el rendiment que integrarà els components de tecnologia amb les persones i processos que fan falta per a assolir els objectius de negoci i de servei.

Entre les activitats d'operacions més comunes hi ha les següents:

- Monitoratge i control.
- Gestió de consoles i ponts d'operació remots.
- Planificació de tasques (*job scheduling*).
- Còpies de seguretat i restauració.
- Gestió d'impressió.
- Gestió i suport de servidors i ordinadors centrals (*mainframes*).
- Gestió de xarxes.
- Gestió de l'emmagatzematge (*storage*) i arxivament.

- Administració de bases de dades.
- Gestió dels serveis de directori.
- Suport de dispositius mòbils i d'escriptori.
- Gestió de programari intermediari (*middleware*).
- Gestió d'Internet i webs.
- Gestió d'instal·lacions.

És important no confondre les activitats agrupades que acabem d'assenyalar amb departaments. Pot ser que en determinades organitzacions les activitats les duguin a terme departaments especialitzats, però es pot esdevenir que un departament sigui el responsable d'una o més d'una d'aquestes activitats. En tot cas, la tasca de decidir la manera com es departamentalitzen les activitats esmentades correspon a l'estructura organitzativa de cada empresa.

Objectius

L'objectiu principal d'aquest mòdul és observar la manera com s'han de garantir determinats processos perquè els serveis puguin funcionar adequadament. És impossible que els serveis siguin perfectes, ja que els errors formen part de l'existència dels serveis, i per tant hi ha d'haver mecanismes que assegurin que aquests errors es poden reparar.

Després d'haver llegit aquest mòdul, heu d'haver assolit els objectius d'aprenentatge següents:

1. Saber que l'entorn tecnològic, incloent-hi l'evolució corresponent, s'ha de considerar un element per a actualitzar la gestió de les operacions.

2. Conèixer detalladament el procés de gestió de les incidències.

3. Distingir de quina manera pot contribuir el procés de gestió de la configuració a fer que la gestió operacional sigui molt més eficient.

4. Conèixer detalladament el procés de gestió de la seguretat.

1. Entorn tecnològic

A més de les activitats operatives esmentades en l'apartat anterior, cal que formi part de les operacions diàries dels serveis la supervisió de les tendències tecnològiques que apareixen en el mercat.

És de sobres sabut que els períodes d'actualització de versions d'aplicacions són molt curts. S'esdevé el mateix, encara que amb uns períodes més llargs, en la infraestructura (maquinari i xarxes). El fet de no incorporar les noves versions pot convertir l'arquitectura tecnològica en un element obsolet que comprometi els resultats que necessita el negoci. Alhora, però, cal considerar un altre factor important que consisteix a no introduir en els entorns de producció tecnologies que no estiguin prou provades i consolidades per a poder assegurar l'estabilitat de la infraestructura.

Una bona gestió del context tecnològic passa per estar atents a les evolucions i oportunitats que ofereixen els avenços tecnològics i per anar-les incorporant a les arquitectures quan es consideri que l'equilibri de cost-risc i benefici és favorable als interessos dels clients.

Una reflexió addicional que cal tenir en compte per a la gestió de l'entorn tecnològic és la tria de solucions obertes[1], és a dir, no exclusives d'un sol proveïdor que no siguin compatibles amb altres entorns o fabricants. L'adquisició de solucions tancades, encara que puguin oferir característiques molt particulars no trobades en altres alternatives, té l'enorme desavantatge de no poder evolucionar fora del marc del proveïdor. Es pot interpretar com una manera d'encadenar-se, i s'incrementa el risc de falta de continuïtat si el proveïdor desapareix. Es torna a imposar el criteri fruit d'una avaluació de l'equilibri entre obtenir resultats molt concrets i estar subjecte, amb el risc que això comporta, a un únic fabricant.

(1)Solucions obertes (*open source*).

2. Gestió d'incidències

La gestió d'incidències és un procés important dins les operacions del servei. De fet, fins i tot de manera informal, sol ser el procés que està més desenvolupat dins els departaments de TI.

Els objectius principals del procés de gestió d'incidències són restaurar les operacions normals de servei i minimitzar l'impacte advers que tinguin les incidències. Per la seva pròpia naturalesa, es tracta d'un procés purament reactiu, això és, reacciona quan les incidències ja s'han produït, i per tant no les ha pogudes evitar.

En aquest punt és important recordar que sol recaure sobre un altre procés, el de **gestió de problemes**, la recerca de les causes que originen les incidències i la possible extirpació corresponent mitjançant el desenvolupament d'una solució definitiva.

El valor que aporta aquest procés resideix en la capacitat que té per a recuperar de seguida una situació de normalitat quan algun aspecte del servei no funciona bé. Des del punt de vista de l'usuari final, és un procés important perquè permet assegurar que la infraestructura tecnològica té un suport i una supervisió. Probablement entra dins la lògica que els recursos o les configuracions corresponents no siguin perfectes, però no hi entraria tant que no hi hagués els grups de suport adequats per a mirar de corregir les situacions d'error que permetin que els processos de negoci s'executin amb normalitat.

Malgrat això, cal destacar que aquest procés està molt lligat al factor temporal, és a dir, normalment al temps de resolució de les incidències. Un error comú consisteix a obstinar-se a corregir del tot la incidència sense tenir en compte que el més important és restaurar ràpidament el servei. Per tant, encara que es pugui esdevenir que es trobin solucions definitives a les incidències dins els temps acordats, el que és habitual és resoldre les incidències amb solucions provisionals. De vegades aquest darrer punt és mal interpretat, en el sentit que es corregeixen les situacions amb nyaps. Aquest no és el sentit correcte. Les solucions provisionals (*workarounds*) permeten restaurar el servei, i en funció de la naturalesa, repetició i impacte de la incidència, es tractarà el tema més a fons, mitjançant l'obertura d'un problema, per a trobar-ne la causa i poder-la eliminar d'arrel. Ha de quedar clar que tota incidència té una o més d'una causa oculta que la genera, però que no sempre caldrà cercar-la. Només quan sigui útil per al negoci en termes de temps i recursos emprats en relació amb el benefici que se'n pot treure.

Centre d'atenció a l'usuari: canal de comunicació de les incidències

En la resolució de les incidències apareixen clarament diverses funcions. El centre d'atenció a l'usuari (*service desk*, CAU) té un paper molt important com a únic punt de contacte (*single point of contact*, SPOC), és a dir, com a canal únic per mitjà del qual haurien de fer constar les queixes, incidències o reclamacions els usuaris. Es recomana que la comunicació d'incidències al proveïdor del servei es faci sempre per mitjà d'aquest canal i no d'especialistes. Entre d'altres, s'enumeren els avantatges següents:

- És més improbable que les incidències quedin desateses. Si una incidència arriba a un especialista pot ser que no quedi registrada i que es quedi oblidada damunt la taula.

- Queda un registre únic i unificat que facilita la gestió durant i després de les incidències.

- És més fàcil assignar la incidència a l'especialista que correspon perquè resolgui la incidència. El criteri de tria d'especialista dels usuaris no sol ser vàlid per desconeixement de l'àrea d'especialització.

- És més fàcil gestionar adequadament els recursos i tenir sempre una resposta. L'assignació de les incidències es fa d'acord amb criteris de disponibilitat dels especialistes.

- S'evita matar mosques a canonades. Si el criteri d'assignació d'una incidència és a càrrec de l'usuari, es pot esdevenir que es posi en contacte amb algun recurs que ha de prioritzar altres aspectes.

Des del punt de vista de l'usuari, la perspectiva no sol ser la mateixa. L'usuari considera que és atès amb més eficàcia i rapidesa quan parla directament amb un especialista. Pot ser que segons com no els falti raó, però les conseqüències que es poden derivar de la llista anterior –que no és exhaustiva– aconsellen optar com a millor pràctica per un model centralitzat en el CAU. Perquè l'usuari no percebi una minva en la qualitat del suport rebut, cal que el CAU estigui configurat i format d'acord amb les necessitats específiques. Un CAU que es limiti a dirigir trucades sense aportar cap valor afegit costarà molt que sigui vist com una millora en la qualitat, per més que ho recomanin els marcs de referència de millors pràctiques.

Responsabilitats del centre d'atenció a l'usuari en la gestió d'incidències

Les funcions del CAU es poden agrupar en registrar la incidència i, si pot ser, resoldre-la en primera línia o, si no, escalar-la a la línia de suport.

a) Registrar la incidència

Dins les responsabilitats del CAU, a més de rebre incidències per molts canals (telèfon, correu electrònic, formulari web, etc.), hi ha la de registrar, categoritzar i prioritzar les incidències. La categoria consisteix a facilitar la classificació d'acord amb el tipus d'element d'infraestructura que falla; per això és molt recomanable disposar d'una eina que estigui integrada en una base de dades de gestió de la configuració, on poden aparèixer tots els elements que constitueixen la infraestructura tecnològica. Per la seva banda, la priorització consisteix a assignar un valor que determinarà l'ordre i els temps compromesos en què s'ha resoldre una incidència. Se sol suggerir que el valor de la prioritat estigui determinat per un valor d'impacte i un d'urgència. L'impacte determina el nombre d'usuaris que es poden veure afectats i també la severitat o criticitat que té el servei sobre el negoci. La urgència, en canvi, determina la demora acceptable sense que es resolgui la incidència.

b) Resoldre en primera línia

El CAU també té la responsabilitat de mirar de fer un diagnòstic inicial i, si pot ser, trobar una solució provisional o definitiva. Per a fer-ho, es pot basar en la seva pròpia experiència o en la consulta a una base de dades de coneixement en què es recullin moltes solucions provisionals i definitives d'incidències que s'han esdevingut en el passat. A més de mirar de trobar una solució, es pot delimitar l'abast de la incidència, i aquesta informació ha de quedar registrada amb l'objectiu que, si fa falta un escalat funcional, els equips que rebin l'assignació puguin disposar de tanta informació com es pugui.

És desitjable que la taxa de resolució en primera línia, això és, en el CAU, sigui tan elevada com sigui possible. Com més a prop sigui del 100% d'incidències resoltes sense necessitat d'escalat, més credibilitat, eficiència i rapidesa de resolució generarà entre els usuaris. Hi ha diferents elements que poden facilitar l'increment d'aquesta taxa, entre els quals hi ha l'accés fàcil a una base de dades de coneixement actualitzada i ajustada al propòsit, la formació tècnica dels operadors, i la creació, documentació, formació i conscienciació dels procediments d'ús.

c) Escalar la incidència

Quan la resolució en primera línia no es pugui fer, el procés d'incidències continuarà en alguna de les línies de suport que rebran l'assignació. De línies de suport n'hi ha sobretot pel que fa a l'especialització que tinguin. Per tant, una vegada reben l'avís d'incidència assignada, han de trobar una solució provisional dins els temps assignats en funció de la prioritat establerta. S'insisteix a no confondre l'escalat funcional que acabem de descriure amb l'objectiu de trobar la causa. A una línia de suport d'incidències no li correspon trobar la causa, sinó trobar una solució que recuperi el servei tan aviat com sigui possible.

Tant si la solució provisional o definitiva la troba el CAU com alguna de les línies de suport addicionals, el pas següent consisteix a resoldre i recuperar el servei, és a dir, a construir la solució si cal i aplicar-la a l'entorn de producció. El pas final del procés és tancar les incidències. El tancament és, en principi, una responsabilitat de l'operador del CAU i consisteix a validar –amb el mètode que es consideri oportú– que l'usuari està satisfet amb la solució aplicada i a acabar de documentar adequadament.

Una gestió adequada de les incidències és clau perquè les operacions del servei siguin correctes. Si no es resolen les incidències dins els intervals acordats amb el negoci, atesa la visibilitat tan directa que té una interrupció de servei, tindrà un impacte molt negatiu sobre la credibilitat i la capacitat del proveïdor del servei.

Més amunt hem parlat del fet que cal acordar els temps amb el negoci. Aquest aspecte és fonamental si no volem que la gestió d'incidències acabi essent un caos, en què el criteri estarà basat més en la gestió de decibels –és a dir, qui crida més– que no pas en la lògica marcada per la necessitat del negoci. Per tant, un factor crític d'èxit consisteix a assegurar que hi hagi acords de nivell de servei i que, a més, recullin com es tractaran les incidències, en funció de la prioritat assignada. Aquests acords de nivell de servei s'haurien de negociar en la fase de disseny del servei i de recollir en un document formal, dit *acord de nivell de servei* (*service level agreement*, SLA), que han de signar les dues parts, client i proveïdor.

És habitual que el mateix procés de gestió d'incidències, per mitjà del CAU, sigui el que s'encarrega de gestionar també peticions de servei, queixes, consultes i reclamacions. No obstant això, algunes de les referències de millors pràctiques, com és ara ITIL® a partir de la versió 3 o una de superior, recomanen fer una gestió diferent malgrat que comparteixen la funció del CAU. Per tant, la gestió d'incidències s'hauria d'ocupar només de tractar les interrupcions no planificades d'un servei o les reduccions en la qualitat corresponents. S'aconsella que les peticions de servei, les queixes, les consultes i les reclamacions es tractin mitjançant el procés de gestió de peticions de servei. Finalment, les peticions de canvi s'haurien de tractar mitjançant el procés de gestió de canvis. El CAU que actua com a punt comú per a cadascun dels casos esmentats és qui ha d'identificar adequadament cada cas i posar en marxa el procés oportú.

Vegeu també

Hem tractat de les peticions de servei en l'apartat 2, "Peticions de servei", del mòdul "Provisió de serveis de SI/TI".

3. Gestió de la configuració

El procés de gestió de la configuració, mitjançant les eines de gestió adequades, vol posar a disposició de tots els processos i funcions un repositori de coneixement que faciliti la presa de decisions i també la gestió global dels serveis.

Un coneixement essencial que ajuda a prendre decisions ràpides i correctes és, sens dubte, saber quins són els elements que constitueixen la infraestructura tecnològica que dóna suport als serveis que calen per a executar els processos de negoci i, encara més important, saber de quina manera estan relacionats entre si aquests components i com depenen els uns dels altres. El propòsit del procés de gestió de la configuració és fonamentalment el que hem descrit en aquest paràgraf.

El marc de referència ITIL® fa servir tres capes diferents per a definir els continguts del sistema de configuració: base de dades de gestió de la configuració, sistema de gestió de la configuració i sistema de gestió del coneixement del servei.

En primer lloc apareix la **base de dades de gestió de la configuració** (*configuration management database*, CMDB), que conté els elements de configuració (*configuration item*, CI).

Per **elements de configuració** s'hi ha d'entendre qualsevol recurs que calgui per al lliurament i suport del servei i la modificació del qual pugui tenir un impacte, de la mena que sigui, sobre la qualitat del servei. Per tant, dins aquesta definició hi podem considerar servidors, encaminadors (*routers*), commutadors (*switchers*), aplicacions, mòduls, discos, etc.

En principi, el nivell de detall –per tant, el desglossament dels CI constituïts per altres CI– és una de les decisions importants a l'hora de dissenyar la CMDB. I això és així perquè cal arribar a un equilibri entre la quantitat d'informació introduïda i l'esforç que es requereix per a tenir-la actualitzada. S'ha de tenir en compte que un element fonamental d'una bona gestió de la configuració és que la informació estigui al dia; si no, les decisions que es prenguin basades en la CMDB poden ser errònies, i per tant el fet de disposar d'aquest tipus de sistemes deixa de generar valor afegit.

S'ha de tenir en compte també que els CI que integren una CMDB no són només tecnològics, que és el que es podria deduir de la llista que hem presentat en el paràgraf anterior. També pot ser un CI la definició d'un servei, o d'un contracte, o d'un proveïdor, o d'un usuari, o d'un departament, o d'un edifici, etc. Per tant, una CMDB conté informació dels elements tecnològics i de gestió que els acompanyen. A més, tal com hem explicat més amunt, el més rellevant és la definició de les relacions entre els diversos CI. La tipologia de relacions pot ser molt variada amb l'objectiu de representar les dependències que hi ha.

Una CMDB conté informació dels elements tecnològics i de gestió que els acompanyen, i de la relació que hi ha entre els elements de configuració.

La segona capa es coneix amb el nom de **sistema de gestió de la configuració** (*configuration management system*, CMS). Aquesta capa inclou l'anterior, però la complementa sobretot amb informació de gestió que hi està associada. Per exemple, el registre d'incidències pot estar vinculat cas per cas amb els CI de la CMDB. També pot estar relacionat amb el registre de problemes i amb el de canvis. Per tant, es pot pensar en un sistema més extens que no solament descriu la tipologia de l'arquitectura tecnològica sinó que, a més, es pot disposar –i en conseqüència gestionar-los– de tots els elements relatius al comportament, a la modificació i a l'addició d'elements. Una dificultat que pot tenir passar a la pràctica aquests conceptes és la de dur a terme un creixement controlat de la informació de manera que continuï essent útil. Quan els vincles entre diferents sistemes de gestió s'estableixen sense un criteri ben fixat, es pot esdevenir que no obtinguem el valor esperat. Per tant, els projectes de posada en marxa de CMS han de tenir present com es produeix el creixement.

La tercera capa es coneix amb el nom de **sistema de gestió del coneixement del servei** (*service knowledge management system*, SKMS). Aquesta capa inclou, a més de les altres dues, tots els repositoris que continguin coneixement sobre experiència, perfils i habilitats que puguin fer servei per a prendre decisions.

És útil relacionar el sistema de capes anterior amb l'anomenat *model DIKW* (*data*, *information*, *knowledge*, *wisdom*, dades, informació, coneixement i saviesa) proposat en el procés de gestió del coneixement d'ITIL®. En realitat es tracta d'un procés de transformació que parteix de la capa més elemental, la de dades, fins a la més sofisticada, la de saviesa. La transformació es duu a terme partint de l'increment, o bé de la comprensió, o bé de la contextualització.

Exemple

Un sistema de CMDB que només ens proporciona una fitxa descriptiva d'un encaminador aïllat sigui un element de la capa de dades. Malgrat això, aquest mateix ítem acompanyat de l'historial d'incidències associat no solament a aquest encaminador sinó també a d'altres, juntament amb informació recollida d'altres processos, podria complementar adequadament una presa de decisió que correspon a la capa de saviesa.

Actualment al mercat hi ha eines molt potents que permeten crear CMDB de força entitat. A més, algunes d'aquestes eines són gratuïtes, encara que requereixen un grau de configuració que potser no està a l'abast de tothom. Les eines de configuració les solen acompanyar les dites *eines de descobriment* (*discovery tools*), que proporcionen en temps real informació sobre el maquinari i programari que hi ha en una determinada infraestructura. A més, permeten fer alertes quan es detecta una discrepància entre la infraestructura real i la documentada en la CMDB, de manera que calgui posar en marxa un procés de reconciliació.

Les activitats principals del procés de gestió de la configuració són la planificació, la identificació, el control, la gestió d'informació i l'auditoria.

- Les activitats de **planificació** i **identificació** estan relacionades amb el fet de planificar i definir tots els elements que integraran la CMDB, i també amb els tipus i la nomenclatura que tindran.

- L'activitat de **control** està més relacionada amb el fet de descriure els procediments que assegurin que cada modificació d'un CI tingui garantida l'actualització de la base de dades. Això requereix un nivell de coordinació important amb el procés de gestió del canvi.

- L'activitat de **gestió de la informació** està relacionada amb el fet de proporcionar el coneixement requerit a la persona adequada quan li cal.

- L'activitat d'**auditoria** té la finalitat d'assegurar que hi ha mecanismes que comproven que la informació continguda en la CMDB és vigent.

Costa entendre que hi ha un procés de gestió de la configuració sense que hi hagi en paral·lel un procés de gestió del canvi. Bàsicament, perquè cal tenir un control adequat que asseguri que qualsevol modificació, addició o supressió d'un CI ha d'estar reflectida en la base de dades; si no, és clar que els continguts poden acabar essent obsolets de seguida i, així, invalidar per complet l'objectiu principal del procés.

La planificació d'un procés de gestió de configuració ha de tenir en compte, entre altres factors, la diversitat i magnitud de la plataforma tecnològica, el fet que hi hagi o no agents que informin sobre el descobriment, les persones que es podran dedicar a recollir i validar informació almenys en una etapa inicial d'abocament (*population*) de la base de dades, les eines de què es disposa, el nivell de detall que es vol aconseguir. En general, se sol recomanar que el començament d'aquests projectes es faci de manera gradual. És a dir, es comença en un àmbit reduït (per exemple, determinant els serveis que són més adequats per al retorn que pot ocasionar controlar-los mitjançant una CMDB) i amb un nivell de detall que sigui assumible en vista de la quantitat de recursos

de què es disposi. A partir d'aquest començament i a mesura que es demostri la viabilitat i retorn del projecte es pot anar incrementant el nombre de serveis que s'hi inclouen o qualsevol altre criteri que s'hagi considerat oportú.

La denominació actual del procés de gestió de la configuració tal com apareix en la darrera actualització d'ITIL® és **gestió de la configuració i dels actius de servei** (*service asset and configuration management*, SACM). Per *actiu de servei* s'hi poden entendre, de manera general, els recursos i les capacitats, però sol quedar reduït al primer bloc. Per tant, en referir-nos a la gestió d'actius, se sol interpretar com el control d'inventari dels recursos. Així, doncs, la gestió de la configuració té un propòsit més extens, ja que en el conjunt de detalls financers relatius als recursos s'hi consideren les relacions i, per tant, les dependències corresponents, de manera que dóna una capa més gran d'informació que afavoreix la presa de decisions.

4. Gestió de la seguretat

Sovint la seguretat s'ha definit com una actitud, com un estat d'ànim, que fa que s'hi impliqui tota l'organització i en tots els aspectes, i que, com la qualitat, comença per la mateixa actitud de l'organització, i no solament dels serveis de SI/TI.

La seguretat s'ha d'aplicar d'extrem a extrem, des dels recursos i les infraestructures connectats fins al disseny mateix dels serveis i les aplicacions amb què funcionen. Disposar d'una gestió de dades i informació segura implica adoptar de manera global aquesta actitud, i més en el moment en què la seguretat de la informació és clau per al negoci.

La seguretat de la informació, consubstancial al negoci, es fonamenta en els punts següents:

- **Confidencialitat**: la informació només ha de ser accessible als destinataris predeterminats.
- **Integritat**: la informació ha de ser correcta i completa.
- **Disponibilitat**: hem de tenir accés a la informació quan la necessitem.

La gestió de la seguretat ha de vetllar perquè la informació sigui correcta i completa, estigui sempre a disposició del negoci i la faci servir només aquella gent que hi està autoritzada.

La gestió de la seguretat és un dels aspectes essencials per a obtenir alts nivells de fiabilitat i disponibilitat, i tan important és determinar quan serà disponible el servei com qui i com el farà servir. La disponibilitat i la seguretat són interdependents i qualsevol fallada en una afectarà greument l'altra.

Les mesures preventives requereixen una anàlisi detallada prèvia de riscos i vulnerabilitats. N'hi ha que tindran un caràcter general (incendis, desastres naturals, etc.) i n'hi ha que tindran un caràcter estrictament tecnològic (fallada de sistemes d'emmagatzematge, atacs de *hackers*, virus informàtics, etc.).

La prevenció adequada dels riscos de caràcter general depèn de la coherència amb la gestió de la continuïtat del negoci i requereix mesures que impliquen la infraestructura de l'organització.

Els objectius principals de la gestió de la seguretat es resumeixen en les accions següents:

- Dissenyar una política de seguretat, en col·laboració amb clients i proveïdors, ben alineada amb les necessitats del negoci.
- Assegurar el compliment dels estàndards de seguretat acordats en els SLA.
- Minimitzar els riscos de seguretat que amenacin la continuïtat del servei.

La gestió correcta de la seguretat no és responsabilitat, almenys exclusivament, de responsables de la seguretat, que desconeixen els altres processos de negoci. Si caiem en la temptació d'establir la seguretat com una prioritat en si mateixa, limitarem les oportunitats de negoci que ens ofereix el flux d'informació entre els agents implicats i l'obertura de noves xarxes i nous canals de comunicació.

La gestió de la seguretat ha de conèixer a fons el negoci i els serveis que presta el departament de SI/TI, per a establir protocols de seguretat que assegurin que la informació sigui accessible quan calgui per als qui estiguin autoritzats a fer-la servir.

Una vegada entesos quins són els requisits de seguretat del negoci, la gestió de la seguretat ha de supervisar que aquests requisits estiguin plasmats convenientment en els SLA corresponents per a garantir-ne, tot seguit, el compliment.

La gestió de la seguretat també ha de tenir en compte els riscos generals a què està exposada la infraestructura de TI, i que no han pas de figurar per força en un SLA, per a assegurar, en la mesura del possible, que no representen un perill per a la continuïtat del servei.

És important que la gestió de la seguretat sigui proactiva i avaluï *a priori* els riscos de seguretat que poden comportar els canvis fets en la infraestructura, les noves línies de negoci, etc.

Perquè aquesta col·laboració sigui eficaç, cal que la gestió de la seguretat:

- Estableixi una clara i definida política de seguretat que serveixi de guia a tots els altres processos.
- Elabori un pla de seguretat que inclogui els nivells de seguretat adequats tant en els serveis prestats als clients com en els acords de servei signats amb proveïdors interns i externs.

- Implementi el pla de seguretat.
- Monitori i avaluï el compliment d'aquest pla.
- Supervisi proactivament els nivells de seguretat analitzant tendències, nous riscos i vulnerabilitats.
- Faci periòdicament auditories de seguretat.

És imprescindible disposar d'un marc general per a enquadrar tots els subprocessos associats a la gestió de la seguretat. La complexitat i les nombroses interrelacions que tenen han de tenir una política global clara en què es fixin aspectes com els objectius, les responsabilitats i els recursos.

En particular, la política de seguretat ha de determinar els punts següents:

- La relació amb la política general del negoci.
- La coordinació amb els altres processos de TI.
- Els protocols d'accés a la informació.
- Els procediments d'anàlisi de riscos.
- Els programes de formació.
- El nivell de monitoratge de la seguretat.
- Els informes que cal emetre periòdicament.
- L'abast del pla de seguretat.
- L'estructura i els responsables del procés de gestió de la seguretat.
- Els processos i procediments emprats.
- Els responsables de cada subprocés.
- Els auditors externs i interns de seguretat.
- Els recursos necessaris: programari, maquinari i personal.

L'objectiu del pla de seguretat és fixar els nivells de seguretat que cal incloure com a part dels acords de nivell de servei, dels acords de nivell de servei interns i dels acords de nivell de servei externs.

Aquest pla s'ha d'elaborar en col·laboració amb el responsable de la gestió del nivell de servei, que és el responsable en darrera instància tant de la qualitat del servei prestat als clients com de la del servei rebut per la mateixa organització de TI i pels proveïdors externs.

El pla de seguretat s'ha de dissenyar amb la finalitat d'oferir un servei més bo i més segur al client, i no pas mai com un obstacle per al desenvolupament de les seves activitats de negoci.

Una bona gestió de la seguretat s'ha de traduir en els objectius següents:

- Que disminueixi el nombre d'incidents relacionats amb la seguretat.
- Que el personal autoritzat tingui un accés eficient a la informació.
- Que hi hagi una gestió proactiva, que permeti identificar vulnerabilitats potencials abans no es manifestin i provoquin una seriosa degradació de la qualitat del servei.

Resum

En aquest mòdul s'han descrit els processos més rellevants que proporcionen el suport i conjunt d'activitats operatives més habituals que garanteixen que els usuaris puguin ser atesos adequadament mentre es lliura el servei.

Bibliografia

Clayton, I. M. (2008). *The Guide to the Universal Service Management Body of Knowledge: A Definitive Guide to Service Management*. Service Management 101.

Du Moulin, T. (2005). *What Does IT Cost? Viewpoint, Focus On: CMDB* (vol. 1, pàg. 1-7). BMC Software.

Du Moulin, T.; Flores, R.; Fine, B. (2008). *Defining IT Success Through The Service Catalog: A Practical Guide* (2a. ed.). Pink Elephant.

Fernández Sánchez, C. M.; Piattini Velthuis, M. (2012). *Modelo para el Gobierno de las TIC basado en normas ISO*. Aenor Ediciones.

Leopoldi, R.; Howells, V. (2004). *The Service Catalog*. HDI.

Menken, I. (2010). *ITIL V3 Implementation Quick Guide: the art of the stress-free IT Service Management* (2a. ed.). Emereo Pty Limited.

Office of Government Commerce (2011). *The official introduction to the ITIL Service Lifecycle*. Londres: TSO.

Quesnel, J. (2010). *Entender ITIL v3: Normas y mejores prácticas para avanzar hacia ISO 20000*. ENI Editions.

Tjassing, R. (2008). *Fundamentos de la Gestión de Sevicios de TI Basada en ITIL V3 (ITSM Library)*. Van Haren Publishing.

UNE-ISO-IEC 20000-1 (2011). *Tecnologías de la Información. Gestión del Servicio. Requisitos del Sistema de Gestión de Servicios (SGS)*. Aenor Ediciones.