05.648 – Treball de Fi de Grau.

2020-21 semestre 2

Arquitectura d'alta disponibilitat de sistemes per entorns sanitaris.

Alumne: David Garcia Ros

Índex de continguts

1. Introducció.

L'atenció sanitària de qualitat i els diferents processos assistencials de qualsevol centre sanitari de referencia cada cop tenen una dependència més important dels sistemes d'informació. Els professionals de salut necessiten i esperen que els programes on consulten i registren les dades dels pacients estiguin operatius les 24 hores del dia, els 365 dies de l'any.

El diagnòstic, el tractament i el seguiment del pacient durant la seva estada a l'hospital o centre d'atenció requereix d'uns recursos que engloben des de professionals especialitzats, infraestructura, tecnologia mèdica, instal·lacions adequades, circuits i processos definits, col·laboració institucional, etc. La qualitat és un màxim que qualsevol organització en general vol obtenir i en el cas dels serveis públics sanitaris ha de ser la seva raó de ser, basant-se en la recerca, la docència, l'excel·lència assistencial i la millora contínua en l'àmbit de salut, innovant contínuament i adaptant-se als canvis constants.

La interconnexió entre centres sanitaris per compartir informació de manera àgil i l'accés a centres de dades tant a nivell autonòmic con nacional és un aspecte bàsic pel tal de garantir l'objectiu principal de totes les institucions hospitalàries: atendre al pacient amb la màxima qualitat.

Crear un entorn d'investigació on els professionals puguin desenvolupar la seva experiència i aportar els seus coneixements es torna essencial i es obligació de la gerència dels centres garantir les condicions necessàries per assolir aquests objectius. Entre elles, l'accés i disponibilitat dels sistemes d'informació.

Els nous models d'assistència al pacient han posat de manifest que cal fer un esforç per adaptar les tecnologies de la informació i la formació dels professionals per tal de donar resposta a situacions on cal fomentar la teleassistència i consultes a distància. En aquest sentit, els diferents centres sanitaris i hospitals d'alta complexitat han impulsat una veritable revolució i adaptació al canvi, posant de manifest, una vegada més, que l'enginy i la resiliència forma part d'aquest col·lectiu de persones que treballen per les persones.

Les consultes remotes als pacients, l'activació de portals web on interactuar amb els professionals sanitaris, o la comunicació àgil de resultats diagnòstics via missatgeria electrònica formen part ja del nostre dia a dia.

El teletreball ha passat a formar part del nostre dia a dia, i totes les empreses i treballadors s'han adaptar a les noves circumstàncies laborals. Els centres sanitaris no han estat una excepció, amb la problemàtica afegida de lliurar als professionals les eines que tradicionalment utilitzen de forma presencial.

L'objectiu d'aquest treball és identificar i explicar diferents alternatives per garantir l'alta disponibilitat dels sistemes d'informació per aquells serveis crítics d'instal·lacions sanitàries de gran abast, com els hospitals.

La finalitat d'aquest treball es detallar els aspectes que cal tenir en compte a nivell d'infraestructura de sistemes per tal de garantir l'alta disponibilitat d'aquests serveis, així com la gestió d'aquestes.

Es tractaran punts com la redundància dels centres de procés de dades, les còpies de seguretat, el sistema d'emmagatzematge, l'evolució segura de la plataforma de servidors, la seguretat en la informació, la xarxa i les comunicacions, el treball en remot, l'assistència remota, la disponibilitat, la gestió de la capacitat, etc.

La principal motivació per fer aquest treball de fi de grau no es altra que aprendre, ajudar, reflexionar, compartir i orientar per tal d'aportar l'experiència personal sobre aquest camp i evolucionar cap a un model on la informàtica i els sistemes d'informació siguin una veritable ajuda als professionals del sector.

El desenvolupament de nous models d'intel·ligència artificial i sistemes predictius obliguen a actualitzar i revisar els models d'alta disponibilitat, incorporant nous circuits a l'activitat assistencial.

Actualment, un dels principals reptes que qualsevol organització ha de gestionar és el tractament de les dades. Assegurar la qualitat de les dades és bàsic per crear models que aportin un veritable valor.

La inèrcia d'aquest darrers anys al món de les TI ens suggereix que els models d'assistència evolucionen cada vegada més a un model predictiu, on les dades s'entrenen i aprenen, per tal d'oferir resultats que ajudin als professionals a diagnosticar més i millor, més ràpid i amb menys probabilitat d'error.

En aquest sentit, la disponibilitat i escalabilitat dels entorns crítics són un dels aspectes que més preocupen a totes les grans organitzacions sanitàries, juntament amb la seguretat i confidencialitat de les dades.

Tenim el privilegi de ser actors del canvi en la societat de la informació i estem obligats a contribuir amb la nostra experiència i assolir nous reptes, per tal de compartir coneixements i fer realitat objectius orientats a un fi comú, ajudar a la població.

Ningú es pot quedar al marge d'aquesta evolució i la societat espera que tots els professionals sanitaris, sigui quina sigui la seva responsabilitat i rol dintre de l'organització, doni el màxim i millorin dia a dia, com sempre han demostrat.

2. Processos crítics en entorns sanitaris.

L'activitat diària de qualsevol centre sanitari es recolza en els sistemes d'informació. Centenars de decisions quotidianes de qualsevol departament es basen en la fiabilitat i disponibilitat de les dades que disposa l'organització i aquella informació que pot contrastar amb altres centres.

En general, les organitzacions estan estructurades per àrees funcionals o departaments, que compleixen funcions específiques dins la empresa. Per mitjà dels recursos humans s'assoleixen els objectius marcats per la direcció o gerència, utilitzant totes les eines tecnològiques disponibles al seu abast.

El departament de gestió i sistemes d'informació té la principal funció de proporcionar les TIC (Tecnologies de la Informació i la Comunicació) per tal de desenvolupar processos de la cadena de valor, independentment de qui els gestionin i com s'estructurin.

És molt important que els serveis SI/TI a les organitzacions estiguin alineats amb la estratègia empresarial, per tal de facilitar l'assoliment d'objectius.

El departament de SI no deixa de ser un proveïdor de serveis per tal de lliurar i garantir els sistemes d'informació necessaris perquè l'activitat natural de l'organització es pugui recolzar en ells. Es indispensable una bona gestió de l'entorn tecnològic per tal de poder evolucionar i oferir avenços que puguin ser d'utilitzat per la empresa.

Les tecnologies de la informació son el conjunt de recursos informàtics, (ordinadors, servidors, bases de dades, xarxes, aplicacions, eines...) que els sistemes d'informació utilitzen en cada moment, adaptant-se a la tecnologia existent.

Moltes organitzacions externalitzen part de les àrees dels departaments de SI, amb diferents objectius, com poden ser reduir costos estructurals, garantir accés d'empreses especialitzades en determinats serveis, etc.

L'impacte dels Sistemes d'Informació a les organitzacions aporta valor a l'estratègia d'aquesta i a les operacions que fan possible assolir els objectius. En aquest sentit, la gestió de qualsevol entitat no es independent dels SI, sinó que cal que estigui alineada amb l'estratègia de negoci.

En aquest sentit, les activitats i processos integrats amb l'atenció directa al pacient es tornen el punt més crític dels hospital i entitats sanitàries. És responsabilitat del departament de SI oferir alta disponibilitat dels sistemes i continua evolució funcional per tal de garantir que els professionals tinguin total garantia i fiabilitat de les eines informàtiques que tenen al seu abast.

2.1 Activitats que requereixen alta disponibilitat.

Dins d'un hospital podem diferenciar tres grans blocs d'activitat: l'assistència, la recerca i l'administració del propi centre.

Cadascuna té diferents serveis i característiques que cal garantir des del punt de vista dels sistemes d'informació perquè els professionals puguin desenvolupar la seva activitat amb garanties.

Les solucions software individuals o integrades donen servei a l'estratègia comuna de la empresa. Fa dues dècades, les funcionalitats dels diferents aplicacions s'integren en paquets més complexes i globals, amb un àmbit d'acció molt més ample.

L'administració d'una entitat hospitalària i en general qualsevol empresa mitjana o gran avui en dia no s'entén sense el concepte de l'ERP (Planificador de recursos empresarials), eina de gestió que engloba els diferents mòduls (Recursos Humans, Finances, Logística, etc.)

Existeixen diferents proveïdors d'ERP la mercat. Potser el més conegut és SAP, però també trobem empreses com Oracle o Microsoft que ofereixen una solució global de gestió.

Per complementar les operatives transaccionals que serveixen de base a l'ERP, existeixen tecnologies de programari orientats a processos amb la finalitat de prendre decisions, amb un component intel·lectual humà que l'ERP no assoleix. Aquestes eines i tecnologies com *DataWarehouse*, *OLAP* o *Dataminning*, generen les solucions anomenades BI (*Bussiness Intelligence*).

L'ERP normalment no avarca totes les funcionalitats que una organització sanitària gran necessita i sovint es complementa la solució amb diferents programaris de tercers que s'integren amb el HIS (*Hospital Infomation Service*).

Per exemple, aplicacions específiques de funcionalitats de recursos humans (formació, gestió de viatges, portal d'empleat, etc..), finances (eines de gestió pressupostària, control de despeses, etc..), aplicacions de gestió assistencial específica de serveis concrets, etc.

En el cas dels hospitals, cal complementar els mòduls estàndards de l'ERP amb solucions verticals que gestionin la informació sanitària. En aquest sentit, existeixen diferents proveïdors i productes certificats per garantir aquesta gestió.

El proveïdor d'ERP més important del món és SAP, que té aliances amb la empresa nord-americana CERNER amb seu a Missouri, i ofereixen una solució sectorial per la gestió hospitalària. El mòdul ISH-MED es una solució d'història clínica electrònica que esta integrada de manera nativa amb SAP, garantint escalabilitat i possibilitant el desenvolupament i evolució contínua amb analistes i programadors externs.

Actualment aquest producte esta present a més de 600 hospital de 36 països del món. Té el gran avantatge que permet desenvolupaments personalitzats de les funcionalitats que inclouen les diferents versions.

La pròpia evolució del mercat en aquest tipus de solucions tendeix a integrar l'ERP al núvol, de fet, pels nous clients SAP ja ofereix la seva plataforma en aquesta modalitat. El negoci esta orientat a que els proveïdors de productes ERP també ubiquin les dades de les organitzacions, aspecte que genera molta controvèrsia. En determinats àmbits, com el sanitari, encara SAP no ofereix una evolució de les instal·lacions locals cap al núvol, encara que sí que aporta la data de fi de suport de les versions actuals.

Dintre del món sanitari, existeixen actors principals que lideren l'evolució del mercat, con poden ser les multinacionals farmacèutiques. La majoria d'aquestes organitzacions integren les seves solucions amb gairebé tots els ERPs del mercat.

Empreses con Roche, Grifols, Jhonson & Jhonson, estan molt presents i ajuden a adaptar-se als canvis de la societat de la informació a l'entorn sanitari.

Cal mencionar d'una manera molt especial una recent onada d'emprenedoria en l'àmbit sanitari, on diferents empreses petites i grans evolucionen solucions aplicades a la sanitat per posar en valor el centre de tota la seva oferta: l'atenció al pacient i millorar l'experiència del pacient en la sanitat. Podem trobar una referència molt destacable a Barcelona, concretament al Hub d'empreses que forma BHH (Barcelona Healt Hub), al Recinte Modernista de l'Hospital de la Santa Creu i Sant Pau. Podem trobar tot un ecosistema d'empreses innovadores on es centra la investigació i desenvolupament dels productes en àmbit sanitari.

D'altra banda, l'activitat de recerca a un centre sanitari és bàsica i està totalment relacionada amb l'activitat assistencial. Existeixen solucions informàtiques de gestió dels projectes d'investigació, que tenen la principal característica d'establir un espai obert de col·laboració entre professionals de diverses disciplines, amb l'objectiu de generar talent creant sinèrgies entre ells.

En moltes ocasions els professionals d'un hospital treballen en estreta col·laboració amb el centres d'investigació i cal establir els lligams informàtics perquè la informació sigui accessible.

Als darrers anys també trobem tecnologies emergents que fan ús de les dades estructurades i no estructurades (no incloses a bases de dades relacionals) per establir patrons que ajudin a predir i diagnosticar determinades patologies.

El processament del llenguatge natural, que treu del text clínic els conceptes mèdics, el seu context i les relacions entre ells, juntament amb l'aprenentatge i entrenament continu de les dades, contribueixen a millorar els resultats d'investigació i formar part dels darrers avenços mèdics.

2.2 Serveis que requereixen alta disponibilitat.

Algunes de les activitats comentades anteriorment (assistència, recerca i administració) requereixen de serveis que estiguin operatius 24X7, degut a la criticitat i relació entre ells.

A continuació s'identifiquen els serveis mínims que un hospital requereix, per donar aquest nivell de disponibilitat.

Serveis Assistencials i de Suport:

- Urgències Generals
- Urgències pediàtriques
- Urgències ginecologia i obstetrícia
- Diagnòstic per la imatge
- Laboratoris Generals
- Farmàcia.
- Anestesiologia.
- Esterilització
- Medicina Intensiva
- Atenció quirúrgica
- Infermeria
- Trasllats sanitaris.

Serveis d'Administració:

- Admissions hospitalàries.
- Facturació de processos assistencials.

Tots aquests serveis requereixen que la infraestructura i el programari necessari per desenvolupar la seva activitat estiguin totalment operatius i disponibles.

La relació entre tots ells és molt estreta i totes les dades del pacient cal que estiguin a un repositori comú, accessible de forma segura i confidencial.

Existeix una integració complexa entre cada solució de programari i és funció del Departament de SI vetllat per la correcta interconnexió de tots els components (bases de dades, aplicacions, webs, etc.) que garanteixen la disponibilitat immediata de les dades.

A més del sistema informàtic, és imprescindible garantir circuits i aplicar la mateixa exigència a la disponibilitat de la tecnologia mèdica aplicada. Es a dir, tots aquells dispositius i serveis que s'integren amb els sistemes d'informació i poden incorporar dades necessàries per avaluar el diagnòstic ràpid i encertat de les patologies que aquests serveis comentats anteriorment cobreixen.

3. Infraestructura.

Garantir una infraestructura d'alta disponibilitat, robusta i estable, és imprescindible a un entorn sanitari on l'atenció al pacient es dona les 24 hores del dia. En aquest sentit, l'accés als recursos han d'estar distribuïts mitjançant duplicitat d'entorns i espais sempre que sigui possible.

3.1 Espais redundats - CPDs.

Els CPDs (Centres de procés de dades) són els espais físics on es concentren els recursos necessaris pel processament de la informació de qualsevol organització. És una sala condicionada per allotjar l'equipament informàtic i electrònic.

Aquest espais han de disposar de determinats requeriments de seguretat i disponibilitat, com:

- Grups electrògens per mantenir l'equipament funcionant en cas de falla del subministrament elèctric.
- Racks o armaris independents per ubicar els servidors, electrònica de xarxa, cabines d'emmagatzematge, etc. Cadascú d'aquests armaris ha de disposar de tomes elèctriques redundades e independents, per tal que possibles tasques puntuals de manteniment no afectin a la resta.
- Equips de refrigeració per tal que els dispositius es mantinguin a temperatura constant, ja que es genera molta calor.
- Accés exclusiu al CPD controlat per targeta d'accés magnètica o empremtes digitals.
- Mesures d'extinció d'incendis, com l'emissió de gasos nitrogen, argó i bióxid de carboni.
- Identificació clara de les sortides del CPD i rampes de fàcil accés per afavorir les tasques de manteniment i moviments de infraestructura.

Normalment es configura una gestió d'alarmes per assegurar que tots els punts anteriors estan plenament operatius. És totalment necessari establir circuits de suport en cas d'avaria de qualsevol dispositiu ubicat a un CPDs i caldrà implicar departaments diferents als propis de SI, com poden ser Seguretat del centre, Enginyeria, Manteniment, etc.

L'objectiu, des del punt de vista de la disponibilitat dels sistemes d'informació, es garantir que aquest espai sempre esta operatiu. En aquest sentit, cal duplicar el CPD. És a dir, establir un altre espai físic igual o semblant que entri en funcionament o assumeixi tot el processament de dades en cas que un tingui problemes de disponibilitat.

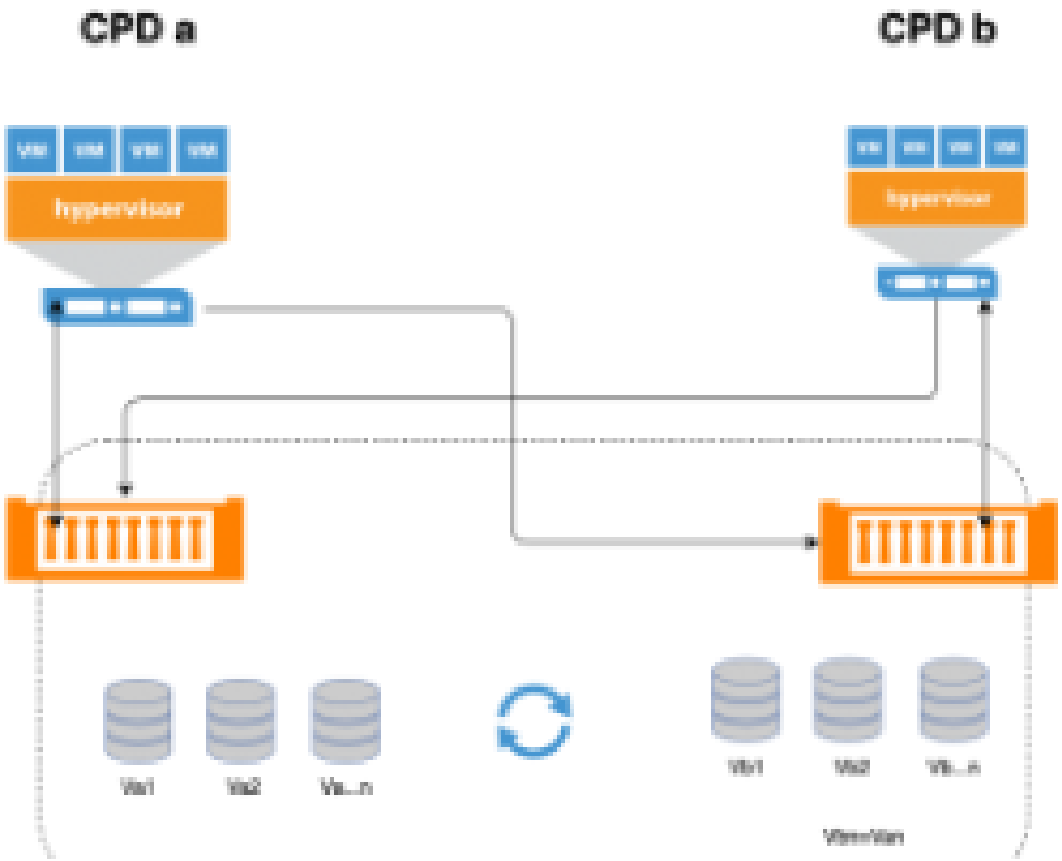
Els darrers anys s'ofereixen serveis per migrar o establir un segon CPD al núvol, utilitzant instal·lacions de tercers que optimitzen l'espai necessari i els recursos que s'han d'invertir a les organitzacions. És una opció que moltes empreses de qualsevol mida utilitzen i totalment valorable. Però, en el cas d'un centre sanitari, sempre que sigui possible és més recomanable treballar en la línia de garantir un segon CPD físic.

De fet, moltes de les aplicacions que s'utilitzen a un entorn sanitari s'ubiquen al núvol, doncs des del punt de vista del proveïdor de software, aquest model resulta més econòmic de mantenir, ja que administren la majoria de clients des d'un mateix punt. És una plataforma amb la que s'ha de conviure i sembla que tard o d'hora, consolidarà la gran majoria dels programaris de qualsevol entorn. Amb tot, cal tenir en compte que les organitzacions sanitàries tracten informació confidencials i sensibles, com les dades de salut i aquesta és una gran barrera avui en dia per migrar determinats serveis al núvol.

Existeixen dues formes de configurar lògicament l'operativitat entre dos o més CPDs, oferint diferents nivells de contingència segons la criticitat dels serveis que ofereixen.

Actiu – Actiu

En aquest tipus de configuracions d'alta disponibilitat s'executa la mateixa aplicació en diferents servidors, encarregant-se l'aplicació o el balancejador hardware del repartiment de la càrrega i gestionar les fallades. A una configuració típica utilitzant balancejadors hardware els clients es connecten a una única IP virtual. En cas de caiguda d'algun node, el balancejador deixaria d'enviar-li les peticions de servei fins que torni a estar disponible. És clarament un sistema distribuït escalable i garantint alta disponibilitat.

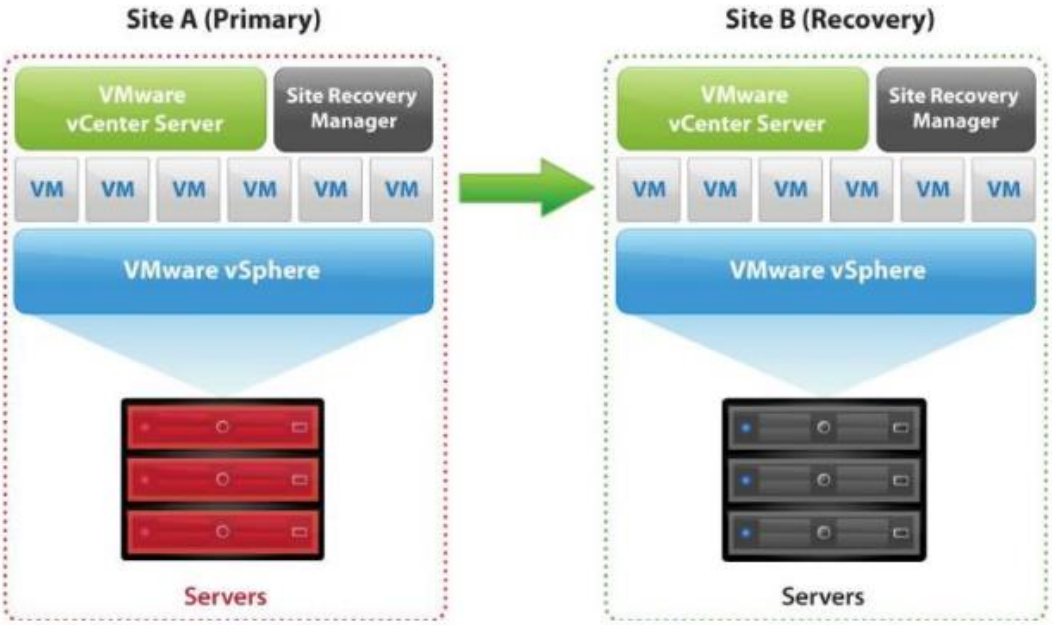


Actiu – Passiu

En aquest model es realitza un model de clúster aprofitant que les dades estan replicades a les cabines d'emmagatzematge situades a cada CPD. D'aquesta manera, els servidors ubicats al CPD principal accedeix a les seves dades locals situades a una cabina d'emmagatzematge local.

En cas de fallada del CPD complet o la pròpia cabina d'emmagatzematge, entraria en funcionament el CPD secundari, utilitzant les dades replicades a l'altre cabina.

Aquesta configuració esta disponible en entorns HP-UX a través de l'eina Serviceguard – Metroclúster i en entorns Microsoft utilitzant GeoSpan.



En qualsevol configuració, els dos CPDs han d'estar connectats mitjançant mànegues de fibra òptica, que garanteixin ample de banda de sobres per les connexions LAN i SAN.

És imprescindible adquirir electrònica de xarxa de CPD redundada, com switchos de FC per connectivitat SAN o switchos per connectivitat Ethernet. Un dels fabricants històricament més fiables es CISCO, que proporciona una gran diversitat de hardware.

La configuració actiu – passiu amb canvi de cabines de discs en cas de contingència requereix d'un temps de l'ordre de minuts en cas de fallada d'algun dels CPDs per entrar en ple funcionament.

També cal tenir en compte inconvenient que pot generar aquest model, com llicenciament extra, marxa enrere complicada, complexitat per les proves de recuperació del servei, etc.

Com veurem en punts posteriors, les plataformes de virtualització de servidors, com VMWare, també permeten alta disponibilitat del servidors. En cas d'intervencions programades es poden moure els servidors virtuals a altres amfitrions físics per no aturar els serveis que presten, com bases de dades, aplicacions web, etc.

En cas d'incidències sobtades o consum excessius de memòria o CPU, el propi sistema operatiu de virtualització s'encarrega de moure els servidors a d'altres equips per continuar donant servei sense afectar en cap moment a la disponibilitat de les dades.

En entorns sanitaris grans, on les aplicacions han d'estat disponibles a qualsevol hora, es recomana una configuració actiu-actiu, ja que no existeix pèrdua de temps en cas d'avaria en alguns dels CPDs. És necessari fer preventius i proves de redundància programades per garantir que el procediment de contingència serà totalment vàlid en cas d'incidència greu a un CPD.

3.2 Emmagatzematge.

Un sistema d'emmagatzematge que garanteixi prestacions d'alt rendiment és imprescindible per cobrir les necessitats que qualsevol organització.

Escollir un model òptim de cabina d'emmagatzematge és un repte important, ja que condicionarà la disponibilitat i accés a les dades de l'organització.

En aquest sentit, un gran avanç els darrers anys ha estat l'emmagatzematge all-flash, que aconsegueix una latència inferior al mill segon davant milers o inclús milions d'IOPS.

La tecnologia all-flash es basa en una memòria no volàtil d'alta velocitat que es programa elèctricament. Aquest tipus de memòria no requereix alimentació per mantenir la integritat de les dades emmagatzemades.

Els avantatges que ofereix aquest tipus de tecnologia son les següents:

- Rendiment d'aplicacions.
  Flash accelera les aplicacions empresarials comuns, com bases de dades Oracle, SQL, SAP, etc.
- Reducció de latències.
  Temps de resposta gairebé immediata per atendre peticions de dades.
- Alts nivells de disponibilitat
  Superior al 99%.

Per garantir total disponibilitat de les dades, una bona estratègia es redundar les cabines en diferents CPDs, amb doble controladora en cadascuna de les unitats d'emmagatzematge i configuració redundada de tos els components.

Han de ser escalables sense aturades de servei, per permetre el creixement d'acord amb les necessitats de l'organització. Les operacions de *failover* i *failback* del sistema actiu-actiu de cabines ha de ser automàtic per tal de reduir els temps de resposta necessaris en cas d'avaries.

Les principals funcionalitats que una cabina d'aquestes característiques ha de proporcionar son:

- Virtualització de l'emmagatzematge intern.
- Tecnologies d'obtenció de còpies instantànies o snapshots.
- Tecnologies de clonatge de volums de dades.
- Funcions de replicació síncrona de dades entre les dues cabines.
- Configuració de seguretat que permeti que cada servidor accedeixi només als volums autoritzats.
- Compressió de dades, de-duplicació, i Thin-provisioning.
- Integració amb plataformes de virtualització, com Vmware.
- Integració amb programaris gestors de còpies de seguretat.
- Encriptació de dades.

Existeixen molts fabricants de solucions d'emmagatzematge amb un llarg recorregut al mercat, com els següents:

HUAWEI Hewlett Packard Enterprise HITACHI Inspire the Next DELL

Exemple de cabina d'emmagatzematge Huawei OceanStor Dorado V6

Finalment, és necessari garantir un suport amb fabricant que permeti solucionar qualsevol incidència que es pugui produir al sistema. Gairebé tots els fabricants utilitzen eines d'intel·ligència artificial per predir les possibles avaries de les cabines, accelerant la resolució d'incidències.

3.3 Virtualització de servidors.

Les plataformes de virtualització de servidors ofereixen múltiples avantatges per garantir la disponibilitat dels Sistemes d'Informació, com per exemple:

- Major disponibilitat dels servidors.
- Menors costos operatius.
- Millora del rendiment de les aplicacions.
- Distribució més eficient de les càrregues de treball.
- Escalabilitat i millor utilització dels recursos.
- Creació ràpida i fàcil d'entorns de proves.
- Integració amb sistemes de còpies de seguretat àgils.

Actualment moltes organitzacions del món aposten per la virtualització de servidors, ja que redueixen la despesa en diferents servidors físics i suports amb fabricants, alhora que optimitzen els recursos. També la reducció en facturació energètica es un aspecte a tenir en compte.

Com a principals inconvenients poden indicar els següents:

- Augment de costos inicials, llicenciament, despeses d'instal·lació, etc.
- Necessitat d'aprendre a gestionar un entorno virtual.
- Dimensionament adequat per garantir redundància.

La idea principal és que un únic servidor físic sigui capaç d'executar n servidors virtuals, amb diferents sistemes operatius i de manera independent. A mesura que les necessitats de còmput s'incrementen, cal afegir nous servidors físics que ubicaran més equips virtuals, permetent balancejar càrrega, gestionar l'emmagatzematge, la xarxa, etc. La escalabilitat de producte que ofereixen aquestes solucions dona molta versatilitat a la infraestructura.

Existeixen molts proveïdors de sistemes de virtualització de servidors, sent els principals els següents:

- VMware VSphere. (líder del mercat)
- Red Hat Virtualization.
- Proxmox VE
- Microsoft Hyper-V
- Citrix Hypervisor
- Oracle VM Server
- IBM Power VM

Cal indicar que la virtualització és la base de computació al núvol, ja que la gran majoria d'aplicacions i serveis que s'ofereixen per internet es basen en plataformes de virtualització que gestiones equips virtuals.

Molts dels sistemes distribuïts basen la seva escalabilitat en la virtualització de servidors i la versatilitat que ofereixen per créixer horitzontalment.

A un entorn sanitari és imprescindible garantir la disponibilitat dels sistemes crítics, i per tant, les plataformes de virtualització ofereixen una molt bona solució.

La possibilitat de fer migracions sense aturades de sistemes, crear entorns de desenvolupament, clonar servidors o realitzar imatges fàcilment abans de fer qualsevol intervenció sobre els sistemes operatius, garanteixen una ràpida resolució d'incidències davant un imprevist.

A més, facilita un entorn on provar els sistemes operatius, les aplicacions, les actualitzacions i les operatives de forma molt controlada, afegint una gran versatilitat i garanties.

A un entorn on les aplicacions han d'estar funcionant 24X7, la virtualització dels entorns productius garanteix una disponibilitat intrínseca.

Cal tenir en compte que el temps de reparació d'un servidor virtual, mitjançant una eina de còpies de seguretat integrada a la plataforma, es redueix molt davant de la restauració d'un entorno físic.

Si un sistema concret té una gran càrrega de treball, funcionalitats com DRS (Distributed Resource Scheduler) del fabricant Vmware, garanteixen l'equilibri de càrrega entre els servidors físics, balancejant els servidors virtuals a un altre amfitrió físic amb més disponibilitat.

La virtualització de la xarxa o l'emmagatzematge també es una funcionalitat molt interessant per garantir alta disponibilitat. Aquestes configuracions desvinculen aquests serveis del maquinari subjacent, reduint moltes de les tasques administratives i reduint així errors manuals i temps d'operació.

Finalment ens referim a un aspecte molt interessant de la virtualització, que és la gestió d'escriptoris d'usuari remots. A més de la plataforma de servidors, també es poden aplicar entorns de virtualització a les estacions de treball, autoritzant que els usuaris es puguin connectar des de Internet a equips virtuals iguals o en unes condicions molt semblant als ordinadors físics.

És molt interesant veure com aquest tipus de productes ja no tan sol garanteixen la infraestructura de servidors, sinó també el lloc de treball del professional, facilitant el tele-treball i accés segur a les dades que han de gestionar.

3.4 Llicenciament.

Un dels aspectes importants a tenir en compte per qualsevol organització són els costos de llicenciament associats a la infraestructura. El departament de Sistemes d'Informació ha de dimensionar correctament la infraestructura necessària per oferir alta disponibilitat, prestant especial atenció als costos de llicenciament.

En aquest sentit, és cert que avui en dia els servidors tenen cada vegada més prestacions i si es treballa amb plataformes de virtualització, la tendència és adquirir menys servidors físics, independentment del número de servidors virtuals que gestionin.

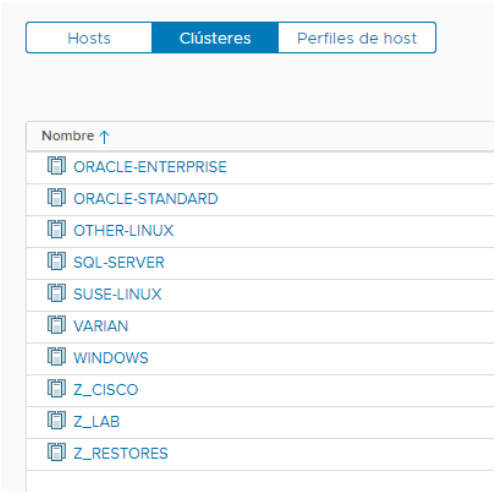
Tot i això, s'han de llicenciar com a mínim els següents productes:

- Sistemes operatius dels servidors virtuals (Microsoft, Linux, etc...)
- Sistemes operatius de la plataforma de virtualització.
- Eines per garantir les còpies de seguretat.
- Bases de Dades (Oracle, SQL, etc..)

Cada fabricant té diferents modes de llicenciament, com poden ser modalitats de compra de llicència en propietat més manteniment i suport anual o bé els modes de llicències per subscripció.

Aquest darrer model sembla que és el que tots els grans fabricants han adoptat com a model d'evolució, sent més flexible des del punt de vista del client, ja que en qualsevol moment pots reduir la quantitat de llicències necessàries si ja no es necessiten. Tot i això, surt més car que el model de llicència perpetua a la llarga, ja que al model de compra en propietat només es paga una vegada i el que es renova anualment és el manteniment.

Com a exemple, una configuració molt interessant por ser, en el cas de plataformes de virtualització, la creació de diferents clústers de servidors físics per allotjar equips virtuals.



Normalment les llicències necessàries es cotitzen en funció de les CPU o Cores per CPU que tinguin els servidors físics, ja siguin amfitrions per virtualització o dedicats en exclusiva per la funcionalitat que ofereixen.

4. Seguretat de la informació.

4.1 Còpies de seguretat.

Tot i que la duplicitat d'infraestructura, els sistemes d'emmagatzemats redundats i la virtualització de servidors ofereixen una alta disponibilitat dels sistemes crítics per qualsevol organització, les còpies de seguretat són un element clau davant una incidència que obligui a restaurar un sistema concret i tornar a garantir l'accessibilitat.

L'objectiu de les còpies de seguretat (*backups*) és disposar de còpies de les dades que existien en els sistemes en diferents moments temporals, de manera que es pugui recuperar les dades reaccionant a incidents com els següents:

- Incidents en un sistema d'emmagatzematge de dades amb pèrdua de dades.
- Manipulació errònia de les dades, ja sigui per errors humans; o per error de programari; o per afectació de programari maliciós, com virus o altres; o per altres motius.
- Necessitat de confirmar quina era la informació present en els sistemes en un moment passat del temps.
- Necessitat de confirmar el correcte funcionament del propi sistema de còpies de seguretat.

Existeixen diferents tipus de còpies de seguretat, com:

- Còpia en mirall o RAID1: que crea una còpia exacta en temps real. És a dir, mentre es treballa es crea una còpia a una ubicació alternativa.
- Còpia completa: còpia de seguretat de totes les dades del sistema a un altre suport.
- Còpia diferencial: còpia de seguretat de totes les dades que han canviat des del backup complet anterior.
- Còpia incremental: còpia només les dades que han variat des de la darrera còpia de seguretat.

La política de seguretat de la informació recull totes les directrius que cal aplicar per garantir una ràpida i senzilla recuperació de les dades.

En aquest sentit, es defineixen diferents destins de les còpies per tal de complir el total de requeriments desitjats. Per exemple:

- CPS: Còpies en el Propi Sistema de producció.

  Alguns sistemes fan servir còpies de dades en el propi sistema.

  - D'aquesta manera, davant d'errors lògics, es facilita l'accés a recuperar dades sense haver d'utilitzar els mecanismes de backup a sistemes externs.
  - Per exemple es fan servir sistemes de protecció interna en els servidors de carpetes, que fan una "imatge" (o snapshot) automàtic cada 3 hores, i que es conserven mentre es disposi d'espai per fer-ho.
  - Per exemple en els entorns vmware es fan snapshots abans d'actuacions importants en un servidor, de manera que si les actuacions no resulten satisfactòries sigui factible recuperar fàcilment la situació anterior.

- CFS: Còpies Fora del Sistema de producció.

  Primera còpia contra un sistema de disc dedicat, suficientment àgil, on es potenciïn tots els mecanismes disponibles de de duplicació, compressió, còpies incrementals, velocitat de recuperació, facilitat de proves de recuperació, etc.

  - Aquesta còpia està en línia i en els locals de l'organització, de manera que es facilita el rendiment i la flexibilitat.

- CFO: Còpies Fora de l'Organització.

  Una segona còpia que permeti tenir dades fora de l'organització, de manera "desconnectada" dels sistemes en funcionament, i on aplicar els cicles de retenció setmanal, mensual, anual, ... habituals definits a la política de còpies de seguretat.

  - Aquesta còpia s'ubica fora del recinte, de manera que s'assegura la disponibilitat en cas d'incidència greu en els Centres de procés de Dades (CPDs).
  - Poden ubicar-se al Cloud, normalment presentades en modalitat SaaS o en les pròpies instal·lacions de l'organització.

Les còpies de seguretat dels sistemes han d'estar accessibles en tot moment i a més, garantir una retenció adequada per tal de poder restaurar informació històrica de determinades àrees, com Recursos Humans, Gestió financera, etc.

En el cas del l'entorn sanitari encara s'afegeix la casuística de que són dades de salut, amb una normativa específica d'accessibilitat a la informació dels pacients.

Existeixen molts programaris per realitzar les còpies de seguretat, amb diferents proveïdors líders en aquestes solucions. Per exemple:

Molts d'aquests productes també incorporen funcionalitats de disaster-recovery per tal de emmagatzemar a una altra plataforma una còpia sincronitzada de les dades reals de producció, ja sigui al núvol o a un altre centre de procés de dades (CPD) alternatiu.

Una de les qüestions que cal resoldre abans d'implementar un projecte d'implantació d'una solució de còpies de seguretat és la següent:

Fins a quin període de temps vull tenir les dades accessibles per tal de restaurar d'una forma àgil els sistemes de l'organització?

En aquest sentit, cal classificar els sistemes d'informació definint objectius segons la criticitat de les dades. A aquests efectes, les dades dels sistemes que gestionen informació crítica dels pacients i que afecten a l'assistència són considerades de criticitat màxima.

Per exemple:

- L'ERP o eina assistencial general d'assistència.
- Els entorns departamentals imprescindibles, com: diagnòstic per la imatge, laboratoris generals, etc.

Gairebé tots els productes de backups es basen en polítiques on es classifiquen els entorns o servidors que cal fer còpia de seguretat periòdica. Sobre aquestes polítiques s'apliquen finestres de retenció de les còpies, definides pels administradors del sistema.

4.2 Restauració informació crítica.

Una de les principals tasques dels administradors o responsables de l'execució de les còpies de seguretat és realitzar proves periòdiques de recuperació dels sistemes.

Mitjançant aquest procediments, s'asseguren que els mecanismes de restauració funcionen correctament i que, davant qualsevol incidència, el procés de recuperació del sistema afectat ja s'haurà provat i validat abans.

Es indispensable, doncs, establir un calendari de restauracions periòdiques dels sistemes crítics con poden ser:

- L' ERP,
- Bases de dades i servidors d'aplicacions / integració associats,
- Directori actiu o base de dades d'usuaris de l'organització,
- Plataforma de correu electrònic,
- Sistemes de fitxers crítics, etc.

Les diferents eines que garanteixen les còpies de seguretat incorporen un catàleg detallat on s'especifica el tipus de còpia i la ubicació de la mateixa. Les cintes tradicionals LTO s'identifiquen amb una etiqueta codificada que permet identificar i associar la mateixa amb el contingut que té.

Aquesta base de dades relacional del producte de *backup* és de vital importància per l'organització i cal que estigui inclosa a les polítiques de criticitat màxima i sempre estigui accessible.

És molt recomanable enviar les còpies en cinta a una instal·lació fora de les instal·lacions de l'empresa, garantint un circuit de custòdia de les mateixes. Tot i això, pels sistemes crítics és indispensable l'accés immediat a les darreres còpies de seguretat. Per tant, cal reservar l'espai necessari a les cabines d'emmagatzematge del propi sistema de recuperació per tal de agilitzar les tasques de restauració de la informació.

És molt habitual utilitzar i validar el procés de restauració de les còpies de seguretat creant entorns de desenvolupament a imatge dels entorns productius, on es connecten els administradors de sistemes i l'equip funcional. D'aquesta forma es certifica que les dades són restaurables i correctes.

En moltes ocasions és difícil replicar exactament els circuits de producció, ja que es poden integrar amb dispositius físics o aparells mèdics molt específics que no poden reproduir-se a un entorn aïllat. Cal tenir en compte aquest aspecte, però intentar garantir que les proves de validacions són lo suficientment reals i semblants al sistema real.

En cas de realització de *backup* al *Cloud*, també és molt important provar els mecanismes i els temps de restauració, ja que en aquest cas s'afegeix la garantia de les comunicacions necessàries per restaurar.

Encara que podem pensar que tota la informació crítica d'una organització es troba als servidors de fitxers, bases de dades, etc, no es pot deixar de banda que en entorns sanitaris també cal garantir la disponibilitat d'estacions de treball concretes o aparells de diagnòstic que per la seva funcionalitat o característiques de connexió específiques.

En aquest sentit existeixen diferents programaris de còpies de seguretat que permeten realitzar "imatges" o còpies de tot el sistema operatiu del servidor, de tal manera que si una estació de treball crítica s'espatlla, els tècnics de suport microinformàtic siguin capaços de restaurar el servei quan abans. En aquests casos, és indispensable comptar amb ordinadors amb maquinari equivalent a l'original, per tal que aquesta còpia de seguretat es pugui restaurar i sigui totalment operativa.

Les còpies de seguretat i la recuperació de cinta, la duplicació remota com emmagatzematge o l'enviament de registres de bases de dades constitueixen solucions tradicionals en matèria de protecció de dades i recuperació davant de desastres. Però aquestes solucions no són capaços de satisfer objectius pel que fa a punt de recuperació i temps de recuperació.

Per les bases de dades, existeixen opcions d'alta disponibilitat que també garanteixen una garantia, com poden ser els sistemes de rèplica de dades com Data Guard d'Oracle, que es basa en la replicació de les bases de dades originals contra unes bases de dades "en reserva".

Aquesta és una opció molt interessant per tal de garantir la total disponibilitat de les bases de dades més crítiques de l'organització, encara que aquestes solucions tenen implicacions que cal analitzar respecte al llicenciament amb fabricant.

5. Evolució de la infraestructura.

5.1 Garantia de l'evolució i suport de la plataforma.

La continua evolució de la tecnologia fa indispensable gestionar l'adaptació constant de la infraestructura i dels sistemes on s'allotgen les diferents solucions de programari.

La pròpia inèrcia del mercat obliga als fabricants de software de tot el món a evolucionar contínuament els productes i limitar temporalment el suport oficial dels mateixos. En aquest sentit, és molt convenient i crític per les organitzacions evolucionar la infraestructura.

Poden distingir dues línies de treball per garantir el correcte seguiment i adequació de l'entorn:

- Control i gestió de la plataforma hardware.
  Implica la gestió i renovació de garanties i suport de tota la infraestructura física del CPD, garantint implicació experta del fabricant davant incidències i problemes que afectin a la disponibilitat dels serveis crítics.
  Els servidors, les cabines d'emmagatzematge, els diferents dispositius de xarxa com concentradors, encaminadors, tallafocs o les llibreries de còpies de seguretat són dispositius físics on cal garantir suport directe del propi fabricant, normalment a través d'empreses de suport TI on aquest delega el contacte directe amb el client final.
  L'anàlisi detallat i preventiu de la infraestructura, i el continu monitoratge és indispensable per trobar punts de millora i aplicar-los. Com poden ser les actualitzacions de firmware dels productes, la revisió proactiva dels sistemes o una adequada gestió de renovacions del suport.

- Control i gestió de la plataforma software.
  Implica la gestió i actualització dels components de programari bàsic dels serveis crítics de l'organització, garantint d'aquesta manera el suport expert del fabricant en cas necessari.
  Els sistemes operatius dels servidors, les versions del programari de tercers que ubiquen, les versions dels sistemes gestors de base de dades o la interrelació amb la gestió del lloc de treball són aspectes on cal focalitzar una continua supervisió per tal de evolucionar la plataforma.
  És molt habitual que sigui la evolució del propi mercat el que obligui a actualitzar els components de programari de la infraestructura. Normalment quan surt una nova versió de sistema operatiu o programari concret, el fabricant ja indica la data de finalització de suport oficial. Ocasionalment el propi fabricant decideix, en funció del mercat i aspectes estratègics, allargar aquesta data o mantenir-la.

L'anàlisi preventiu de tots els aspectes relacionats amb el suport del programari oficial que dona servei als processos crítics de les organitzacions, en concret les sanitàries, és un aspecte bàsic on cal estar molt atents i treballar amb marge temporal per poder actuar amb garanties. En moltes ocasions, depenent del volum de les organitzacions, es torna adequat gestionar projectes puntuals d'actualització de les solucions de programari.

Els canvis de versions o actualitzacions dels ERP són projectes complexes on intervenen molts factors, com les validacions funcionals, les integracions amb d'altres sistemes, els pilots amb usuaris claus que verifiquin les noves funcionalitats, etc.

Un dels errors més habituals és no actuar proactivament ni ser totalment conscient de les dates de fi de suport oficial del programari o les dependències dels components que estan relacionats. En aquest sentit, cal una estratègia comuna del departament de sistemes d'informació per tal de garantir l'actualització i compatibilitat de versions tant de programari com de maquinari.

Igual que en el cas del llicenciament de les plataformes de maquinari o programari, els fabricants de tot el món ofereixen suport anual sobre els productes que ofereixen, que cal renovar per garantir els circuits de resolució de problemes i gestió d'incidències.

És molt important que sigui una persona qualificada del departament de TI qui s'encarregui de gestionar totes les renovacions de suport i adequar les necessitats a l'organització.

Hi ha diferents tipus d'assistència i nivells de suport, que normalment s'ofereixen per diferents vies, com poden ser el correu electrònic, el telèfon, el suport presencial o l'assistència remota.

Els diferents nivells de suport són els següents:

- N1: Incidències bàsiques on la funció dels seus especialistes és recopilar tota la informació que sigui possible del problema i ajudar a resoldre incidències bàsiques.

- N2: Segon nivell on tècnics més especialistes en l'àrea computacional. Són equips de persones orientades a resolució de problemes amb una complexitat més avançada.

- N3: Tercer nivell amb tècnics de nivell expert orientats a la resolució de problemes o incidents de difícil identificació o solució.

- N4: Quart nivell normalment facilitat per fabricant de programari o maquinari on es poden requerir actualitzacions de producte o resolució d'incidències complexes.

5.2 Entorns de desenvolupament de programari.

Per la gestió i la implantació de qualsevol sistema informàtic identifiquem diferents entorns, tot i que depèn de la tipologia del programari i el projecte concret poden variar.

- Entorn de desenvolupament
  Sistema on els desenvolupadors d'aplicacions treballen a la creació i adaptació dels diferents mòduls funcionals de la solució.

- Entorn d'integració.
  Sistema on es facilita la unió entre els diferents desenvolupaments i es permet verificar que els treballs no interfereixen entre sí.

- Entorn de proves.
  Entorns on realitzar els tests de funcionalitats dels sistemes. El seu objectiu és detectar el major número d'errades possibles. És utilitzat tant pel personal de TI com el client final.

- Entorn de preproducció.
  Sistema amb una còpia idèntica del sistema real dels usuaris. La finalitat d'aquest entorn és validar la usabilitat dels desenvolupament a un entorn real. Es permet realitzar proves d'actualitzacions i minimitzar les causes que poden generar caigudes del sistema.

- Entorn de producció.
  Plataforma on s'executa el programari, utilitzat per l'usuari. Aquest entorn ha de gaudir d'una major infraestructura que els anteriors entorns i major capacitat de gestió de tràfic o connexions concurrents.

A banda de l'entorn de producció, la resta d'entorns normalment no han d'estar operatius 24X7, i en determinades ocasions, es pot plantejar integrar-los en plataformes al núvol, si els requeriments d'infraestructura poden suposar un inconvenient de costos i manteniment.

En determinades solucions de programari, el propi fabricant obliga a utilitzar entorns de desenvolupament amb unes determinades condicions de qualitat i integració entre ells, per garantir que els canvis a producció compleixen uns requeriments de validació i no es permet la modificació del sistema productiu sinó s'ha generat i provat els canvis als entorns previs.

És molt recomanable actualitzar periòdicament alguns d'aquests entorns a partir de còpies de seguretat del sistema de producció, per tal de tenir les dades actualitzades i les proves siguin molt més semblants al sistema real. D'altra banda, aquestes actualitzacions serveixen per validar que el procés de recuperació de les còpies de seguretat funciona correctament.

Les organitzacions sanitàries, igual que la resta d'empeses, han de comptar amb aquests entorns per garantir que els canvis i noves funcionalitats que s'apliquen sobre el sistema productiu estiguin totalment validades i no tinguin un impacte negatiu sobre l'activitat diària dels usuaris sobre el sistema.

Afegim a l'entorn sanitari la problemàtica de la confidencialitat de les dades de salut. Exceptuant l'entorn de producció és desitjable que les dades, exceptuant l'entorn de producció, estiguin anonitmitzades, de tal manera que els desenvolupadors no accedeixin a informació confidencial. L'entorn de producció ha de gaudir d'una gestió molt acurada de rols i permisos per tal de garantir que els professionals només pugin accedir a les dades dels pacients que tracten al seu departament.

Existeixen casos documentats de problemes legals derivats de l'accés no justificat a les històries clíniques de pacients i cal posar especial focus en aquesta qüestió, garantint una traçabilitat dels accessos indeguts i prenent les accions sancionadores oportunes.

El fet de no validar correctament una funcionalitat implica que l'atenció al pacient es veurà afectada i per això, es indispensable una total coordinació entre les diferents àrees de desenvolupament.

L'entorn de producció té unes connotacions de disponibilitat especial, doncs és el sistema on cal garantir que la disponibilitat és total. Tot i això, en determinades ocasions, cal realitzar intervencions sobre el sistema que impliquen aturades programades, ja que no és possible aplicar els canvis de configuració sense aturar la plataforma.

És molt important realitzar plans d'intervenció documentats i coordinar les tasques de forma efectiva per tal de minimitzar al màxim el temps d'aturada del sistema productiu.

En entorns sanitaris és especialment complex pactar finestres d'aturades, degut a que l'atenció al pacient i la disponibilitat del sistema sempre ha d'estar activa, però cal acordar amb la direcció del centre una sèrie d'hores en determinades jornades de l'any on es puguin aplicar aquests canvis o intervencions.

Els propis projectes d'actualitzacions de programari, l'aplicació de pegats de seguretat sobre els sistemes o les pròpies incidències obliguen a realitzar aturades i cal planificar-les adequadament. Normalment es realitzen fora de l'horari laboral i de màxima activitat hospitalària per minimitzar l'impacte assistencial.

6 Model de gestió.

La principal funció del Departament de Sistemes d'Informació és gestionar i organitzar el coneixement de tot un equip humà per tal que la infraestructura i les diferents aplicacions s'utilitzin de forma adequada per aconseguir els objectius de l'organització, ajudant el l'execució dels seus processos.

Les principals responsabilitats són les següents:

1) Desenvolupament d'aplicacions,
2) Instal·lació i manteniment dels recursos d'infraestructura
3) Disseny i gestió de xarxes i comunicacions.
4) Monitorització i controls dels recursos.
5) Integració d'aplicacions.
6) Gestió de personal i externalització de part o tot els recursos.

A les organitzacions sanitàries del Departament de SI/TI no deixa de ser un "proveïdor" de la resta de serveis o departaments del centre. Normalment són els propis departaments assistencials els que, juntament amb el departament d'Informàtica, expressen i valoren els requeriments i necessitats que cal donar solució.

L'ERP (Enterprise Resource Planning), el HIS (Hospital Information Service) o el LIS (Laboratory Information Service) són plataformes de programari i mòduls complexes que sovint requereixen desenvolupaments i adaptacions a mida per tal de donar solució a les peticions derivades de la pròpia evolució del centre sanitari.

Noves proves, nous diagnòstics, noves patologies, etc, requereixen una adaptació constant dels productes i en aquest sentit, és ideal comptar amb un equip de desenvolupament competent que estigui gestionat per un cap de projecte o cap d'aplicacions alineat perfectament amb les prioritats marcades des de la direcció.

A una gran organització sanitària s'acostumen a separar les diferents direccions que depenen directament de la gerència del centre, com poden ser:

- La Direcció Financera,
- La Direcció Mèdica / Assistencial,
- La Direcció Infermera,
- La Direcció de Serveis Generals,
- La Direcció de Recursos Humans,
- La Direcció de Sistemes d'Informació.

De cadascuna d'aquestes direccions pengen directament departaments assistencials, de gestió administrativa, tecnològics, de suport, etc.

Tots ells tenen diferents necessitats dels Sistemes d'Informació que cal satisfer. Per això es indispensable una oficina o departament de gestió de projectes que sigui transversal i amb una visió global de l'estratègia de l'organització.

La informació s'ha de compartir, ja que per exemple, una intervenció quirúrgica sobre un pacient s'ha de reflectir a la seva històrica clínica, caldrà material quirúrgic amb una clara traçabilitat, s'haurà de traslladar a planta per tal de recuperar-se de l'operació, caldrà gestionar dinars i sopars per aquest pacient, caldrà dotar un servei d'oci amb televisions a les habitacions, caldrà realitzar seguiment d'infermeria, caldrà realitzar proves de laboratori per valorar evolució, caldrà fer interconsultes amb altres especialitats si aplica, caldrà administrar medicació, caldrà gestiona l'alta, etc, etc, etc.

És a dir, moltes accions que cal centralitzar a una o diferents eines integrades que permetin gestionar la totalitat de l'estada d'una persona a un centre sanitari.

En una organització amb centre d'investigació s'afegeixen els requeriments propis de la seva activitat, com estar a l'avantguarda de nous programes que ajudin a desenvolupar aquesta tasca innovadora.

Per gestionar tota aquesta demanda els departaments de TI acostumen a assignar caps de projectes que canalitzin les peticions i abordin les necessitats amb el coneixement que poden tenir. És factible que determinades figures estiguin relacionades amb l'àmbit clínic. No és estrany trobar directors de SI o personal de gestió de projectes que són metges, ja que coneixen de primera mà les necessitats del personal facultatiu del centre.

La externalització de determinats serveis o processos dels departaments de TI és una solució vàlida per alliberar de càrrega estructural. Serveis com el desenvolupament d'aplicacions, l'administració de sistemes, els serveis d'atenció a l'usuari, l'administració de la xarxa, els serveis d'impressió, etc. son àmbits on es molt normal externalitzar-los.

Per fer seguiment del compliments dels nivells de servei s'acostuma a treballar amb alguna eina de tíqueting, com poden ser Jira Service Desk, OTRS o Remedy, per exemple. S'apliquen ANS (Acords de nivell de servei) que permeten garantir els temps de resposta i la qualitat del servei.

La correcta gestió dels canvis TI és indispensable. En aquest sentit existeixen metodologies com ITIL, que ajuden a assolir aquest objectiu. Són conjunts de conceptes i bones pràctiques per gestionar la qualitat i eficiència a les operacions de TI.

7 Conclusions.

Les organitzacions sanitàries públiques i privades tenen la responsabilitat de donar un servei assistencial de màxima qualitat als ciutadans.

El nivell d'excel·lència que aconsegueixen i el seu prestigi es fonamenta en diferents aspectes, com per exemple: el conjunt de professionals de l'organització, la recerca contínua i els projectes d'investigació, la gestió que des de gerència es fa del centre, l'equipament tecnològic, els serveis de suport, les infraestructures, etc.

El paper dels Sistemes d'Informació és molt important, ja que té una implicació directa en la pressa de decisions assistencials i en la disponibilitat dels recursos que fan servir els diferents col·lectius d'un centre d'aquestes característiques: personal facultatiu, administratiu, infermer, logístic, tècnic, diagnòstic, etc.

El fet que la capacitat i disponibilitat dels sistemes informàtics afecti d'una manera tant directe als circuits i processos assistencials fa que les connotacions i criticitat dels sistemes siguin diferents a d'altres tipus d'empreses on l'impacte pot ser evidentment econòmic, però no implica el diagnòstic i tractament de malalties o intervencions sobre les persones.

En aquest sentit, aquest treball de fi de grau proposa una sèrie d'aspectes bàsics que serveixen per garantir l'alta disponibilitat dels sistemes.

Un cop identificats els processos crítics per l'organització cal assegurar que la infraestructura es dimensioni adequadament per tal de poder donar servei totes les hores de l'any. Òbviament caldrà establir un calendari d'aturades de manteniment dels sistemes, pactats amb la direcció corresponent, però l'objectiu ha de ser consolidar un 100% de disponibilitat.

L'alta disponibilitat requereix de duplicitat d'infraestructura, ja sigui en instal·lacions locals o remotes. Els dispositius de xarxa, cabines d'emmagatzematge, servidors físics i centres de procés de dades (CPDs) han d'estar replicats per garantir el funcionament ininterromput dels sistemes, vers incidències o averies que obliguin a que part de la infraestructura no estigui operativa mentre es soluciona el problema.

Aquest treball orienta sobre diferents aspectes per garantir aquesta duplicitat, basant-nos en els productes del mercat i els fabricant més rellevants i consolidats.

S'analitzen els requeriments bàsics que han de tenir els Centres de Procés de Dades o CPDs per donar servei continuats, així com els nivells de redundància i processos de recuperació.

La virtualització de servidors ofereix una molt bona solució per garantir escalabilitat horitzontal, a l'hora que permet molta flexibilitat per treballar amb diferents sistemes operatius i una ràpida creació d'entorns de proves per validacions i tests.

A banda de la rèplica de maquinari físic i els sistemes de programari que ofereixen continuïtat de negoci en cas de falles, un aspecte a destacar i que el treball aborda de forma explícita són els sistemes de còpies de seguretat i restauració d'informació crítica per l'organització.

En aquest sentit, és molt important identificar i garantir els processos indispensables per garantir l'activitat assistencial i administrativa de l'entorn sanitari.

No es pot deixar de banda l'evolució del mercat i els canvis que impulsa la tecnologia. Els nous sistemes predictius basats en intel·ligència artificial, *Machine Learning*, o les bases de dades no relacionals, estan abordant d'una manera molt important el diagnòstic mèdic. Cada cop són més necessaris aquest tipus de solucions que ajuden els facultatius en la seva tasca diària.

Això, juntament amb la gestió del cicle de vida de les solucions de programari, obliguen a evolucionar i garantir suport oficial de tota la infraestructura i el software instal·lat. Una correcta gestió de versions i control de garanties és bàsic per poder conviure amb la pròpia inèrcia del mercat.

L'ERP és l'eina d'ús comú proposada, tot i que en el món sanitari existeix el mòdul específic de Sanitat, que comporta una sèrie de característiques diferenciadores vers la resta. La integració d'aquest mòdul es especialment complex, ja que els centres sanitaris tenen normalment moltes aplicacions departaments específiques, comercialitzades per proveïdors especialistes en àmbit assistencial.

Aplicacions de tractament d'imatge cardíaca, radiològica, gastrointestinal, dermatològica, etc. s'han d'integrar amb la història clínica del pacient, normalment emmagatzemada a l'ERP. Generació d'informes amb resultats de laboratoris, diagnòstics, altes i baixes, informes clínics o classificació de pacients crítics a urgències generals (Triatge) són només alguns dels exemples de sistemes integrats amb les solucions verticals de sanitat que ofereixen els ERPs del mercat.

Certament ha estat un treball interessant des del punt de vista de recerca d'informació i contrast de punt de vista amb professionals dels sector, que m'han ajudat a definir i validar la proposta.

8 Bibliografia.

https://www.computerworld.es/cloud/la-nube-no-ignora-los-atributos-tradicionales-del-cpd-confianza-control-y-seguridad

https://lynxview.es/redefiniendo-la-contingencia-en-la-era-devops/

https://empresas.blogthinkbig.com/cpd-centro-procesamiento-nube-cloud/

http://servinfor.webcindario.com/?page_id=394

Administracion 24X7. Centros de Procesos de Datos para contingència y continuidad de negocio. (Comunicacion_TCO-295-2007WD)

https://www.sap.com/spain/index.html

https://www.commvault.com/es-es/

https://www.veritas.com/protection/netbackup

https://www.seisamed.com/como-disenar-y-organizar-las-areas-criticas-de-un-hospital

https://www.cerner.com/es/es

https://www.huawei.com/es/

https://softwarepara.net/hospitales/

http://www.recercasantpau.cat/es/

http://www.santpau.cat/

https://barcelonahealthhub.com/

http://systemadmin.es/2010/05/alta-disponibilidad-cluster-activo-activo-y-activo-pasivo

https://trustnet.com.mx/2020/10/20/alta-disponibilidad-esquemas-activo-activo-y-activo-pasivo/

https://www.vmware.com/es.html