LES PÍNDOLES DEL DPD

PÍNDOLA 41.- Seguretat al núvol en els serveis de salut

L'Agència Europa d'Informació i Seguretat (ENISA) ha publicat el seu últim informe anomenat '*Cloud Security for Healthcare Service*' on proporciona un conjunt de consells i bones pràctiques sobre seguretat i protecció de dades a l'hora d'utilitzar serveis al núvol en l'àmbit sanitari.

I. Introducció

La pandèmia de COVID-19 ha impulsat l'ús de la tecnologia basada en el núvol dins del sector sanitari, especialment en telemedicina, en consultes mèdiques i en intel·ligència artificial per a propòsits de tria. La integració d'aquests serveis de computació al núvol en el sector incrementa l'eficiència operativa però alhora planteja preocupacions relatives a la seguretat i a la protecció de dades. L'objectiu d'aquest informe és ajudar a garantir la seguretat (tant en l'àmbit de la ciberseguretat com en l'àmbit de la protecció de dades) de les solucions al núvols destinades a serveis de salut.

II. Solucions al núvol en l'àmbit sanitari

Existeixen diferents tipus de serveis al núvol: **IaaS** o infraestructura com a servei, on el proveïdor proporciona recursos computacionals en línia, **PaaS** o plataforma com a servei, on es proveeixen servidors preparats per executar les aplicacions del client, **SaaS** o software com a servei, on el proveïdor entrega directament aplicacions web als clients. D'altra banda el model de desplegament d'aquestes solucions es pot classificar segons si el núvol és privat, públic, híbrid o governamental.

Concretament en l'àmbit sanitari cada cop existeixen més tipus de solucions al núvol, que es poden desplegar en els diferents tipus de serveis i models descrits. A continuació s'enumeren els més importants descrivint breument les seves funcionalitats:

- Sistemes de planificació de recursos (ERP): aquests sistemes permeten dur a terme la gestió de pacients, inventari, assegurances mèdiques, recursos humans i d'altres dades no clíniques.
- Sistemes d'informació de salut (HIS): s'utilitzen per gestionar dades sanitàries dels pacients (registres, imatges, vídeos, etc.). Serveis al núvol relacionats: registres de salut electrònics, sistemes d'arxivament i comunicació d'imatges, sistemes d'informació radiològica, sistemes d'informació de laboratori, suport de decisió clínica o monitorització remota de pacient.
- Anàlisi de dades de salut: tant la intel·ligència artificial com l'aprenentatge automàtic s'utilitzen en salut per donar suport a la recerca mèdica, per fer diagnosis, anàlisis de dades, recomanacions de tractaments o compromisos amb les pacients.
- Dispositius mèdics: permeten als pacients mesurar la freqüència cardíaca o el nivell d'insulina, entre altres coses, des de casa mentre les dades estan disponibles directament per als professionals sanitaris que els permet fer un seguiment del tractament o programar una cita.
- Serveis de telemedicina: és un servei sanitari proporcionat mitjançant tecnologia de telecomunicacions. Les àrees d'aplicació comprenen la teleconsulta i l'assistència de telefonia mitjançant eines de conferències o videoconferències.

III. Consideracions de ciberseguretat i protecció de dades

A continuació s'identifiquen els principals reptes i obstacles relatius a la ciberseguretat i protecció de dades dels serveis sanitaris basats en el núvol anteriorment comentats; com son la falta de confiança en les solucions al núvol, la manca de seguretat i coneixements tècnics, la poca inversió actual en

ciberseguretat, la manca de legislació tant europea com nacional en aquest àmbit, la dificultat dels proveïdors per identificar els requisits legals i la complicada integració de núvol amb els sistemes heretats.

Aquests son els **reptes pertinents a la protecció de dades** més comuns a l'hora de desplegar serveis d'aquest tipus:

- Privacitat per disseny i per defecte: Esdevé un requisit legal, establert per l'RGPD, seguir un enfocament de privacitat per disseny i per defecte alhora de desenvolupar i desplegar el servei. Es recomanen tècniques com la minimització, pseudonimització, transparència, control de les dades personals per part dels subjectes, etc. per assolir aquest requisit. Incloent la preceptiva realització de l'Avaluació d'impacte relativa a la Protecció de Dades (AIPD).
- Gestió de dades: depenent del tipus de servei al núvol la informació d'entrada pot arribar de diverses fonts, per tant establir la legitimació en el tractament i els controls per assegurar la precisió han d'estar sempre en marxa. Les organitzacions han d'establir el seu propi marc de governança de dades per entendre quin tipus de dades és el més delicat i després aplicar-hi els controls requerits.
- Supressió de dades: s'han de poder esborrar les dades després que expiri el termini de conservació, però també a petició del subjecte sense demora indeguda, si per exemple les dades ja no són necessàries per als propòsits inicials o si el subjecte retira el consentiment.
- Portabilitat de dades: la transferència de les dades d'un proveïdor a un altre sense pèrdua és un des reptes més comuns pel que fa la computació al núvol. Pel nostre cas, l'assistència sanitària, existeixen certes normes (com l'HL7) per garantir la interoperabilitat.
- Encriptació: és important garantir la confidencialitat i la integritat de les dades en tots els diferents canals de transferència i emmagatzematge. Les mesures d'encriptació s'han d'aplicar tant a nivell de client com de servidor, així com en el canal que els connecta.

D'altra banda, les **amenaces més comunes en matèria de ciberseguretat** són les següents: **fenòmens naturals**, fallades en la **cadena de subministrament** (proveïdors del servei al núvol, de xarxa), **errors humans** (accessos no autoritzats a dades, desacatar les normes, canvis no intencionats, errors dels administradors del servei), **accions malintencionades** (malware, hijacking, phishing, denegacions del servei, abús de recursos computacionals del núvol, intercepció de dades en trànsit, atacs a aplicacions mòbils, amenaces internes, interfícies insegures), **fallades del sistema** (de hardware, software, de configuració, de falta de manteniment, de xarxa).

IV. Mesures de seguretat al núvol en serveis de salut

Aquesta secció proporciona un conjunt de directrius i mesures per tal de garantir la ciberseguretat i la protecció de dades per als clients de serveis al núvol en del sector sanitari:

- Involucrar a les parts interessades necessàries (DPD, departament legal, TIC, de risc, etc.) en el procés de contractació. La sol·licitud de requisits ha de comportar el compliment de la normativa.
- Realitzar una avaluació de riscos d'acord amb les directrius nacionals o seguint una metodologia coneguda per identificar les amenaces i riscos de ciberseguretat i protecció de dades (AIPD) per als nous serveis al núvol i avaluar l'impacte en el risc de seguretat global.
- Assegurar la selecció de proveïdors que ofereixin garanties suficients per aplicar les mesures tècniques i organitzatives adequades, de manera que el tractament sigui conforme als

requisits de la normativa de protecció de dades i garanteixi la protecció dels drets de l'interessat, incloent:

- Assegurar un pla de resposta per definir les accions que s'han de prendre després d'un incident de seguretat al proveïdor de serveis (que ha de tenir un procés per a gestionar incidents de seguretat d'acord amb la legislació europea o nacional).
- Assegurar que el proveïdor de serveis notifiqui amb antelació els temps d'inactivitat planificats (per exemple les aturades per manteniment).
- Eliminar les dades del proveïdor de serveis al núvol (i retornar si fos necessari), immediatament després de la terminació de l'acord contractual o si s'assoleix la limitació del termini de conservació de dades.
- Definir requisits per al registre d'esdeveniments (*logs*) i verificar si el proveïdor de serveis al núvol els compleix.
- Identificar l'abast de la responsabilitat de la gestió vulnerabilitats tècniques i la gestió dels pedaços (*patch)*. Determinar i configurar els processos per a la gestió vulnerabilitats.
- Incloure la informació i els actius emmagatzemats en l'entorn del núvol en l'inventari d'actius. Indicar on s'emmagatzemen les dades i supervisar i enregistrar els canvis d'actius.
- Assegurar que les dades en la ubicació del proveïdor de serveis al núvol estiguin encriptades durant tot el cicle de vida de les dades (creació, emmagatzematge, ús, compartició, arxivament i supressió).
- Definir requisits de seguretat i procediments per a la gestió de claus.
- Assegurar que totes les dades es proporcionen en format estàndard a petició del proveïdor de serveis al núvol.
- Identificar tots els dispositius com ara ordinadors portàtils, dispositius mòbils, dispositius mèdics, etc. del personal que es connecta al servei al núvol.
- Assegurar que les polítiques d'accés especifiquin requisits de seguretat per a l'accés a les dades, interfícies d'aplicació, sistemes i la xarxa per a cada servei al núvol.
- Establir un programa de sensibilització i formació orientat a grups de destinació regular per a tots els actors que s'ocupen de dades sensibles com ara registres de salut electrònics o diagnòstic mèdic.
- Assegurar que el trànsit entre les connexions no fiables i de confiança dels entorns de xarxa i les instàncies virtuals està restringit i monitoritzat.
- Assegurar que el proveïdor aplica una segmentació adequada per a: les dades, aplicacions (físiques i virtuals), infraestructura i xarxa entre diferents inquilins per restringir l'accés d'un als recursos d'altres.

V. Riscos en protecció de dades

D'altra banda, l'Agència Espanyola de Protecció de Dades (AEPD) analitza, en la guia '*Tecnologías y Protección de Datos en las AA.PP'*, un conjunt de tecnologies senyalant els riscos relatius a la protecció de dades que les administracions públiques, com a responsables, han de tenir en compte a l'hora d'incorporar-les com a suport als tractaments que realitzin.

LES PÍNDOLES DEL DPD

En concret, sobre les tecnologies al núvol (*cloud computing*) posa èmfasi en els següents punts:

- La contractació d'un servei al núvol no suposa un desplaçament total de les obligacions de gestió de la seguretat a l'encarregat del tractament sinó que correspon sempre al **responsable del tractament** la presa de decisions amb relació als requisits de protecció de dades personals, que hauran de comptar amb els **requisits que s'estableixen a l'article 32 del RGPD**.

- Per evitar produir-se una infracció de la normativa de protecció de dades, el **responsable** ha d'escollir a un encarregat que **ofereixi garanties**, oferint-li, a través d'un contracte, les **instruccions i maneres de procedir** quan realitzi tractaments de **dades personals.**

- L'administració també ha de **gestionar els riscos** en cas que el proveïdor del núvol decideixi **discontinuar el servei** o canviar les condicions en que es presta, així com el risc legal de que existeixin **canvis normatius** o d'altres naturaleses que impedeixin la utilització dels serveis. En aquest sentit s'han de desenvolupar mesures i plans de contingència de **migració dels serveis** a altres sistemes.

- En cas de produir-se **violacions de seguretat**, el responsable ha de posar en marxa una sèrie de mecanismes de forma urgent, i notificar a **l'Autoritat de Protecció de Dades**, en un termini de 72h la informació que tingui al respecte. L'Autoritat pot ordenar al responsable **comunicar als usuaris** que s'hagin vist afectats de manera que puguin adoptar mesures de seguretat i protecció.

- A l'hora de dissenyar el tractament, s'ha d'avaluar la incorporació i aplicació de mecanismes de **minimització** de dades en funció del risc, **limitar l'extensió** de les dades, pujar al núvol solament dades **anonimitzades** o **pseudonimitzades**, emprar **xifrat** homomòrfic, etc.

- És important també analitzar formalment i avaluar rigorosament els **riscos de reidentificació**, així com el nivell de maduresa dels **processos d'anonimització** utilitzats per l'organització.

Per a més informació:

- https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services
- https://ticsalutsocial.cat/dpd-salut/avaluacio-dimpacte-relativa-a-la-proteccio-de-dades-aipd-en-salut/
- https://www.aepd.es/es/media/guias/guia-tecnologias-admin-digital.pdf

Per qualsevol dubte o aclariment addicional podeu adreçar-vos al DPD de Salut:

dpd@ticsalutsocial.cat
https://ticsalutsocial.cat/oficina-dpd/
Tel.: 93 553 26 42 (9:00 a 14:00 h.)