ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

Ревизија
сврсисходности
пословања

Информациона безбедност у здравственим информационим системима

2020. година

Зашто смо одабрали тему
„**Информациона** безбедност у **здравственим** информационим системима“?

Значај дигитализације

Značaj digitalizacije za reviziju poslovanja korisnika javnih sredstava

01. jun 2019. godina

tweet!

Дигитализација поступка ревизије већ 2020. године

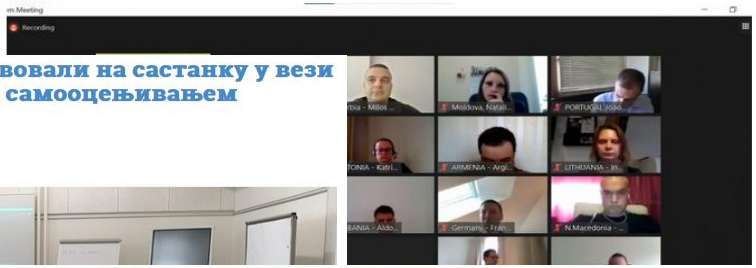
23. новембар 2018. година

tweet!

Представници ДРИ учесници на е-семинару ЕУРОСАИ ИТ Радне групе „ВРИ и дигитални заокрет: Развијање ИТ вештина и капацитета за ИТ ревизију“

13. новембар 2020. година

tweet!



Представници ДРИ учествовали на састанку у вези са самооцењивањем ИТ и самооцењивањем ревизије ИТ у Берну

05. март 2020. година

tweet!

Размена искуства у ИТ подршци у поступку ревизије

15. новембар 2018. година

Учешће представника ДРИ на радионици посвећеној ИТ ревизији

21. септембар 2018. година

tweet!

Зашто смо одабрали тему „**Информациона** безбедност у **здравственим** информационим системима“?

Стратешки план ДРИ 2019-2023.

- У будућим ревизијама, пре свега правилности и сврсисходности пословања, планираћемо теме које имају потенцијал да максимално допринесу користима за друштво и грађане. Бавићемо се претежно темама из **здравства**, социјалне заштите, заштите животне средине итд
- Потциљ 1.7. – Здравство: ДРИ ће својим радом допринети **унапређењу здравствене заштите** грађана... Здравствени систем Србије суочен је са **изазовима** који са собом носе започете структурне реформе: **увођење ИЗИС-а**, е-рецепта... **Државна ревизорска институција ће и у наредном периоду спроводити ревизију здравствених** и апотекарских **установа** и других институција задужених за планирање, финансирање и остваривање права пацијената, са циљем да се обезбеде подаци о коришћењу ресурса за одржавање и унапређење здравственог стања грађана и дају **препоруке за унапређење функционисања здравственог система.**
- Потциљ 2.5. - Унапредити јавно управљање и коришћење информационих технологија (ИТ): ДРИ је кроз своје **ревизије у претходном периоду** утврдила да **већи број субјеката ревизије није предузео неопходне мере у области безбедности ИТ система** − укључујући и **права на приступ подацима**, поверљивост података и мере којима се обезбеђује **обављање послова у ванредним околностима**; нису спровели неопходне **процене ИТ ризика**, нити су усвојили **стратегије које регулишу развој ИТ технологија**. Ово неадекватно планирање ИТ развоја довело је до **кашњења у реализацији пројеката** укључујући и **увођење нових интегрисаних пословних ИТ система** што је резултирало додатним трошковима. ДРИ ће помоћи да се унапреди способност и поузданост ИТ система.

Зашто смо одабрали тему
„**Информациона** безбедност у **здравственим** информационим системима“?

Значај дигитализације

"DA SAM ZNALA ŠTA NAS ČEKA, PRIORITET BI BILA DIGITALIZACIJA ZDRAVSTVA" Premijerka Ana Brnabić o elektronskim zdravstvenim kartonima, ubrzanim testovima na koronu i trendu obolelih

Tanjug · 14.07.2020. 01:04 · Komentara (3) Tweet

Preciznost cifara

"Kad smo počeli borbu protiv korone, nismo imali nikakav sistem. Pitajte Batut kako se prikupljaju te cifre – tako što zovemo telefonom i svaka lokalna samouprava vam javlja podatke. Onda smo napravili kakav takav sistem", kaže Brnabić.

"Napravili smo ad hok bazu za kovid, za grip nemamo takvu... Ovaj put smo očekivali pohvalu što se borimo kao društvo", kaže Brnabić.

Rebić: Informaciona bezbednost strateški prioritet Srbije

Brnabić: Ubrzano raditi na digitalizaciji zdravstvenog sistem

25.01.2021. 19:26 · Komentara (3) Tweet

Формира се Координационо тело за дигитализацију у здравственом систему

Београд, 14. јануар 2021.

На седници је донета одлука о образовању Координационог тела за дигитализацију у здравственом систему

Основне информације

Руковалац подацима који чине Интегрисани здравствени информациони систем Републике Србије је **завод за јавно здравље основан за територију Републике Србије**.

Надзор над спровођењем овог закона врши **министарство надлежно за послове здравља**.

Одредбе Закона о здравственој документацији и евиденцијама у области здравства
(члан 44. став 4 и члан 52.)

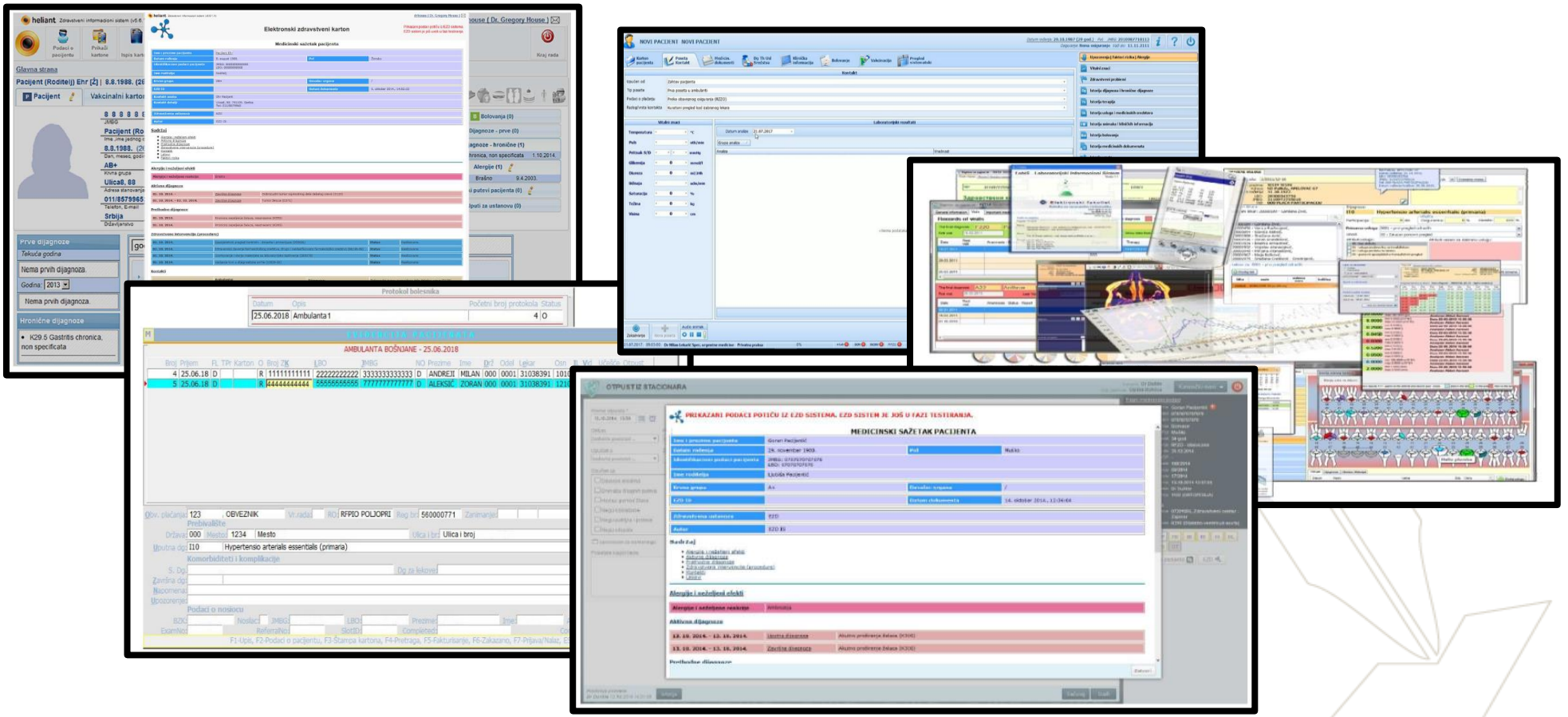
У Институту „Батут“ је тренутно у функцији неколико информационих система (база података) које администрирају запослени у Центру за информатику и биостатистику

Интегрисани здравствено информациони систем чине:

- здравствено-статистички систем
- информациони системи организација здравственог осигурања
- здравствени информациони системи здравствених установа, приватне праксе и других правних лица

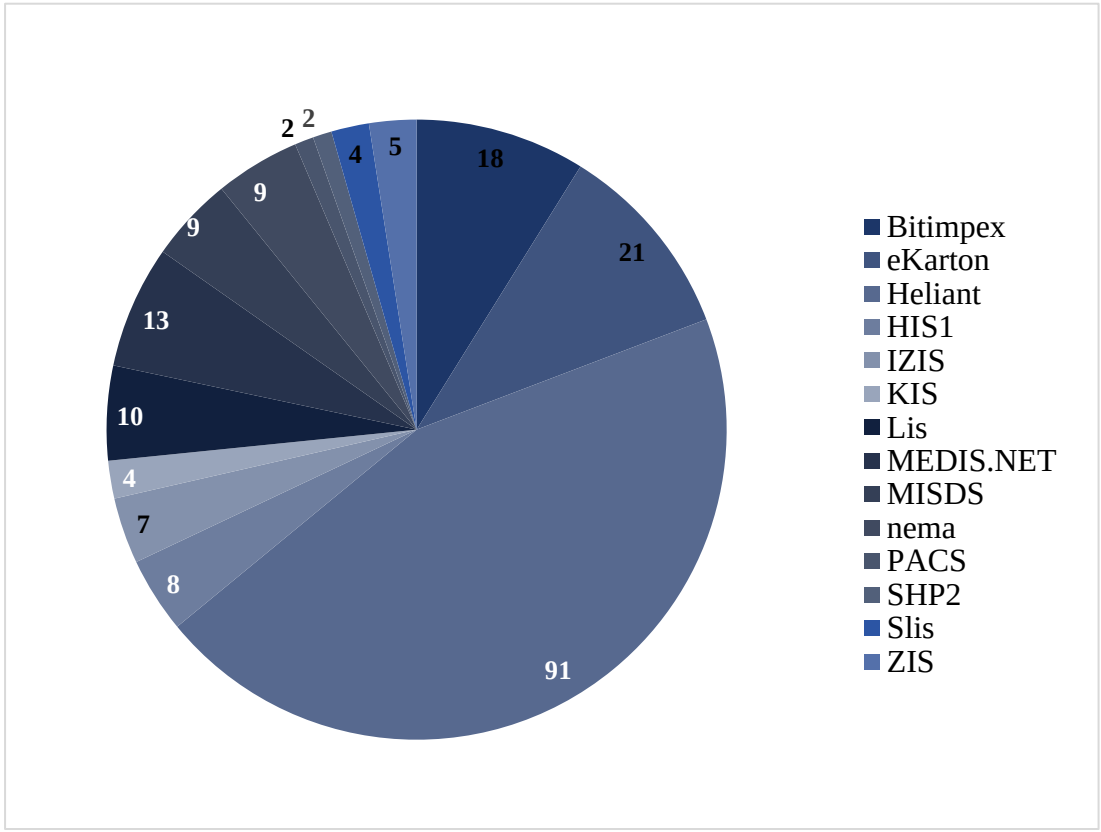
Основне информације

- Најзаступљенији ИС-и у самим здравственим установама су: Heliant, BitImpeks, eKarton, Medis.Net, HIS итд.



Основне информације

- Најзаступљенији ИС-и у самим здравственим установама су: Heliant, BitImpeks, eKarton, Medis.Net, HIS итд.



Циљ ревизије

- да се оцени у којој мери су примењене мере у здравственим информационим системима у Републици Србији испуниле неопходне циљеве када је у питању информациона безбедност.

Ревизијска питања:

1. У којој мери су успостављени системи управљања здравственим информационим системима омогућили испуњење пословних циљева, успостављање јасно дефинисане организационе структуре и управљање ризицима?
2. Да ли је успостављен ефективан оквир за континуитет пословања у случају ванредних околности?
3. Да ли успостављене мере безбедности података у здравственим информационим система обезбеђују доступност, поверљивост и интегритет?

Субјекти ревизије

Министарство здравља

Покрајински секретаријат за здравство Војводине

Институт за јавно здравље Србије "Др Милан Јовановић Батут"

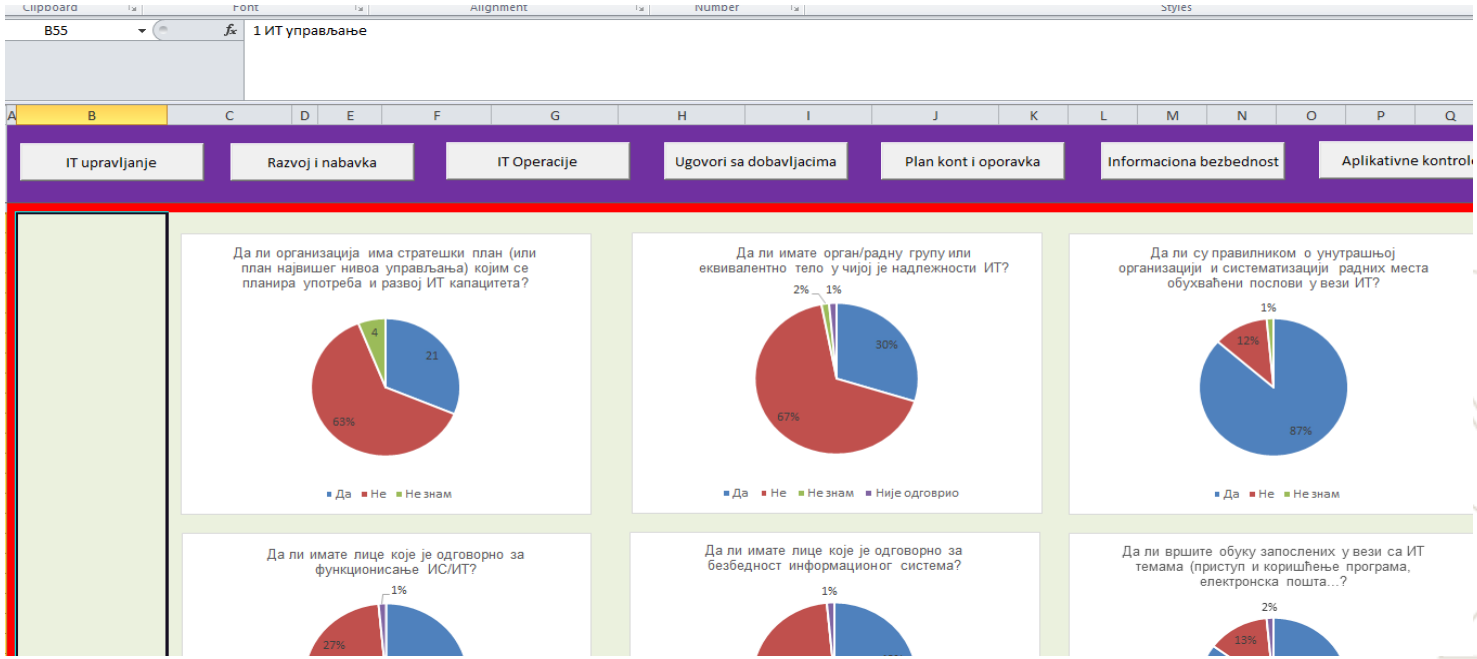
- Оснивачи здравствених установа
- Руковалац подацима у ИЗИС-у

Период обухваћен ревизијом

- ревизија била усмерена на период 2017-2019. год.

Методологија рада и ограничења

- Да бисмо одговорили на ревизорска питања, анализирали смо законску и подзаконску регулативу, користили стручну литературу (WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions), као и све податке добијене од субјеката ревизије и извора информација - здравствених установа. Анализирали смо податке и информације за период од 2017. до 2019. године.
- Извршена је процена ризика у 7 ИТ области, тј. у укупно 45 подобласти, и на основу ове процене, одређене су три области које су ревидиране



Ограничења

- Услед ситуације са вирусом COVID-19 у току целе 2020.-те године и посебно ангажовања и надлежности Министарства здравља, Института „Батут“, Покрајинског секретаријата, и здравствених установа у време и након окончања ванредног стања, и у време након тога у борби за сузбијање вируса, дошло је до споријег прикупљања документације;
- Доношење закључака на бази анализе ограниченог броја здравствених установа, самим тим је било немогуће генерализовање налаза, односно закључака ревизије.

Узорак

- Критеријуми за одабир здравствених установа били су: географска припадност, здравствени информациони систем, величина установе

ИТ области

- **ИТ управљање**
  - ИТ стратегија и стабилно финансирање
  - Организациона ИТ структура
  - Процена ИТ ризика
- **Континуитет пословања и опоравак од катастрофе**
  - Континуитет пословања
  - Опоравак од катастрофе
  - Резервне копије
- **Информациона безбедност**
  - Организација ИТ безбедности
  - Уговори са пружаоцима услуга
  - Приступ систему и приступ подацима осигураника

ИТ области

- ИТ управљање
  - ИТ стратегија и стабилно финансирање
  - Организациона ИТ структура
  - Процена ИТ ризика
- **Континуитет пословања и опоравак од катастрофе**
  - Континуитет пословања
  - Опоравак од катастрофе
  - Резервне копије
- Информациона безбедност
  - Организација ИТ безбедности
  - Уговори са пружаоцима услуга
  - Приступ систему и приступ подацима осигураника

ИТ области

- ИТ управљање
  - ИТ стратегија и стабилно финансирање
  - Организациона ИТ структура
  - Процена ИТ ризика
- Континуитет пословања и опоравак од катастрофе
  - Континуитет пословања
  - Опоравак од катастрофе
  - Резервне копије
- **Информациона безбедност**
  - Организација ИТ безбедности
  - Уговори са пружаоцима услуга
  - Приступ систему и приступ подацима осигураника

ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

КЉУЧНА ПОРУКА

Потребно је да Министарство здравља, Институт „Батут” и Покрајински секретаријат за здравство унапреде мере информационе безбедности што ће допринети већој поузданости здравствених информационих система у Републици Србији.

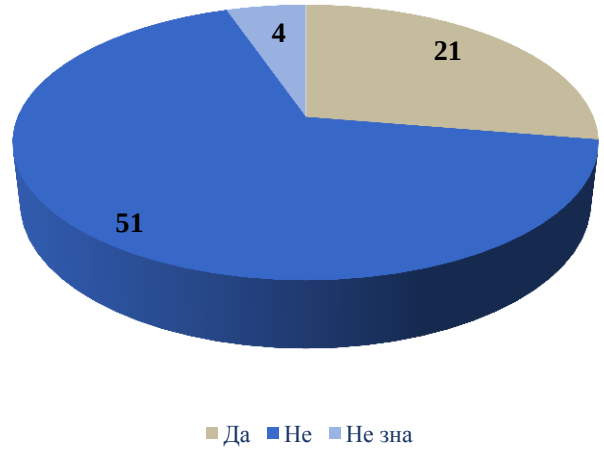
Постојећи системи ИТ управљања у здравству нису у потпуности омогућили испуњење пословних циљева, тачније пуну имплементацију Интегрисаног здравственог информационог система, процену ИТ ризика и успостављање адекватне организационе ИТ структуре

- Стратешко планирање
- Стабилно финансирање које обезбеђује одржив систем
- Одговарајућа ИТ организација и усвојене процедуре
- Управљање ИТ ризицима

Не постоји стратешко планирање развоја и одржавања Интегрисаног здравственог информационог система, иако је то и законска обавеза Владе Републике Србије, што је довело до неправовременог и несвеобухватног развоја и одржавања здравствених информационих система

- Влада Републике Србије није донела Стратегију развоја и организације Интегрисаног здравственог информационог система.

Да ли здравствене установе имају стратешки план?



Министарство здравља, Покрајински секретаријат за здравство Војводине и здравствене установе, због непостојања стратешког планирања, нису обезбедиле стабилно финансирање здравствених информационих система самим тим ни развој и одржавање тих система, што за последицу има застареле рачунаре и сервере, застареле па самим тим и небезбедне оперативне системе, непостојање обука за запослене и недовољан број ИТ стручњака

- Просечно могуће набавити око 10-14 рачунара годишње по установи, без улагања у осталу опрему (мрежна, штампачи) и сервере, што је неодрживо

у динарима

Редни број	Година	Услуге по уговору	Нематеријална имовина	Машине и опрема
1	2017	50.000.000	280.000.000	30.000.000
2	2018	214.000.000	326.000.000	60.000.000
3	2019	185.369.000	490.000.000	34.631.000
Укупно за три године		449.369.000	1.096.000.000	124.631.000
Просечно по години и установи		4539080,808	11070707,07	103859,1667

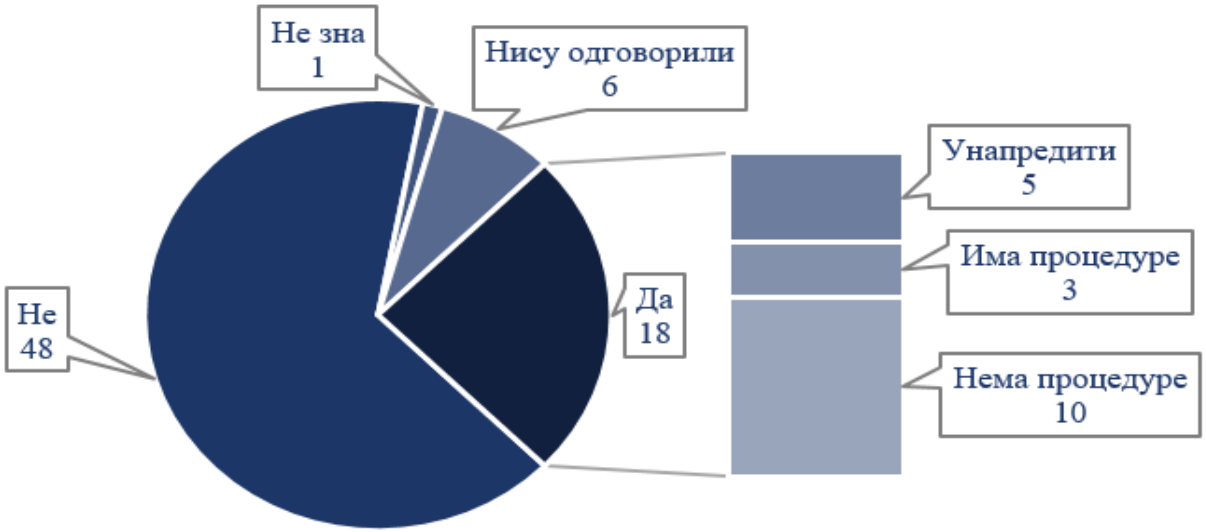
Финансирање из буџета

у динарима

Редни број	Година	Компјутерске услуге	Текуће поправке и одржавање опреме	Набавка - Рачунарска опрема
1	2017	74.695.055	6.093.097	15.292.398
2	2018	88.782.355	10.395.568	18.648.520
3	2019	92.993.297	11.769.076	28.582.651
Укупно за три године		256.470.707	28.257.741	62.523.569
Просечно по години и установи		2590613,202	285431,7273	631551,202

Финансирање из средстава ЗУ (33)

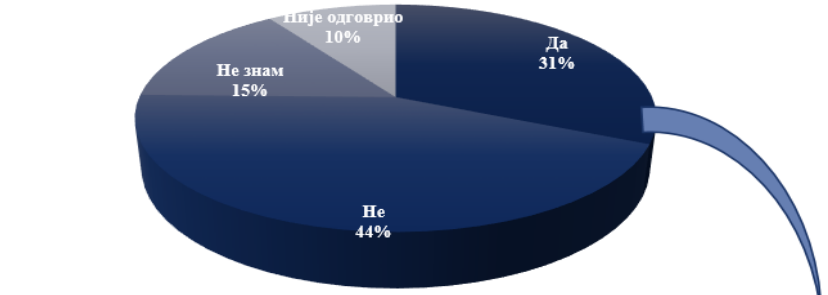
Министарство здравља, Институт за јавно здравље Србије „Др Милан Јовановић Батут“ и здравствене установе нису усвојиле процедуре за управљање ИТ пословима, иако су то и законски били у обавези, што онемогућава или отежава контролу ових послова од стране руководства или континуитет обављања послова у случају замене запослених на ИТ пословима



Да ли здравствене установе имају процедуре за управљање ИТ системима?

Министарство здравља и Институт за јавно здравље Србије „Др Милан Јовановић Батут“, као и установе које смо обухватили анкетом, нису успоставили управљање ИТ ризицима, иако је ово и законска обавеза, пре свега због непознавања ове проблематике, недовољно искуства и обученог ИТ кадра, а што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја, а који се могао спречити, или великих нефинансијских губитака (података на пример) због неблаговременог предузимања мера

Да ли су здравствене установе успоставиле управљање ИТ ризицима?



Ефективно управљање континуитетом пословања у случају ванредних околности у Интегрисаном здравстеном информационом систему није у потпуности успостављено, што за последицу може имати нефункционисање делова система у дужем временском периоду

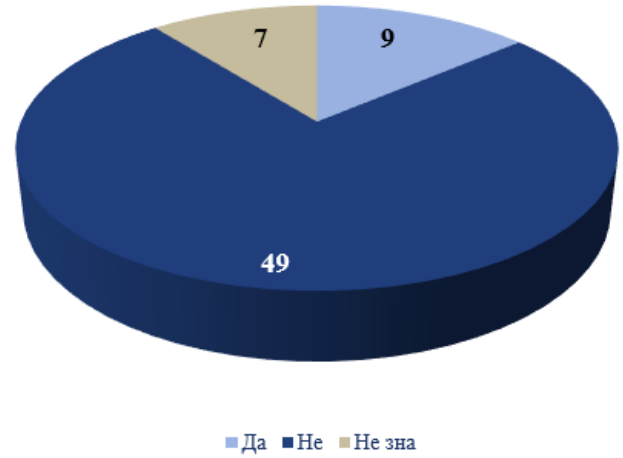
- План континуитета пословања
- План опоравка од катастрофе
- Управљање резервним копијама
- Тестирање планова континуитета пословања и опоравка од катастрофе

У систему Интегрисани здравствени информациони систем, нису усвојена ни имплементирана правила и процедуре за континуитет пословања код већине анкетираних установа, као ни на нивоу субјеката ревизије, Института за јавно здравље Србије „Др Милан Јовановић Батут“ и Министарства здравља, због недостатка довољно стручног знања и недостатка кадровских капацитета, иако је то и законска обавеза, а што може за последицу имати нефункционисање система у неодређеном временском периоду, па самим тим и отежано пружање услуга здравственим осигураницима

Да ли постоје планови/процедуре за континуитет пословања (одговори се односе на анктериране ЗУ)?

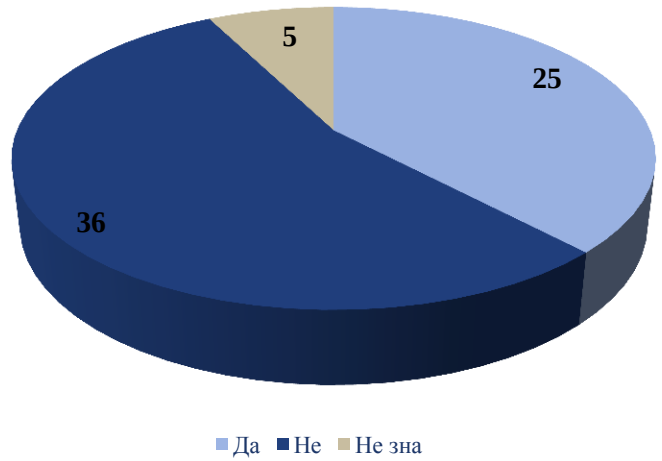
Институт за јавно здравље Србије „Др Милан Јовановић Батут“, Министарство здравља и анкетиране здравствене установе због недостатка потребне опреме, адекватног ИТ кадра и недовољно стручног знања нису обезбедиле ефективан план континуитета пословања у ванредним околностима – план опоравка од катастрофе, иако им је то била законска обавеза, што за последицу може имати нефункционисање информационог система у дужем временском периоду

Да ли постоје планови/процедуре за континуитет пословања у ванредним околностима – опоравак од катастрофе (одговори се односе на анктериране ЗУ)?



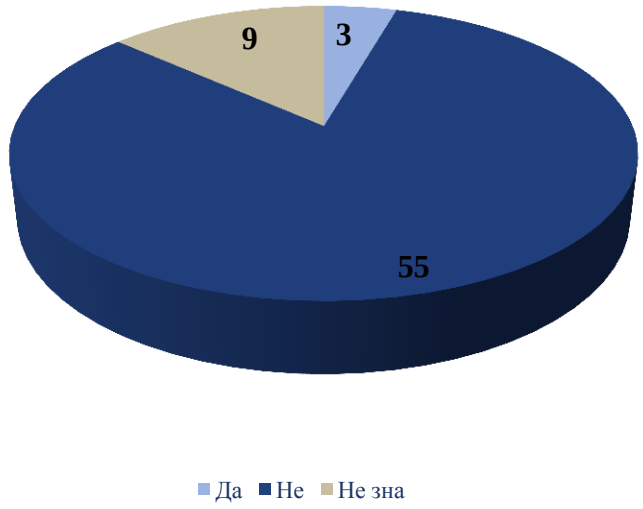
Резервним копијама података из здравствених информационих система се не управља на документован начин, зато што здравствене установе нису усвојиле одговарајуће процедуре, што су биле обавезе по закону, што отежава или онемогућава контролу овог процеса

Да ли су резервне копије смештене у безбедан простор за одлагање ван објекта?



Министарство здравља и Институт за јавно здравље Србије „Др Милан Јовановић „Батут“, као и здравствене установе које смо обухватили анкетом, не врше тестирање планова за континуитет и опоравак од катастрофе, зато што немају довољно ресурса за то - пре свега запослених са довољно знања и искуства, иако је верификација тих планова обавеза свих оператора ИКТ система од посебног значаја, а што за последицу може имати нефункционални систем у току и након ванредне ситуације у дужем временском периоду

Да ли се спроводи тестирање планова за континуитет пословања и опоравка од катастрофе?



Здравствене установе обухваћене анкетом нису усвојиле и примениле свеобухватне мере заштите информационих система, а Министарство здравља и Институт за јавно здравље Републике Србије „Др Милан Јовановић Батут“ нису успоставили управљање информационом безбедношћу Интегрисаног здравственог информационог система и контролу примене мера заштите као приоритет, што је неопходно како би била осигурана поверљивост, доступност и поузданост података о личном здрављу грађана

- Организација ИТ безбедности
- Заштита података у уговорима са пружаоцима услуга
- Правила и процедуре за контролу приступа информационом систему
- Управљање подацима о здравственим осигураницима

У систему Интегрисани здравствени информациони систем, организација ИТ безбедности није успостављена на адекватан начин, иако је то законска обавеза и субјеката ревизије и здравствених установа, што за последицу има већи степен рањивости овог система па самим тим и осетљивих података здравствених осигураника

- Обуке запослених на ИТ пословима везане за безбедност ИТ
- Усвојен акт о информационој безбедности
- Усвојене и примењене процедуре које се односе на информациону безбедност
- Успостављена одговарајућа организациона ИТ структура са јасно утврђеном поделом послова и дужности запослених
- Одређивање одговорног лица за обавештавање о инцидентима

Организација ИТ безбедности

- Обуке запослених на ИТ пословима везане за безбедност ИТ — 2
- Акт о информационој безбедности — 25
- Процедуре које се односе на ИТ безбедност — 17
- Одговарајућа ИТ организациона структура — ?
- Одговорно лице за обавештавање о инцидентима — 12

Организација ИТ безбедности

Процедуре које се односе на ИТ безбедност

Организација ИТ безбедности

Организациона ИТ структура

Институт за јавно здравље Србије „Др Милан Јовановић Батут“, Министарство здравља и анкетиране здравствене установе и поред тога што у уговорима са пружаоцима услуга постоји део који се односи на поверљивост података, нису успоставили механизам за контролу да ли пружалац услуга ту обавезу поштује, због недостатака кадровских капацитета, недоумица у вези законске регулативе и недовољно стручног знања, што за последицу може имати одавање осетљивих података здравствених осигураника.

- Не постоје радна места које у опису послова има и праћење безбедносних клаузула у уговорима са пружаоцима услугаЗакон о заштити података о личности
- Само три здравствене установе усвојиле процедуре које се односе на одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга.
- У 6 случајева уговори нису садржали одредбе о поверљивости података

- Закон о правима пацијената
- Закон о заштити података о личности
- Закон о информационој безбедности

У информационим здравственим системима није успостављен процес одобравања и укидања приступа на задовољавајући начин, због тога што нису усвојене процедуре које уређују овај процес и није успостављена контрола тог процеса, иако је то законска обавеза, што за последицу може имати угрожену безбедност података здравствених осигураника

- Неусвајање процедура
- Контрола процеса
- 27 здравствених установа је доставило тражене процедуре.
- Али, од тог броја, само 3 здравствене установе усвојиле процедуре које детаљније уређују питања контроле логичког и физичког приступа

- Не постоје администратори, посао обављају пружаоци услуга
- Постоји више администратора, али користе исти налог
- Недостатак стручног ИТ кадра
- Едукација

Здравствене установе нису успоставиле максималну могућу заштиту приступа подацима осигураника (уз употребу електронске здравствене књижице или на начин који осигурава да се подацима осигураника не приступа без знања осигураника), нити су успоставиле мере контроле и заштите излазних података, што за последицу може имати неовлашћен приступ или изношење здравствених података

- Приступ основним подацима осигураника – да буде потврђено лично присуство осигураника, тј треба да се осигура да ће се његовим подацима приступити само када осигураник буде лично присутан или кад је дао сагласност.

- Излазни подаци - да се они генеришу само у законом уређене сврхе, заштита свих тих излазних података се постиже искључиво успостављањем строгих механизама контроле који се односе на то како се и коме ти подаци могу даље дистрибуирати.

Препоруке ДРИ

Министарству здравља, да:

- да предузме активности у смислу припреме предлога Стратегије развоја и организације интегрисаног здравственог информационог система и Акционог плана за примену Стартегије и да приликом припреме финансијских планова осигура стабилно финансирање циљева из Акционог плана за примену Стратегије

Покрајинском секретаријату за здравство Војводине, да:

- да приликом припреме финансијских планова осигура стабилно финансирање циљева из Акционог плана за примену Стратегије кроз детаљно планирање средстава за развој, набавку и одржавање информационих система у области здравства

Институту Батут, да:

- да уреди процес обраде података од стране пружаоца услуга у здравственим информационим системима на законом прописан начин, што подразумева обавезну примену мера заштите података, и може укључити процес сертификације и издавања посебног или општег писменог овлашћења другим обрађивачима

Хвала члановима тима и колегама у ДРИ!

Хвала свима са којима смо сарађивали у току ревизије!

Хвала вама на пажњи!

www.dri.rs

kancelarija@dri.rs