ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

Ревизија
сврсисходности
пословања

Информациони системи у правосуђу

Основне информације

- Правосудни информациони систем (ПИС) је прави пример тога како **дигитализација** може довести до **ефикаснијег рада и значајних уштеда** (до сада преко 7 милијарди динара).

- Ипак, поред нових функционалности **неопходно је усавршавати и све друге компоненте** информационих система.

- **Управљање** информационим системима АВП, СИПРЕС, САПС и ПИС потребно је уредити тако да се **омогући равноправно коришћење папирних и електронских докумената** и на тај начин додатно повећа ефикасност система, омогуће додатне још значајније уштеде и грађанима пруже нове е-услуге, **процедурама** уреде послови који се односе на овај систем и **финансијским плановима** омогући замена старих и небезбедних рачунара и оперативних система.

- Систем **информационе безбедности** је неопходно унапредити применом додатних неопходних мера заштите које обухватају усвајање и примену аката и процедура које се односе на ову област, одговарајућу ИТ организациону структуру, управљање континуитетом пословања и управљање ИТ ризицима.

- Потребно је унапредити **механизам сарадње са пружаоцима услуга** одговарајућим **процедурама** које треба да уреде мере заштите система, и омогуће контролу примене тих мера. Такође, **обраду података о личности** треба уредити на јасан начин, заснован на примени законских одредби

Основне информације

- Законом о уређењу судова, у члану 70. прописано је да су између осталог послови правосудне управе које врши министарство надлежно за правосуђе: уређење и развој правосудног информационог система.
- Судови су самостални и независни државни органи. Број судског особља одређује председник суда актом о унутрашњем уређењу и систематизацији радних места у суду. Председник суда руководи судском управом и одговоран је за правилан и благовремен рад суда. Суд републичког ранга, апелациони суд и суд са 30 и више судија има управитеља суда. Председник суда поверава управитељу суда обављање материјално-финансијских и организационо-техничких послова. Послови управитеља суда се детаљније уређују Судским пословником.

Судови опште надлежности	
Апелационих судова	4
Виших судова	25
Основних судова	66

Судови посебне надлежности			
Управни суд	1	**Прекршајних суд**	44
Седиште Управног суда у Београду	1	Одељења Прекршајног суда	3
Одељења Управног суда	3	**Привредни Апелациони суд**	1
Прекршајни Апелациони суд	1	**Привредних судова**	16
Седиште Апелационог суда у Београду	1	Подручја Виших судова	25

Основне информације

- У области правосуђа у Републици Србији, у употреби је више од 20 информационих система, који се користе за вођење предмета, размену података, увид у податке итд. Користе се у основним, вишим и апелационим судовима, прекршајним и привредним судовима, основним, вишим и апелационим јавним тужилаштвима, итд.
- АВП (Аутоматско Вођење Предмета). Сви основни и виши судови, осим Вишег суда у Сремској Митровици, са припадајућим судским јединица, користе децентрализован систем за управљање судским предметима, популарни назван АВП (аутоматско вођење предмета). Извршава се на серверима који се налазе у судовима, за разлику од преостала три система.
- САПС (Стандардизована апликација правосуђа Србије) тренутно је у употреби у: Врховном касационом суду и Управном суду у Београду, свим Апелационим судовима (Београд, Ниш, Нови Сад и Крагујевац) и Вишем суду у Сремској Митровици. САПС је информациони систем која се води и којом се управља централизовано.
- СИПРЕС (Систем прекршајних судова) Свих 45 прекршајних судова има аутоматизовани, централни информациони систем.
- ПИС (Правосудни информациони систем) Централизовани систем за размену података

Основне информације

Проблеми који су идентификовани у досадашњем периоду коришћења информационих система у правосуђу су: :

- застарели рачунари и небезбедни оперативни системи
- информациона безбедност није на неопходном нивоу
- није обезбеђен континуитет пословања у ванредним околностима и у случају раскида сарадње са пружаоцима услуга
- пружалац услуге има приступ продукционој бази
- обрада података о личности није уређена тако да су јасно разграничене улоге Министарства правде, судова и пружалаца услуга

Циљ ревизије

- да се оцени ефективност информационих система у правосуђу у Републици Србији.

Ревизијска питања:

1. У којој мери је успостављено ефективно управљање информационим системима у правосуђу?
2. У којој мери успостављене мере информационе безбедности обезбеђују поузданост информационих система у правосуђу?
3. У којој мери је успостављен механизам сарадње са пружаоцима услуга испунио све неопходне циљеве, укључујући и поузданост података?

Субјект ревизије

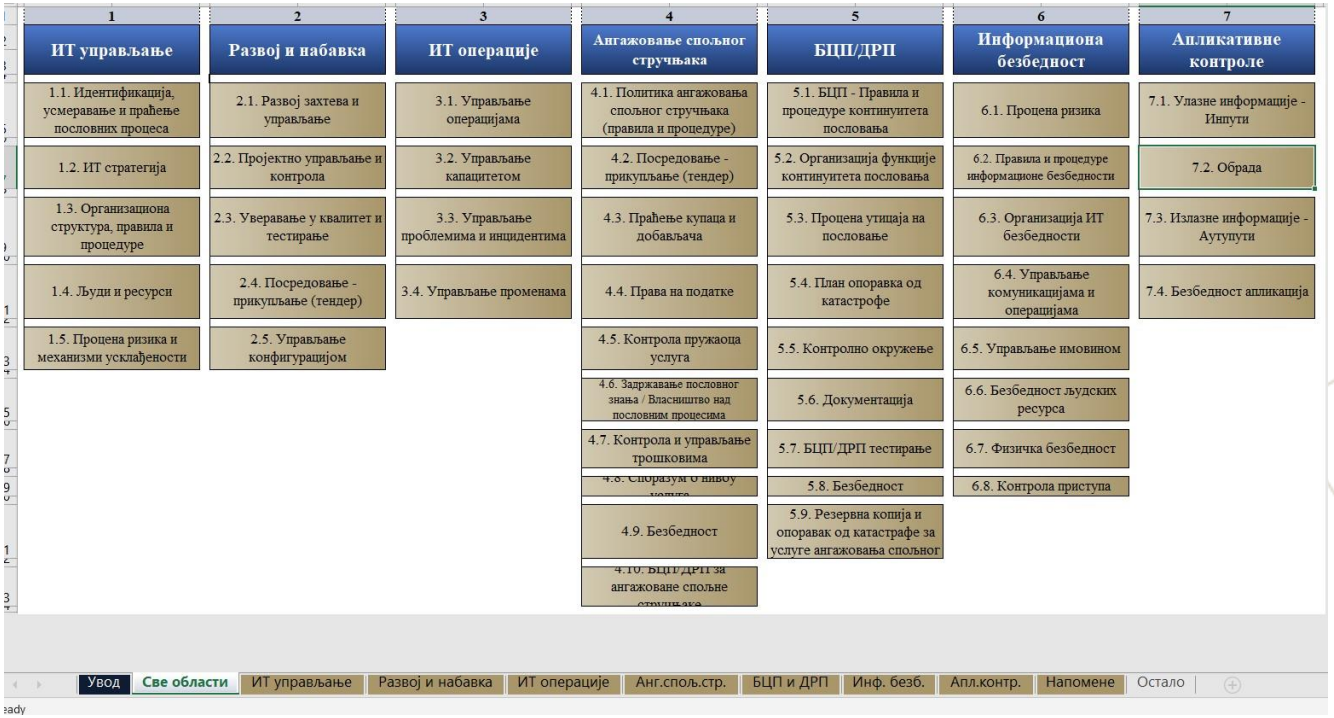
Министарство правде

Период обухваћен ревизијом

- ревизија обухватила период 2019-2021. 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 субјекта ревизије и извора информација – судова.
- 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



ИТ области

- **ИТ управљање**
  - Планирање и стабилно финансирање
  - Управљање системом
  - Измене
- **Информациона безбедност**
  - Организација ИТ безбедности
  - Континуитет пословања
  - Управљање ризицима
- **Сарадња са пружаоцима услуга**
  - Правила и процедуре
  - ИТ безбедност и заштита података о личности

ИТ области

- ИТ управљање
  - Планирање и стабилно финансирање
  - Управљање системом
  - Измене
- **Информациона безбедност**
  - Организација ИТ безбедности
  - Континуитет пословања
  - Управљање ризицима
- Сарадња са пружаоцима услуга
  - Правила и процедуре
  - ИТ безбедност и заштита података о личности

ИТ области

- ИТ управљање
  - Планирање и стабилно финансирање
  - Управљање системом
  - Измене
- Информациона безбедност
  - Организација ИТ безбедности
  - Континуитет пословања
  - Управљање ризицима
- Сарадња са пружаоцима услуга
  - Правила и процедуре
  - ИТ безбедност и заштита података о личности

ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

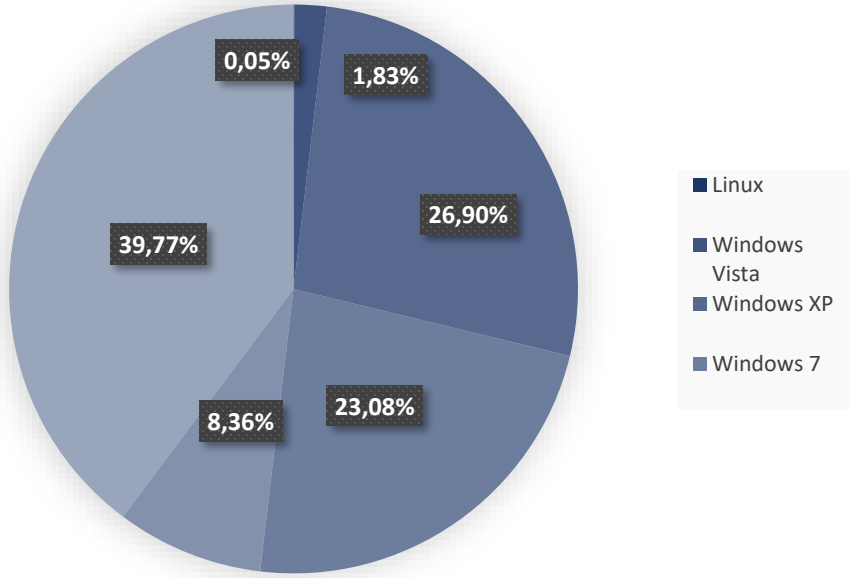
КЉУЧНА ПОРУКА

Неопходно је да Министарство правде унапреди управљање, обезбеди виши ниво поузданости информационих система и омогући грађанима коришћење додатних електронских услуга.

Ефективно управљање информационим системима у правосуђу није у потпуности успостављено због недостатка финансијских средстава у буџету Министарства правде за финансирање информационих система (дакле не мисли се само на годишње одржавање софтвера, потребно је финансирати и обнављање опреме, других компоненти, набавку нових верзија софтвера, антивирусних пакета, обуку ИТ кадра итд.), зато што организација ИТ није успостављена тако да су усвојена правила и процедуре у области ИТ и да је организациона структура таква да може да одговори захтевима који обухватају сложеност послова, континуитет пословања и контролу, и што није омогућено равноправно коришћење папирних и електронских докумената.

- Планирање и стабилно финансирање
- Управљање системом (организација, процедуре, итд.)
- Измене (равноправно третирање папирних и електронских докумената)

Није обезбеђено стабилно финансирање информационих система у правосуђу због недостатка финансијских средстава, што за последицу има застареле рачунаре и застареле, самим тим и небезбедне оперативне системе, и недовољан број запослених на ИТ пословима. Законом о уређењу судова прописано је да су између осталог послови правосудне управе које врши министарство надлежно за правосуђе: уређење и развој правосудног информационог система. Број запослених на ИТ пословима у суду одређује председник суда актом о унутрашњем уређењу и систематизацији радних места у суду, у складу са кадровским планом.



Оперативни систем који се користе у информационим системима у правосуђу

Број запослених на ИТ пословима	Број судова
0	5
1	22
2	5
3	3
4	5
5	1
15	1

Број запослених на ИТ пословима у судовима

Због тога што сваки суд посебно уређује ИТ послове, на нивоу целокупног система правосуђа није успостављено управљање тако да су прописане процедуре које уређују ову област и није успостављена адекватна ИТ организациона структура, што за последицу има отежану или онемогућену контролу обављања ових послова, континуитет пословања и/или пренос знања у случају раскида радног односа са запосленим који обавља те послове, или замену запосленог. Потребно је обезбедити одговарајући ниво образовања и способности лицима који управљају и користе систем, неопходно је успоставити праћење активности, ревизије и надзора у оквиру управљања информационом безбедношћу, тачније, потребно је процедурама уредити ове и друге послове како је прописано Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја.

- Нису прописане процедуре које се односе на послове дефинисане Правилником о унутрашњем уређењу и систематизацији радних места у Министарству
- Локалне процедуре (у судовима) у вези са ИКТ заснивају се на пословним политикама које се не креирају у потпуности, нити се контролишу централизовано, већ се израђују локално.
- Од 53, у 32 суда не постоји посебна организациона јединица која обавља ИТ послове.

Због функционалних недостатака у садашњим софтверским решењима и потребе измене одговарајућих закона, није омогућено равноправно коришћење папирних и електронских докумената, у складу са Законом о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, што за последицу има смањену ефикасност система и то како када су у питању финансијска средства која се троше због папирне доставе, тако и када је у питању време потребно за штампу, паковање, слање и доставу.

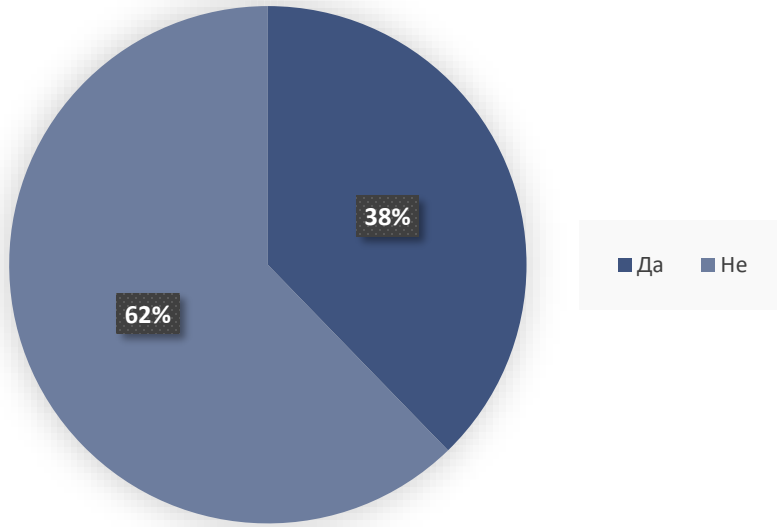
- Електронском документу се не може оспорити пуноважност, доказна снага, као ни писана форма само зато што је у електронском облику.
- Увођење Правосудно-информационог система и велике уштеде које су већ остварене у протеклом периоду (процена Министарства правде да се ради о износу већем од 7 милијарди динара) прави је пример и доказ да се исти послови могу обављати на много ефикаснији начин разменом докумената у електронском, уместо у папирном формату.
- Равноправни третман електронских и папирних докумената омогућиће додатне финансијске уштеде, уштеде у времену рада запослених, али и боље услуге грађанима

Министарство правде и судови нису успоставили управљање информационом безбедношћу информационих система у правосуђу на свеобухватан начин јер нису усвојене и примењене мере заштите које обухватају управљање ИТ ризицима, организациону ИТ структуру и усвајање и примену одговарајућих правила и процедура у области информационе безбедности и управљање процесом континуитета пословања, што је неопходно како би била осигурана поузданост система.

- Организација ИТ безбедности
- Континуитет пословања
- Управљање ризицима

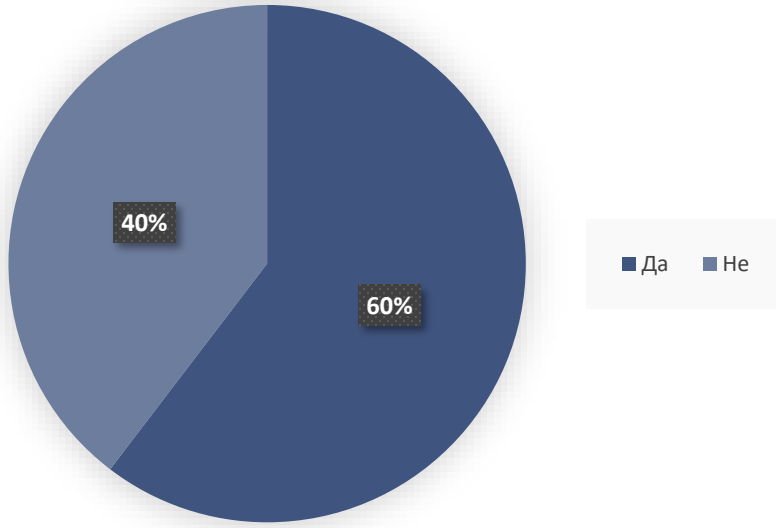
Организација ИТ безбедности у правосуђу, због недостатка довољно стручног знања и недостатка кадровских капацитета, **није успостављена** тако да обухвата примену адекватних докумената која уређују ову област – акт о информационој безбедности, управљање инцидентима, приступ систему и примену других мера заштите ИКТ система, и адекватну организациону структуру ИТ безбедности, што за последицу има већи степен рањивости информационог система.

Да ли је суд донео акт о информационој безбедности?



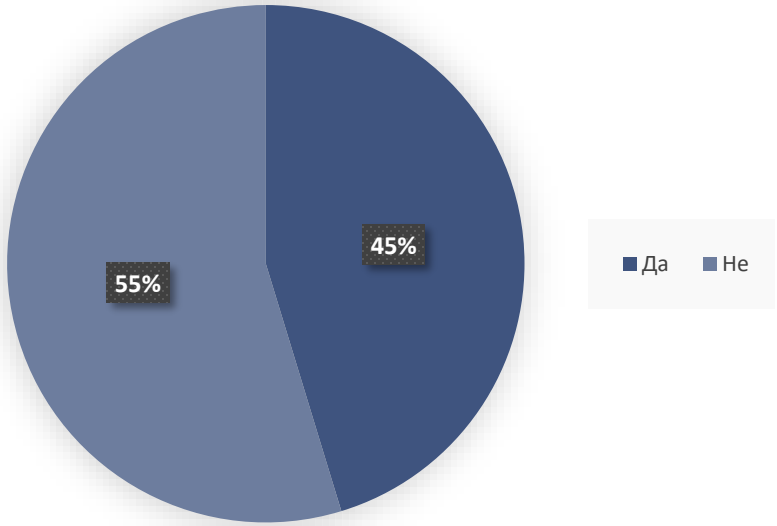
Организација ИТ безбедности у правосуђу, због недостатка довољно стручног знања и недостатка кадровских капацитета, **није успостављена** тако да обухвата примену адекватних докумената која уређују ову област – акт о информационој безбедности, управљање инцидентима, приступ систему и примену других мера заштите ИКТ система, и адекватну организациону структуру ИТ безбедности, што за последицу има већи степен рањивости информационог система.

Да ли је суд организовао обуке запослених о ИТ темама?



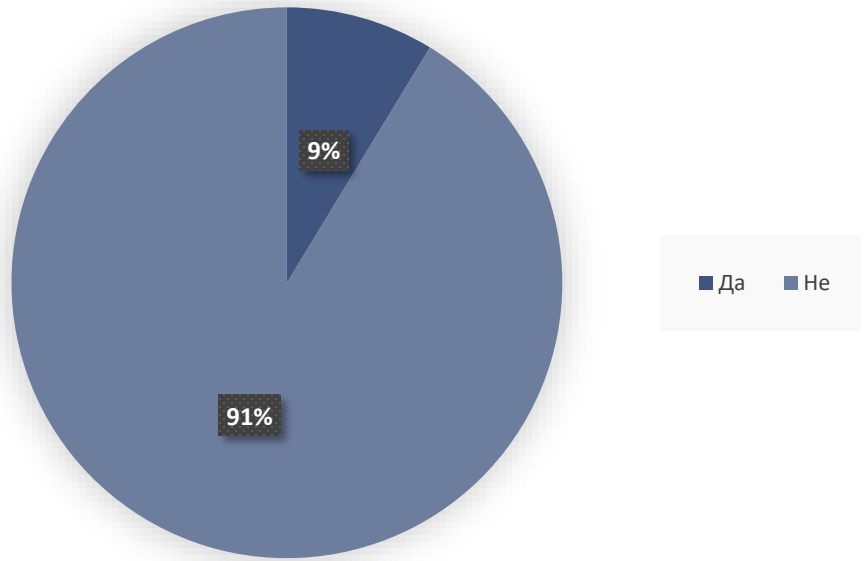
Организација ИТ безбедности у правосуђу, због недостатка довољно стручног знања и недостатка кадровских капацитета, **није успостављена** тако да обухвата примену адекватних докумената која уређују ову област – акт о информационој безбедности, управљање инцидентима, приступ систему и примену других мера заштите ИКТ система, и адекватну организациону структуру ИТ безбедности, што за последицу има већи степен рањивости информационог система.

Да ли суд има одговорно лице за информациону безбедност?



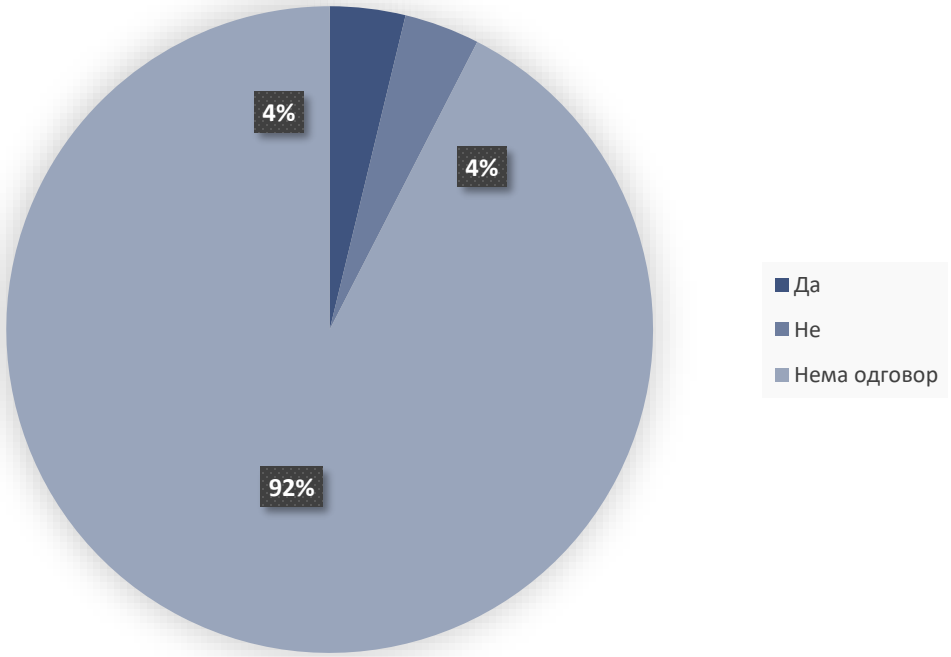
Министарство правде и судови у Србији, због тога што не располажу потребним ресурсима, нису у потпуности успоставили мере које обезбеђују континуитет пословања у ванредним околностима и у случају прекида сарадње са пружаоцем услуга, што за последицу може имати нефункционисање информационог система у дужем временском периоду.

Да ли постоји План континуитета пословања (BCP у судовима?



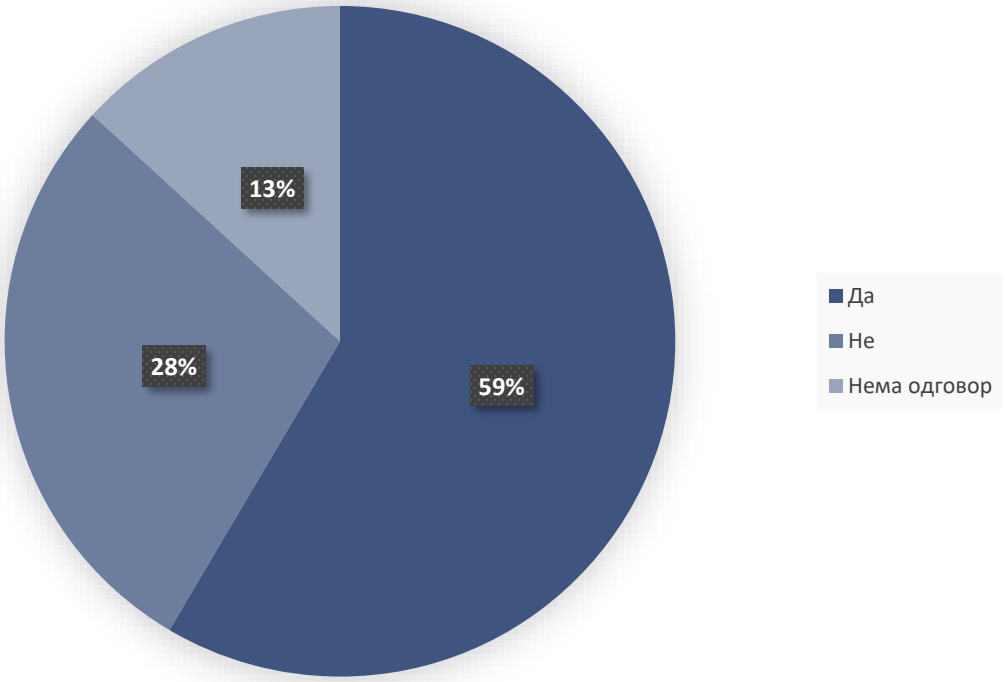
Министарство правде и судови у Србији, због тога што не располажу потребним ресурсима, нису у потпуности успоставили мере које обезбеђују континуитет пословања у ванредним околностима и у случају прекида сарадње са пружаоцем услуга, што за последицу може имати нефункционисање информационог система у дужем временском периоду.

Да ли је, у склопу управљања континуитетом пословања, у судовима усвојен план опоравка активности у случају хаварије (DRP)?



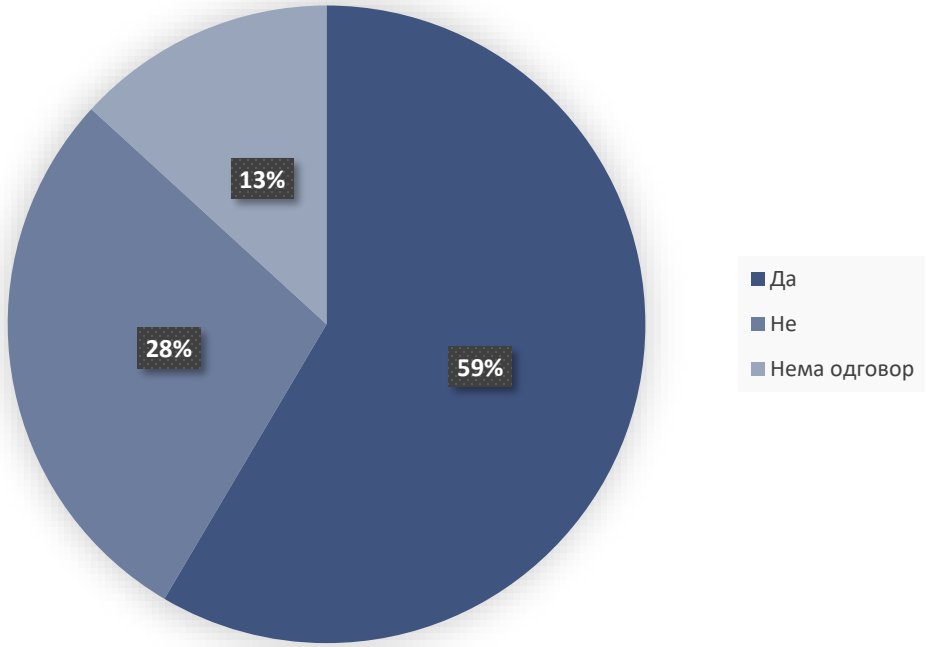
Министарство правде и судови у Србији, због тога што не располажу потребним ресурсима, нису у потпуности успоставили мере које обезбеђују континуитет пословања у ванредним околностима и у случају прекида сарадње са пружаоцем услуга, што за последицу може имати нефункционисање информационог система у дужем временском периоду.

Да ли суд има усвојене процедуре и дефинисане одговорности у вези са креирањем резервних копија података?



Министарство правде и судови у Србији, због непознавања ове проблематике, недовољно искуства и обученог ИТ кадра, нису успоставили управљање ИТ ризицима, 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, нарочито када се документација налази у електронском облику.

Да ли су у систему управљања ризицима обухваћени и ИТ ризици?

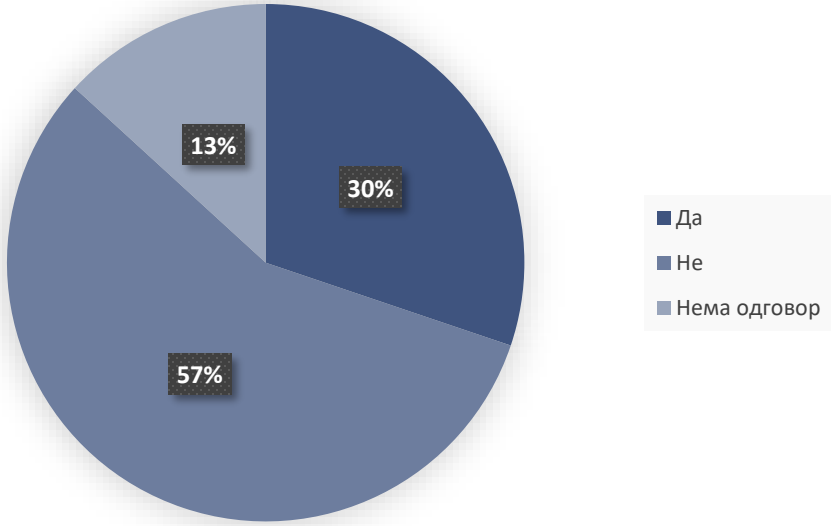


Није успостављен ефективан механизам сарадње Министарства правде и судова са пружаоцима услуге, зато што нису усвојена и имплементирана правила и процедуре када је у питању ова област, пружаоци услуга имају приступ продукционим базама и процес обраде података о личности није уређен на начин прописан законом

- Правила и процедуре
- ИТ безбедност и заштита података о личности

Због недовољно стручног кадра и знања, Министарство правде и судови у Србији није усвојили и имлементирали правила и процедуре које се односе на безбедност података када је у питању сарадња са пружаоцима услуга тако да и поред тога што у уговорима са пружаоцима услуга постоји део који се односи на поверљивост података, није успостављен механизам за контролу којом се утврђује да ли пружалац услуга поштује обавезе у вези са поверљивошћу података па је самим тим и нижи степен поузданости система. **Пружаоци услуга имају приступ продукционим базама.** Законом о информационој безбедности и Уредбом о ближем уређењу мера заштите информационо-комуникационих система прописана је обавеза обезбеђивања механизма који одржава уговорени ниво

Да ли постоји процедура/акт којим се уређује питања информационе безбедности, заштите пословних или личних података којима имају приступ добављачи услуга?



Због сложеног система у којем су судови руковаоци подацима, а информационе системе у којима се обрађују подаци набавља Министарство правде, није успостављена обрада података о личности на начин који је законом прописан јер је обрађивач – Министарство правде, обраду поверило другим обрађивачима – пружаоцима услуга, без посебног или општег овлашћења како то прописује Закон о заштити података о личности. Последица је смањени степен поузданости система.

- У закону о уређењу судова, чланом 70. прописано је, између осталог, да су послови правосудне управе које врши министарство надлежно за правосуђе – уређење и развој правосудног информационог система. Остали информациони системи нису поменути, нити је назначено да ли се појам „правосудни информациони системи“ односи и на друге информационе системе или само на правосудни информациони систем.
- Ако се обрада врши у име руковаоца, руковалац може да одреди као обрађивача само оно лице или орган власти који у потпуности гарантује примену одговарајућих техничких, организационих и кадровских мера, на начин који обезбеђује да се обрада врши у складу са одредбама овог закона и да се обезбеђује заштита права лица на које се подаци односе (став 1). Анализом претходно описаних постојећих и недостајућих мера заштите може се закључити да све неопходне мере нису прописане.

Препоруке ДРИ

Министарству правде, да:

- приликом будућег развоја и одржавања информационих система омогући равноправно коришћење папирне и електронске документације
- приликом припреме финансијских планова осигура стабилно финансирање циљева који обухватају одрживи развој, набавку и одржавање свих компоненти информационих система (хардвер, софтвер, људске ресурсе, стручну обуку).
- успостави мере информационе безбедности које обухватају усвајање и имплементацију аката која уређују ову област – акт о информационој безбедности, управљање инцидентима, приступ систему , и адекватну организациону структуру ИТ безбедности, како би биле примењене све неопходне мере безбедности и заштите података у информационим системима у правосуђу.
- уреди процес обраде података када је у питању сарадња са пружаоцима услуга на начин који јасно разграничава улоге Министарства, судова и пружалаца услуга када је у питању обрада података о личности.
- да изради и судовима упути одговарајућа упутства у циљу усвајања и имплементирања правила и процедура

Хвала на пажњи!

www.dri.rs

kancelarija@dri.rs