

Obrazložitev rebalansa proračuna za leto 2026

1544 - Urad Vlade Republike Slovenije za informacijsko varnost

Poslanstvo predlagatelja finančnega načrta

Osnovno poslanstvo Urada Vlade Republike Slovenije za informacijsko varnost (URSIV) kot pristojnega nacionalnega organa za informacijsko/kibernetsko varnost je dvig odpornosti na kibernetske grožnje, ki lahko ogrozijo posameznike, podjetja, državne organe in družbo v celoti.

Delovanje predlagatelja finančnega načrta prispeva k doseganju ciljev naslednjih podprogramov, programov in politik

- 05 - ZNANOST IN INFORMACIJSKA DRUŽBA
 - 0505 - Informacijska družba in elektronske komunikacije
 - 050505 - Informacijska in kibernetska varnost

Proračunski uporabniki znotraj predlagatelja finančnega načrta

- 1544 - Urad Vlade Republike Slovenije za informacijsko varnost

Proračunski uporabniki ter njihovi neposredni učinki

1544 - Urad Vlade Republike Slovenije za informacijsko varnost

Oris proračunskega uporabnika

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je bil kot samostojna vladna služba vzpostavljen 20. 7. 2021 in pričel z delovanjem 31. 7. 2021, ko je prevzel naloge Uprave Republike Slovenije za informacijsko varnost. Dne 19. 6. 2025 je stopil v veljavo nov Zakon o informacijski varnosti - ZInfV-1 (Uradni list RS, št. 40/25), ki v nacionalni pravni okvir prenaša Direktivo 2022/2555/EU Evropskega parlamenta in Sveta z dne 14. 9. 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2).

Naloge URSIV podrobno opredeljuje 10. člen novega zakona. URSIV kot pristojni nacionalni organ za informacijsko varnost povezuje deležnike v nacionalnem sistemu informacijske in kibernetske varnosti ter na strateški ravni koordinira operativne zmožljivosti v sistemu.

URSIV pozornost posveča zavezancem po ZInfV-1 iz skupine bistvenih subjektov v visoko kritičnih sektorjih energije, prometa, bančništva, infrastrukture finančnega trga, zdravja, pitne vode, odpadne vode, digitalne infrastrukture, upravljanja storitev IKT, javne uprave in vesolja, zavezancem po ZInfV-1 iz skupine pomembnih subjektov v kritičnih sektorjih poštne in kurirske storitve, ravnanje z odpadki, izdelava, proizvodnja in distribucija kemikalij, pridelava, predelava in distribucija živil, proizvodnja različnih proizvodov, digitalni ponudniki, raziskave in lokalna samouprava. URSIV izvaja naloge enotne kontaktne točke za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic EU in z evropsko mrežo skupin CSIRT ter druge naloge mednarodnega sodelovanja.

Ursiv izvaja tudi naloge nacionalnega certifikacijskega organa za kibernetsko varnost. Znotraj URSIV sta organizirana vladni odzivni center za kibernetsko varnost SIGOV-CERT in nacionalni koordinacijski center za kibernetsko varnost NCC-SI.

V okviru URSIV deluje tudi inšpekcijska služba, ki izvaja nadzor nad izvajanjem ZInfV-1. URSIV obvešča vlado, Svet za nacionalno varnost (SNAV) in osrednji organ za odzivanje na hibridne grožnje v primerih kritičnih incidentov ali če obstaja kritična ocena ogroženosti. S tem je URSIV umeščen v sistem nacionalne varnosti.

05 - ZNANOST IN INFORMACIJSKA DRUŽBA

0505 - Informacijska družba in elektronske komunikacije

050505 - Informacijska in kibernetska varnost

Opis podprograma

Namen podprograma je celovito izboljšati kibernetsko odpornost zavezancev in nacionalnega sistema informacijske varnosti. Ukrepi in projekti omogočajo razvoj in upravljanje sistema, pripravo usmeritev, priporočil in druge dokumentacije za zavezance kot pomoč pri doseganju skladnosti z Zakonom o informacijski varnosti (ZInfV-1), krepitev zmogljivosti, pravočasno koordinacijo incidentov in odziv ter obveščanje deležnikov, skrajševanje odziva na incidente, omejevanje posledic incidentov z izdajanjem odločb/odredb, pripravo analiz in priporočil, sodelovanje na vajah zagotavljanja kibernetske varnosti s simulacijo postopkov odzivanja na incidente.

Ključni cilji podprograma vključujejo učinkovito podporo zavezancem pri izpolnjevanju zahtev ZInfV-1 in dvig njihove zrelosti; med drugim se izvajajo predvsem naloge podpore zavezancem pri doseganju skladnosti z ZInfV-1, priprava smernic, priporočil in druge strokovne dokumentacije kot pomoč zavezancem, izvajanje strokovnih seminarjev ali delavnic ter priprava pojasnil zakona.

Podprogram omogoča nacionalno in mednarodno koordinacijo ter situacijsko zavedanje na področju kibernetske varnosti, sodelovanje s CSIRT skupinami, sodelovanje in izmenjava informacij na mednarodni ravni, sodelovanje v mreži CyCloNe, priprava nacionalnih analiz in poročil o stanju ogroženosti, priprava poročil o incidentih, sodelovanje z regulatorji, priprava predlogov predpisov, upravljanje platforme za samoregistracijo, prigrasitev incidentov in izmenjavo informacij (ISAC).

V okviru podprograma se podpira razvoj strokovnih kompetenc in kadrovske zmogljivosti Republike Slovenije na področju kibernetske varnosti z izvajanjem programov usposabljanja, izobraževanja, vaj, certificiranja ter drugih aktivnosti za krepitev znanja in veščin javnega sektorja, gospodarstva, akademskega okolja in raziskovalnih organizacij.

Podprogram omogoča izvedbo raziskav, razvoja, inovacij, razvoja tehnologij ter prenosa znanja na področju kibernetske varnosti z vključevanjem slovenskih deležnikov v nacionalne in evropske razvojne aktivnosti ter podporo sodelovanju med javnim sektorjem, gospodarstvom in raziskovalno-izobraževalnimi institucijami.

V okviru podprograma se financira delovanje inšpekcije z namenom spodbujevanja skladnosti z zahtevami. Izvajajo se digitalno podprti ozko usmerjeni tematski nadzori na daljavo, usmerjeni na ključna tveganja z uporabo specialnih orodij (SecurityScorecard, UpGuard, Shodan, ipd.) in odprtokodnih orodij (Nmap, Spiderfoot, ipd.) skladno z načelom sorazmernosti po Zakonu o prekrških in ZInfV-1.

V okviru podprograma se razvija institucionalni okvir certifikacije kibernetske varnosti v okviru evropskega okvira certificiranja kibernetske varnosti ter vzpostavljajo zmogljivosti za izvajanje nalog, povezanih z ugotavljanjem skladnosti in nadzorom proizvodov z digitalnimi elementi v skladu z Aktom o kibernetski odpornosti (CRA), vzpostavljena evidenca in metodologija nadzora nad skrbniki odprtokodne programske opreme.

Ukrepi

1544-21-0001 - Delovanje Urada Vlade RS za informacijsko varnost

Opis ukrepa

Z izvajanjem ukrepa se bo zagotavljalo kadrovske in materialne vire za delovanje Urada Vlade RS za informacijsko varnost.

Izhodišča in kazalniki na katerih temeljijo izračuni in ocene pravic porabe

Izhodišče delovanja je interno vzpostaviti celovit sistem upravljanja kritičnih funkcij, ki bo zagotavljal neprekinjeno, pravočasno in kakovostno izvajanje ključnih nalog URSIV tudi ob odsotnostih zaposlenih, kadrovske spremembah ali drugih izrednih okoliščinah. Cilj vključuje identifikacijo kritičnih procesov in ključnih kompetenc, določitev usposobljenih namestnikov, zagotovitev potrebnih pooblastil in dostopov, pripravo ter redno posodabljanje dokumentiranih postopkov za izvajanje nalog, sistematičen prenos znanja med zaposlenimi ter redno preverjanje učinkovitosti sistema nadomeščanja in poslovne kontinuitete z namenom zmanjševanja organizacijskih tveganj ter zagotavljanja nemotenega delovanja urada. Krepitev podpornih zmogljivosti za učinkovito izvajanje zakonskih nalog in razvoj URSIV tako, da bo omogočala učinkovito, pravočasno in zakonito izvajanje povečanega obsega nalog URSIV, zlasti zaradi novih nacionalnih pristojnosti, izvajanja evropske zakonodaje ter priprave, izvajanja in poročanja projektov, financiranih iz evropskih sredstev. Pomemben pogoj za doseganje tega cilja je zagotovitev ustrezne kadrovske kvote in dovoljenega števila zaposlenih, ki bo sledilo dejanskemu obsegu in zahtevnosti nalog urada. Obstoječe kadrovske zmogljivosti namreč dolgoročno ne omogočajo vzdržnega izvajanja vseh zakonskih, razvojnih in projektnih nalog, zato je treba s strateškim kadrovskim načrtovanjem zagotoviti ustrezne pogoje za nemoteno delovanje urada, pravočasno izvajanje nalog, razvoj zaposlenih ter zmanjševanje organizacijskih tveganj, povezanih s kadrovsko podhranjenostjo in odvisnostjo od posameznih nosilcev ključnih procesov. Nadaljevati digitalizacijo, standardizacijo in optimizacijo podpornih poslovnih procesov z namenom poenotenja delovnih postopkov, izboljšanja upravljanja dokumentacije ter zmanjšanja administrativnih bremen. Cilj vključuje razvoj in uporabo digitalnih rešitev, standardizacijo internih pravil, obrazcev in postopkov, vzpostavitev sistema spremljanja ključnih kazalnikov uspešnosti, izboljšanje upravljanja podatkov in dokumentacije ter spodbujanje kulture stalnih izboljšav. S tem se bodo povečali učinkovitost, preglednost, sledljivost in kakovost podpornih storitev, izboljšala podpora odločanju vodstva ter ustvarili pogoji za nadaljnji organizacijski razvoj in digitalno preobrazbo URSIV. Glavni kazalniki so: - ustrezna kadrovska popolnitev - poslovne izboljšave - izvajanje nalog v predpisanih zakonskih rokih - pravočasen prenos EU direktiv - nemoteno delovanje organa in sekundarna lokacija - ustrezna licenčna oprema za digitalizacijo procesov za obdelavo velikega števila nalog relativno na število zaposlenih

Pravne podlage

Oznaka	Naziv
ZInfV	Zakon o informacijski varnosti

Neposredni učinki

C7746 - Mednarodna umestitev URSIV

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

Polna operativna zmogljivost URSIV po vseh ključnih sektorjih je izrednega pomena za zagotavljanje kibernetске varnosti na nacionalni ravni. URSIV je pristojni nacionalni organ po Zakonu o informacijski varnosti, ki koordinira celotno delovanje sistema kibernetске varnosti na državni ravni, razvija zmogljivosti za izvajanje kibernetске obrambe, sodeluje z organi in organizacijami, ki delujejo na področju informacijske varnosti, zavezancem nudi strokovno pomoč in krepi odpornost z izvajanjem preventivnih dejavnosti, pripravlja predloge predpisov s področja informacijske in kibernetске varnosti ter izvaja še številne druge naloge, ki so z vidika kibernetске varnosti na nacionalnem nivoju ključnega pomena. Z razširitvijo kroga zavezancev in novimi nalogami, ki jih je z novim zakonom o informacijski varnosti ZInfV-1 prinesla implementacija določb direktive NIS 2 v nacionalno zakonodajo, se bo pomen stalnega vzdrževanja operativne zmogljivosti URSIV še povečal, kar tudi pomeni, da bo potrebno stalno vzdrževanje oziroma tudi nadgradnja njegovih kadrovskih in operativnih zmogljivosti. V zadnji letih se je kadrovska zasedba URSIV nekoliko okrepila, vendar pa stanje še vedno ni zadovoljivo, saj URSIV nima niti odobrene realizacije predhodno načrtovanih kvot za zaposlitve niti ni upoštevano povečanje kvot zaradi prevzemanja zgoraj opisanih novih nalog.

Na mednarodni ravni je članstvo URSIV v organizacijah znotraj EU in zvezi Nato, kot tudi v Organizaciji za varnosti in sodelovanje (OVSE) in Organizaciji združenih narodov (OZN) pomembno za uspešno mednarodno sodelovanje Republike Slovenije na področju kibernetске varnosti. Slovenija je aktivna v Agenciji EU za kibernetско varnost ENISA in Evropskem kompetenčnem centru za kibernetско varnost ECCC. V okviru članstva v EU in obveznosti še iz NIS 1 direktive je Slovenija dolžna aktivno sodelovati v NIS skupini za sodelovanje in njenih podskupinah ter mreži CyClone, po novem pa tudi v delovnih skupinah mreže nacionalnih koordinacijskih centrov za kibernetско varnost znotraj ECCC. Za uspešno izvajanje vseh omenjenih mednarodnih aktivnosti, kot tudi za aktivnosti na nacionalni ravni, ki jih nalaga ZInfV-1, mora URSIV pospešiti pridobivanje kvalitetnih človeških virov. Obrazložitev prispevka k nadrejenemu cilju (rezultatu) Umestitev URSIV v mednarodne organizacije, ter njena kadrovska popolnitev je nujna z vidika izvajanja vseh z ZInfV-1 naloženih nalog. Oboje pozitivno vpliva na cilj/rezultat polno delovanje organov informacijske varnosti. Kazalnik mednarodne umeščenosti je bil dosežen, prepočasno pa je doseganje kazalnika število zaposlenih (kadrovska popolnitev) glede na že obstoječe, še bolj pa na dodatne nove naloge URSIV.

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I10632 - Umeščenost v EU-ENISA in NATO-CDC.		1	2019	1,00	2020	1,00	1,00
					2021		1,00
					2022	1,00	1,00
					2023	1,00	1,00
					2024	1,00	4,00
					2025	1,00	1,00
					2026	1,00	
					2027	1,00	
					2028	1,00	
I13352 - Delujoča enotna kontaktna točka za mednarodno sodelovanje	URSIV, ZInfV-1	število	2027	1,00	2026	1,00	
					2027	1,00	
					2028	1,00	
					2029	1,00	
					2030	1,00	
I13354 - Število mednarodnih skupin,		število	2027	50,00	2026	45,00	
					2027	50,00	

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
mrež, odborov in drugih formatov z aktivnim sodelovanjem URSIV					2028	50,00	
					2029	55,00	
					2030	57,00	

Obrazložitev sprememb ciljnih vrednosti na kazalniku I10632 - Umeščenost v EU-ENISA in NATO-CDC.

URSIV je umeščen v organizacije na EU in NATO ravni.

Obrazložitev sprememb ciljnih vrednosti na kazalniku I13354 - Število mednarodnih skupin, mrež, odborov in drugih formatov z aktivnim sodelovanjem URSIV

Rast sama po sebi ni uspeh. Če URSIV opusti pet manj pomembnih skupin in svoje omejene kadrovske zmogljivosti osredotoči na HWPCI, NIS Cooperation Group, ENISA, NATO, CRI, CECSP, WB3C in druge ključne formate, je lahko rezultat za državo boljši, čeprav je številka nižja.

Opisi kazalnikov

Kazalnik	Opis
I13352	ZInfV-1 določa, da ima URSIV funkcijo enotne kontaktne točke za čezmejno sodelovanje ter naloge zastopanja Republike Slovenije v Svetu EU, Evropski komisiji, ENISA, NATO in drugih relevantnih strukturah; določeno je tudi periodično poročanje prek enotne kontaktne točke. Notranja organizacijska enota Sektor za mednarodne zadeve in odnose z javnostmi opravlja naloge kontaktne točke mednarodnega sodelovanja, dnevno pripravlja oziroma koordinira nacionalna stališča, vodi bilateralno in multilateralno sodelovanje ter usmerja delo predstavnikov in atašejev. Za delujočo enotno kontaktno točko se šteje stanje, ko so določeni nosilec in nadomeščanje, ažurni kontaktni podatki, vzpostavljeni postopki za sprejem, posredovanje in koordinacijo čezmejnih obvestil ter je v posameznem letu mogoče z evidencami izkazati izvajanje obveznosti mednarodnega poročanja, usklajevanja nacionalnih stališč in čezmejnega sodelovanja. Vrednost 1 pomeni, da so navedeni bistveni pogoji izpolnjeni; vrednost 0 pomeni, da najmanj eden od bistvenih pogojev ni zagotovljen.

C8670 - Kadrovska popolnitev URSIV

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

Polna operativna zmogljivost URSIV po vseh ključnih sektorjih je izrednega pomena za zagotavljanje kibernetске varnosti na nacionalni ravni. URSIV je pristojni nacionalni organ po Zakonu o informacijski varnosti, ki koordinira celotno delovanje sistema kibernetске varnosti na državni ravni, razvija zmogljivosti za izvajanje kibernetске obrambe, sodeluje z organi in organizacijami, ki delujejo na področju informacijske varnosti, zavezancem nudi strokovno pomoč in krepi odpornost z izvajanjem

preventivnih dejavnosti, pripravlja predloge predpisov s področja informacijske in kibernetske varnosti ter izvaja še številne druge naloge, ki so z vidika kibernetske varnosti na nacionalnem nivoju ključnega pomena. Z razširitvijo kroga zavezancev, ki ga bo v prihodnje prinesla implementacija določb direktive NIS 2 v nacionalno zakonodajo, se bo pomen stalnega vzdrževanja operativne zmogljivosti URSIV še povečal, kar tudi pomeni, da bo potrebno stalno vzdrževanje oziroma tudi nadgradnja njegovih kadrovske in operativnih zmogljivosti. Ob tem je bil URSIV določen še kot nacionalni kompetenčni center na področju kibernetske varnosti, za katerega delovanje bodo prav tako nujno potrebe nadaljnje kadrovske krepitve. V letu 2022 se je kadrovska zasedba URSIV okrepila, vendar pa še vedno stanje ni zadovoljivo, saj URSIV nima niti odobrene realizacije predhodno načrtovanih kvot za zaposlitve, niti ni upoštevano povečanje kvot zaradi prevzemanja zgoraj opisanih novih nalog. Na mednarodni ravni je članstvo URSIV v Evropsko uniji (EU) in zvezi Nato, kot tudi v Organizaciji za varnosti in sodelovanje (OVSE) in Organizaciji združenih narodov (OZN) pomembno za uspešno mednarodno sodelovanje Republike Slovenije na področju kibernetske varnosti. Slovenija je aktivna tudi v ENISA (Agencija EU za kibernetsko varnost), ki se je z novim stalnim mandatom okrepila in postala še bolj aktivna. V okviru članstva v EU in obveznosti iz NIS direktive, je Slovenije dolžna aktivno sodelovati v NIS skupini za sodelovanje in njenih podskupinah ter mreži CyClone. Za uspešno izvajanje vseh omenjenih mednarodnih aktivnosti, kot tudi za aktivnosti na nacionalni ravni, ki jih nalaga ZInfV, mora URSIV pospešiti pridobivanje kvalitetnih človeških virov. Ustrezna kadrovska popolnitev za izvajanje vseh nalog URSIV bo pozitivno vplivala na rezultat polno delovanje organov informacijske varnosti.

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I10631 - Število zaposlenih	URSIV	št. zaposlenih	2019	8,00	2020	17,00	11,00
					2021		11,00
					2022	31,00	21,00
					2023	30,00	30,00
					2024	40,00	33,00
					2025	36,00	39,00
					2026	0,00	
					2027	0,00	
					2028	0,00	
I12667 - Število zaposlenih URSIV	URSIV	št oseb	2024	34,00	2025	36,00	39,00
					2026	46,00	
					2027	48,00	
					2028	50,00	

Obrazložitev sprememb ciljnih vrednosti na kazalniku I10631 - Število zaposlenih

Kazalnik se ne uporablja več.

Obrazložitev sprememb ciljnih vrednosti na kazalniku I12667 - Število zaposlenih URSIV

Kadrovske okrepitve zaradi novih obveznosti URSIV po ZInfV-1.

Opisi kazalnikov

Kazalnik	Opis
I10631	Število zaposlenih na URSIV.
I12667	Število zaposlenih oseb v URSIV.

C8672 - Polno delovanje URSIV

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

Polna operativna zmogljivost URSIV za izvajanje vseh nalog po ZInfV-1 bo dosežena postopno z ustrežno kadrovsko popolnitvijo, tehnično opremljenostjo, usposabljanjem zaposlenih in zagotovitvijo virov za izvedbo nacionalnih in mednarodnih projektov na področju kibernetske varnosti. Polno izvajanje vseh nalog URSIV bo pozitivno vplivalo na dvig ravni kibernetske varnosti v Republiki Sloveniji.

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I12668 - Izvajanje nalog po ZInfV	URSIV	%	2024	70,00	2025	75,00	88,10
					2026	80,00	
					2027	85,00	
					2028	85,00	
I13359 - Število rednih in izrednih sestankov koordinacije sistema informacijske in kibernetske varnost	Izvedeni sestanki in zapisniki sestankov (interna dokumentacija).	število	2027	12,00	2026	10,00	
					2027	12,00	
					2028	12,00	
					2029	12,00	
					2030	12,00	

Obrazložitev sprememb ciljnih vrednosti na kazalniku I12668 - Izvajanje nalog po ZInfV

URSIV bo s kadrovsko in finančno okrepitvijo, ki jo zahtevajo obstoječe in nove naloge po ZInfV-1 postopoma dosegel polno (100%) izvajanje nalog po ZInfV-1.

Opisi kazalnikov

Kazalnik	Opis
I12668	Izvajanje vseh nalog, ki jih ima URSIV po ZInfV.
I13359	URSIV kot pristojni nacionalni organ za informacijsko varnost izvaja najmanj enkrat mesečno nacionalno koordinacijo za zagotavljanje kibernetske varnosti. V tem okviru se izvaja sodelovanje, izmenjava podatkov in usklajevanje operativnih odzivov s CSIRT skupinama in z deležniki, ki zagotavljajo nacionalno varnost. V primeru pomembnih incidentov se izvede tudi izredna koordinacija. Zagotavlja se tedensko in mesečno situacijsko zavedanje, mesečno ocenjevanje stopnje ogroženosti, priprava tedenskih in vsebinsko usmerjenih analiz in priporočil ter ukrepov glede zagotavljanja informacijske in kibernetske varnosti na ravni države. Izvaja se tudi sodelovanje in izmenjava podatkov s področnimi regulatorji.

1544-21-0002 - Izvajanje nalog URSIV

Opis ukrepa

Znotraj ukrepa se bodo zagotavljala sredstva za izvajanje zakonskih nalog Urada Vlade RS za informacijsko varnost, delovanju Varnostno operacijskega centra (SIGOV-CERT), koordinaciji sistema kibernetске varnosti, enotne kontaktne točke, izvajanju usposabljanj zavezancev po ZInfV-a, sodelovanju z deležniki, izvajanju in sofinanciranju projektov, vzpostavitvi sistema certifikacije skladno z evropskimi predpisi ter drugim aktivnosti za izboljšanje stanja na področju informacijske/kibernetске varnosti. Ukrep vključuje tudi sodelovanje v mednarodnih projektih (kot npr. Varni internet), sodelovanje z javnim zavodom Arnes pri projektih osveščanja za večjo informacijsko/kibernetско varnost.

Izhodišča in kazalniki na katerih temeljijo izračuni in ocene pravic porabe

Delovanje Urada Vlade Republike Slovenije za informacijsko varnost je v letu 2025 s sprejemom novega zakona, ki ureja področje informacijske in kibernetске varnosti implementiral Direktivo (EU) 2022/2555 (Direktiva NIS 2). S tem se je zagotovila uspešna uskladitev obsežnih sistemskih rešitev širokega kroga deležnikov. Z novim zakonom ni le zagotovljen prenos evropskih zahtev, temveč so celovito pokrita dodatna področja, kot so certifikacija na področju kibernetске varnosti ter nacionalnih posebnosti, med katerimi izstopajo kibernetска obramba, vrednotenje kibernetских incidentov in okrepljena vloga pristojnih organov. Zakon in naloge, ki se izvajajo tako vzpostavlja celovit in robusten nacionalni okvir za sistematično obvladovanje kibernetских tveganj, kar bo vplivalo k zagotavljanju enotnega sistema informacijske varnosti na nacionalni ravni in v evropskem ter svetovnem kontekstu. Rezultat v EU indeksu kibernetске varnosti Kazalniki delovanja so s področja: - Izvajanja koordinacije sistema informacijske in kibernetске varnosti - Upravljanje in koordinacija kibernetских incidentov - Delovanje CSIRT za subjekte javne uprave na državni ravni - Podpora zavezancem in pripravljena gradiva za pomoč zavezancem - Delovanje situacijskega centra - Delujoča enotna kontaktna točka za mednarodno sodelovanje - Pripravljena gradiva za pomoč zavezancem in izdelana poročila - Uvedba in izvajanje metodologije - stopenjskega modela inšpekcijskega nadzora - Vzpostavljen sistem certificiranja kibernetске varnosti in varnih digitalnih proizvodov - Usposobljene odgovorne osebe zavezancev

Pravne podlage

Oznaka	Naziv
ZInfV	Zakon o informacijski varnosti

Neposredni učinki

C7747 - Ozaveščanje ciljnih skupin

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

Znotraj ukrepa se bodo zagotavljala sredstva za sofinanciranje projektov in aktivnosti za izboljšanje stanja na področju informacijske/kibernetске varnosti. Ukrep vključuje izvedbo vaj, tekmovanj, konferenc, delavnic in programov ozaveščanja za različne ciljne skupine.

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I10633 - Izvedene vaje in tekmovanja s področja kibernetске varnosti		število	2019	1,00	2020	1,00	5,00
					2021		8,00
					2022	3,00	4,00
					2023	3,00	14,00
					2024	4,00	8,00
					2025	5,00	7,00
					2026	6,00	
					2027	6,00	
					2028	6,00	
					2029	6,00	
					2030	6,00	
I13358 - Število usposobljenih odgovornih oseb zavezancev po ZInFV-1	Lastna dokumentacija (prijave se zbirajo preko sistema prijav SAOD, na URSIV se hranijo podatki o dejanskih udeležencih)	število oseb	2027	300,00	2026	350,00	
					2027	400,00	
					2028	450,00	
					2029	450,00	
					2030	450,00	
I13360 - Število pregledov zavezancev na državni ravni z javno izpostavljenimi storitvami s strani CSIRT SIGOV-CERT	Dokumentacija URSIV in število izdelanih poročil s strani izvajalcev pregleda.	število subjektov na leto	2027	0,00	2026	15,00	
					2027	15,00	
					2028	15,00	
					2029	15,00	
					2030	15,00	

Obrazložitev sprememb ciljnih vrednosti na kazalniku I10633 - Izvedene vaje in tekmovanja s področja kibernetске varnosti

Predvidoma bodo izvedene dve NATO in ena nacionalna vaja, dve tekmovanji in ena konferenca.

Opisi kazalnikov

Kazalnik	Opis
I10633	URSIV podpira in sodeluje pri izvajanju vaj in tekmovanj s področja kibernetске varnosti. Vaje (kot na primer: Locked Shields) vključujejo različne subjekte na slovenski ali mednarodni ravni. Na tekmovanjih (kot na primer bsides, cybernight in EUROpean Cybersecurity Challenge pa sodelujejo mladi. Meri se število vaj, konferenc, delavnic in programov ozaveščanja, pri izvedbi katerih sodeluje URSIV.

Kazalnik	Opis
I13358	<p>Usposabljanje odgovornih oseb bistvenih in pomembnih subjektov na področju obvladovanja tveganj informacijske in kibernetske varnosti izvaja Urad Vlade RS za informacijsko varnost (URSIV) na podlagi šestega odstavka 20. člena Zakona o informacijski varnosti (ZInfV-1, Uradni list RS, št. 40/25) in Uredbe o usposabljanju odgovornih oseb na področju obvladovanja tveganj informacijske in kibernetske varnosti. Usposabljanje je za udeležence brezplačno, traja najmanj osem pedagoških ur in se izvaja v obliki predavanj in delavnic (vključno s praktično simulacijsko vajo). Program usposabljanja (Priloga 1 k Uredbi) obsega šest vsebinskih sklopov: Uvod v informacijsko in kibernetsko varnost, zakonodaja, predpisi in mednarodni standardi Ocena vplivov na poslovanje in neprekinjeno poslovanje (BIA/BCP) Varnost dobavnih verig Upravljanje sredstev in upravljanje tveganj Odzivanje na incidente informacijske varnosti Izvajanje dolžnega nadzorstva in pogoste ugotovitve neskladij iz inšpekcijskih nadzorov Program je dopolnjen z dodatnima tematskima enotama »Komuniciranje z javnostjo v primeru kibernetskih incidentov«, ki nastopa kot samostojna vsebinska točka. Na usposabljanje se lahko prijavijo izključno odgovorne osebe bistvenih ali pomembnih subjektov iz prvega odstavka 20. člena ZInfV-1: predstojniki subjektov javne uprave ter odgovorne osebe pravnih oseb (fizične osebe, ki vodijo, nadzorujejo ali upravljajo poslovanje pravne osebe oziroma so po zakonu, aktu o ustanovitvi ali pooblastilu pristojne in dolžne zagotoviti zakonito delovanje subjekta). Udeležba je brezplačna, število mest pa omejeno – prijave se zbirajo do zapolnitve prostih mest. Po uspešno zaključenem usposabljanju udeleženci prejmejo e-potrdilo z veljavnostjo štirih let; prijava na ponovno usposabljanje je mogoča šest mesecev pred potekom veljavnosti potrdila.</p>

Kazalnik	Opis
I13360	Naloge CSIRT opravlja notranja organizacijska enota URSIV. CSIRT je skupina, ki se odziva na incidente na področju računalniške varnosti, sprejema prijave o kršitvah varnosti, izvaja analize in pomaga prigrasiteljem pri obvladovanju incidentov. Subjekti javne uprave na državni ravni so ministrstva, organi v njihovi sestavi, vladne službe in upravne enote ter tisti javni infrastrukturni zavodi, ki so ustanovljeni v skladu z zakonom, ki ureja znanstvenoraziskovalno in inovacijsko dejavnost. Mednje spadajo tudi drugi subjekti javne uprave iz Priloge 3 ZInfV-1. Skupina CSIRT morajo zagotavljati visoko stopnjo razpoložljivosti lastnih komunikacijskih kanalov, ustrezne prostore in podporne informacijske sisteme, imeti ustrezen sistem za upravljanje in usmerjanje zahtevkov, zagotoviti zaupnost in zanesljivost svojih dejavnosti, dovolj osebja za zagotavljanje neprekinjene razpoložljivosti storitev, nadomestne sisteme in nadomestni delovni prostor, da se zagotovi neprekinjeno izvajanje njihovih storitev. Namen pregledov je vpogled v realno stanje subjektov, ki ponujajo javno izpostavljene storitve z vidika ranljivost in zagotavljanja splošne varnosti sistemov. Na podlagi pregledov subjekti dobijo informacijo o stanju, predloge za izboljšave njihove pregledane infrastrukture (programske, spletne, strojne). Ostali zavezanci pridobijo anonimizirano informacijo o rezultatih pregledov. Število je odvisno od interesa zavezancev in podanega interesa: 2024 (planirano 5, izvedeno 7) 2025 (planirano 10, izvedeno 20)

C8671 - Projekti kibernetike varnosti

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

URSIV že sodeluje v nekaterih nacionalnih in mednarodnih projektih na področju kibernetike varnosti. Število projektov bo s polno operativnostjo Nacionalnega koordinacijskega centra za kibernetiko varnost NCC-SI še naraslo. URSIV bo na ta način slovenskim deležnikom pomagal pri pridobivanju EU sredstev, prav tako pa bo tudi sam pridobil dodatne vire za izvedbo svojih aktivnosti za podporo izobraževanja in usposabljanja ter RRI na področju kibernetike varnosti.

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I12671 - Sodelovanje v projektih	URSIV	št.projektov	2023	1,00	2025	4,00	9,00
					2026	5,00	
					2027	5,00	
					2028	5,00	

Obrazložitev sprememb ciljnih vrednosti na kazalniku I12671 - Sodelovanje v projektih

Predvidoma bodo v izvajanju projekti Endurance, Akadimos, Aliens-SOC, SECIS in En-SOC.

Opisi kazalnikov

Kazalnik	Opis
I12671	Sodelovanje URSIV v nacionalnih in mednarodnih projektih na področju kibernetске varnosti.

Skupine projektov

1544-21-S001 - Izgradnja zmogljivosti za informacijsko varnost

Opis skupine projektov

skupino projektov sestavljajo projekti, ki se izvajajo iz več virov. Namen je omogočati investicije v infrastrukturo izvajalskih organizacij s področja kibernetске varnosti (URSIV, SI-CERT oz. ARNES) iz integrale. Izvajali so se tudi projekti iz Načrta za okrevanje in odpornost, ki se zaključijo z 31.8.2026. Pomemben vir sredstev za projekte je program Digital EUrope Programme in Horizon. Razvojne aktivnosti iz projektov omogočajo razvoj metodologij, mednarodno in nacionalno sodelovanje več organizacij, dostop do informacij.

Neposredni učinki:

C7748 - Tehnična opremljenost URSIV

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

Opis cilja

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I10634 - Izvedena nabava tehnične opreme	URSIV	%	2019	1,00	2020	100,00	100,00
					2021		51,00
					2022	100,00	100,00
					2023	100,00	75,00
					2024	100,00	85,00
					2025	100,00	70,41
					2026	100,00	
					2027	100,00	
					2028	100,00	
I12670 - Sekundarna lokacija SIGOV-CERT	URSIV	1	2025	0,00	2025	1,00	1,00
					2026	1,00	
					2027	1,00	
					2028	1,00	

Obrazložitev sprememb ciljnih vrednosti na kazalniku I12670 - Sekundarna lokacija SIGOV-CERT

Rezervna lokacija SIGOV-CERT bo vzpostavljena v skladu z načrtom.

Obrazložitev sprememb ciljnih vrednosti na kazalniku I10634 - Izvedena nabava tehnične opreme

V letu 2027 je načrtovana polna nabava potrebne tehnične opreme na letni ravni.

Opisi kazalnikov

Kazalnik	Opis
I12670	Zagotovitev operativne sekundarne lokacije za potrebe delovanja SIGOV-CERT.

C7749 - Zagotavljanje operativne zmogljivosti SI-CERT

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

SI-CERT, ki deluje kot organizacijska enota ARNES, potrebuje za uspešno izvajanje zakonsko določenih obveznosti in zahtev, ki izhajajo iz EU direktive NIS 2, na voljo ustrezne kadrovske in tehnološke kapacitete. S sprejetjem ZInfV-1 se je tako nabor nalog kot tudi število zavezancev za poročanje o incidentih povečalo. Poleg tega se trend in kompleksnost kibernetičnih incidentov zadnjih nekaj let krepi. SI-CERT poleg ustrezne kadrovske popolnitve, ki bo omogočala tudi izvajanje dežurstev izven delovnega časa, za izvedbo rednih nalog potrebuje tudi materialne pogoje in visoko tehnološko programsko opremo. NIS 2 zahteva tudi redundanco, kar pomeni, da mora imeti SI-CERT vzpostavljeno in povsem opremljeno rezervno lokacijo.

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I10635 - Število zaposlenih SI-CERT	ARNES SI-CERT	št. zaposlenih	2019	8,00	2020	9,00	9,00
					2021		10,00
					2022	10,00	11,00
					2023	12,00	10,00
					2024	12,00	11,20
					2025	12,00	11,20
					2026	14,00	
					2027	15,00	
					2028	15,00	
I10636 - Sekundarna lokacija SI-CERT	ARNES SI-CERT	1	2019	0,00	2020	0,00	1,00
					2021		1,00
					2022	1,00	1,00
					2023	0,00	1,00
					2024	1,00	1,00
					2025	1,00	1,00
					2026	1,00	
					2027	1,00	

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
					2028	1,00	

Obrazložitev sprememb ciljnih vrednosti na kazalniku I10635 - Število zaposlenih SI-CERT

Načrtovana je postopna kadrovska popolnitev za zagotovitev minimalnih pogojev za izvajanje nalog SI-CERT. V letu 2026 so potrebni viri za plače ocenjeni na 747.000,00 EUR, v letu 2027 pa na 855.000,00 EUR.

Obrazložitev sprememb ciljnih vrednosti na kazalniku I10636 - Sekundarna lokacija SI-CERT

Rezervna lokacija v Mariboru je bila sicer vzpostavljena že pred leti, a bo potreben nakup nove opreme, saj se je prejšnja že amortizirala.

Ocena potrebnih virov za ta namen je 52.500 EUR v letu 2026 in 55.125 EUR v letu 2027 (5% letna rast).

Opisi kazalnikov

Kazalnik	Opis
I10635	Število zaposlenih na ARNES SI-CERT.
I10636	SI-CERT vzpostavi rezervno lokacijo v Mariboru.

C9090 - Izvedba projekta SECIS

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I13084 - Število članov skupnosti NCC-SI	NCC-SI	število subjektov	2025	0,00	2026	10,00	
					2027	20,00	
					2028	30,00	
					2029	40,00	
I13085 - Število izvedenih projektov/leto		projekt	2025	0,00	2026	3,00	
					2027	4,00	
					2028	5,00	
					2029	6,00	

Opisi kazalnikov

Kazalnik	Opis
I13084	Skupno število članov (podjetij, organizacij) v skupnosti NCC-SI.
I13085	Število projektov, ki jih letno izvaja NCC-SI.

C9091 - Izvedba projekta ALiEnS-SOC

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I13083 - Projekt ALiEnS-SOC izveden		%	2025	0,00	2026	50,00	
					2027	60,00	
					2028	100,00	

Obrazložitev sprememb ciljnih vrednosti na kazalniku I13083 - Projekt ALiEnS-SOC izveden

Vrednost se je spreminjala zaradi daljše dinamike projekta (prej je bilo navedeno, da bo zaključen že v 2027)

Opisi kazalnikov

Kazalnik	Opis
I13083	Polna izvedba projekta ALiEnS-SOC.

C9092 - Izvedba projekta ENDURANCE

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I13082 - Projekt ENDURANCE izveden	EK, URSIV	%	2025	0,00	2026	50,00	
					2027	65,00	
					2028	100,00	

Obrazložitev sprememb ciljnih vrednosti na kazalniku I13082 - Projekt ENDURANCE izveden

V opisu se je zgolj smiselno popravila ciljna vrednost glede na to, da projekt traja več let.

Opisi kazalnikov

Kazalnik	Opis
I13082	Polna izvedba projekta ENDURANCE.

C9093 - Izvedba projekta AKADIMOS

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I13081 - Projekt AKADIMOS izveden	EK, URSIV	%	2025	0,00	2026	50,00	
					2027	100,00	
					2028	0,00	

Opisi kazalnikov

Kazalnik	Opis
I13081	Polna izvedba projekta AKADIMOS.

C9094 - Izvedba projekta CYSSDE

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

Izvedba Komunikacijske podpore za projekt CYSSDE v Sloveniji.

Kazalniki

Cilj nima določenih kazalnikov.

1544-26-S001 - NOO projekti URSIV

Opis skupine projektov

Skupina vključuje projekte, ki se financirajo s sredstvi iz Načrta za okrevanje in odpornost (NOO).

Neposredni učinki:

C9033 - Izvedba projekta SiQUID

Lastnik cilja: PU - 1544 (Urad Vlade Republike Slovenije za informacijsko varnost)

Prispeva k rezultatu: C7750 - Polno delovanje organov v sistemu informacijske varnosti

Izvedba NOO projekta SiQUID z vzpostavitvijo omrežja QCI in povezavo sedmih državnih organov na šestih lokacijah.

Kazalniki

Kazalnik	Vir	ME	Izh. leto	Izh. vred.	Leto	Cilj. vrednost	Dos. vrednost
I13055 - Vzpostavljeno omrežje QCI	URSIV	%	2025	0,00	2026	100,00	

Opisi kazalnikov

Kazalnik	Opis
I13055	Vzpostavljeno omrežje kvantne komunikacijske infrastrukture in vanj povezano sedem vladnih organov na šestih lokacijah.