



Adimen Artifiziala

modu seguruan
erabiltzeko gida

Aurkibidea

01. Sarrera	3
1. 1. Testuingurua	3
1. 2. Dokumentuaren helburua	4
1. 3. Argibideak	4
02. AA modu seguruan erabiltzeko neurriak.....	5
2. 1. 1. urratsa: AAren erabilera arautu.....	6
2. 2. 2. urratsa: AAren erabilpen kasuak inbentariatu	7
2. 3. 3. urratsa: AA erabiltzeko arriskuak aztertu.....	8
2. 4. 4. urratsa: AAren erabilera kontrolatu.....	9
2. 5. 5. urratsa: Ebaluatu emaitzak... eta hasi berriro	10
03. Ondorioak.....	11

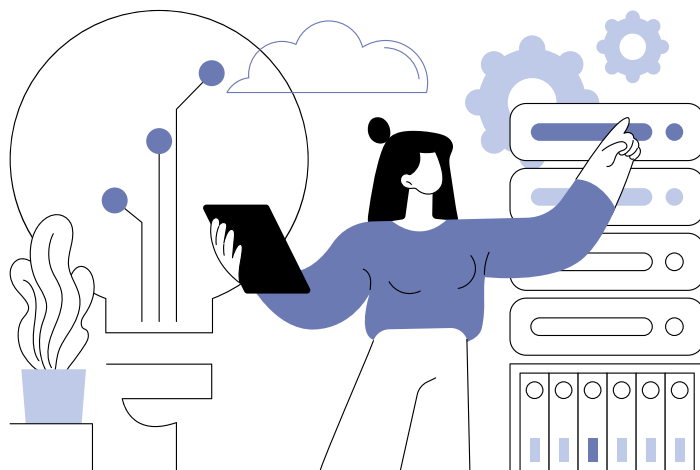


01.

Sarrera

Adimen artifiziala azkar txertatu da eguneroko bizitzan, lanean eta herritarrek zerbitzu digitalekin duten harremanean. Testuak, irudiak, kodeak, laburpenak, gomendioak edo informazio-bolumen handien analisiak sortzeko gai diren tresnek aukera handiak ematen dituzte produktibitatea, irisgarritasuna eta berrikuntza hobetzeko. Hala ere, modu arduratsuan ezagutu eta kudeatu beharreko arriskuak ere badakartza.

Dokumentu honen helburua da AA modu seguruan erabiltzeko erreferentzia argi eta praktikoa eskaintzea. Helburua ez da teknologia mehatxu saihestezin gisa aurkeztea, baizik eta erabilera egokiak eta desegokiak bereizten laguntzea, erabaki informatuak sustatzea eta pribatutasunarekin, informazioaren segurtasunarekin, emaitzen fidagarritasunarekin, jabetza intelektualarekin, mendekotasun teknologikoarekin eta araudia betetzearekin lotutako arriskuak murriztea.



AAren erabileraren segurtasuna ez dago erabilitako teknologiaren mende soilik. Tresnak nola aukeratzen diren, zer datu sartzen diren, nork baliozkotzen dituen emaitzak, zer kontrol dauden, erabiltzaileei nola ematen zaaien informazioa eta denboran zehar arriskuak nola berrikusten diren ere ikusi behar da. Horregatik, gomendatutako ikuspegiak antolaketa-, teknika- eta prestakuntza-neurriak uztartu behar ditu, betiere edozein erabiltzailek ulertzeko moduko hizkera erabiliz.

1.1.

Testuingurua

AA sortzaileak eta AAKo beste sistema batzuek aukera ematen dute zereginak automatizatzeko, erabakiak hartzen laguntzeko, erabiltzaileei arreta hobetzeko, patroiak detektatzeko eta analisi prozesuak bizkortzeko. Eremu publikoan, enpresarialean eta herritarrean, gaitasun horiek balioa sor dezakete, baldin eta proportzionaltasunez, gardentasunez eta giza ikuskapenarekin aplikatzen badira.

Aldi berean, AA erabiltzeak nahi ez diren ondorioak eragin ditzake, irizpide argirik gabe erabiltzen bada. Arrisku garrantzitsuenen artean, hauek nabarmentzen dira: datu pertsonalak edo konfidentzialak sartzeko baimendu gabeko tresnetan, erantzun okerrak edo asmatuak sortzea, informazioaren gaineko kontrola galtzea, alborapenakiko esposizioa, hirugarrenen eskubideek babestutako edukiak erabiltzea, jurisdikzio ez-egokietan kokatutako zerbitzuak erabiltzea eta sistema korporatiboetan AAren irtenbideak modu ez-seguruan integratzea.

Testuinguru horretan, Cyberzaintzak AAren erabilera seguru, arduratsu eta proportzionatuaren ikuspegia sustatzen du, pertsonen eta erakundeek beren onurak balia ditzaten eragindako pertsonen segurtasuna, pribatutasuna, konfiantza eta eskubideak arriskuan jarri gabe. Ikuspegi hori CyberOrratz zibersegurtasun ereduan oinarritzen da, zeinak haren ezarpen maila bakoitzerako aplikatu beharreko segurtasun kontrolak ezartzen baititu, Adimen Artifizialerako kontrol espezifikoak kontuan hartuta.

1. 2.

Dokumentuaren helburua

Dokumentu honen helburua da adimen artifizialaren erabilera segurua bideratzeko irizpideak eta neurri praktikoak ezartzea. Horretarako, AAn oinarritutako tresnak edo zerbitzuak erabili aurretik eta erabili bitartean kontuan hartu beharko liratekeen gutxieneko neurriak deskribatzen dira, bai banakako ikuspegitik, bai antolamendu-ikuspegitik.

Dokumentuaren helburua da edonork ulertzea zer neurri hartu behar dituen AA tresna bat erabiltzean, zer irizpide hartu behar dituen kontuan haren erabilera segurua den zehazteko eta zer mekanismo hartu behar dituen kontrolatzeko. Gainera, oinarri komun bat eskaintzen du erakundeek beren barne politikak antolatu, AA soluzioen inbentarioa egin, arriskuak aztertu, baimendu gabeko erabilerak kontrolatu eta haien segurtasuna etengabe gobernatu ahal izateko.



1. 3.

Argibideak

Dokumentu hau adimen artifizialeko tresnen laguntzaz egin da, neurri batean, eta Cyberzaintzak berrikusi du.



02.

AA modu seguruan erabiltzeko neurriak

AA modu seguruan erabiltzeko, gomendio orokorretatik neurri zehatz eta egiaztagarrietara igaro behar da, eta erakunde bakoitzaren testuingurura egokitu behar da. Kapitulu honetan deskribatutako neurriek esparru praktiko bat eraikitzea dute helburu: erabilera-arauak definitzea, zer irtenbide erabiltzen diren jakitea, arriskuak aztertzea, kontrol proportzionatuak aplikatzea eta erabiltzaileak gaitzea.

Neurri horiek ez dira jarduketa isolatutzat hartu behar. Modu osagarrian funtzionatzen dute: AA erabiltzeko politika bat aplikatzea zaila da tresnen inbentariarik ez badago; inbentario batek balioa galtzen du arriskuak aztertzen ez badira; eta kontrol teknikoak ez dira nahikoak erabiltzaileek zer egin dezaketen eta zer saihestu behar duten ulertzen ez badute. Helburua da gobernu ziklo bat sortzea eta AAren erabilera etengabe hobetzea.

Hemen proposatutako neurriak aplikagarriak dira erakunde batek edo haren erabiltzaileek beren jarduerak gauzatzean erabiltzen dituzten adimen artifizialeko sistemen, zerbitzuen, tresnen, ereduen eta funtzionalitateen erabileran. Barnean hartzen ditu soluzio propioak nahiz hirugarrenen soluzioak, doako edo ordainpeko tresnak, hodeiko zerbitzuak, aplikazio korporatiboetan integratutako funtzionalitateak eta erakundearen ekipo edo sareetatik egindako erabilera puntualak.

Irismenak, gutxienez, informazio korporatiboa, datu pertsonalak, barne dokumentazioa, kodea, kredentzialak, bezeroen informazioa, hornitzaileen informazioa, lege betebeharre lotutako datuak edo erakundearen segurtasunean, pribatutasunean, jarraitutasunean, ospean edo araudia betetzean eragin dezakeen erabilera desagokiko edozein eduki tratatzen duten AAren erabilerak hartzen ditu barne.

Neurri horiek honela laburbiltzen dira, eskematikoki:



1

AAREN
ERABILERA
ARAUTU

2.1. 1. urratsa: AAren erabilera arautu



Lehen urrats horren helburua da arau argiak ezartzea adimen artifizialaren zer erabilera dauden baimenduta, zeinek behar duten baimena eta zeinek egon behar duten debekatuta. AAren erabilera-politika bati esker, erabiltzaileek jakin dezakete nola jokatu, bat-bateko erabakiak murrizten dira eta esparru komun bat eskaintzen da informazioa babesteko, aplikatu beharreko araudia betetzeko eta erabilera desegoki baten ondoriozko kalteak saihesteko.



Erantzukizun nagusia informazioaren segurtasunaz arduratzen den pertsonari edo funtzioari dagokio, negozioaren, datu pertsonalen babesaren, araudia betetzearen eta informazio sistemen ardura duten arloekin koordinatuta. Goi-zuzendaritzak politika onartu behar du, eta bermatu behar du behar bezala komunikatzen dela, praktikan aplikatzen dela eta arriskuak, tresnak edo arau-esparrua aldatzen direnean berrikusten dela.

Hala, erakundeak Adimen Artifiziala Erabiltzeko Politika bat zehaztu, onartu eta zabaldu beharko luke, honako alderdi hauek aintzat hartuta:

- Erabilera baimenduak, baldintzatuak eta debekatuak**

definitzea: Baimendutako erabilerak baimen gehigarririk gabe egin daitezkeenak dira, arrisku garrantzitsurik sartzen ez dutelako; adibidez, erakundeak aldeztu aurretik baimendutako AA bati eskatzea testu publiko baten idazketa hobetzen edo ideia orokorrak sortzen laguntzeko, informazio konfidentzialik eman gabe.

Erabilera baldintzatuak erabilgarriak izan daitezkeenak dira, baina aurrez kontrolak egin behar dira, hala nola AA erabiltzea barne-dokumentazioa berrikusteko, analisi teknikoak babesteko, aktak laburtzeko edo kodea sortzeko. Kasu horietan, baimena, onartutako tresnak erabiltzea, datuak anonimotzea edo giza azterketa indartua eska daiteke.

Debekatutako erabilerak barne hartu behar dituzte sekretuak, kredentzialak, beharrezkoak ez diren datu pertsonalak, informazio sailkatua, dokumentazio konfidentziala edo baimendu gabeko erabaki automatizatuak sartzea dakartenak. Adibidez, ez litzateke sartu behar AAren tresna publiko batean identifikazio datuak, espedienteak, pasahitzak edo argitaratu gabeko informazio estrategikoa duten pertsonen zerrenda bat.

- Zehaztu zein informazio sar daitekeen AAko tresnetan:**

Politikak modu errazean azaldu behar du zein informazio mota erabil daitekeen eta zein ez. Arau praktikoa bat da informazio publikoa edo berariaz baimendua ematea eta informazio konfidentziala, beharrezkoak ez diren datu pertsonalak, sekretu teknikoak, gakoak, tokenak, argitaratu gabeko kontratuak edo murrizketak dituzten dokumentuak debekatzea.

Ahal denean, datu anonimizatuen edo seudonimizatuen erabilera sustatu behar da. Adibidez, pertsonen benetako izenak sartu beharrean, "A erabiltzailea" edo "B saila" erabil daiteke, betiere helburua inor identifikatu gabe lor badaiteke.

- AAko zein tresna erabil daitezkeen ezartzea:** Tresna guztiek ez dituzte berme berak eskaintzen. Politikak adierazi behar du baimendutako tresnen zerrenda bat dagoen, ber betekizun bete behar dituzten eta zer baldintzatan erabil daitezkeen.

Irizpide garrantzitsuen artean daude datuen kokapena eta tratamendua, kontratu baldintzak, datuak ereduak entrenatzeko erabiltzeko aukera, segurtasun bermeak eta eskura dagoen trazabilitatea.

- AAk sortutako emaitzak nola tratatu behar diren definitzea:**

AAren emaitzak zirriborrotzat edo laguntzat hartu behar dira, ez egia automatikotzat. Dokumentuetan, erabakietan, komunikazioetan edo sistemetan sartu aurretik berrikusi behar dira. Hori bereziki garrantzitsua da testu juridikoetan, teknikoetan, medikoetan, finantzarioetan, segurtasunekoetan edo pertsonen eskubideetan eragina dutenetan. Era berean, funtsezkoa da zehaztea ea AAri jarduerak modu autonomoan egiten utziko zaion (eragileen bidez) edo laguntza informazioa soilik sortzen utziko zaion.

Adibide erraz bat: AA batek segurtasun gomendio bat sortzen badu, arduradunak egiaztatu behar du gomendioa teknikoki zuzena, proportzionala eta ingurune errealaari aplikagarria dela, zabaldu edo ezarri aurretik. Era berean, kontuan hartu behar da ea AAri gomendio hori autonomoki betearazten uzten zaion.

- Erabilera-, baimente- eta gainbegiratze-erantzukizunak esleitzea:**

politikak identifikatu behar du nork baimendu ditzakeen erabilera berriak, nork baliozkotzen dituen emaitzak, nork ebazten dituen zalantzak, nork kudeatzen dituen salbuespenak eta nork berrikusten duen betetze-maila. Horri esker, AA erabiltzea ez dago erabiltzaile bakoitzaren irizpidearen mende soilik.

- Pribatutasun, segurtasun, jabetza intelektual eta betetze baldintzak sartu:**

Datu pertsonalen babesari, konfidentzialtasunari, sekretu profesionalari, egile eskubideei, hirugarrenen edukien erabilerari, trazabilitateari, ebidentzien kontserbazioari eta aplikagarria den araudi markoaren betetzeari buruzko ohartarazpen argiak gehitu behar dira.

- Politika aldian behin berrikustea:**

AAk azkar eboluzionatzen du. Horregatik, politika aldian behin berrikusi behar da, betiere tresna berriak, erabilera kasu berriak, gertakariak, arau aldaketak edo arrisku garrantzitsuak agertzen badira.

2

AAREN
ERABILPEN
KASUAK
INBENTARIATU

2.2. 2. urratsa: AAREN erabilpen kasuak inbentariatu



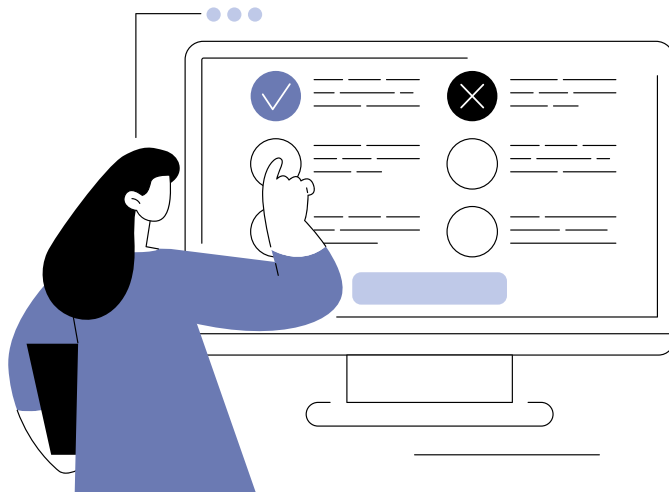
Bigarren urrats honen helburua da erakundearen barruan AAREN zer tresna, eredu, zerbitzu eta erabilera-kasu dauden jakitea. Ezagutzen ez dena ezin da behar bezala babestu eta gobernatu. Inbentario batek aukera ematen du baimendutako eta baimendu gabeko erabilerak identifikatzeko, arriskuak sailkatzeko, arduradunak esleitzeko, integrazioak kontrolatzeko eta zer segurtasun-neurri aplikatu behar diren erabakitzeke.



Arduradun nagusiak informazio-sistemen ardura izan beharko luke, informazioaren segurtasunean, datuen babesean, erosketetan, betetzean eta arlo erabiltzaileetan parte hartuta. Erantzukizuna ez da mugatzen hasierako zerrenda bat sortzera: inbentarioa eguneratuta mantentzea, altak eta bajak berrikustea, eta arriskuen eta aldaketen kudeaketarekin koordinatzea.

Horrela, erakundeak erabilitako adimen artifizialeko soluzioen inbentario eguneratua egin beharko luke, honako alderdi hauek kontuan hartuta:

- **Erabilitako AAKo tresnak, ereduak, zerbitzuak eta osagaiak identifikatzea:** Inbentarioak baimendutako soluzio korporatiboak zein erabiltzaileek detektatutako edo aitortutako tresnak jaso behar ditu. LLM motorrak, AA agenteak, testu edo irudi sorgailuak, analisi dokumentalerako tresnak, produktibitate kopilotuak, gomendio motorrak, chatbotak, aplikazioetan integratutako modeloak eta AAKo APIak sartu behar dira.
- **Helburua edo erabilera-kasua dokumentatzea:** Inbentariatutako elementu bakoitzak hizkuntza argian deskribatutako helburua izan behar du. Adibidez: "komunikazio publikoak idazteko laguntza", "tiketen aurretiazko sailkapena", "barne-dokumentuen laburpena" edo "segurtasun-ekitaldietan patroik anomaloak detektatzea".
- **Hornitzailea, barne jabea eta eremu erabiltzailea identifikatu:** Inbentarioak zerbitzua nork ematen duen, barruan nork administratzen duen eta zein arlotan erabiltzen duen adierazi behar du. Horrek intzidentziak kudeatzea, kontratuak berrikustea, zerbitzuko bajak eta erantzukizunak aztertzea errazten du.
- **Sailkatu kritikotasuna eta lotutako arriskua:** AAREN erabilera guztiek ez dute arrisku maila bera. Tresnak datu pertsonalak, informazio konfidentziala, prozesu kritikoak, pertsonengan eragina duten emaitzak edo erabaki garrantzitsuak tratatzen dituen baloratu behar da. Eduki publikoa duen informazio-txatbot batek oso arrisku desberdina du erabaki administratiboak babesten dituen edo informazio sentikorra aztertzen duen AA batek baino.
- **Beste sistema batzuekiko integrazioak identifikatzea:** Irtenbidea aplikazio korporatiboekin, dokumentu-biltegiekin, postarekin, identitate-sistemeekin, datu-baseekin, segurtasun-tresnekin edo hodeiko plataformekin konektatzen den dokumentatu behar da. Integrazioek handitu egiten dute akats edo erabilera desegoki batek izan dezakeen eragina.
- **Informazio sentikorra, datu pertsonalak edo informazio konfidentziala prozesatzen duen adierazi:** Puntu hau funtsezkoa da pribatasun eta segurtasun neurriak aplikatzeko. Tresnak datu pertsonalak tratatzen baditu, hauek ebaluatu behar dira: legitimazio-oinarria, minimizazioa, eragindako pertsonen emandako informazioa, hornitzailearen bermeak eta, hala dagokionean, inpaktuaren ebaluazioaren beharra.
- **Sortutako emaitzen tratamendua erregistratzea:** Inbentarioak islatu behar du ea emaitzak zirriborro, gomendio, ebidentzia, eduki publiko, erabaki baterako sarrera edo irteera automatizatu gisa erabiltzen diren. Zenbat eta inpaktu handiagoa izan emaitzan, orduan eta handiagoa izan behar du giza ikuskapenak.
- **Alta, aldaketa eta baje trazabilitatea mantentzea:** AA-irtenbide baten inkorporazio, aldaketa garrantzitsu edo erretiratze oro erregistratu egin behar da. Adibidez, tresna bat barneko dokumentu-biltegi batera konektatzen hasten bada, inbentarioa eguneratu egin behar da, arriskua materialki aldatzen delako.



3

AA ERABILTZEKO
ARRISKUAK
AZTERTU

2.3. 3. urratsa: AA erabiltzeko arriskuak aztertu



Hirugarren urrats honen helburua da AAren erabilera kasu bakoitzaren ondoriozko arriskuak identifikatzea, baloratzea eta tratatzea, ezarri aurretik eta funtzionamenduan zehar. Arriskuen analisiak aukera ematen du erabilera bat onargarria den, zer kontrol aplikatu behar diren, zer hondar-arrisku hartzen diren eta zer erabilera mugatu edo baztertu behar diren erabakitzeko.



Informazioaren segurtasunaz arduratzen den pertsonak izan beharko luke erantzukizuna, erabilera-kasuaren jabe den arloaren, datuak babesteko, betetzeko eta erosteko arduradunen eta informazio-sistemen arduradunaren laguntzarekin. Erabilerak pertsonen eskubideei edo erabaki garrantzitsuei eragin badiezaieke, bereziki garrantzitsua da parte-hartze juridikoa eta pribatutasunakoa.

Beraz, erakundeak Adimen Artifizialeko soluzioen erabilerari lotutako segurtasun arrisku espezifikoak azterketa egin beharko luke, non alderdi hauek jasoko diren:

- **Erabilera kasua eta erakundearentzat duen balioa identifikatzea:** Arriskuak aztertu aurretik, zer egin nahi den deskribatu behar da, zer tresnarekin, zer datu erabiliko diren, nork erabiliko duen sistema eta zer emaitza lortzea espero den (informazioa, jarduerak, etab.). Erabilera kasuaren garrantzia ere baloratu behar da: ez da gauza bera dibulgazio testu bat idazteko laguntza bat edo espedienteak lehenesten dituen, gertakariak sailkatzen dituen edo pertsonengan eragina duten erabakiak babesten dituen tresna bat.
- **Kontuan hartu beharreko arriskuen katalogoa zehaztea:** Erakundeak erabilera-kasu bakoitzerako kontuan hartu beharreko arrisku espezifikoak katalogoa ezarri beharko du. Arrisku horiek hainbat motatakoak izan daitezke, ondoren adierazten den bezala:
- **Erabilera-kasuari berari dagozkion arriskuak:** ebaluatu egin behar dira aplikatu beharreko jurisdikzioa, datuak babesteko araudia, Adimen Artifizialaren Europako Araudian sartzeko aukera (arrisku onartezinako, handiko, mugatuko edo gutxieneko arriskuko AA-sistemak), obligazio sektorialak, kontratu-betekizunak eta konfidentzialtasunetik, jabetza intelektualetik edo sekretu profesionaletik eratorritako edozein muga, bai eta beste informazio-sistema batzuekin, datu-tratamenduekin edo prozesu korporatiboekin integratzeari lotutako inplikazioak ere.
- **Arrisku etikoak eta konfiantzazkoak:** AAK alborapenak, emaitza diskriminatzaileak, azalpen gutxiegi edo ulertzeko zailak diren gomendioak sor ditzake. Horregatik, aztertu behar da ea erabilera kasuak gardentasuna, azalgarritasuna, trazabilitatea edo mekanismoak eskatzen dituen pertsona batek emaitza berrikusi eta, beharrezkoa izanez gero, zuzendu ahal izateko. AAren jardueraren osotasuna eta trazabilitatea, zentzurik zabalenean, funtsezko faktoreak dira.
- **AAren erabilera okerrarekin lotutako arriskuak:** Baimendu gabeko erabilerak, baimendu gabeko datuekin egindako erabilerak edo jarraibide maltzurak sartzea ere kontuan hartu behar dira. Adibidez, erabiltzaile batek informazio konfidentziala kopiatu dezake laburtzeko kanpoko tresna batean, nahiz eta horretarako baimenik ez izan.
- **AAri emandako datuen gaineko arriskuak:** Arrisku garrantzitsuenen artean daude datuen ihesa, baimenik gabeko ereduak entrenatzeko informazioa erabiltzea, kontrolatu gabeko biltegiratzea, informazio sentikorraren inferentzia eta datuen pozoitzea. Arreta berezia jarri behar da datu pertsonaletan, kredentzialetan, sekretuetan, barne dokumentazioan eta hirugarrenen datuetan.
- **AAren ereduaren beraren gaineko arriskuak:** Erakundeak bere ereduak garatzen edo doitzen baditu, eredu manipulatze, eredu erauzteko, etsaien erasoak gertatzeko, osotasuna galtzeko, hirugarrenen osagaiekiko mendekotasuna izateko eta entrenamenduaren parametroak edo datuak azaltzeko arriskuak baloratu behar ditu. Erakundeak hirugarrenen ereduak erabiltzen baditu, eredu horien erabilera-baldintzekin lotutako arriskuak baloratu behar ditu (kostuen eredu barne), baita izan ditzaketen aldaketak, eredu horien erabilgarritasuna, bermatutako zerbitzu-mailak eta abar ere.
- **AAk sortutako emaitzen gaineko arriskuak:** Emaitzek akatsak, haluzinazioak, existitzen ez diren erreferentziak, alborapenak, baimenik gabeko informazioa edo justifikatu gabeko ondorioak izan ditzakete. Adibidez, AA batek egiazkotzat jo dezake indargabetutako arau bat, iturri bat asma dezake edo benetako ingurunerako desegokia den jarduera bat gomendatu dezake. Arrisku horiek ebaluatzea funtsezkoa da, AAren emaitzen (informazioa edo ekintzak) gaineko erantzukizuna (baita legala ere) erakundearena baita beti.
- **Probabilitatea, inpaktua eta arrisku onargarria baloratu:** Analisiak gertatzeko probabilitatea eta arrisku bakoitzaren inpaktua zenbatetsi behar ditu, erabilera-kasuaren balioa eta arrisku hori arintzeko dauden neurriak kontuan hartuta. Halaber, erakundeak AA erabiltzeko onargarritzat jotzen duen arrisku-atalasea zein den zehaztu beharko da.
- **Tratamendu eta onarpen formaleko ekintzak definitzea:** Arrisku ez-onargarrietarako ekintza zehatzak definitu behar dira: datuak mugatzea, hornitzailea aldatzea, anonimizazioa aplikatzea, giza berrikuspena txertatzea, profilak murriztea, baimendu gabeko tresnak blokeatzea, erregistroak indartzea, auditoretzak egitea edo erabilera kasua baztertzeko. Hondar-arriskua formalki onartu behar du erakundeak.

4

AAREN
ERABILERA
KONTROLATU

2. 4. 4. urratsa: AAren erabilera kontrolatu



Laugarren urrats honen helburua da AA soluzioen eta tresnen erabilera kontrolatzea, murrizketa proportzionatuak aplikatzea eta erabilera ez-seguruak edo baimendu gabeak detektatzea ahalbidetuko duten mekanismo teknikoak eta antolakuntzakoak izatea. Kontrol horiei esker, AAren erabilera politika ez da soilik adierazpen bat, baizik eta praktika egiaztagarri bat.



Erantzukizun nagusia informazio sistemen arduradunari dagokio, informazioaren segurtasunarekin eta betetze, pribatutasun eta erabiltzaileekiko harreman arloekin koordinatuta. Kontrolen aplikazioak proportzionatua izan behar du, aplikatu beharreko araudia errespetatu behar du eta modu argian jakinarazi behar zaie eragindako pertsonari.

Hala, erakundeak adimen artifizialeko tresnen erabilera kontrolatzeko tresnak eta mekanismoak zabaldu beharko lituzke, honako helburu hauek lortzeko:

- **AAko tresnen erabilera ingurune korporatiboetatik identifikatzea:** Erakundeak aukera izan behar du jakiteko, teknikoki bideragarria den neurrian, zer AA zerbitzu erabiltzen diren bere sare, ekipo edo nortasun korporatiboetatik. Hori web-segurtasuneko tresnen, CASBen, SASeren, nabigazio-erregistroen, aplikazioen inbentarioen edo endpointen kontrolen bidez egin daiteke.
- **Baimendu gabeko tresnetan murrizketak edo blokeoak aplikatzea:** tresna batek berme nahikorik eskaintzen ez duenean edo politika korporatiboa betetzen ez duenean, blokeatzeko edo mugatzeko aukera izan behar du. Adibidez, AAren soluzio korporatibo bat baimendu daiteke, eta sartutako datuak kontrolik gabeko entrenamendurako erabiltzen dituzten tresna publikoak blokeatu.
- **Profilen, arloen edo informazio motaren arabera bereizitako politikak definitzea:** Pertsona guztiek ez dituzte gaitasun berberak behar. Zilegi da AA erabiltzea plantilla osoari idazketa orokorrerako, baimendutako profiletarako dokumentuak aztertzeke tresnak erreserbatzea eta informazio sentikorra edo datu pertsonalak tratatzen dituztenei kontrol indartuak eskatzea.
- **Informazio sentikorra sartzeko saiakerak detektatzea eta blokeatzea:** Bideragarria eta proportzionatua denean, datuen ihesa prebenitzeko mekanismoak integratu behar dira, datu pertsonalak, informazio konfidentziala, kredentzialak, gakoak, kode sentikorra edo baimendu gabeko tresnetan sailkatutako dokumentazioa sartzeara eragozteko edo ohartarazteko.
- **Erregistroak eta erabilera-ebidentziak mantentzea:** Trazabilitatea beharrezkoa da gehiegikeriak detektatzeko, gertakariak ikertzeko eta betetzen dela frogatzeko. Erregistroak arriskuaren arabera izan behar dira, eta erabiltzaileen pribatutasuna errespetatu behar dute. Kontua ez da modu indiskriminatu zaintzea, baizik eta segurtasuna kudeatzeko nahikoa ebidentzia izatea.
- **Erabilera desagokiak edo portaera anomaloak monitorizatzea:** Arrisku patroien aurreko alertak definitu behar dira, hala nola baimendu gabeko tresnen erabilera masiboa, ezohiko kokapenetatik sartzeara, dokumentu

sentikorren karga errepikatuak edo kontrolak saihesteko saiakerak. Alerta horiek segurtasun-gertaera gisa tratatu behar dira.

- **AAren erabilera-politikaren aplikazioa erraztea:** Kontrolek pertsonari lagundu behar diete, ez prestakuntza ordeztu. Adibidez, informazio sentikorra bidali aurretik automatikoki ohartaraziz gero, akatsak saihestu eta ikaskuntza praktikoa indartu daiteke.
- **Pertsonak AAren erabilera seguruan prestatzea:** Erakundeak ziurtatu behar du erabiltzaileek AAren erabilera baimenduak eta debekatuak ezagutzen dituztela, baita haren erabileraren inguruan gerta daitezkeen ohiko akatsak ere. Erabiltzaileek adibideak izan behar dituzte zer egin daitezkeen eta zer ez jakiteko, jakiteko AAk datuak asma ditzakeela, alborapenak erreproduzitu ditzakeela edo erantzun sinesgarri baina okerrak sor ditzakeela, eta jakin behar dute AA modu seguruagoan erabiltzeko jarraibide argiak eman behar direla, emandako informazioa mugatu behar dela, azalpen egiaztagarriak eskatu behar direla, ziurgabetasunari buruzko ohartarazpenak eskatu behar direla eta emailtzak iturri fidagarriekin kontrastatu behar direla.



5

EBALUATU
EMAITZAK... ETA
HASI BERRIRO

2.5. 5. urratsa: Ebaluatu emaitzak... eta hasi berriro



Azken urrats horren helburua da aldian-aldian eta modu egituratuan egiaztatzea ea adimen artifizialaren erabilerak espero diren emaitzak modu seguruan, fidagarrian, proportzionatua eta barne arauen arabera sortzen dituen, eta, funtzionamendu tekniko ez ezik, emandako balio erreala, emaitzen kalitatea, arriskuen kontrola eta hartutako neurrien egokitasuna ere ebaluatzea. Hori prozesu zikliko gisa ulertu behar da, non, aldaketen aurrean edo erabilera-aldien ondoren, erakundeak emaitzak ebaluatzen, ikasten eta etengabe berrikusten dituen aurreko faseak, tresnak, ereduak, erabilerak eta mehatxuak eboluzionatu egiten baitira.



Erantzukizun nagusia informazioaren segurtasun-funtzioari dagokio, informazio-sistemaren arduradunarekin eta arlo erabiltzaileekin koordinatuz, eta, hala dagokionean, datuak babesteko, betetzeko, auditoretza egiteko edo arriskuak kudeatzeko funtzioekin koordinatuz. Erabilera-kasuaren jabe den arloak aktiboki parte hartu behar du, eta AAren erabilgarritasuna eta fidagarritasuna ebaluatu behar ditu testuinguru errealean; segurtasun-, pribatutasun- eta betetze-funtzioek, berri, zehaztu behar dute arriskuek onargarriak izaten jarraitzen duten edo kontroletan doikuntzak egin behar diren.

Horregatik, erakundeak Adimen Artifiziala erabiltzeko zabalduetako neurriak kudeatzeko prozesu bat garatu beharko luke, non alderdi hauek jasoko diren:

- **Erabilera-kasuak aurreikusitako helburua betetzen duen ebaluatzea:** Egiaztatu behar da AA tresnak espero den onura ekartzen duen eraginkortasunari, denboren murrizketari, emaitzen kalitateari, zerbitzuaren hobekuntzari edo zereginetarako laguntzari dagokienez, eta kasu jakin batzuetan egiaztatu behar da tresna horiek ulergarriak, osoak eta erabilgarriak direla.
- **Emaitzen kalitatea, zehaztasuna eta fidagarritasuna berrikustea:** AAren emaitzak aldian-aldian ebaluatu behar dira, behar bezala erabiltzen direla ziurtatzen duten berrikuspen eta egiaztapenen bidez, bereziki erabakietan, dokumentuetan edo analisi sentikorretan eragina dutenean; horretarako, akatsak, omisioak, inkoherezak, alborapenak edo egiaztatu ezin diren erreferentziak aztertu behar dira, eta egiaztatu behar da, adibidez, gomendio teknikoak zuzenak, proportzionalak, testuinguruarekin bateragarriak eta barne-politikekin eta erregulazio-baldintzekin bat datozenak direla.
- **Arriskuek onargarriak izaten jarraitzen dutela egiaztatzea:** Arriskuen analisia aldian behin edo aldaketa garrantzitsuen aurrean berrikusi behar da (hornitzaile, funtzionalitate, erabiltzaile, datu edo integrazio gisa), konfidentzialtasuna, datuen babesa, trazabilitatea, hornitzailearekiko mendekotasuna edo emaitzen fidagarritasuna bezalako alderdiak ebaluatuz, eta, hondar-arriskua onargarria izateari utziko balio, hainbat neurri hartu beharko lirakeke, hala nola erabilera mugatzea, giza ikuskapena indartzea, datuak anonimizatzea, konfigurazioak doitzeta, sarbideak murriztea, kontratuak eguneratzea edo erabilera etetea.
- **Gorabeherak, desbideratzeak eta aurreikusi gabeko erabilerak aztertzea:** ebaluazioak kontuan hartu behar ditu AA erabiltzean detektatutako gorabeherak (akats garrantzitsuak, zalantza errepikariak, baimendu gabeko erabilerak edo desbideratzeak), kontroletan edo politikan ahuleziak identifikatzeko eta neurri egokiak hartzeko. Adibidez, barne-informazioa tratatzeko tresna publikoak erabiltzen direla detektatzen bada, horren zergatia aztertu beharko da, alternatiba seguruak eskaini eta komunikazioa eta erabilera-arauak indartu.
- **Hobekuntza ekintzak zehaztea eta zikloa berriro hastea:** Aurreko alderdi guztien ebaluazioak ekintza zehatzetara eraman behar du, emaitzak positiboak badira eta arriskuak kontrolatuta badaude erabilerak mantenduz edo zabalduz, edo politika, inbentarioa, arriskuen analisia, kontrolak, erantzukizunak eta jarraibideak berrikusiz, arazoak detektatuz gero, AAren etengabe bilakaera eta etengabe berrikuspen, ikaskuntza eta egokitzapen beharra bere gain hartzen dituen etengabe hobekuntza ikuspegi batean.



03.

Ondorioak

Adimen artifiziala azken urteotako eraldaketa teknologiko garrantzitsuenetakoa da. **Zereginetan laguntzeko, analisiak bizkortzeko, edukiak sortzeko eta zerbitzu berriak emateko duen gaitasunak balio handia eman diezaieke** pertsonari, erakundeei eta administrazio publikoei. Baina balio hori soilik izango da jasagarria baldin eta segurtasunez, erantzukizunez eta konfiantzaz erabiltzen bada.



Erronka nagusia ez da soilik tresna jakin bat aukeratzea, baizik eta **tresna horren erabilera behar bezala gobernatzea**. AA seguru batek **arau argiak eskatzen ditu, erabilera kasuak ezagutzea, arriskuen analisia, kontrol proportzionatuak, giza ikuskapena eta etengabeko prestakuntza**. Elementu horiek gabe, teknikoki aurreratua dagoen tresna batek ere arrisku larriak sor ditzake: informazioa erakustea, erabaki okerrak, konfiantza galtzea, arauak ez betetzea edo erakundeak behar bezala kontrolatzen ez dituen zerbitzuekiko mendekotasuna.



Horregatik, gomendatutako hurbilketak praktikoa eta orekatua izan behar du. Kontua ez da AA modu orokorrean debekatzea, ezta mugarik gabe baimentzea ere. Zertarako erabil daitekeen, zer datuekin, nork, zer baldintzatan eta zer berrikuspen-mekanismeekin identifikatu behar da. **Gakoa da erabilera onuragarriak eta arrisku txikikoak ahalbidetzea, erabilera sentikorrek indartzea eta eskubideak, segurtasuna edo konfiantza publikoa arriskuan jar dezaketenak saihestea.**



Herritarrentzat eta publiko orokorarentzat, funtsezko mezua erraza da: **adimen artifiziala laguntza bat izan daiteke, baina ez du giza irizpidea ordezkatzeko**. Komeni da informazio pertsonala edo konfidentziala baimenik gabeko tresnetan ez sartzea, emaitzak beti berrikustea, egiaztatu ezin diren erantzunekin ez fidatzea eta teknologia modu kontzientean erabiltzea. Segurtasuna ondo informatutako eguneroko erabakiekin hasten da.



Erakundeentzat, erronka zabalagoa da: **kontrola galdu gabe berritzea ahalbidetuko duen gobernu-esparrua eraiki behar dute**. AAren erabilera-politikak, irtenbideen inbentarioak, arriskuen azterketak, kontrol-tresnek eta trebakuntzak sistema integratu gisa funtzionatu behar dute. Horrela baino ezin da frogatu AA modu proportzionalan, trazagarrian, berrikusgarrian eta segurtasun, pribatutasun, gardentasun eta pertsonetikiko zerbitzu balioekin lerrokatuta erabiltzen dela.

Azken batean, AAren erabilera segurua ez da berrikuntzarako oztopo bat, berrikuntza fidagarria izateko baldintza bat baizik. Cyberzaintzak, zibersegurtasuna bultzatzeko eta koordinatzeko duen zereginetik abiatuta, AAren ezarpena irizpidearekin, bermeekin eta haren onurak modu arduratsuan babestera eta aprobeztatzera bideratutako ikuspegiarekin egiten lagun dezake.



Sarean ere, auzolana.
Por ti hacemos red.

Informazio orokorra:

945 236 636

info@cyberzaintza.eus



www.zibersegurtasun.euskadi.eus

EUSKO JAURLARITZA



GOBIERNO VASCO