EUSKO JAURLARITZA GOBIERNO VASCO

AURRERA!

72. zk.

2020ko ekaina

Berrikuntza eta Teknologia Berrien dibulgaziozko aldizkaria
Bulego Teknologikoak argitaratua
Informazioaren eta Komunikazioaren Teknologien Zuzendaritza

AURKIBIDEA

Aurrera aldizkariaren ale berri honen lehen artikuluan kontzeptu berri bat aurkeztuko dizuegu, gaur egun enpresa askotan gorabidean dagoena, *«**RPA**: Prozesuen Automatizazio Robotikoa»*. Artikuluan ikusiko dugun bezala, tresna ona izan daiteke enpresa askok haien prozesuak digitalizatzeko.

Bigarren artikuluan, *«Eusko Jaurlaritzaren eta haren sektore publikoaren zibersegurtasun-ereduaren bilakaera»* izenekoan, Eusko Jaurlaritzaren **zibersegurtasun-eredua**ren oraina eta, batez ere, etorkizuna aztertuko dugu, Interneten egunero gertatzen zaizkigun mehatxuei aurre egiteko.

Eusko Jaurlaritzako lanpostu korporatiboetan ezartzen ari diren Windows10 eta Office365 gaiei buruzko aholkuekin jarraituz, oraingo honetan Office 365 berriak dituen produktuetako bati erreparatuko diogu, **«Teams»**-ari buruz, hain zuzen ere. Aplikazio horri esker, pertsona askok beren etxe partikularretatik lankideekin harremanetan jarraitu ahal izan dute Covid-19 koronabirusak eragindako osasun-krisialdian, eta, pixkanaka-pixkanaka, gure lanpostutik ere gero eta gehiago erabiliko dugu.

Kontrazalean, «Ni.eus» aurkezten dizuegu, PuntuEUS Fundazioak abian jarri berri duen **euskarazko posta elektroniko**ko zerbitzu berria, bereziki Internet erabiltzen duten pertsona «euskaldunei», partikularrei, elkarteei eta enpresei zuzendua.

Azken hilabeteetan, Covid-19 **koronabirusa** ospetsu egin da eta zoritxarrez mundu osoko milioika pertsonen bizitza markatu du. Hala ere, eta jende askok uste duenaren kontra, koronabirusak ez dira berriak, June Almeidak aurkitu baitzituen 1967an. *«Protagonistak»* atalean, zientzialari eskoziar honen bizitza errepasatuko dugu, teknologiari esker birusak hobeto ikusteko metodo bat garatu baitzuen.

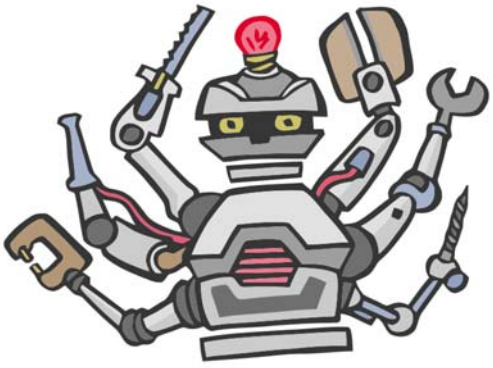
RPA: prozesuen automatizazio robotikoa

Gaur egun, prozesuen automatizazio robotikoa, Inteligentzia Artifizialarekin eta Big Datarekin batera, enpresak beren «eraldaketa digitala» gauzatzeko erabiltzen ari diren funtsezko piezetako bat da.

[1] **RPA:** ingelesezko hizkiak dira eta *«Robotic Process Automation»* adierazi nahi dute (euskeraz, «Prozesuen automatizazio robotikoa»).

Soluzio teknologiko berri hauek «software-robotak» eta adimen artifiziala (ingelesez, *«Artificial Intelligence»* edo AI) erabiltzen dituzte prozesuak kudeatzeko.

Askotan, lanean egiten ditugun zereginak errepikakorrak eta monotonoak izaten dira, eta, normalean, pertsonek balio erantsi gutxi ematen diete.



Lantegietan, lanak esfortzu fisiko handiak egitea suposatzen duenean edo zeregin errepikakorrak egin behar direnean, makinak edo robotak erabili ohi dira. Bada, filosofia hori bera aplikatzen zaio orain mundu ez-fisikoari, hau da, **prozesuei**, eta kasu honetan RPA[1] edo *«prozesuen automatizazio robotikoa»* deitzen zaio, eta hori da dagoen alde bakarra.

Ikus dezagun zertan datzan zehazki.

RPA

Enpresek urte asko daramatzate automatizazio-softwarea erabiltzen. Hala ere, gaur egun teknologia hori inoiz baino gehiago hazten ari da enpresa eta sektore askotan.

Instalatzen den robota (edo bot-a) **software** batean datza, eta sistemekin interakzioan jarduten du pertsona batek egingo lukeen bezala, botoi batzuk sakatzen ditu, formulario bat betetzen du edota dokumentu baten edukia irakurtzen du, adibidez. Hala ere, gure enpresan RPA bat instalatzen badugu, ez dugu robot bat gure aulkian eserita ikusiko, beste aplikazio edo software batek bezala funtzionatuko du eta.

Prozesuen automatizazioaren helburua da zeregin errepikakorrak, monotonoak eta konplexuak gauzatzeko denbora optimizatzea (normalean, zeregin horiek eskuz egiten ditugu eta). Horri esker, bi gauza lortzen dira: erantzuteko denbora murriztea eta nekeak eragindako akatsak minimizatzea.

Gaur egun automatizatzen ari diren zeregin ohikoenetako batzuk honako hauek dira:

- ✓ Formularioak kudeatzea eta aldez aurretik artxibatuta ditugun datuekin betetzea

- ✓ Datu-base bateko erregistroak bilatzea, sortzea, eguneratzea edo ezabatzea
- ✓ Aldez aurretik ezarritako egitura duten txostenak egitea

- ✓ Kalkuluak eta baliozkotzeak eskatzen dituzten txostenak sortzea
- ✓ Transferentziak monitorizatzea

Gaur egun, «software-robotak» edozein aplikazio informatikorekin lan egiteko gai dira, kalkulu-orri sinple batekin edo web-aplikazio batekin, adibidez, eta baita Bezero/Zerbitzari sistemekin ere.

LEHEN URRATSAK

Askok uste dute prozesu bat automatizatzea software bat instalatzean datzala. Baina automatizatu nahi diren prozesuak aldez aurretik aztertu eta ondo aukeratu behar dira, eta ondoren prozesuak nola exekutatu eta nola mantendu behar diren zehaztu behar da, eta baita nola egin nahi dugun haien jarraipena ere.

Beraz, lehenengo urratsa automatizatu beharreko **prozesuen diagrama** definitzea da, eta, ondoren, hura osatzen duten **jarduerak** eta **zereginak** (parte-hartzen duten arduradunen **rolak** zehaztu ere). Hori egin eta gero, aldez aurretik definitutako ataza bakoitzean erabiltzen diren **aplikazioak** zein diren zehaztu behar ditugu, RPArekin zer interakzio mota izango duen zehaztu ahal izateko (adibidez, sarbideak eta robotentzat beharrezkoak diren gainerako konfigurazioak).

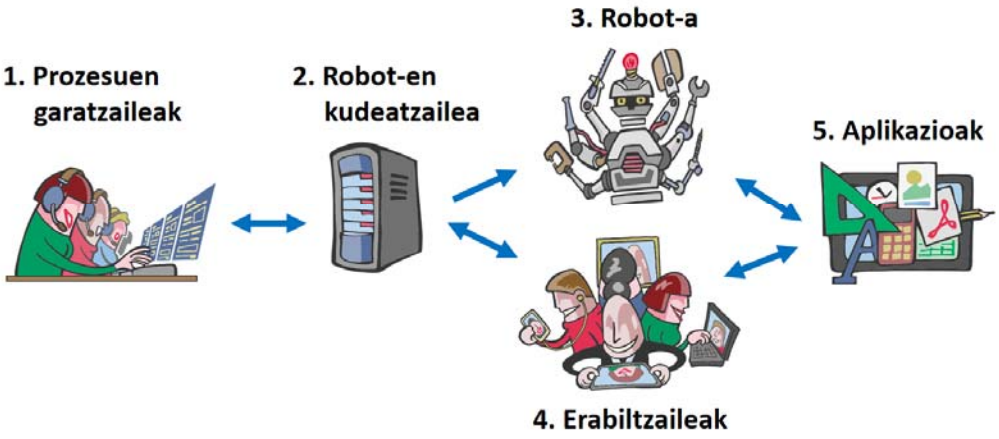
«Prozesuak» + «jarduerak» + «atazak» geruzak (eta «aplikazioak») zehaztu ondoren, **robot**-en geruza diseina dezakegu.

Merkatuan badira aplikazioak, adibidez *«low-code»*[2] delakoan oinarritutakoak, enpresei software-robotak diseinatu eta mantentzea errazten dietenak.

Hurrengo urratsa enpresak bere egitura teknologikoa eta giza baliabideak berrantolatzea da (kasu honetan, lanpostu batzuen rola aldatu behar du eta berriak sortu).

RPA baten puzzlea osatzen duten piezak, funtsean, honako hauek dira:

1. **Garatzaileak**: RPAk garatuko dituen zereginak edo prozesuak identifikatzeaz arduratzen diren pertsonak dira.
2. **Roboten kudeatzailea**: atazak esleitzeaz eta monitorizatzeaz arduratzen da.
3. **Software-robota**: negozio-aplikazioekin zuzenean elkar eragiteaz eta lana egiteaz arduratzen da.



Deloitte-ko «Automatización Robótica de Procesos (RPA)» [2017] txostenean oinarritutako eskema

4. **Erabiltzaileak**: robotak izapidetu ezin dituen gorabeherak (edo salbuespenak) konpontzeaz arduratuko dira.
5. **Aplikazioa**: robotak erabiltzaileekin elkarreragiteko erabiltzen duen programa edo plataforma da.

ONURAK

Prozesuen automatizazio robotikoak onu-

[2] **Low-Code:** aplikazioak garatzeko plataforma sorta bat da, eskuz kodearen garapena ahalik eta gehien murriztuz. Normalean, erabiltzen dira interfaze bisual bat, *«drag and drop»* utilitateak (arrastatu eta askatu) eta aldez aurretik konfiguratutako osagaiak. Horri esker, IKT gaietan ezagutza tekniko gutxi duten pertsonek nahiko erraz garatu eta zabaldu ditzakete enpresa-aplikazioak.

2014an erabili zen lehen aldiz *«Low-Code»* hitza, Clay Richardson eta John Rymer analistek Forrester enpresarentzat idatzitako txosten batean.

rak dakarzkie bai enpresei bai automatizatu nahi den lana egiten duten pertsonei. Hona hemen esanguratsuenak:

- **Kostuak**: pertsona batek egiten dituen eskuzko lanak eta zeregin errepikakorrak RPA softwareak kudeatuko ditu hemendik aurrera, eta, beraz, kudeaketaren kostua murriztu egingo da.
- **Denbora**: lana epe laburragoan egiten da, eta pertsonek beste lan batzuk egin ditzakete.
- **Kalitatea**: automatizazioak akats kopurua asko murrizten du, eta horrek esan nahi du azkenean zerbitzu hobea lortzen dela.
- **Malgutasuna**: arrazoiren batengatik negozio-prozesuak aldatzen badira, nahikoa da RPAren arauak berriz diseinatzea (eguneratzea) eta robota berriz konfiguratzea, eta hori denbora gutxian egin daiteke.
- **Jarraipena**: neurketak online egin daitezke definitu diren prozesuetan etengabeko hobekuntzak ezartzeko.
- **Digitalizazioa**: RPAek ez dituzte paperezko formatuan dauden atazak prozesatzen. Hau da, automatizatu nahi diren zeregin edo prozesu guztiak dokumentu digitalizatuekin egin behar dira. Beraz, zeharka bada ere, RPAek prozesu askoren digitalizazioa bultzatzen dute.

IRIZPIDEAK

Merkatuan hainbat robot mota daude[3]; horregatik, garrantzitsua da argi izatea zein irizpide hartu beharko genituzkeen kontuan RPA bat edo beste bat aukeratzerakoan:

- ✓ **Arkitektura**: lehenik eta behin, garrantzitsua da tresna nola egituratzen den jakitea, horren arabera diseinu konplexuak sortu ahal izango baitira.
- ✓ **Erabilgarritasuna**: erabiltzeko erraztasuna kontuan hartu beharreko gaia da beti, horren arabera errazago ezarriko baita eta pertsonek probetxu handiagoa atera ahal izango baitiote.
- ✓ **Integrazioa**: garrantzitsua da jakitea RPAk zer gaitasun duen beste sistema eta teknologia batzuekin erlazionatzeko, bere lana osatzeko hainbat sistemekin elkarreragin behar baitu.
- ✓ **Salbuespenak**: askotan oharkabean pasatzen den beste alderdi bat da RPAk negozio-salbuespenak maneiatzeko eskaintzen duen gaitasuna, eta pertsona batek eskuzko jarduera bat egitea suposatzen duena.
- ✓ **Segurtasuna**: RPAk sarbideen eta rolen kudeaketa ona izan beharko du.

[3] **Bot motak:**

Front office robotak: kanpora zuzendutako prozesuez arduratzen dira, adibidez salmentekin edo bezeroaren arretarekin lotutakoak. Prozesu horietan beti egongo dira pertsonak, giza irizpidea eskatzen duten erabakiak hartzeko.

Adibidez, *«call center»* batek RPA bat erabil dezake laguntzaile gisa. Call centerreko langileek online sistema ugari erabiltzen dituzte bezeroaren historia, eskaeraren egungo egoera eta abar ezagutzeko.

Back office robotak: enpresaren funtzionamenduari euskarria ematen diote, eta arretarik gabeko prozesuak edo *«background»* prozesuak dira.

Artxiboen transferentziak, txostenak sortzea edo monitorizazio-sistemak bezalako zereginak egiten dituzte. Bulegoko ordutegitik kanpo jaurti ohi dira, gainontzeko sistemak ez asetzeko.

Adibidez: bezeroarekin egindako transakzioetan bildutako datuak automatikoki txosten batean txertatu daitezke, eta gero beste pertsona batekin partekatu (posta elektroniko baten bidez, adibidez).

RaaS

Teknologia Berrien munduan ohikoa bihurtu den kontzeptuetako bat «SaaS» siglak dira, eta *«Software as a Service»*-ari erreferentzia egiten diote. Hodeian instalatuta dauden aplikazioak biltzen ditu, eta enpresaren bat behar dituenean erabiltzen dira (normalean, zerbitzu hori harpidetza bidez kontratatzen da). Bada, era berean, beste akronimo bat sortu berri da, automatizazio robotikoa identifikatzeko, «RaaS», hain zuzen ere, (*«Robot as a Service»* edo *«Robotics as a Service»*).

Beraz, automatizazio robotikoa hodeian ere inplementatu daiteke, eta enpresei beharrezko automatizazio-aplikazioak eskaini ahal zaizkie, eta beste zerbitzu bat izango balitz bezala erabiliko genuke.

Modalitate honen adibide tipikoa da dendek edo arropa-biltegiek beren stock-aren kudeaketa automatikoa egiteko egiten duten erabilera.

Pertsona, talde edo sail bakoitzak benetan behar dituen baimenak baino ez ditu izan behar (adibidez: pertsona batzuek lan-fluxu bat editatzeko baimenak izan beharko dituzte, eta beste batzuek, berriz, lan-fluxu hori soilik ikusi beharko lukete). Gainera, komenigarria litzateke pertsona bakoitzak egiten dituen ekintzen erregistroa gordetzea.

«Zeharka bada ere, RPAek prozesu askoren digitalizazioa bultzatzen dute»

- ✓ **Konfigurazioa**: garrantzitsua da RPA batek prozesu automatizatuak kontsola zentral batetik monitorizatzeko eta kudeatzeko aukera izatea. Horri esker, eragiketen jarraipena egin eta sor daitezkeen arazoak identifikatu ahal izango dira.
- ✓ **Inplementazioa**: arretaz aztertu behar ditugu plataforma berriak eskaintzen dituen funtzioak, Ekoizpen Ingurune batean inplementatua izateko, adibidez. Horrek suposatzen du, besteak beste, makinen artean bertsioak banatzea, inguruneko aldagaiak pertsonalizatzea, segurtasun-kontrolak ematea, etab.
- ✓ **Euskarria**: beste alderdi garrantzitsu bat hornitzaile[4], euskarri eta dokumentazio ona izatea da, softwarea erabiliko duten pertsonei eman beharreko formakuntza ahaztu gabe.

Prozesuak automatizatzeko orduan, komenigarria da etorkizunean pentsatzea, eta aztertzea ere nola heda litekeen RPA enpresako beste arlo batzuetara gure negozioa handitzen doan heinean; izan ere, prozesu indibidualak automatizatzean zentratzen bagara (modu isolatuan), ziurrenik arazoak izango ditugu etorkizunean RPA hedatzeko.

SEKTOREAK

RPAak pixkanaka hedatzen ari dira, eta, gaur egun, arrakasta gehien izaten ari diren sektoreak **manufakturazioa**rekin, **muntaketa**-fabrikekin eta **osasun**-sektorearekin (farmazeutikak...) lotutakoak dira.

RPAk gero eta gehiago erabiltzen ari diren beste sektore bat bezeroari arreta emateko **telefono-zerbitzuena** da. Adibidez, enpresa askok txat-robot adimendunak erabiltzen dituzte giza elkarrizketa simulatzeko eta bezeroen arazoak konpontzeko.

Beste sektore bat **aseguruena** da. Normalean, aseguru-enpresek dokumentu eta lan-fluxu ugari erabiltzen dituzte. Kasu horietan, robotek erreklamazio baten ia etapa guztiak kudeatzen dituzte, adibidez: kexa bat jasotzen dute, bidalitako datuak deskargatzen eta egiaztatzen dituzte, eta ordainketa kalkulatzen dute (pertsonek bakarrik parte-hartzen dute giza irizpidea behar duten salbuespenak aztertu behar direnean).

Enpresa teknologikoetan ere gero eta gehiago erabiltzen ari dira robotak. Oso ohikoa da pertsona baten pasahitza berrezartzeko eskaera egitea. Kasu horietan, robotak eskaera jasotzen du, egin beharreko ataza aztertzen du (arau

batzuetan oinarrituta egon daiteke), eta, ondoren, eskatu duen pertsonaren pasahitza berrezartzen du, pertsona batek prozesu osoan parte-hartu beharrik gabe. Beste erakunde batzuek botak erabiltzen dituzte VPNak sortzeko.

Beste sektore garrantzitsu bat **finantza-erakundeena** da. Bankuetako prozesu automatizatuei esker, gaur egun zenbait erabaki hartzeko behar diren datuak ebaluatzeko prozesua eraginkorragoa da. Adibidez, bezero baten kaudimena kalkulatzeko, kreditu bat emateko edo ez emateko, etab. ❑

[4] **Hornitzaileak:** RPA sistemen hornitzaile batzuen zerrenda:

- Automation Anywhere
- Blue Prism
- HelpSystems
- Kryon Systems
- Kofax
- NICE
- Pegasystems
- Redwood
- UiPath
- WorkFusion
- ...

Eusko Jaurlaritzaren eta haren sektore publikoaren zibersegurtasun-ereduaren bilakaera

Interneten eragiten dizkiguten arriskuak gero eta sofistikatuagoak dira, eta, beraz, ondo prestatuta egotea komeni da.

Interneten zelatatzen gaituzten mehatxuen testuingurua dibertsifikatu egin da, eta gero eta konplexuagoa da, baliabide eta motibazio ugari dituzten sare kriminalak baitaude haien atzean.

Eragile edo motibazio ohikoenak sare kriminalak, «hacktibistak», ziberespioitza edo ziberterrorismoa izaten dira, eta ezaugarri nagusiak hauek dira:

- ✓ Erasoak gero eta zuzenagoak dira
- ✓ Jarduteko erraztasuna -> ekonomikoa
- ✓ Jurisdikzio konplexua -> zigorgabetasuna
- ✓ Motibazioa sakabanatzea

Mehatxuen etengabeko bilakaerak ikuspegi zabalagoa eskatzen du zibersegurtasunaren arloan. Hori dela eta, erakundeek beren gaitasunak hobetu behar dituzte, beste batzuk sartuz.

Adibide gisa, iaz euskal erakunde publiko baten aurkako eraso zibernetiko bat gertatu zen, —kasu honetan, Europa Ekialdeko zibergaizkile talde antolatu batek egina, zigorgabetasun handia dakarrena—, eta horrek eragin larria izan zuen erasotako erakundeak ematen dituen zerbitzuetan.

Erasoa zabaltzeko erabilitako sistema nahiko sinplea izan arren, oso arrakastatsua eta iraunkorra izan zen denboran zehar. Normalean, eraso horiek sistemen ahulezien edo engainuen bidez sartzen dira erakundeetan (ingeniaritza soziala[5]). Afekzio-erradioa handitzeko edo informazio garrantzitsua eskuratzeko, datuak biltzen edo ex filtratzen dituzte; eta hainbat hilabete egon daitezke «lo» (aktibatu gabe) berriro aktibatu arte, eta momentu horretan infektatutako aktiboak erasotzen dituzte blokeatu arte (ordenagailuak, zerbitzariak...).

Une horretan, gaizkileek enpresari kriptomonedetan erreskatea eskatuko diote blokeatutako aktiboa libre uzteko.

Eraso hori, zehazki, mundu mailan antolatutako kanpaina baten barruan egin zen, eta Euskadin eragin handia izan zuen.

«"Segurtasun Plan Zuzentzailea"-ren helburua da BATERAren bidea zehaztea datozen 4 urteetarako zibersegurtasunaren arloan»

Eraso horrek, zerbitzu informatikoen erabilezintasuna eta informazio-ihesak eragin zituen. Aktiboen berreskurapena oso konplexua eta motela izan da, eta kostu ekonomiko handia izan du.

IKASITAKO IKASGAIAK ETA ERRONKA BERRIAK

Egoera horiek guztiek uzten dizkiguten ikasgaiak aztertzea garrantzitsua da eta etorkizuna prestatzea. Beraz, zibersegurtasunak planteatzen dizkigun erronka berri hauei erantzun behar diegu:

1. **Jarduera-eremua zabaltzea** («perimetrotik ateratzea»). Gaur egun, mehatxu nagusiak ziberespazioan daude, eta horrek erasotzaileen portaerak aztertzea eta

[5] **Ingeniaritza soziala:** (ingelesez *«Social Engineering»*) Pirata informatiko batek pertsona bati informazioa ateratzeko erabiltzen dituen engainu eta gainerako teknika guztiak biltzen ditu, pertsona hori «informazio sentikorra» adierazten ari dela konturatu gabe (adibidez, pasahitz bat) edo pertsona batek ekintza zehatz bat egitea (adibidez, irekitzea birus bat duen artxiboa).
Informazio gehiago nahi izanez gero, Aurrera aldizkariaren 13. zenbakian (2004ko martxoa) argitaratutako *«Gizarte ingeniaritza»* izeneko artikulua kontsulta dezakezue.

ikastea suposatzen du. Beraz, beharrezkoa da gure informazio-aktiboen jarraipena eta monitorizazioa egitea, gure informazio-sistemetatik harago.

2. **Ikerketa- eta adimen-mekanismoak indartzea**. Zibermehatxuen etengabeko bilakaerak eta sofistikazioak mehatxuak detektatzeko eta aztertzeko mekanismo iragarleak indartzea eskatzen dute.
3. **Disuasioa indartzea**. Erakundeen erresilientzia indartzea. Gure informazio-sistemen prebentzio-, detekzio- eta erantzun-gaitasunak zabaltzea. Jarduteko denborak aurreratzea eta murriztea. Zaintza-mekanismoak eta euste-neurrien aplikazioa hobetzea.
4. **Entrenamendua eta kontzientziazioa**. Gure erakundeko langileen artean ziberariketak eta segurtasun-ebaluazioak sustatzea. Laburbilduz, kontzientziazio eta formakuntza-kanpainak areagotzea.
5. **Gertakariei erantzuteko gaitasuna handitzea**. Beharrezkoa da intziden-tziak kudeatzeko tratamendu bat antolatzea, erantzun sendoa eman ahal izateko. Komeni da kanpo-lankidetzako elementuak integratzea, susperraldian laguntzeko eta lankidetza judizial eta polizialeko neurriak ezartzeko.
6. **Diseinuan segurtasuna aplikatzea**. Segurtasun-eskakizunak proposatzea ne-gozio-eskakizun gisa. Eskakizun horiek berrikusteko eta neurtzeko mekanismoak ezartzea. BATERA[6] zerbitzuetan segurta-sun handiagoa sartzea (azpiegiturak, Backup, lanpostua, misiorako eta bizitza-rako aplikazio kritikoak).
7. **Esparru Erregulatzailea** Marko Opera-tiboarekin lerrokatzea. SEN, ISO 27000, ISO 22301.

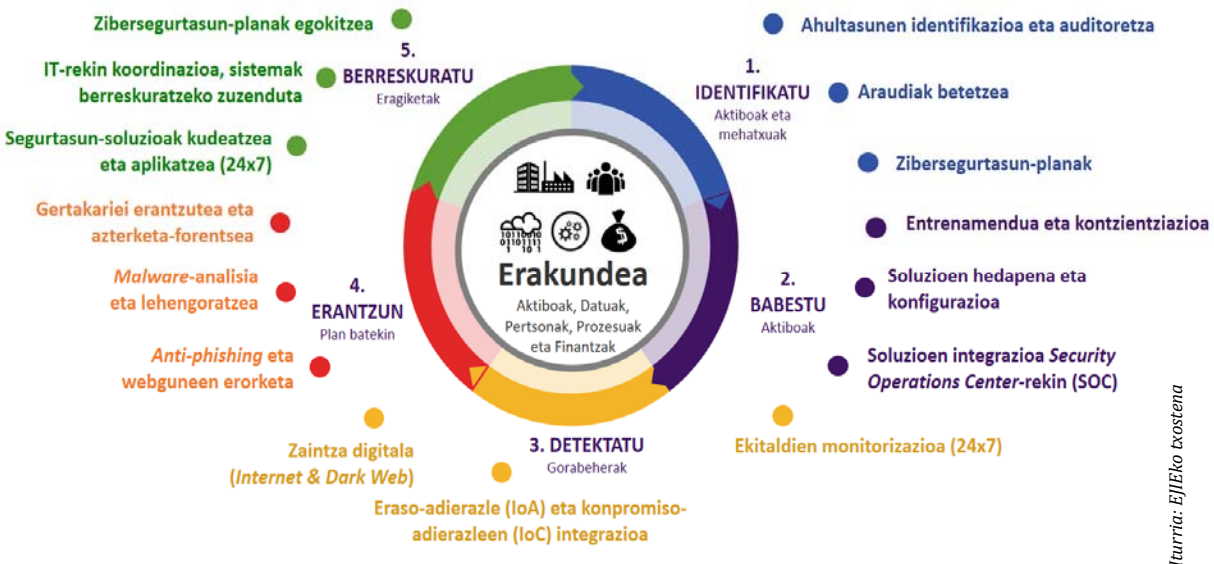
Eta, jakina, sistema zaharkituekiko babes- eta euskarri-zerbitzu tradizionalak mantendu eta indartzea.

IKUSPEGI OPERATIBOA

BATERAn IT segurtasun-euskarri gisa jarduten duten zerbitzu nagusiak **ITren esparru arautzaile eta gobernu-esparru batean** jasota daude.

Hauek dira esparru horren osagai nagusiak:

1. Segurtasuneko Bulego Tekniko bat EJIEn, DBEO, SENa, azpiegitura kritikoak eta oinarrizko zerbitzuak eta zerbitzu digitalak betetzeko, eta baita ISKS betetzeko ere (ISO 27001 arauaren arabera) eta negozioaren jarraipeneko aholkularitza emateko.
2. *«Security Operation Center»* bat, ondorengo gaietaz arduratuko dena: segurtasun-ekitaldiak monitorizatzeaz, kontrol-sistemaren kudeaketaz eta bilakaeraz, segurtasun-gorabeherak konpontzen laguntzeaz, ahultasunak aztertzeaz, segurtasun-auditoretzez eta kontzientziazio- eta prestakuntza-auditoretzez.



Iturria: EJIEko txostena

[6] **BATERA:**

2015eko uztailaren 27an, Gobernu Kontseiluak *«Gobernu Kontseiluaren erabaki-proposamena, Informazioaren eta Komunikazioaren Teknologien arloko konbergentzia-prozesuari buruzkoa»* onartu zuen, hau da, «BATERA» abian jartzea, Euskal Autonomia Erkidegoko (EAE) sektore publikorako IKTen kudeaketa-eredua ezartzen duen konbergentzia-prozesua.

Geroago, Gobernu Kontseiluak, **2016ko ekainaren 21ean**, *«Informazioaren eta Komunikazioaren Teknologien arloko konbergentzia-prozesuari buruzko erabaki-proposamena»* izeneko akordioa onartu zuen. Akordio horretan, dokumentu exekutiboa onartu eta konbergentzia-prozesua ezartzea baimendu zen, aurkeztutako jarduera-plan orokorraren arabera.

[7] **CSIRT**: «Informatikako Larrialdiei Erantzuteko Taldea» kontzeptuaren siglak dira.

[8] **CERT:** «Herritarren eta enpresen segurtasun-gorabeherei erantzuteko zentroa»-ren siglak dira.

[9] **CISO:** informazioaren Segurtasunerako zuzendariaren siglak dira.

[10] **MITRE ATT&CK**: (Taktikak, Teknikak eta Aurkarien Ezagutza Komuna). Mundu osoko behaketetan oinarritutako jokabide kaltegarriak deskribatzeko eta sailkatzeko modu bat da. Hau da, zerrenda egituratu bat da eta taktika eta tekniketan bildutako erasotzaileen portaera ezagunak biltzen dira, eta matrize batzuetan antolatzen dira. Zerrenda hau erasotzaileek sareak arriskuan jartzen dituztenean erabiltzen dituzten portaeren irudikapen integrala da, eta hainbat neurri, irudikapen eta erasorako eta defentsarako beste mekanismo batzuk ezagutzeko baliagarria da.

3. Segurtasun-plataformen kudeaketa bat: segurtasun-azpiegituren eragiketa osatzeko, segurtasun-eguneratzeen segurtasun-gorabeheren tratamendua egiteko, zerbitzuen partxeatze eta bastionatuaren tratamendua egiteko eta «backup» kudeaketaren tratamendua gauzatzeko.

4. CSIRT[7] bat, gorabeherei erantzuteko zentroa: alerta goiztiarrak eta analisi forentseak egiteko, beste CERT[8]-ekiko erlazioa mantentzeko eta baita krisien kudeaketa egiteko ere.

5. Bilakaera teknologikoko zerbitzu bat, segurtasun-proiektuen ezarpenetan, segur-tasun-teknologia berrien ebaluazioan, gainerako bulego teknikoekiko elkarrizketan eta CISO[9]-ren laguntzan parte hartzen duena.

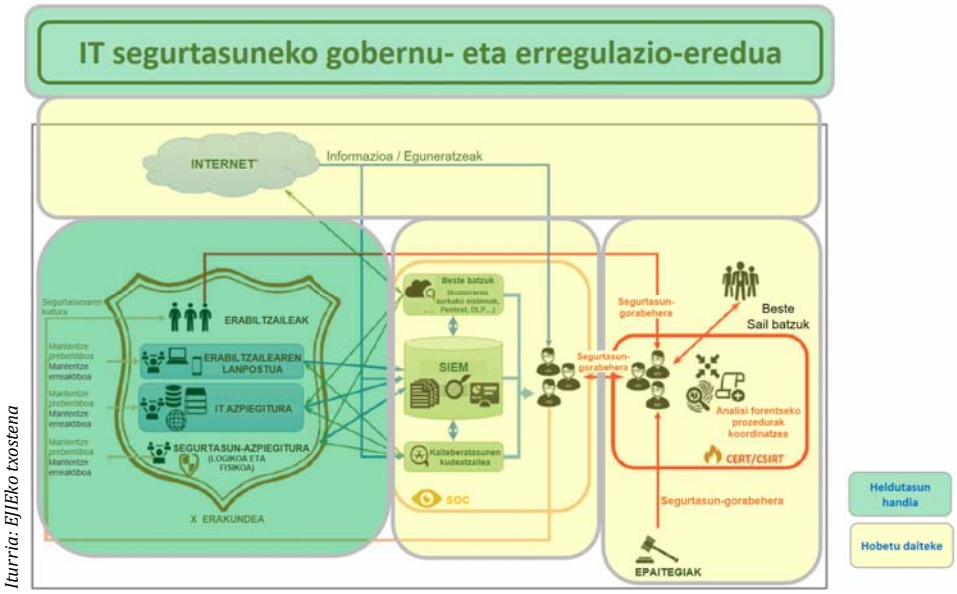
Gaur egun, BATERAko euskarri-zerbitzuen heldutasuna handia da; izan ere, erasoak normalean jaso arren, ez dute eragin garrantzitsurik izan. Hala ere, arriskua areagotu egiten da eta segurtasuna indartzeko beharra nabarmentzen da.

SEGURTASUN-ZERBITZU BERRIAK

Jarraian, BATERAn lehentasunez eskaini nahi diren segurtasun-zerbitzu berriekin lotutako alderdi garrantzitsuenak aztertu eta aurkeztuko dira.

Esan dugun bezala, zibersegurtasunaren arloko egungo testuingurua gero eta konplexuagoa da. Mugikortasuna gero eta handiagoa den heinean, eta, ondorioz, «cloud»-eko zerbitzuak eta barne-zerbitzuen esposizio-maila ere gero eta handiagoak direnez, **arrisku-maila** proportzionalki handitzen da. Bestalde, sare kriminalak gero eta espezializatuagoak dira, eta gero eta gehiago zuzentzen eta lantzen dituzte erasoak, egiten duten «inbertsioa»-ren itzulera lortzeko.

Horregatik, testuinguru horrek ikuspegi zabalagoa eskatzen du zibersegurtasunaren arloan, eta, horregatik, EJIE, BATERA proiektuaren barruan, gaur egun eskaintzen dituen «Segurtasun-zerbitzuen bilakaera» azterketa-fasea ireki du. Fase horrek lehendik dauden gaitasunak hobetzeko eta egungo egoeraren mehatxuei aurre egitea ahalbidetuko duten gaitasun eta funtzionalitate berriak sartzeko aukera ematen du.



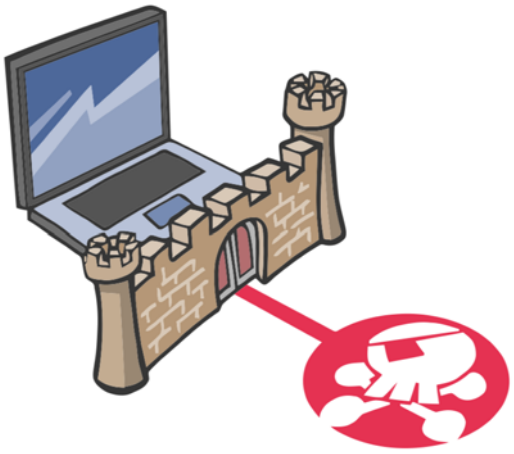
Iturria: EJIEko txostena

Bilakaeraren fase honen abiapuntu gisa, «Segurtasun zerbitzuen bilakaera plana» edo «Segurtasuneko plan zuzentzailea» prestatzen ari da, BATERAk datozen 4 urteetarako Zibersegurtasunaren arloan izango duen bidea markatzeko. Plan hori gauzatzeko, nazioarteko erreferentziak erabiliko dira segurtasuna antolatzeko, hala nola «NIST Cyber Security Framework» edo «MITRE ATT&CK»[10] matrizea.

Plana amaitu gabe dagoen arren, lehentasunez egin beharreko zenbait behar identifikatu dira dagoeneko, eta honako hauek dira:

1. **Backup Zerbitzua**ren bilakaera: EJIEk ematen dituen IT zerbitzuak arriskuan jartzen dituen edozein segurtasun-erasoren aurrean, segurtasun-kopiak dira zerbitzua berrezartzea bermatzen duen azken baliabidea. Beraz, beharrezkoa da kopia horiek gordetzen dituzten gordailuak blindatzea.
2. **SIEM**[11] teknologia. Gaur egungo segurtasun-mehatxuen aniztasunak eta espezializazioak eta BATERA bezalako IT ingurune baten konplexutasunak eta tamainak ia ezinbestekoa egiten dute segurtasun-elementuen trazabilitatea (*«log»*-ak) zentralizatu eta horien analisia automatizatzea, segurtasun-gorabeherak detektatzeko eta ikertzeko. SIEM tresnak eraginkorrak izan daitezen, segurtasunaren ikuspegitik garrantzitsuak diren gertakari-iturri guztiak sartu behar dira, eta, ondoren, korrelazio-arauak sortu behar dira, gertaerak automatikoki aztertzeko, jarduera susmagarriak edo segurtasun-gorabeherak bilatzeko. Soluzioen kalitatea, batez ere, eskaintzen dituzten korrelazio-arauen kalitatean datza; kalitate horren arabera, eraginkortasunaren, eguneratzearen eta azken gertakariei eta gertakari globalei emandako erantzunaren arabera. Azken finean, SIEMek, aztertu ondoren, eskaintzen duen gertaeren fidagarritasunaren arabera.
3. **EDR**[12] soluzioak: lanpostua, gailu mugikorra edo zerbitzariak (*«endpoint»*-ak) dira erasotzaileek erakundeetan sartzeko eta sistemak konprometitzeko erabiltzen dituzten ate nagusiak. Mehatxu berri horiei aurre egin ahal izateko, produktu jakin batzuk behar dira. Produktu horiek gai izan behar dute, batetik, jokabide-eredu anomaloak automatikoki detektatzeko (susmagarriak izan daitezkeen mehatxu bat izan daitekeelako), eta, bestetik, balizko arrisku horri erantzuteko eta mehatxua gelditzeko.
4. **Identitateen kudeaketa**. Gaur egungo munduan, informazioa edonon dago eta edozein gailutatik kontsumitzen da. Paradigma-aldaketa horren ondorioz, **identitatea** erakundeen zibersegurtasun-estrategiaren oinarrizko eta funtsezko zutabe bihurtzen da. Ideia horretatik abiatuta, *«Zero Trust»* (zero konfiantza) bezalako ekimenak sortzen dira: *«ez fidatu, beti egiaztatu»*. Merkatujoerak adierazten du identitatea lehentasunezko alderdia dela honako eremu hauetan:

«"Zero Trust": ez fidatu, beti egiaztatu»



- Aplikazioak eta baliabideak Cloud-en
- Araudia betetzea (DBEO)
- Mugarik gabeko lankidetza
- Segurtasun-maila handiagoko *«passwordless»* (pasahitzik gabe) autentifikatzeko modu berriak
- *«Zero Trust»* joera

Ikusten dugunez, zibersegurtasun-mehatxuek aurrera egin ahala, segurtasun informatikoaren mundua ere aldatzen ari da. ❑

[11] **SIEM:** mehatxuak identifikatu eta gordetzeko aukera ematen duen teknologia da. Hainbat iturritako informazioa biltzeko gai da, eta, agregazio- eta testuinguru-adimeneko mekanismoen bidez, monitorizaziorako eta erantzunerako gaitasun handiak eskaintzen ditu. Detekzio- eta babes-denborak errazten eta bizkortzen ditu.

[12] **EDR:** «Esposiziopeko sistemen babesa» kontzeptuaren siglak dira.

ALBOAN:

Windows10 eta Office365i buruzko aholkuak: «Teams», taldean lan egiteko modu berri bat

«Teams-ek eskaintzen duen funtzionalitaterik garrantzitsuena bideo-deia da»

Asko dira Microsoftek Office365 paketean eskaintzen dizkigun produktuak. Gaur, Covid-19 koronabirusak eragindako osasun-krisiaren ondorioz bizi behar izan dugun berrogeialdian pertsona askok aurkitu duten tresna bati erreparatuko diogu: *«Teams»* funtzionalitateari buruz ari gara, hain zuzen ere.

FUNTZIONALITATEAK

«"Taldeak" pribatuak edo publikoak (irekiak) izan daitezke »

Teams (ingelesezko hitzak *«Taldeak»* esan nahi du), funtsean, komunikazio-plataforma bateratu bat da, txat-a, bideo-deiak egiteko aukera eta dokumentuak bildu eta trukatzeko gune bat konbinatzen dituena, hori guztia lantalde bat osatzen duten pertsonen arteko lankidetza errazteko. Teams (Skype enpresariala ordezkatzen duena), azken batean, taldean lan egiteko aukera ematen digun aplikazioa da, fisikoki bananduta egon arren.

Teams-en barruan bi kontzeptu erabiltzen dira:

1. **Taldeak**: enpresaren proiekturen batekin lotutako pertsona-taldeak, edukiak eta tresnak dira. «Talde» berri bat sortzerakoan, jakin behar dugu taldeak **pribatuak** izan daitezkeela (gonbidatuek bakarrik dute sarbidea), edo **publikoak eta irekiak** (enpresako kide guztiek sar daitezke). Beraz, taldekideak izango dira elkarrizketak, artxiboak eta kanaletan argitaratutako oharrak ikusi ahal izango dituzten bakarrak.
2. **Kanalak**: talde baten barruan sortzen diren atalak dira, elkarrizketak gaika edo proiektu espezifikoen arabera antolatuta edo sailkatuta mantentzeko. Kanal baten barruan partekatzen diren fitxategiak («Fitxategiak» erlaitzean jasota geratzen dira) automatikoki sortzen den SharePoint batean biltegiratzen dira. Kanalak, laburbilduz, taldearen elkarrizketa egiten den eta elkarlana gauzatzen den tokia dira.

BIDEO-DEIAK

Teams-ek gaur egun hainbat funtzionalitate eskaintzen ditu, hala nola:

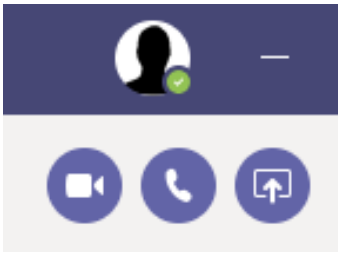
- ✓ Fitxategiak partekatzea
- ✓ Bideo-deiak egitea
- ✓ *«Wiki»* bat
- ✓ Egutegi bat
- ✓ Txat bat

Pertsona askorentzat Teams-ek eskaintzen duen funtzionalitaterik garrantzitsuena (eta konfinamenduan gehien erabili dena), zalantzarik gabe, **bideo-deia** da.

Beste pertsona batekin bideo-deia egiten hasteko, nahikoa da Teams-en sartzea (web bidez edo gure ordenagailuan instala dezakegun aplikazioaren bidez) eta pertsona horren izena bilatzea enpresaren direktorioan eta, jarraian, deiaren botoia sakatzea. Beste pertsonak gure deiaren abisua bere ordenagailuan jaso eta «erantzun» botoia sakatzen duenean,

elkarrizketari ekin ahal izango diogu.

Une horretan arreta eskaini ezin digun pertsona bat aurkitzen denbora ez galtzeko (adibidez, bere lanpostuan ez dagoelako edo beste elkarrizketa batean lanpetuta dagoelako), Teams-ek Outlook-eko egutegiarekin konektatuta dagoenez, pertsona hori beste bilera batean dagoen edo ez ikus dezakegu, eta beste aukera bat izan daiteke pertsona horren argazkiaren ondoan agertzen den marka aztertzea. Marka hori berdea bada, horrek esan nahi du pertsona hori bere lanpostuan dagoela eta gure deiari erantzuteko libre dagoela (erabilgarri, alegia); marka gorria bada, berriz, ezin izango gaitu artatu, okupatuta baitago.

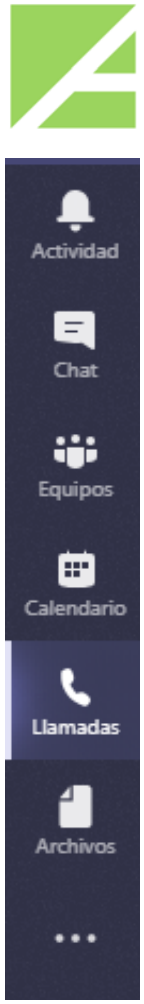


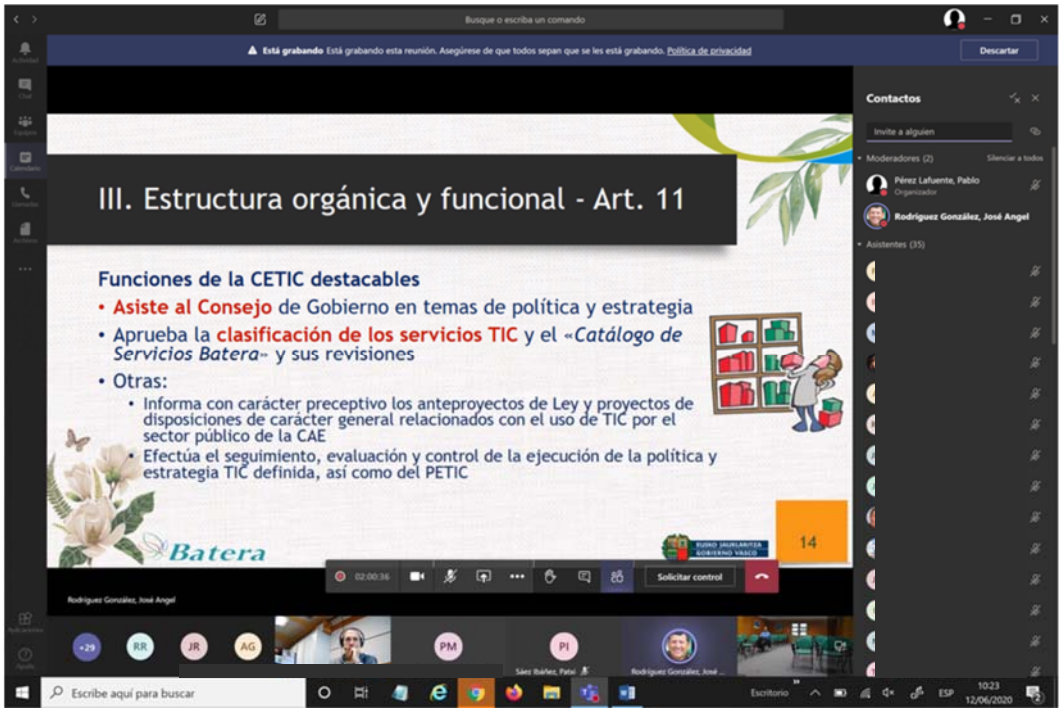
Bideo-deien zerbitzua ez dago bi pertsonaren arteko elkarriz-ketara mugatuta; aitzitik, hainbat pertsonak aldi berean parte-hartu dezakete sortutako bideo-deian, inolako arazorik gabe.

Bideo-deiek eskaintzen duten beste aukera interesgarri bat da **dokumentuak partekatzea**. Aukera honen bidez, elkarrizketa batean parte hartzen duten gainerako lankiderekin gure ordenagailuan daukagun dokumentu bat partekatu dezakegu (bileran zehar gai bat azaltzeko erakutsi nahi duguna).

Teams erabili ahal izateko, nahikoa da gure ordenagailua Office365 berrira migratu izana, eta gure ordenagailuak webcam bat, bozgorailu batzuk eta mikrofono bat (edo kasko batzuk) izatea. Deien zerbitzua **plataforma anitzekoa** denez, **telefono mugikorretik** zuzenean erantzun ditzakegu bideo-deiak (horretarako, egin behar dugun gauza bakarra dagokion aplikazioa edo *app*-a instalatzea da).

Ez ahaztu irudi batek mila hitzek baino gehiago balio duela, beraz animatu eta hasi Teams erabiltzen. ❑





Office365 berriaren atarira sartzeko webgunea: https://portal.office.com

Kontrazala

72. zk.

2020ko ekaina

IXTEKO

«Ni.eus», e-posta zerbitzua euskaraz

PuntuEUS Fundazioak eta Guebs euskal enpresak «ni.eus» izeneko euskarazko **posta elektroniko**ko zerbitzua garatu berri dute.

Ni.eus posta elektronikoak pertsonen arteko harreman digitaletan .EUS domeinua erabiltzeko aukera ematen du: doako bertsioan ni.eus domeinuan (adibidez: ximun@ni.eus) edo *«premium»* planaren kasuan, .EUS domeinua pertsonalizatuz (adibidez: info@ane.eus edo kaixo@mendielkartea.eus).

Argazkia: Domeinuak.eus-en webgunea

Zerbitzu berri hau Internet erabiltzen duten pertsona «euskaldunei», partikularrei, elkarteei eta enpresei zuzenduta dago.

Posta-zerbitzu berri honen alderdi garrantzitsuenetako bat **pribatutasuna** da. Ni.eus-ek erabiltzaileen datuen pribatutasuna eta segurtasuna bermatzen ditu: iragarkirik gabe, *«tracking»* gabe eta komunikazio zifratuak. Azken batean, ez du inolako iragarkirik erakusten, eta ez du erabiltzaileen erabileraren jarraipenik egiten.

Gainera, edozein lekutan dago eskuragarri, telefono mugikorrean edo ordenagailuan konfigura baitaiteke, eta online ere erabil daiteke *webmail*-en bidez. Gainera, zerbitzu osagarriak eskaintzen ditu, hala nola egutegia, helbide-liburua, birbideratzea, etab.

Informazio gehiago hemen:
https://www.domeinuak.eus

PROTAGONISTAK

June Almeida, koronabirusak aurkitu zituen zientzialaria

June Dalziel Almeida eskoziar birologoa izan zen (Glasgow-n jaio zen, 1930eko urriaren 5ean eta Bexhill-en hil zen, 2007ko abenduaren 1ean). Izan ere, berak garatutako teknikak erabiliz, mikroskopio batean koronabirus bat ikusi zuen lehen pertsona izan zen.

16 urterekin ikasketak utzi behar izan zituen unibertsitatera joateko nahiko baliabide ekonomikorik ez zuelako, eta Glasgow Royal Infirmary–n histopatologiako teknikari gisa hasi zen lanean. Handik gutxira Londreseko St. Bartholomew Ospitalera joan zen bere ikasketekin jarraitzeko. 1954ko abenduaren 11n ezkondu eta Kanadara joan zen, non Ontario Cancer Instituten lan egin zuen elektromikroskopista beza-la. Prestakuntza arautu gutxi izan arren, mailaz igotzen joan zen, batez ere erakusten zituen gaita-sunengatik.

Argazkia: National Geographic-en webgunea

Geroago, 1964an, A. P. Waterson-ek, St. Thomas's Hospital Medical School-eko Mikrobiologia irakasleak, konbentzitu zuen Ingalaterrara itzultzeko eta bere ospitalean lan egin zezan. Han garatu zuen **birusak** hobeto ikusteko metodo bat. B hepatitisaren birusarekin eta hotzeria arruntaren birusarekin lan egin zuen batez ere. Lan horri esker, June Almeidak errubeolaren birusaren lehen irudiak sortu zituen mikroskopio elektroniko bat erabiliz. Handik gutxira, 1967an, June Almeidak 34 urte zituenean, David Tyrrell irakaslearekin batera, koronabirus mota berri baten karakterizazioan lan egin zuen. Familia honek SARS eta SARS-CoV2 birusak ditu bere barruan, gaur egun **Covid-19** ospetsua sortzen duen birusa, hain zuen.

Informazio gehiago hemen:
https://es.wikipedia.org/wiki/June_Almeida