

eman ta zabal zazu



Universidad
del País Vasco

Euskal Herriko
Unibertsitatea

Internerako sarbide eta nabigazio segururako arautegia

Aurkibidea

EDUKIA

| | |
|---|----------|
| 1. Helburua | 3 |
| 2. Aplikazio eremua | 3 |
| 3. Arautegia..... | 4 |
| 3.1 Arau Orokorrak..... | 4 |
| 3.3 SEGURTASUN NEURRIAK | 6 |
| 4. Erantzukizunak..... | 7 |
| 4.1 Erabiltzaileen erantzukizunak | 7 |
| 4.2 UPV/EHUren erantzukizunak | 7 |
| 5. Arautegia ez betetzea | 7 |
| 6. Berrikuspena eta ebaluazioa | 8 |
| 7. Erreferentziak | 8 |

1. HELBURUA

Arautegi honen helburua da Universidad del País Vasco/Euskal Herriko Unibertsitatearen (aurrerantzean UPV/EHU) Informazio Sistemen erabiltzaileek Internetera egindako sarbidea arautzea, dela bertako egoitzetatik dela sistema horien bidez, erabiltzaile guztiek oro arauok ezagutu eta bete beharko dituzten erabilera arauak osatuz.

Oro har, UPV/EHUko erabiltzaileek Interneterako sarbidea baliatuko dute, produktibitateko eta jakintzarako tresna gisa, zeinek bere jardura akademikoetan, irakaskuntzakoetan, ikerkuntzakoetan eta administrazio eta gestiorako prozesuetan.

Bi dira arautegi hori artezten duten printzipio orokorrak:

- UPV/EHUren sarearen bidez Internetera sartu eta erabiltzeko arau egokiak eta ezegokiak ezartzea, eta arau horiek betetzen direla zaintzea.
- Unibertsitate komunitatearen eta Interneteko erabiltzaileen eskubideak, arduraz eta legez errespetatu eta babestea.

Dokumentu hori UPV/EHUren barne erabileratzat jotzen da eta, beraz, ezingo da zabaltu, segurtasunaren arduradunak baimena eman ezean.

2. APLIKAZIO EREMUA

Arau hau UPV/EHUren jardura eremu osoan aplikatu behar da, edukiak **UPV/EHUren Informazioaren Segurtasun Politikan** definitutako gidalerro orokorragoetatik eratorritako edukiak izanik.

Arau hau nahitaez bete beharko dute UPV/EHUko zerbitzuak modu iraunkorren edo aldi baterako erabiltzen dituzten erabiltzaile guztiek, bai eta kanpoko erakundeetako langileek ere, UPV/EHUren informazio sistemen erabiltzaile direnean edo berorietarako sarbidea dutenean.

Erabiltzaile guztiek izango duten Interneterako sarbidea izango da:

- Lanpostuen bidez, horretarako dauden UPV/EHUko ordenagailuen bidez, betiere ikastegi, gunee, informatika gela edo sarbide sare bakoitzaren berezitasunak errespetatuz.
- Norberaren gailuen bidez, erabilera orokorreko sareen edo gonbidatuentzat diren gailuen bidez.

Arautegi hau UPV/EHUko IKTen Segurtasun Batzordeak onartu du eta, horrela, ezarri dira UPV/EHUK erabiltzaileen eskura jartzen dituen informazio tratamendurako baliabideak behar bezala erabiltzeko jarraibide orokorrak, nork bere eginkizunak bete ditzan eta, hurrenez hurren, deskribatutako betebeharrak gain hartu eta hurrengo epigrafeetan xedatutakoa betetzeko konpromisoa bere egin dutelarik.

3. ARAUTEGIA

3.1 ARAU OROKORRAK

Internetarako sarbidea UPV/EHUn aktibo bat da, erabiltzaileen eskura jartzen duena, jarduera akademikoetan, irakaskuntzakoetan eta ikerkuntzakoetan zein administrazio eta kudeaketa prozesuetan laguntzeko. Baliabide hori arlo pertsonalerako erabil liteke noizean behin edo behin-behinean, norberaren edo besteen produktibitatea oztopatu gabe eta UPV/EHUn jarduerari trabarik jartzen ez zaion bitartean. Bitarteko horren bidez helarazitako informazio guztiak oro UPV/EHUrekin lotutako informazio gisa tratatuko dira eta bat etorri behar dute beherago zerrendatutako arauekin.

Interneten erabilerak dakartzan arriskuak ahalik eta txikienak izan daitezzen, gutxieneko segurtasun neurri batzuk hartu behar dira, internet behar bezala baliatzea helburu hartuta.

Honako hauek dira neurriok:

- Internet arduraz erabili behar da, helburu profesionaletarako edo irakaskuntzarekin, ikerkuntzarekin eta kudeaketarekin lotutako helburuetarako.
- Ezin sar daiteke UPV/EHUn etika kodea betetzen ez duten webguneetan, iraingarri edo legez kanpokoetan.
- Ez deskargatu Internetetik jabetza eskubidearen legeen bidez babestutako edozein material (softwarea barne), kasuan kasuko baimen edo zuzenbide lizentziarik gabe, zuzeneko estekak zein "peer-to-peer" (P2P) motako programak erabiliz.
- Ezin argitaratu leku pertsonaletan edo beste edozeinetan, UPV/EHUn edozein informazio edo beronen izenean, unean uneko informazioaren edo berori erabiltzeko eskubideen jabearen baimenik gabe.
- Debekatuta dago **baimenik gabe** sartzea edo ahalegintzea UPV/EHUn edo bereaz kanpoko ekipamendu, zerbitzu, aplikazio, datu edo azpiegituretan.
- Erabat debekatuta dago beste edozein erabiltzailearen informazioa aurrez pentsatuta suntsitu edo aldatzea, bai eta beste edozein erabiltzailearen pribatasuna eta intimitatea urratzea ere.

- **Bisitatutako orriaren egiazkotasuna ziurtatzea.** Informazio trukeak edo transakzioak egin behar direnean, garrantzitsua da ziurtatzea bisitatutako orria benetan dela dioena. Web orria ziurtagiri digitalaren bidez (HTTPS protokoloa) autentifikatuta dagoenean, benetakotasuna egiaztatuko du erabiltzaileak.
- **Saioak itxi konexioa amaitzean.** Oso komenigarria da saioak ixtea konexioa edo informazio trukea amaitzean; izan ere, sarri askotan lehenetsita egoten baita konexioa irekita mantentzea. Gainera, ez da izaten nahikoa nabigatzailea ixtea. Horren ondorioz, gerta liteke beste pertsona batzuek sarbidea izatea behar bezala itxi gabeko saioan erabilitako kontuetara eta informazioa. Webgune gehienek "deskonexio", "logout" edo antzeko aukera bat dute eta komeni da erabiltzea.
- **Kode kaltegarriaren aurkako erremintak erabiltzea.** Ugaria da oso Interneten barrena dabilen kode kaltegarria, hainbat alderdi desberdin dituen. Era honetako eraso horien aurkako lehenengo babesa da antibirus bat erabiltzea, behar bezala etengabe eguneratuta behar duena. Horrez gain, behar bezala konfiguratuta eduki behar dira firewall edo suebakia, programa espioien aurkako software espezifikoa (spyware) eta abar.
- Sistema eragilea, nabigatzailea eta segurtasun tresnak eguneratuta edukitzea. Ezinbestekoa da sistema eragilea eguneratuta edukitzea, bai eta Internetera sartzeko tresnak (nabigatzaileak) eta segurtasunekoak ere (biruskontrakoak, suebakiak, etab.), fabrikatzaileak igorritako azken segurtasun adabakiak baliatuta. Kode kaltegarria etengabe sortzen denez, oso garrantzitsua da birusen aurkako sinadurak ahalik eta maiztasun handienaz eguneratzea. Sistemek konfiguratuta egon behar dute eguneraketa hori automatikoki egiteko. Era berean, oso garrantzitsua da ERABILTZAILLEENTZAKO ZERBITZUARI eguneratze prozesu honetan hautematen den edozein arazoren berri ematea.
- **Nabigatzailearen segurtasun mailak erabiltzea.** Web nabigatzaileek badituzte segurtasun maila desberdinetan konfiguratze aukerak. Egokiena da segurtasun maila "ertain-altua" mantentzea, "ertainetik" beherako mailak erabiltzea komeni ez delarik. Horretarako, erabil daitezke nabigatzaileak eskainitako tresnak.
- **Informazio pribatua ezabatzea.** Web nabigatzaileek informazio pribatua biltegitratzen dute erabiltzen diren bitartean, hala nola nabigazio historia, onartutako cookieak, pasahitzak, etab.; informazio hori sistemari sar litekeen erasotzaileak eskura lezakeelarik. Beraz, komeni da informazio hori aldi-aldi ezabatzea, nabigatzaileak eskaintzen dituen tresnak erabiliz.
- **Orri edo webgune ez fidagarriak edo susmagarriak ez bisitatzea.** Segurtasun-intzidentek saihesteko, komeni da kode maltzurra izan dezaketen orriak ez bisitatzea.

- **Ez deskargatu kode edo programa ez fidagarririk.** Ziurtatu behar da programak deskargatzeko baliazten diren guneen fidagarritasuna, beti ere webgune ofizialak erabiliz.
- **Osagarri ezezagunak ez instalatzea.** Web orri batzuk kargatzen direnean, bertako edukira sartu ahal izateko, mezu bat agertu ohi da jakinarazteko erabiltzailearen ordenagailuan osagarri bat (plug-in, add-on, etab.) instalatu behar dela. Oso gomendagarria da lehenik eta behin aztertzea osagarri hori instalatzea komeni den eta, nolana ere, beti unean uneko osagarriaren banatzaile edo hornitzaile ofizialaren orritik egitea.
- UPV/EHUko Erabiltzaileentzako Zerbitzuari berehala jakinarazi beharko zaio Interneten erabileran gertatzen den ezohiko edozein gertaeraren berri.

3.3 SEGURTASUN NEURRIAK

Informazioa sarearen bidez transmititzea ez da beti segurua. Segurtasun mailak unean une erabiltzen ari den sistema informatikoa araberakoak izango dira, bai eta sistema eguneratuta dagoen eta biruskontrakoak bezalako segurtasun neurri gehigarriak erabiltzen diren ere. Gogoratu behar da informazioa galtzea erabiltzaileen erantzukizuna dela.

UPV/EHUK informazioa eskaintzen du informazioaren galtzea saihesti ahal izateko metodo ohikoenen, baimenik gabeko sarbideen eta abarren inguruan. Horren ondorioz:

- Erabat debekatuta dago pasahitzak eta posta-kontuak beste erabiltzaile batzuekin partekatzea.
- Pasahitz sendoak erabili behar dira, UPV/EHUren pasahitzak sortzeko eta erabiltzeko arautegian xedatutakoarekin bat etorrita.

UPV/EHUko azken erabiltzaileen eta unibertsitateak azaldutako zerbitzuaren babestearren eta Interneterako sarbidea behar bezala funtzionatzen dela eta arautegi hori betetzen dela bermatuko bada, UPV/EHUK eskura leudekeen eta hartu beharreko neurri teknikoak hartuko ditu komunikazioen osotasuna, erabilgarritasuna eta konfidentziasuna ziurtatzeko. Bestek beste, badira elementuak UPV/EHUren sarearen eta Interneten artean trafikoa etengabe kudeatu, kontrolatu eta monitorizatzeko, bai eta sareko suebakiak, sareko antibirusak, eraso banatua detektatzeko sistemak (DDoSSen aurkakoa), intrusioak prebenitzeko sistemak (IPS) eta beste ere.

UPV/EHUK, helburu bereko segurtasun sistemen bidez, erabili ahal izango ditu elementu horiek erregistratutako datuak, sareak, sistemek eta zerbitzuek behar bezala funtzionatzen dutela jarraitu eta kontrolatzeko, bai eta sarean dagoen informazioa babesteko ere.

Erregistro horiek Datu Pertsonalak Babesteko eta Eskubide Digitalak Bermatzeko abenduaren 5eko 3/2018 Lege Organikoaren 87. artikuluan ezarritako bermeen arabera erabiliko dira.

4. ERANTZUKIZUNAK

UPV/EHUko erabiltzaile guztiek erantzukizuna dute zein bere eginkizunen garapenari eragiten dioten arauak ezagutzeko, bai eta ez-betetzeak izan ditzakeen ondorioen berri izatekoa ere.

4.1 ERABILTZAILEEN ERANTZUKIZUNAK

- Interneterako sarbidea duten erabiltzaile guztiak oro dira Interneterako sarbidearen eta norberak egindako erabileraren arduraduna.
- Datu korporatiboen sarera konektatzen diren erabiltzaileek konpromisoa hartzen dute UPV/EHUK emandako ordenagailu korporatiboen konfigurazioa errespetatzeko, UPV/EHUko zerbitzu informatikoek instalatutako programak besterik erabiliko ez dutelarik.
- Unibertsitate komunitateko erabiltzaileek zerbitzua, sarea eta beste hornitzen dituzten erakundeek ezarritako irizpideetara egokitu beharko dute, kanpo baliabideak erabiltzerakoan. UPV/EHUko baliabideak erabiltzen direnean beste sare batzuetara sartzeko, uneoro bete beharko dira sare horietarako ezarritako arauak.

4.2 UPV/EHUREN ERANTZUKIZUNAK

- Internetera behar bezala sartzeko behar diren baliabide teknologikoak edukitzea eta mantentzea.
- Zaintzea erabiltzaileek Interneteko zerbitzuak arautegi instituzionalaren arabera eta indarrean dauden arauak errespetatuz erabil ditzaten.
- Internet gaizki erabiltzeagatik ezarri beharreko zehapenak ezartzea.
- UPV/EHUK onartutako etika kodean oinarrituta desegokitzat iriztitako guneetarako sarbidea mugatzea.

5. ARAUTEGIA EZ BETETZEA

Arautegi hau ez betetzeak, hala balegokio, egindako arau haustearen ondoriozko diziplina erantzukizuna lekarke, aplikatu beharreko arautegian aurreikusitako arau hausteen, zehapenen eta prozeduraren araubideari jarraiki. Aurrekoari kalterik egin gabe, unibertsitateak, xede horretarako izapidetutako prozeduraren ondoren, eskatuko du ez betetze horren ondorioz ondasunetan eta eskubideetan eragindako kalte-galerak ordain daitezen, administrazio publikoen zerbitzuko agintari eta langileen ondare erantzukizuna arautzen duten xedapenekin bat etorri.

6. BERRIKUSPENA ETA EBALUAZIOA

UPV/EHUko Segurtasun Batzordeari dagokio segurtasun arautegi hau kudeatzea eta eskumena du honako hauek egiteko:

- Arauak aplikatzerakoan sortutako zalantzak interpretatzea.
- Arautegia berrikustea, edukia eguneratzeko beharrezkoa denean edo berrikusteko ezarritako gehieneko epeak betetzean.
- Eraginkortasuna egiaztatzea.

Berrikusteko beharra gomendatuko luketen inguruabarrak egonez gero, segurtasun arautegi hau berrikusiko da eta, aldaketarik egonez gero, UPV/EHUko Segurtasun Batzordeak onartu beharko du.

Berrikuspena bideratuko da informazioaren segurtasunaren kudeaketa hobetzeko aukerak identifikatzera, bai eta lege esparruan, azpiegitura teknologikoan, antolaketa orokorrean eta abarretan izandako aldaketetara egokitzea ere.

Informazioaren Segurtasuneko arduraduna izango da onartutako dokumentu honen bertsioa zaindu eta zabaltzeko erantzukizuna.

7. ERREFERENTZIAK

- Barnekoak:
 - Informazioaren Segurtasun Politika, Gobernu Kontseiluak 2013ko martxoaren 21ean onartutakoa:
<https://www.euskadi.eus/web01-bopv/es/bopv2/datos/2013/05/1302239a.shtml>
 - <https://www.ehu.eus/es/web/gardentasun-ataria/etika-kodearen-proposamena>
- Kanpokoak:
 - Segurtasun Eskema Nazionala arautzen duen 311/2022 Errege Dekretua, maiatzaren 3koa.

| | |
|----------|-------------------|
| Bertsioa | Onartu da: |
| 1.0 | 2024ko azaroak 20 |