

Sarrera

Eibarko Udalak, Segurtasunerako Eskema Nazionala betetzeko duen konpromisoaren baitan, **Informazioaren Segurtasun Politika** bat definitu, dokumentatu eta zabaltzea du helburu, Alkatetzaren 2019ko otsailaren 15eko ebazpenez onartua.

Konpromiso hori informazioaren tratamenduari eta segurtasunari dagokienez erabiltzaile guztiek bete behar dituzten obligazioak jasotzen dituzten laster garatuko diren araudiekin eta prozedurekin osatzen da (edo osatuko da). Bien bitartean, erabiltzaileek dekalogo hau beteko dute Informatika eta Komunikazio Sistemen segurtasuna, errendimendua eta pribatutasuna bermatzeko.

Informazio hori eskuragarri dago hemen: www.eibar/eus/segurtasundokumentua.

1. Baliabideen erabiltzailea

- 1.1. Informatika eta Komunikazio Zerbitzuetako erabiltzaileek arduraz erabiliko dituzte bai ekipo informatikoak, bai azpiegitura osagarri guztia ere. Era berean, saihestuko dute instalazioaren osotasun fisikoari, nahita edo nahi barik, kalte egin diezaiokeen edozein ekintza egitea (triskantzak, lapurretak, baimendu gabeko lekualdatzeak, desmuntatzea, deskonfigurazioa, etab.).
- 1.2. Erabiltzaileek erretzu egingo diete beren ekipoetarako sarbidea laguntza teknikoko langileei, konponketa-, instalazio- eta mantentze-lanetarako.
- 1.3. Portaera susmagarri edo ustekabekoak detektatzeko eta haiei erantzuteko asmoz, jardueren erregistro-sistemak ezarri edo aktibatu behar dira, sistemen, aplikazioen eta erabiltzaileen jardueren EAEko Administrazioaren eta bere Erakunde Autonomoen informazio-aktiboetan sortutako datuak gordeko dituztenak.

2. Erabiltzaileen kontuak eta sarbide-kredentzialak erabiltzea

- 2.1. Erabiltzaileen kontuak pertsonalak dira. Ondorioz, **ezingo zaie beste pertsona batzuei sarbidea ahalbidetu**, betiere Eibarko Udaleko Segurtasun Arduradunaren edota Segurtasun Batzordearen berariazko baimena jasotzen ez bada.
- 2.2. Erabiltzaileak dira **kontu pertsonala erabiltzeko baimena duten bakarrak**, eta kontziente izan behar dira haien izenean egiten diren ekintzen erantzule direla, sarbidea duten zerbitzu elektronikoetan.
- 2.3. Erabiltzaileak **dira beren gako pribatuak, eta edozein elementurenak** (txartel edo gailu kriptografikoa, artxibo informatikoa, "software" programa, eta abar) **edota kodea** (PINa, pasahitza, etab.) **gordetzearen azken erantzuleak**.
- 2.4. Erabiltzaileak **kontuz eta arduraz** arituko dira ekipo, zerbitzu edota informazio elektronikoetara sarbidea izateko **kredentzialak, gako pribatuak eta elementu edota kodeak babesten eta zaintzen; isilpean gordeko dituzte**, eta Informatika sailari ahalik eta azkarren jakinarazi beharko diote, galduz gero edo segurtasuna arriskuan egonez gero.

3. Ekipo informatikoak erabiltzea

- 3.1. Inolaz ere, ezingo dira Eibarko Udalaren baliabide informatikoak antolaketa juridikoaren aurkakoak diren jardueretarako erabili, eta, bereziki, izaera pertsonaleko datu-babesaren arloko legeen aurka, jabetza intelektualeko legeen aurka eta, hala bada kasua, Eibarko Udaleko legeen aurka.
- 3.2. Ekipo informatikoak **ezingo dira erabili asmo partikularretarako**.
- 3.3. Erabiltzaileek adskribatuta dauden zerbitzuari dagozkion eginkizunen helburuetara eta beren lanari dagozkionekin bateragarriak diren erabileretara bideratuko dituzte baliabideak. Bestelako edozein xede duen erabilerarako Segurtasun Arduradunaren (Eibarko Udalaren idazkari orokorra) baimen berariazkoa beharko da.
- 3.4. **Ekipo informatiko eta periferikoak ezingo dira aldatu**, ezta Eibarko Udalarenak ez diren beste ekipo batzuekiko konexioa ere, baimena eskuratzen ez bada.
- 3.5. Ez da informaziorik erauziko ez euskarri digitaletan ez bitarteko elektronikoz, horretarako baimena eduki ezik, arreta handiz arituz baldin eta bereziki babestu beharreko informazioa bada, edo konfidentziala edo babestu beharrekoa bada.
- 3.6. Eibarko Udaleko sare-konexioen hartuneak ezin dira erabili Informatika sailak jakin eta baimendu barik (informatika@eibar.eus). Ezin dira konektatu gailu errepikatzaile ezta kontzentratzailek ere, kabledunak edo inalanbrikoak, Informatika sailaren teknikariek ez badute berariazko baimenik eman, eta betiere haien gainbegiratzearekin egingo da lan.
- 3.7. USB euskarriak edo euskarri magnetikoak erabiltzea: Halako gailuak, erabiltzen dituen erabiltzailearen zaintzapean egongo dira eta pertsona horrek beharrezkoak diren neurriak hartuko ditu kalteak edo lapurretak saihesteko, bai eta baimenik gabeko hirugarrenek sarbiderik ez izateko ere.

4. Birus informatikoak eta beste "malware" mota batzuk

- 4.1. Erakundearen lan-ekipo guztiek (mahai gaineko ordenagailua, eramangarria, etab.) "software" kaltegarria (birusak, harrak, eta abar) kontrolatzeko mekanismoak izan behar dituzte, eta aktibatuta egon behar dute.
- 4.2. Birusek, harrek, eta abarrek eragindako infekzio baten susmoa badago, berehala eman beharko zaio horren berri Informatika sailari.

5. "Software-a"

- 5.1. Zerbitzu elektronikoen funtzionamendu egokia bermatzeko, **debekatu egiten da lan-ekipoetan erakundearenak ez diren "software" edo programak instalatzea**. Instalatu beharko balira, Segurtasun Arduradunari eskatuko zaio azter ditzala. Halaber, ezingo da egin lan-ekipoetan instalatutako "software"-aren kopiarik.
- 5.2. Debekatu egiten da lizentziarik gabeko aplikazio informatikoak instalatzea eta erabiltzea.
- 5.3. Debekatu egiten da egile- eta kopia-eskubideak hautsiz dokumentuak, liburuak, irudiak, filmak edo musika deskargatzea edo banatzea.
- 5.4. Erabiltzaileek **ezingo dute erakundearen instalatutako "software"-a aldatu**, eta inolaz ere ezingo da desaktibatu.

6. Internet eta posta elektronikoa

- 6.1. **Interneterako sarbidea erabiltzeak lanari lotutako helburuei erantzun behar die.**
- 6.2. Segurtasun-neurriengatik, beharrezkoak diren iragazki mugatzaileak ezarri ahal izango dira Interneterako sarbideen segurtasuna eta erabilera ona bermatzeko.
- 6.3. Eibarko Udaleko posta elektronikoa zerbitzua **erabilera profesionalerako posta-kontua** jaso duten erabiltzaile guztiek erabiliko dute, eta arretaz jokatzeko betebeharra dute zerbitzua erabiltzean.
- 6.4. Eskatu gabeko mezu elektronikoa masiboa saihesteko, "spam" izenez ere deitua, oro har, posta elektronikoa helbidea pertsona edota entitate ezagunetara baino ez zaie eman behar. Ez da posta elektronikoa helbidea sartu behar instituzionalak ez diren foro edo web-orrietan. Mezu elektronikoa ezezagun edo eskatu gabekoak jasotzen direnean, ez zaie erantzun behar; izan ere, erantzunez gero, helbidea berretsi egiten baita.
- 6.5. Jasoz gero igorle edota eduki zalantzazkoa duten mezu elektronikoa, berehala jarri beharko da harremanetan Informatika sailarekin, mezuok aztertzeko.

7. Izaera pertsonaleko datuen tratamendua eta erabilera

- 7.1. Erabiltzaileek bakar-bakarrik izango dute sarbidea beren jarduerarako beharrezkoak diren eta soilik baimenduta dauden eginkizunetan aritzeko informazioan.
- 7.2. Informazio horren sarbidean, erabiltzaileak behartuta daude Eibarko Udalak datuen babeserako araudian ezarritako segurtasun-neurriak betetzera (www.eibar.eus/RGPD).
- 7.3. Izaera pertsonaleko datuen tratamenduaren edozein fasetan parte hartzen duten pertsona guztiak **behartuta daude haiekiko sekretu profesionala gordetzera.**
- 7.4. Euskarri informatiko batek (disco gogorra, USB, CD...) edo dokumentu batek, formatu elektronikoa edo paperean, datu pertsonalak gordetzen baditu, botatzen direnean beharrezkoak diren neurriak hartuko dira bertan bildutako edo inprimatutako informazioa berreskuratzea eragozteko.
- 7.5. Eibarko Udaletik izaera pertsonaleko datuak atera behar dituzten erabiltzaileek **Segurtasun arduradunaren baimena eskatu beharko dute,** eta bidezkoak diren segurtasun-neurriak hartu informazio hori babesteko. Halaber, Segurtasun arduradunak erregistro eguneratu bat eraman beharko du informazio horren irteerari buruz.
- 7.6. Izaera pertsonaleko datuen segurtasunari eragin diezaiokeen edozein gorabehera edo arazo Eibarko Udaleko DBLOren Segurtasun arduradunari jakinarazi beharko zaio (Antolaketa eta Langileria zuzendaria).

8. Informazioaren segurtasun-gorabeherak

- 8.1. Informazioaren segurtasunari eragiten dion gorabeheraren bat gertatzen denean, erabiltzaileek Segurtasun arduradunari jakinarazi beharko diote zer gertatu den eta zer neurri hartu diren, hark bidezkoak diren neurriak har ditzan.

9. Mahaiak garbi eta ordenagailua blokeatuta

- 9.1. Erabiltzaileek bere lanlekutik aldendu edo ordenagailua aldi batez lagatzen dutenean, **beren ekipoak duen blokeo-sistema aktibatuko dute** (pasahitzaz babestutako pantaila-babeslea, terminalaren blokeoa, eta abar), ez daitezten pantailan datuak bisualizatu, eta baimenik ez duten hirugarrenek ekipora edo aplikazioetara sarbiderik izan ez dezaten.
- 9.2. Era berean, Izaera pertsonaleko datuak dituzten paperezko dokumentu guztiak, erabiltzen ari diren bitartean, haien ardura duenak babestu beharko ditu, une oro, baimenik ez duten pertsonak sartzea saihestuz.

10. Jardueraren monitorizazioa

- 10.1. Eibarko Udalak zerbitzuaren lege-, segurtasun- eta kalitate-arrazoiak direla-eta, eta une oro horretarako indarreko legediak ezartzen dituen baldintzak betez, honako hauek egin ahalko ditu:
 - Berrikusi ekipoen egoera, instalatutako software-a, gailuak eta bere ardurapeko komunikazio-sareak.
 - Monitorizatu bere sistemetan jasotako informaziorako sarbideak.
 - Ikuskatu kredentzialen eta aplikazioen segurtasuna.
 - Monitorizatu internet zerbitzuak, posta elektronikoa eta beste lankidetzatresna batzuk.
- 10.2. Eibarko Udalak monitorizazio-jarduera hori arriskuaren maila proportzionalean egingo du, bidezkoak diren legezko kautelekin eta jurisprudentzian adierazitakoekin, eta erabiltzaileen eskubideak betez.