



6.2 Gailu digitalen babesa

Gaur egun, teknologia gure eguneroko bizitzaren parte da, eta **gailu digitalak**, hala nola ordenagailuak, telefono mugikorak eta tabletak, ezinbesteko tresna bihurtu dira. Hala ere, gailu horiek erabiltzeak **segurtasun-arriskuak** dakartza, hala nola birusak, hackeoa eta datu-lapurreta. Horregatik, beharrezkoa da neurri egokiak hartzea gure gailuak seguru mantentzeko eta informazio pertsonala babesteko.

Enpresetan **gailu digitalen segurtasuna** bermatzeko **neurriak eta praktika onak** funtsezkoak dira informazioaren babesa eta enpresaren ospea zaintzeko. Horretarako, **kontrol edo neurriu bai teknologiko bai antolakuntzakoak** ezartzea beharrezkoa da.

Nola Babestu Gailu Digitalak?

Gailu digitalen babesa hainbat praktika seguruetan oinarritzen da. Lehenik eta behin, garrantzitsua da **pasahitz sendoak** erabiltzea. Pasahitz batek gutxienez 12 karaktere izan behar ditu, eta zenbakiak, maiuskulak, minuskulak eta ikurrak konbinatu behar ditu. Gainera, ez da komeni pasahitz bera hainbat kontutan erabiltzea; horretarako, pasahitz-kudeatzaile bat erabil daiteke.

Bigarrenik, **softwarea eguneratuta** mantentzea funtsezkoa da. Sistema eragileek eta aplikazioek segurtasun-eguneratzeak jasotzen dituzte, malwarearen eta zibererasoen aurka babesteko. Horregatik, komenigarria da eguneratzeak automatikoki deskargatzeko aukera aktibatuta izatea.

Hirugarrenik, **lotura susmagarriak** saihestea eta deskargatutako fitxategiekin kontuz ibiltzea ezinbestekoa da. Erabiltzaileek ez dituzte ezezagunen mezu elektronikoetan datozen estekak ireki behar, eta ez dute software susmagarria instalatu behar. Horrez gain, antibirus eta antimalware programak erabiltzea gomendatzen da, ClamAV bezalako tresnak erabiliz.

Gailu digitalen babes fisikoa?

Garrantzia hartzen du antolakuntzako kontroletan **gailu digitalen babes fisikoak**. Hori dela eta, gailuak kokapen seguruetan mantendu behar dira, eta sarbide kontrolak ezarri behar dira baimenik gabeko pertsonak gailuetara iritsi ez daitezen. Horretarako, honako neurriak hartu behar dira:

- **Sarbide kontrolak:** Gailuak sarbide mugatuak dituzten lekuetan kokatu behar dira, hala nola, bulegoetan edo segurtasun guneetan.
- **Segurtasun neurriak:** Gailuak fisikoki babesteko, sarrailak, segurtasun kamerak eta alarmak erabil daitezke.



Gailuen Babesa Hezkuntzan, Lanean eta Eguneroko Bizitzan

Segurtasun digitalaren garrantzia ez da esparru pertsonalera mugatzen; **hezkuntza-** eta **lan-arloetan** ere funtsezkoa da.

Hezkuntza-arloan, ikasleek eta irakasleek kontuan hartu behar dute segurtasuna ikaskuntza plataforma digitalak erabiltzean. Esate baterako, fitxategiak deskargatu aurretik birusik ez dutela ziurtatu behar dute eta dokumentuak partekatzeko baimen egokiak konfiguratzea komeni da. Horrez gain, sare seguruetan konektatzea eta informazio pertsonala modu arduratsuan kudeatzea ezinbestekoa da.

Lan-arloan, enpresek politika argiak definitu behar dituzte gailu digitalen erabilerari dagokionez. Langileek pasahitz sendoak sortu eta aldian-aldian aldatu behar dituzte, baita azken saioen hasierak kontrolatu ere. Enpresek, gainera, Eraldaketa Digitalaren Plana (EDP) ezarri beharko lukete, langileak segurtasun digitalean trebatuz eta babes-neurri eraginkorrak ezarriz.

Herritar gisa ere, segurtasun digitalaren kontzientzia hartzea beharrezkoa da. Adibidez, Wi-Fi sare publikoak erabiltzean arriskuak saihestu behar dira. Wi-Fi publikoetara konektatzean, erabiltzaileek beren datuak interzeptatuak izateko arriskua dute, eta hackerrek informazio pertsonala lapurtu dezakete. Hori saihesteko, VPN bat erabiltzea edo banku-transakzioak sare mugikorraren bidez ez egitea gomendatzen da.

Enpresetako Gailu Digitalen Erabilera Politika

Bestalde, ezinbestekoa da segurtasun-politika eta prozedura argiak garatzea eta ezartzea. Langileei informazioaren segurtasunari buruzko prestakuntza eta sentsibilizazio-programak eskaintzea garrantzitsua da, arriskuak murrizteko eta jokabide seguruak sustatzeko, honen bidez segurtasun ohiturak barneratu eta praktikan jar ditzaten; **erabiltzaileen kontzientzia digitala landu behar da**. Gainera, segurtasun-auditoriak eta ikuskaritzak aldian behin egitea eta gertakarien aurrean erantzuteko eta kudeatzeko planak garatzea komeni da.

Enpresetan, langileen eta bezeroen datuak babesteko, beharrezkoa da egurtasun-protokolo argiak ezartzea. Enpresa batek gailu digitalen erabilerarako honako neurriak har ditzake:

- Pasahitz sendoen erabilera eta bi faktoreko autentifikazioa aktibatzea.
- Sistema eragileak eta aplikazioak beti eguneratuta mantentzea.
- Antibirus eta antispam programak instalatzea.
- Wi-Fi sare pribatuak erabiltzea eta sare publikoetara ez konektatzea.
- Langileei alfabetatze teknologikoko saioak eskaintzea, segurtasun digitalean trebatzeko.



Ondorioa

Gailu digitalen babesa ezinbestekoa da informazio pertsonala eta profesionala seguru mantentzeko. Pasahitz sendoak erabiltzea, softwarea eguneratzea, Wi-Fi sare publikoak saihestea eta antibirusak aktibatuta edukitzea neurri eraginkorrak dira arriskuak gutxitzeko.

Enpresek Eraldaketa Digitalaren Plana ezarri beharko lukete, langileei segurtasun digitalean trebatuz eta politika egokiak garatuz. Hezkuntza- eta lan-arloetan, segurtasun digitalean jantzitako erabiltzaileek mehatxuak detektatu eta saihesteko gaitasuna izango dute. Azken finean, zibersegurtasuna guztion ardura da, eta neurri egokiak hartuz, gailuak eta datuak seguru mantendu daitezke.

(azken eguneratzea: 2025/05/20)

Eusko Jaurlaritzaren Lanbide Heziketako Sailburuordetza. Lan honek Creative Commons Aitortu-EzKomertziala-PartekatuBerdin 4.0 Nazioarteko Baimena dauka (CC BY-NC-SA 4.0).

