ZIBERERASOEN AURREAN EUSKAL ENPRESEN BABES ETA ERRESILIENTZIA MAILA HANDITZEN LAGUNTZEN DUTEN GOMENDIO OROKORRAK

1. Gailuen konfigurazio segurua

Gailuak eta aplikazioak modu seguruan **konfiguratzeko politika** ezarri, kontuan hartuz konfigurazio lehenetsiak ez direla beti egokienak zibersegurtasunaren ikuspegitik.

2. Aplikazioen kontrol eta konfigurazio segurua

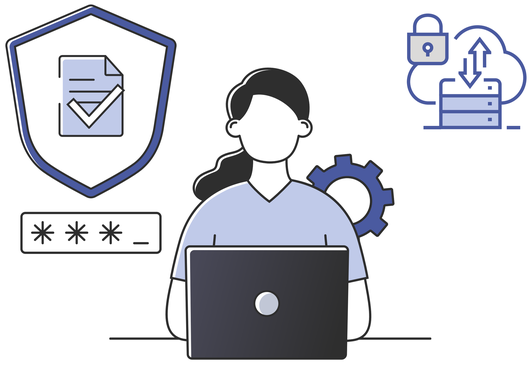
Aplikazio kopurua mugatu, ohiko lan eragiketarako direnak bakarrik instalatuz eta erabiliz. Halaber, gomendatzen da erabiltzaileen baimenak ahalik eta pribilegio gutxienari buruzko legea aplikatuz mugatzea, eguneroko lanean aritzeko behar diren lanak bakarrik egin ahal izan ditzaten. Erabiltzaileek administratzaile rolik ez izatea gomendatzen da.

3. Programa maltzurretatik babestea

ransomware babesa duen **birusen kontrako soluzio bat erabili eta eguneratuta mantendu**. Era berean, oso gomendagarria da EDR soluzioa gehitzea eta aldian behin eskaneatzea. Halaber, erabiltzen ez diren **gailuak itzaltzea** gomendatzen da, sistemaren konpromisoaren kasuan eraginik izan ez dezaten.

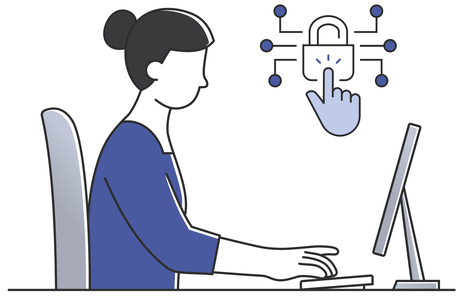
4. Konexioen babesa

Urruneko sarbidea behar izanez gero, gaitu **VPN** baten bitartez eta kontrol bat eramanez eta baimendutako sarbide guztien inbentario zehatza eginez. Halaber, **perimetroa mugatzea** eta ohikoak ez diren lekuetatik datozen sarbideak blokeatzea, adibidez, gure azpiegiturara konexiorik egin behar ez luketen herrialdeetatik. Era berean, **irteerako konexioak** maltzurtzat katalogatutako ospe handiko guneetara **mugatzea**.



5. Segurtasun kopiak

Segurtasun **kopien politika** ezarri eta mantendu, 3, 2, 1 ildoa kontuan hartuta: hiru segurtasun kopia bi euskarritan, eta horietako bat saretik kanpo gorde. Kopiak **maiztasun jakin batekin egin**, beharrezkoa izanez gero, jarduera ahalik eta epe laburrenean berreskuratzeko. Era berean, kopia horien **funtzionamendua eta kontserbazio-prozesua baliozkotzea** gomendatzen da.



6. Segurtasun eguneratzeak

Eguneratze politika ezarri, ahalik eta denbora laburrenean aplikatu ahal izateko, ahultasunak modu horretan ustiatzea ekidinez. Kopia horien funtzionamendua eta lehengoratze prozesua baliozkotzea gomendatzen da. Bereziki azpimarratzea adabakiak aplikatzeari lehentasuna ematea agerian dauden inguruneetan, eta, bereziki, ahulezia handien eta kritikoen kasuan.

7. Sarbideen kontrola

Hainbat faktoreren bidezko autentifikazioa aktibatzea, ahal den guztietan, batez ere kanpoko sarbide, pribilegioak dituzten kontuetarako sarbide eta abar eskatzen dituzten kasuetan. Era berean, **pasahitzak aldatzeko politika bat ezartzea**, aldaketa periodikoa jasoko duena, eta 6 hilabeteko epean aldatu ez badira, berriketa behartuz. Hori bereziki garrantzitsua da administrazio-rola duten erabiltzaileen kasuan.

8. Kontzientziazioa

Langileei gogorarazi **kontu handiz jokatu** behar dutela mezu elektronikoak eta eranskinak erabiltzean.

9. Alerta goiztiarra

Jarduera maltzurra identifikatuz gero, gainerako organismoetatik **isolatu eta ezarritako kanalen bidez jakinarazi** berehala segurtasun sistemen arduradunari, eragina arintzeko neurri egokiak har ditzan.

MALWARE EDO PHISING KANPAINA AKTIBO BAT IDENTIFIKATUZ GERO, JAKINARAZI AHAL DIGUZU HEMEN:

900 104 891
telefono zenbakira deituz

incidencias@bcsc.eus
helbidera mezu bat bidaliz