# EUSKAL ENPRESEN BABES ETA ERRESILIENTZIA MAILA HANDITZEKO NEURRI TEKNIKOAK

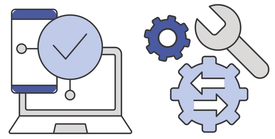
## NABIGAZIOA

- Langileei jakinarazi garrantzitsua dela **modu seguruan** nabigatzea, lan-eremuan behar diren lekuetara bakarrik sartuz.
- **Kontu handiz sartu** posta elektronikotik iristen diren leku ezezagunetara edo esteketara.
- Erabiliz gero, **egiaztatu proxya** behar bezala konfiguratuta dagoela leku maltzurretarako sarbidea blokeatzeko.
- **Suebakiak konfiguratu**, ospe zerrendetan maltzur gisa katalogatutako web orriak blokea ditzaten.

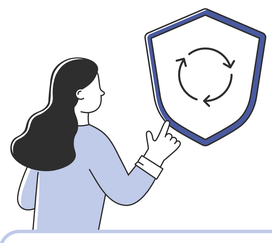
## POSTA

- SPF, DKIM, DMARC eta DNSSEC erregistroen **konfigurazio egokia** ezarri eta berrikusi.
- Posta elektronikoaren konfigurazioa berrikusi, eta **babes-iragazkiak** (malwareak, phishinga eta abar detektatzea) ondo daudela egiaztatu, eraginkortasunez konfiguratuta egotea baieztatuz.
- Balioetsi kaltegarriak izan daitezkeen **fitxategi-mota batzuk blokeatzea**; adibidez, makroak txertatzeko aukera ematen dutenak edo gutxienez, makroen exekuzioa blokeatu, ahal bada. Era berean, komando lineako tresnen exekuzioa mugatzea, hala nola powershell edo wmic.

## GAILUEN KONFIGURAZIO SEGURUA



- Zibersegurtasuneko **jardunbide egokiak** kontuan hartu sistemak zabaltzeko orduan.
- **Ahultasunak kudeatzeko prozesu** bat ezarri eta jarraitu.



## SEGURTASUN-EGUNERATZEAK

- **Sistemak eguneratuta izan**, ahultasun ezagunen ustiatzea saihesteko.
- Eguneratzeen osotasuna egiaztatu, **iturri fidagarrietatik** lortzen direla egiaztatuz.
- Erakunde batean softwarea eguneratzean edo adabakiak egitean, **mailaka egin**, akats edo eguneratze maltzurren eragina ahalik eta txikiena izan dadin.

## MONITORIZAZIOA

- **Aktibatu segurtasun-ekitaldien/logen bilketa** (sistema, komando-lineako tresnak barne), endpointa, firewalls, proxy, etab.) eta berrikusi jarduera anomaloaren bila.
- **Segurtasun-gertaerak** (sistema, endpoint, suebakiak, proxya eta abar) **ikuskatu eta berrikusi** ohikoak ez diren jardueraren bila.
- **Sistemaren gertaerak monitorizatu** kontu pribilegiatuei lotutako jarduera susmagarria identifikatzeko, hala nola, huts egindako kautotze-saioak, biltegiratze partekatuko unitateetara sartzeko saioak edo ohiz kanpoko sistemetan saio-hasierak.
- Ziurtatu sareko gailuek **konfigurazio-aldaketa guztiak** erregistratzen eta ikuskatzen dituztela. Sareko gailuen eta arau-multzoen konfigurazioak etengabe berrikusi, komunikazio-fluxuak baimendutako arauen azpimultzora mugatuta daudela ziurtatzeko.

## KONEXIOEN BABESA

- **Sarearen segmentazio egokia** erabili.
- Ziurtatu sistemen arteko konexioak egin daitezkeela **gutxieneko pribilegioaren printzipioa** kontuan hartuta.

- Egiaztatu definitutako konexioak **dokumentatuta eta baimenduta** daudela.
- Berariazko **sareak edo VLAN** sareak erabili sistema kritikoenen kudeaketa-interfazeetan sartzeko; esaterako, sare- eta biltegiratze-sistemetan.
- Azpiegitura-sistemen artean "alde batetik bestera mugitzeko" erabil daitezkeen **sistemen komunikazioa monitorizatu** eta sistema horiek behar bezala indartuta daudela egiaztatu.
- **TOR trafikoa blokeatzea** baloratzea.

## SARRERA-KONTROLA

- Ahal den guztietan, **bigarren autentifikazio-faktore bat** erabili.
- Ziurtatu domeinu-erabiltzaileak enpresako langileen **azpimultzo espezifiko bati esleituta** daudela. Ahal bada, "Denak", "Domeinuaren erabiltzaileak" edo "Erabiltzaile kautotuak" taldeek ez dute sistema kritikoetan zuzenean sartzeko edo autentifikatzeko gaitasunik izan behar.
- Erabiltzaileei esleitutako baimenek **gutxieneko pribilegioaren** kontzeptuaren arabera dokumentatuta eta konfiguratuta egon behar dute.
- Erabiltzaileek egiten dituzten ekintzak **monitorizatzeko gaitasuna** izatea.
- Aldian-aldian **baimenen esleipena** berrikusi, beharrezkoak ez direnak murriztuz.

## NEGOZIOAREN JARRAIPENA

- **Krisi-batzorde bat** ezartzea, pertsonak, rolak eta harremanetarako informazioa identifikatuz, gertakaririk gertatuz gero jakinarazi daitezen.
- Gorabeherei **erantzuteko planak** egitea.
- Hondamendien aurrean **leheneratze-planak** egitea.
- Negozioaren **jarraipeneko planak** egitea.
- **Simulazio-ariketak** egitea plan horiek baliozkotzeko.
- **Hornitzaile kritikoak identifikatzea** eta zibersegurtasun-intzidenteren bat izanez gero gutxieneko epeetan jakinarazteko betebeharra ezartzen duten **klausulak finkatzea**.

## ALERTA GOIZTIARRA

- Zibersegurtasun-hornitzaileen edo zibersegurtasun-erakunde publikoen **oharrak eta alertak** bezalako argitalpenak jarraitu malware-kanpainien edo ahultasunen inguruan informatuta mantentzeko.

Zibersegurtasuneko zerbitzu espezializatuak behar izanez gero, zibersegurtasun-katalogoa kontsulta dezakezu hemen: **https://www.basquecybersecurity.eus/eu/enpresak-bilatu/index.html**

Malware- edo phising-kanpaina aktibo bat identifikatuz gero, **incidencias@bcsc.eus** helbidean jakinarazi, kanpaina arintzeko eta, hartara, ez zabaltzeko.