

SEGURTASUNA

KANPOKO LANGILEENTZAKO INFORMAZIO SISTEMEN ERABILERA ARAUA

Dokumentuaren sailkapena: Publikoa



2025eko maiatza



Arabako Kalkulu Gunea, A.B.
Centro de Cálculo de Álava, S.A.

Dokumentu hau indarrean egongo da formalki berrikusi edo eguneratu arte. Berrikuspen bat egingo da arau, teknologia eta antolamendu aldaketetara egokitzen dela ziurtatzeko. Gainera, testuinguruan, legerian edo barne prozesuetan egiten den edozein aldaketa garrantzitsu, berehala berrikusi beharko da.

Aurkibidea

Ingurunea	4
Arauaren xedea	4
Arauaren irismena	4
Arauaren garapena	4
Monitorizazioa	12
Baliabideen erabilera okerraren ondorioak	13

Ingurunea

Arabako Kalkulugunea SAK (AKSA aurrerantzean) hirugarren erakundeekin sortzen dituen harremanetan, AKSAREN edo haren erakunde bezeroen informazioa eskuratzea eta beraien informazio sistemetan sartzea beharrezkoa izaten da. Horrenbestez, informazio hori eta hura tratatzen duten sistemak babesteko neurriak ezarri behar dira, segurtasunekoak, antolaketakoak eta teknikoak. Honelako informazioa eskuratuz gero, kanpoko langileek zenbait erantzukizun hartzen dituzte, eta errespetatu egin behar dituzte. Hauek dira:

- beste erabiltzaile batzuen eskubideak (AKSAkoak eta hirugarren entitateetakoak).
- informazio sistemen eta baliabide fisikoen (propioak nahiz hirugarren entitateenak)
- osotasuna.
- baliabideen (AKSAREN eta hirugarren entitateenak) eskuragarritasuna.
- indarrean dagoen legeria.

Ohar argigarria: Arauan zehar AKSAREN elementuen "jabetza" aipatzen da. Ulertu behar da jabetzaren kontzeptua bakarrik dagokiola AFAK AKSAREN barne erabilerarako edo AKSAREN bezeroak kudeatzeko egindako erabilera emakidari.

Era berean, "kanpoko langiletzat" hartzen dira AKSARI zerbitzuak ematen dizkioten enpresa hornitzaileetako langileak, praktiketako langileak, zaintza zerbitzuetako langileak eta abar, AKSAK gaitutako informazio sistemarako sarbidea dutenak, informazio sistemak AKSAK kudeatutako azpiegiturretan dauden ala ez kontuan hartu gabe.

Arauren xedea

AKSAREN eginkizuna kanpoko langileek betetzea errazten duten informazio sistemak behar bezala erabiltzen direla bermatzea da agiri honen helburua.

Arauren irismena

Agenteak

Arau hori hau kanpoko langile guztiak bete behar dute, hurrengo apartatuan aipatzen diren baliabideak erabiltzen dituzten unetik aurrera.

AKSAREN bezero diren eta AKSAREKIN aktibo informatikoak edo komunikazioetakoak partekatzen dituzten beste erakunde batzuetako langileek beren erakundeko politikak, arauak, eskuliburuak eta abarrekoak bete behar dituzte.

Baliabideak

AKSAK (beretzat nahiz bere bezero diren erakundeentzat) ostatatzen, kudeatzen, edukitzen edo administratzen dituen informazio sistema, azpiegitura eta informazio guztiei aplikatu behar zaizkie dokumentu honetan ezarritako arauak.

Arauren garapena

Orain AKSAREN informazio sistemen erabilera ona, eskuragarritasuna eta zerbitzu maila arautzen dituzten arauak definituko ditugu. Arauok behin eta berriro, nahita edo zabarkeriaz urratzen dituzten edo kasu egiten ez dieten kanpoko langileekin AKSAK egoki irizten dien jarduketak teknikoak (kalteen eragina gutxitzeko) edo kontratu izaerako jarduketak egin ahalko ditu.

AKSAren jarduketek, dokumentu honetan aipatutako puntuai dagokienez, indarrean dagoen legeriatik eratorritako betebeharrak guztiak zehatz-mehatz beteko dituzte, eta uneoro langile erabiltzaileen eskubideak errespetatuko dituzte.

AKSAk dauzkan informazio sistemak helburu profesionalekin bakarrik erabili behar dira; ezin dira helburu pertsonalekin erabili.

Bestalde, **AKSAk debekatu egiten du** kanpoko langileei eskaintzen dizkien baliabide partekatuetan **informazio pertsonala gordetzea**. Gainera, AKSAk debekatzen du lanpostuetan (PCetan, ordenagailu eramangarrietan eta abarretan) informazio pertsonalik ez gordetzea, beste pertsona batzuek erabili ahal dituztelako. Kanpoko langileek jakin behar dute ezin diotela AKSAri erreklamatu ekipoetan gordetako informazio pertsonala eta ezin diotela erantzukizunik eskatu beste pertsona batzuek informazio hori eskuratuz gero.

Kanpoko langileek honako hauek errespetatu behar dituzte: jasaten dituzten baliabideen osotasuna, beste erabiltzaile batzuen eskubideak, indarrean dauden legeak eta erregulazioak, bai eta AKSA indarrean dauden araudi, politika, prozedura eta abar guztiak ere.

AKSAk kanpoko langile guztiei eskaintzen die Segurtasun arduradunaren laguntza informazioaren segurtasunaren inguruko zalantzak edo iradokizunak jakitera emateko. Era berean, arau honetan aipatutako arauak, politikak, prozedurak, gidaliburuak eta abarrek ez egutzen ez dituzten enpresa hornitzaileek AKSAko Segurtasun arduradunarekin harremanetan jarri behar dute beraien kopia eskuratzeko .

Informazioaren konfidentzialtasuna

AKSAk eta zerbitzuak hornitzen dizkion enpresak sinatutako kontratuak informazioaren konfidentzialtasunari buruzko klausulak ezartzen ditu. Kanpoko langileek klausula horiek ezagutu behar dituzte, eta enpresa hornitzailearen eginkizuna klausula horien berri ematea da.

Kontratu bakoitzaren klausula berezietan gain, AKSAk bere bezero diren erakunde guztiekin daukan konfidentzialtasun konpromisoa bete behar dute kanpoko langile guztiek:

I. AKSA indarrean egiten duten langileek, beren funtzioak betetzean, AKSAren eta haren bezeroen datu pertsonalak eta negozio informazioa eskuratzeko baimena daukate.

II. Aurreko apartatuan aipatutako informazioa konfidentziala da, besterik adierazi ezean. Informazio ez-konfidentzialtzat hartuko da soilik AKSAk hedabide publikoen bidez komunikatu duena.

III. Langileok sekretu profesionala gorde beharra daukate aurreko puntuari dagokionez. Gainera, informazio hori gorde behar dute eta, bereziki, datu pertsonalak tratatzeari buruzko betebeharrak bete behar dituzte, baita indarrean dauden gainerako araudiak (lege izaerakoak nahiz barnekoak) bete ere.

IV. Betebeharrak horiek ere AKSArekin harremana amaitutakoan ere bete behar dituzte.

V. Langile horiek erantzukizuna daukate AKSAren aurrean, lanpostuari dagozkion konfidentzialtasun betebeharrak eta datu pertsonalak babesteko betebeharrak erruduntasunez ez betetzearen ondorioz sor litezkeen gaitz eta kalteak ordaintzeko”.

Konfidentzialtasun konpromiso horrek esan nahi du, besteak beste, kanpoko langileek:

- Saihestuko dute informazioa ezagutaraztea, aldatzea, suntsitzea edo gaizki erabiltzea, euskarria edozein dela ere, eta informazioaren osotasunari eutsiko diote une oro.
- Informazio konfidentziala duten paperezko txostenak minimizatuko dituzte, eta, paperean ateratzea beharrezkoa denean, leku seguruan gordeko dira.
- Eskuratu behar ez den informazioa eskuratuz gero, ahalik eta lasterren jakinarazi beharko zaio AKSAko Segurtasun arduradunari.

AKSAk agindutako eginkizunen ondorioz eskuratzen duten informazioa babesteko betebeharra dute kanpoko langileek.

- AKSArekiko kontratu harremana amaitutakoan, kanpoko langileek konpromisoa hartzen dute kontratu harremanak iraun duen bitartean ikasitako informazioa edo jakintza beren mesedetan edo inoren mesedetan ez erabiltzeko. Gainera, AKSAren informazioa edo haren bezero diren erakundeen informazioa itzuli edo suntsitu behar da (suntsiketaren frogak erakutsiz, bidezkoa bada), AKSAk une bakoitzean emandako irizpideak betez.

Pasahitzen politika eta sarbide kontrola

AKSAren informazio sistemetara sartu behar duten kanpoko langileek beren pertsonari esleitutako identifikatzaile bat izango dute, pasahitzak, PINak eta abar isilpean gordeta, eta beren identifikatzailearekin egiten diren ekintzen erantzule izango dira. Horregatik, inork ezin du inola ere bere nortasuna ezkutatu edo manipulatu.

Sarerako edo baliabide korporatiboetarako konexioak gaitzeko, AKSAk informazio hau eskatu ahal izango du:

- Izen-abizenak
- NANA
- Kanpoko e-maila
- Telefono mugikorraren zenbakia
- Eskatutako identifikatzailearekin lotutako proiektuaren/zerbitzuaren ardura duen AKSAko pertsona
- Zerbitzua ematen duen kontratuaren/zerbitzuaren amaiera data
- VPNri lotutako informazioa

AKSAren informazio sistemek beraietan sartzen diren erabiltzaileak identifikatzeko mekanismoak dituzte, baita baliabideak eskuratzeko baimena duten kontrolatzeko eta eskuraketa hori nola egin dezaketen (irakurketa, aldaketa eta abar) kontrolatzeko mekanismoak ere. Horregatik, erabiltzaileek beraiei esleitutako identifikazioak bakarrik erabil ditzakete, eta pasahitzak, PINak eta abarrekoak isilpean gorde behar dituzte. Beren identifikazioarekin egiten diren ekintzen erantzule izango dira.

Gainera, erabilitako pasahitzei dagokienez, kanpoko langileek hau egin behar dute:

- Kalitatezko pasahitzak ezarri (gutxienez 8 eta gehienez 10, ahal denean, zenbakizko karaktereak / bereziak / alfanumerikoak).
- Pasahitza aldatu, beste pertsona batek ezagutzen duela susmatuz gero.
- Ez berrerabili pasahitz zaharrak.
- Pasahitz lehenetsiak edo hasieran esleitutakoak aldatu.
- Saio hasierako prozesu automatizatuetan pasahitzik ez sartu.
- Pasahitzekin lotutako edozein gorabehera jakinarazi.

Era berean, debekatuta dago berariazko baimenik gabe beste eskubide edo sarbide batzuk lortzen saiatzea, AKSAk definitutakoez bestelakoak badira. Halaber, ez dago baimenduta jarduera arrastoen erregistroak (logak) desitxuratzea, ez eta sarean edo informazio sistemetan dagoen edozein informazio baimenik gabe deszifratzea ere.

Gorabeherak (teknikoak edo segurtasunekoak) administratzeko, mantentzeko edo konpontzeko Informazio Sistemetara sartzen diren langileek, mantentze- edo segurtasun-arrazoiengatik soilik jo ahal izango dute gorabehera jakin baten arrastoak detektatzeko, aztertzeko eta jarraitzeko aukera ematen dieten datu pertsonalak, AKSArenak edo haien erakunde bezeroenak dituzten fitxategietara.

Ondorioz, uneoro gorde beharko dute isilpekotasuna, eta Segurtasun arduradunaren baimena beharko dute hirugarrenek AKSaren baliabideetara edo haren bezeroetara sartzeko aukera izan dezaten.

Inola ere ez zaizkie identifikazio datuak eta autentifikazioa eman behar hirugarrenei, ezta AKSAko langileei ere.

Saioak blokeatzea eta jaramon egiten ez zaien ekipoa

Kanpoko langileek saioa blokeatu behar dute ordenagailua erabili gabe denboraldi luze batez uzten dutenean edo ekipoari jaramon egiten ez zaionean. AFA-AKSaren domeinuari konektatutako ekipoetan, saioa automatikoki blokeatzen da, aktibitate ezagatik, AFA-AKSAn ezarritako lanpostu politikarekin bat etorritz.

Lizentziak eta aplikazioak

Kanpoko langileek ez dituzte erabili behar beste makina edo segurtasun sistema batzuk kaltetu ahal dituzten programak (malwarea, birusak, troiarrak eta abar). Horregatik, kanpoko langileek haren eguneratze zikloa mantentzen duen softwarea erabili beharko dute, bereziki segurtasun eguneratzeena.

Kanpoko langileek erabiltzen duten softwarearen lizentziaren eta copyrightaren baldintzak errespetatu behar dituzte. AFA-AKSaren sareari konektatutako ekipoak dauzkaten kanpo langileei beren funtzioak behar bezala betetzeko behar duten softwarea ematen die AKSAk. Software hori AKSaren "software plataforman" baimenduta edo aztertzeko prozesuan dago. Beraz, AKSaren ekipoetan erabiltzen den software orok lizentzia egokia eduki behar du.

AKSaren ekipoak erabiltzen ez dituztenek softwarearen legez kanpoko erabileraren ondorioz sortzen diren kalteen erantzukizuna hartuko dute; AKSAk ez du instalazio horiengatik inolako erantzukizunik bere gain hartuko.

Era berean, debekatuta dago jabetza intelektualak babestutako edozein obra, dokumentu edo asmakuntza mota erabiltzea, erreproduzitzea, lagatzea, eraldatzea edo publikoki komunikatzea, kasuan kasuko baimenik gabe. Gainera, debekatuta dago iruzurrezko jatorria duen eta jabetza intelektualaren aurkako delitua den edozein eduki lortzea.

Komunikazio eta lankidetzaren tresnak

Posta elektronikoa, banaketa zerrendak, hodeiko zerbitzuak (biltegiatzea eta abar), lankidetzako tresnak, intranet/extranet, berehalako mezularitza zerbitzuak edo eztabaida foroak pertsonen arteko komunikazioa eta informazioa zenbait solaskideri aldi berean bidaltzea errazten duten tresnak dira.

Horregatik, AKSAk ematen dituen honelako komunikazio eta lankidetzaren tresnen bidez egindako jarduera guztien erantzule dira kanpoko langileak. Langile horiek beren lana egitearekin zerikusia duten jarduera pertsonaletarako erabili behar dituzte komunikazio zerbitzuok. Uneoro eduki iruzurtia, iraingarria, lizuna edo mehatxagarria daukaten mezuak, kateatutako gutunak, eskema piramidalak eta antzekoak, edo indarrean dagoen legerian jasotzen diren eskubideen aurkako edukia duten mezuak bidaltzea galarazi behar du. Era berean, ez dago baimenduta AKSaren informazioa kanpora bidaltzea, informazio hori publikoa ez bada eta erakundearen interesak arriskutan jar baditzake.

Posta elektronikoko korporatiboa AKSAk kanpoko langileei helburu profesionalekin soilik eman diezaiekeen tresna bat da, kontrolatu edo monitorizatu egin daitekeena eta helburu pertsonalekin erabili behar ez dena. AKSArekiko harreman profesionala amaitu ondoren, AKSAk kanpoko

langileei emandako tresnak eskuratu ahal izango ditu, interesgarria izan daitekeen informazioa berreskuratzeke.

Kanpoko langileek, AKSAk emandako posta elektronikoko kontuarekin, onartzen dute AKSAren aburuz posta indiskriminatua diren mezuak (SPAM) markatu/ezabatu ahal direla.

Bestalde, AKSAk fitxategi mota batzuk bidaltzea edota jasotzea blokeatu ahal du, informazio sistemen segurtasun edota errendimendu jarraibideen arabera.

Komunikazioen azpiegitura

AKSAk komunikazioetarako azpiegitura bat dauka, erakundearen konektibitatea (erakundearen barruan, eta gainerako erakunde edota pertsonekin) errazteko.

Komunikazio azpiegitura horren diseinua erakundearen ohiko kontsumoetan oinarrituta eta beraien eraginkortasuna eta segurtasuna hobetzen dituzten metodologiak erabiliz egin da.

Horregatik, ez dago baimenduta inolako zerbitzu telematikorik (posta elektronikoko zerbitzaria, web zerbitzariak, FTP eta abarrak) edo komunikaziorako inolako gailurik jartzea AKSAk kudeatutako sarean, AKSAren azpiegiturak administratzeaz arduratzen diren pertsonen berariazko baimena gabe.

Era berean, kanpoko langileek ez dute komunikazioetako azpiegitura erabili behar AKSAren sarean edo hirugarrenen sarean zehar dabilen informazioa bidegabe eskuratzeko, suntsitzeko edo manipulatzeko, edo beren nortasuna ezkutatzeko edo manipulatzeko.

Azpiegiturak administratzen dituzten langileek edo lan hori eskuordetzen zaien langileek ez dituzte murrizpen horiek izango; baldintza bakarra da beraien jardura planeatutako ekintzak egitera edo gorabeherak konpontzera orientatuta egon behar dela.

Sarean eta internet zerbitzuetan sartzea

Kanpoko langileek ez dituzte partekatutako baliabideak pilatu behar, baldin eta horrek erakundeko kideek edo beste erakunde batzuetako kideek beren lana modu egokian egitea galarazten badu. AKSAk sareko eta Interneteko zerbitzuetako sarbidea mugatzeko mekanismoak sortu ahal ditu.

Kanpoko langileek informazioa bidaltzeko edota jasotzeko erakundeen baliabideak erabili behar badituzte, eta horrela gainerako langile erabiltzaileak blokeatzeko aukera dagoela susmatzen badute, bidalketa edota jasotze horiek azpiegitura administratzen duten langileekin koordinatu behar dituzte.

Lehenago azaldu dugunez, kanpoko langileak dira AKSAk eskaintzen dizkion ekipamenduaren eta sarearen erabilera egokiaren arduradunak. Zenbait baliabidea (zerbitzariak, aplikazioak, datu baseak, sarea) erabiltzaile talde batek konpartitzen ditu. Horregatik, baliabide horiek azpiegitura administratzen duten langileek kudeatuko dituzte.

Inprimaketa zerbitzuen erabilera

Pertsona bakoitzak jaso behar ditu tokiko edo saileko inprimagailuetara inprimatzeko bidaltzen dituen kopiak.

"Jaberik gabeko" dokumentuak aurkitzen dituen edozein pertsonak dokumentu horiek ezabatu edo suntsitu behar ditu, baldin eta beraiak gainbegiratu ondoren ez badu aurkitzen jabearen erreferentziarik. Erreprografiako ekipoek berriki inprimatutako dokumentuak bakarrik eduki behar dituzte.

Informazio trukea

Informazioa trukatzean eta biltegitratzean, informazioa babestuta dagoela bermatu beharko da, segurtasun arriskuak prebenituz, hala nola baimenik gabeko sarbideak eta datu galerak, besteak beste. Kanpoko langileen erantzukizuna da tresna korporatiboetan partekatzen den informazioa.

Informazioa hodeian partekatuz gero, erakundeak onetsitako biltegitratze plataformak baino ez dira erabili behar. Plataforma horietan, informazio konfidentziala duten fitxategi guztiak zifratu edo babestu behar dira pasahitzaren bidez. Kanpoko langile baimenduek baino ezin izango dute artxibo partekatueta sartu, eta sarbide horretarako balio epe bat ezarri beharko da, baimendutako denbora amaitu ondoren baimenak baliogabetzen direla ziurtatuz.

AKSAk informazioa trukatzeko tresna korporatiboak lehenestea gomendatzen du, eta ez du gomendatzen bilketa erauzgarria¹ erabiltzea. Salbuespenezko kasuetan, beste aukera bideragarriarik ez badago, euskarri horiek erabiltzeko baimena emango da, eta euskarri horietan dagoen informazioaren arduradunen baimena beharko da.

Biltze erauzgarria erabiltzeko baimena izanez gero, informazioa zifratuta edo pasahitz bidez babestuta egon beharko da. Era berean, gailua galdu edo lapurtuz gero, kanpoko langileek berehala eman beharko diote informazioaren berri segurtasuneko taldeari, izan daitezkeen arriskuak arintzeko.

Isilpeko informaziorako sarbidea baimen bidez emango zaie beren eginkizunak betetzeko hala eskatzen duten kanpoko langileei soilik, pertsonala eta besterenezina izanik. Gainera, datu pertsonalak dituen informazioa kanpora bidaltzeko, tratamenduaren arduradunaren baimena behar da, eta, pertsona hori ez badago, AKSAko Segurtasunaren arduradunarena.

Emandako sarbideek alde zehaztutako denbora muga izango dute, eta automatikoki baliogabetuko dira epea amaitzean. Salbuespenezko kasuetan, denbora luzapenak justifikatu egin beharko dira eta dagokion arduradunak onetsi beharko ditu, arrazoia erregistratuta utziz.

Informazio trukean ezarritako jarraibideen ez-betetzereen bat antzeman ez gero, gorabehera gisa jakinarazi eta kudeatuko da (ikus apartatua: [Gorabeherak](#)).

Ekipamendu informatikoa

Ekipamendu informatikotzat hartzen da lan eginkizunak betetzeko hornitzen den gailu elektronikoro (ordenagailu eramangarria, mahai gainekoa, telefonoak, gailu mugikorak, tabletak, monitorea, teklatuak, etab.), osagaiak eta tresnak, maila pertsonalean erabiltzea baimenduta ez daudenak. Kanpoko langileen ardura da esleitutako ekipoa zaintzea eta egoera onean mantentzea erabiltzen duten bitartean.

AKSAk ekipamendu informatikoaren erabilera berrikusteko eskubidea gordetzen du beretzat, modu desegokian erabili dela susmatzen badu.

"Gailu mugigarrien erabiltzaileak" dira beren lanpostuaren ezaugarriengatik ordenagailu eramangarria, smartphonea, sakelako telefonoa, tableta eta antzekoak erakundearen barruan nahiz kanpoan erabiltzen dituzten pertsonak.

Arau honetako gainerako apartatuak betetzeaz gain, kanpoko langileek beste neurri batzuk ere hartu beharko dituzte, instalazioetatik atera daitezkeen gailuak baitira:

- Gailua bere kontrolpean eduki beti, batez ere leku publikoetan.
- Ez biltegitratu isilpeko informaziorik modu lokalean ekipoa.

¹ Informazioa formatu elektronikoa eta erraz garraiatzeko moduan gordetzeko gaitasuna duen edozein gailu. (CDak, DVDak, USB giltzak, sakelako telefonoak...)

- Wi-Fi sare seguru eta onetsietara soilik konektatzea.
- VPN korporatibo bat erabiltzea laneko informazioa edo sistemak eskuratzeko bulegotik kanpo.
- Besteak beste, Bluetooth, Wi-Fi eta NFC funtzioak desaktibatzea gomendatzen da, erabiltzen ari ez direnean.
- Galdu edo lapurtuz gero, berehala jakinarazi CAUri, gailua blokeatzeko eta biltegiatutako informazioa babesteko.
- Debekatuta dago gailu korporatiboetan "jailbreak²" edo "rooting³" egitea, horrek sartuta dauden segurtasun neurriak ezabatzen baititu.
- Baimendu gabeko edozein aldaketa erakundearen politiken urraketatzat hartuko da.
- Kanpoko langileak dira beren gailua eta maneiatzen duten informazioa babestearen arduradunak.

Ikusten bada ekipamenduak higadura normala gainditzen duten kalte esanguratsuak dituela, CAUri jakinarazi beharko dio, eta kaltearen inguruabarrak adierazi. Era berean, AKSAk kalteak zabarkeriak, erabilera okerrak edo kanpoko faktoreek eragin zituzten ebaluatuko du.

AKSArekiko harremana amaitu ondoren, agindutako lanak egiteko entregatu den material guztia itzuli behar zaio AKSAri.

Informazioaren segurtasunarekin lotutako araudia betetzea

Identifikatutako edo identifika daitezkeen pertsona fisikoen gaineko edozein informazio hartzen da datu pertsonaltzat. AKSAk, bere eginkizunak betetzeko, datu pertsonalen tratamendua egin behar du. Horrelako datuen tratamendua legeak arautzen du (bai estatuko legeriak bai autonomikoak).

Horregatik, beren funtzioak betetzeko datu pertsonalak erabiltzen dituzten langileek prestakuntza egokia eduki behar dute eta datu pertsonalak babesteari buruz, beren betebeharrei buruz eta legea haustearen ondorioei buruz indarrean dagoen legezko araudia ezagutu behar dute.

Datu pertsonalak babesteari buruzko legeriak pertsona horiei betebeharrak ezartzen dizkie, besteak beste:

- Datu pertsonalak baimendu gabeko erabileren kontra babestea.
- Datu pertsonalen fitxategi berririk ez sortzea, Segurtasun arduradunaren baimenik gabe.
- Segurtasun arduradunari jakinaraztea datu pertsonalei eragiten dien edozein gorabehera.
- Aldi baterako fitxategiak sortzea, definitutako sarbide kontrola duten baliabideetan, eta fitxategiok suntsitzea, sortu ziren helbururako erabilgarri ez direnean.
- Kanpora daturik ez bidaltzea, Segurtasun arduradunaren baimenik gabe.
- Botatzen diren edo berrerabiltzen diren euskarrietako informazioa suntsitzea.
- "Datu pertsonalen gaineko administrazio betebeharren prozedura" (intraneten edo segurtasun arduradunaren bidez eskuragarri) erabiltzea datu pertsonalak eskuratzeko, zuzentzeko, ezeztatzeko eta aurka egiteko eskaeren aurrean.
- Datu pertsonalak Fitxategiaren arduradunaren eta Segurtasun arduradun egokiaren jarraibideekin bat etorri tratatzea.
- Kanpoko langileek bete egin behar dituzte datu pertsonalen tratamenduaren baldintzak, ezarritako kontratuan jasotakoak.

² iOS duen gailu batean Applek ezarritako mugak ezabatzeko prozesua.

³ Prozesu horren bidez, "supererabiltzaile" edo administratzaile baimenak lortzen dira sisteman inolako mugarik gabe sartzeko.

Gorabeherak

AKSAren edo haren bezeroen baliabideen segurtasuna kaltetu ahal duen edozein akats edo anomalia dagoela jakin edo susmatuz gero, kanpoko langileek CAUri jakinarazi beharko diote (945 181818 - luz.: 54600 edo cau@araba.eus), "Zibersegurtasun gorabeherak kontrolatzeko eta kudeatzeko prozeduran" zehazten den bezala. CAU izango da gorabehera erregistratu eta aztertu behar duena.

AKSAri lotutako informazio sistemetan jasotzen diren segurtasun gorabeherak, nahiz eta AKSAk ez kudeatu, AKSAko Segurtasun arduradunari jakinarazi behar zaizkio ahalbait arinen, gehienez ere 24 orduko epean.

Hauek dira gerta litezkeen gorabeheretako batzuk:

- Identifikazio pertsonala eta pasahitza blokeatzea behin eta berriz (jatorri ezezagunarekin).
- Hardwarearen edo softwarearen funtzionamendu arraroa (Malwareri lotuak).
- Informazio baliabideak eskuratzean urraketak.
- SPAM/Phishing (zuzenduak): Mezu elektronikoko susmagarriak edo eskatu gabeak.
- Entitateak ordeztzea.
- Erakundeari zuzendutako erasoak detektatzea.
- Identifikazio pertsonalak eta pasahitzak estutasunean jartzea.
- Informazioa edo baliabideak baimenik gabe eskuratzeko.
- AKSAren eta antzeko erakundeen datuak edo informazioa galtzea.
- Informazioa baimenik gabe aldatzea.
- Sistemen ahuleziak hautematea.

Nahitaezkoa da AKSAren informazio sistemetan eragina izan dezaketen segurtasun gorabehera larrien berri ematea AKSAko Segurtasun arduradunari.

Edonork helarazi ahal izango dizkio AKSAko Segurtasun arduradunari informazioaren segurtasunarekin eta politika hauetan jasotako jarraibideekin zerikusia izan dezaketen iradokizunak, ahuleziak edo arrisku egoerak.

Informazioaren kopia

Kanpoko langileek ez dute AKSAren edo zerbitzua ematen dieten erakundeen informazioaren kopia paraleloak egin behar, erakundearen operatibo dagoen lekutik kanpo. Beraz, ezin da informazioari kopiatu edozein biltegitratze gailutan (fisikoki edo hodeian), haren jabearen edo AKSAren Segurtasun arduradunaren berriazko baimenik gabe.

AKSAk kudeatzen ez duen azpiegitura batean AKSAren informazio sistemak dauzkaten enpresa hornitzaileek datuen segurtasun kopiak egin beharko dituzte, AKSAko Segurtasun arduradunak emandako jarraibideak betez.

Aldi baterako kopiak suntsitu egin behar dira, beharrezko izateari uzten dioten unean. Kanpoko langileek kontu berezia izan beharko dute ordenagailuko "zakarrontzien" barruan, aldi baterako karpitetan eta abarrekoetan publikoa ez den informazioaren kopiarik ez uzteko.

Informazioaren biltegitratzea lanpostuan

AKSAren zerbitzari korporatiboetarako sarbidea daukaten kanpoko langileek ez dute AKSAren negozioerako edo haren bezeroentzat informazio garrantzitsua dena biltegitratu behar beren laneko ekipo pertsonaletan. Informazioa AKSAren Datuen zerbitzarietan biltegitratu behar da. AKSAren zerbitzari korporatiboetarako sarbiderik ez duten kanpoko langileen kasuan, AKSArekin

adostutako eskuragarritasun, osotasun eta konfidentzialtasun baldintzak betetzen dituzten kokalekuetan gorde behar dute informazioa.

AKSAren edo zerbitzua ematen zaien erakundeen negozioarako esanguratsua ez den informazioa ezin da AKSAren zerbitzari korporatiboetan biltegitatu, sareko baliabideak modu egokian erabili ahal izateko. Gailu mugigarriak erabiltzen dituen kanpoko langile orok, ahalik eta lasterren, negozioaren informazioa AKSAren zerbitzari korporatiboetan ostatatu behar du.

Segurtasun fisikoa eta mahai garbien politika

Langile guztiak kontu handia izan behar dute, aplikazioek ematen duten informazioa baimenik gabeko pertsonak ikusi ezin izateko.

Gainera, lanpostua utzi baino lehen, egiaztatu behar dute beren lana egiteko erabiltzen dituzten materiala eta dokumentazioa batuta utzi dituztela.

Laneguna amaitzean, ordenagailuak itzali behar dira. Piztuta eduki behar badira, pantaila blokeaturik geratu behar da.

Informazioa tratatzeko sistemak dauden instalazioetan fisikoki sartzeari murriztuta dago, horretarako baimendutako langileen kasuan izan ezik. Betiere, ezarritako segurtasuneko sarbide kontrolak errespetatuko dira.

AFA-AKSAren eraikinetan lan egiten duten kanpoko langileek identifikazio pertsonaleko txartela edo BISITARI txartela ikusgarri eraman behar dute.

Bestalde, AFA-AKSAren instalazioetan ez dauden edo AKSAk kudeatzen ez dituen informazio sistemetan lan egiten duten kanpoko langileek aurreko paragrafoetan azaldutako neurrien antzekoak aplikatu behar dituzte, AKSArekin sinatutako konfidentzialtasun akordioak bermatzeko moduan.

Beste dokumentu batzuk

AKSAk informazio sistemetakoa kanpoko langileei jakinarazten die araudi honetaz gain beste prozedura, araudi, gidaliburu, segurtasun politika eta abarreko batzuk daudela, Intraneten Segurtasun arloan argitaratuak; horiek jakitea eta betetzea nahitaezkoa da. Intraneten sartzeko baimenik ez duten kanpoko langileek AKSAko Segurtasun arduradunarekin harremanetan jarri beharko dute informazio hori eskatzeko.

Informazio sistemen segurtasunaren inguruko dokumentu berriak eta dauden dokumentuen berrikuspenak ohiko moduetan emango dira jakitera.

Monitorizazioa

AKSAren azpiegitura teknologikoari konektatutako kanpoko langileek badakite AKSAren sarera, saretik edo sarean sartzeko erabiltzen diren informazio sistemen jabe bakarra AKSA dela. Horregatik, langile horiek ulertzen dute ez daukatela jabetza eta konfidentzialtasun eskubidea hura erabiltzerakoan. Horrek esan nahi du AKSAk uneoro egin ditzakeela kontrolak, kanpoko langileen nortasunean eta komunikazioen eta biltegitatzeen edukian oinarrituak, uneoro indarrean dagoen legeria errespetatuz, ukitutako pertsonari ezer jakinarazi beharrik gabe.

Horrenbestez, AKSAk bere informazio sistemen inguruko jarduera oro monitorizatzeko eskubidea gordetzen du beretzat, kanpoko langile guztiak baliabide informatikoak modu egokian erabiltzen dituztela eta baliabide horiek behar bezala dabilzala ziurtatzeko, betiere indarrean dagoen legeria betez.

AKSaren aplikazioaren batean atzematen bada kanpoko langileren batek gaizki erabili duela, jakinarazi egingo zaio. Beharrezkoa bada, baliabidea ondo erabiltzeko prestakuntza emango zaio. Asmo txarreko erabilera atzematen bada, AKSAk egoki irizten dien ekintzak egingo ditu.

Azkenik, AKSAk kontrolak egin ahalko ditu indarrean dauden arauak, prozedurak, politikak eta abarrekoak ondo betetzen direla ziurtatzeko.

Baliabideen erabilera okerraren ondorioak

Langileen lankidetzatza

AKSaren baliabide informatikoetako eta sare azpiegiturako kanpoko langileek, hala eskatzen zaienean, sistemen administratzaileekin eta Segurtasun arduradunarekin batera lan egin beharko dute, ahal duten neurrian, segurtasuneko edo baliabideen erabilera okerreko gorabehereri buruz egiten diren ikerketetan, eta eskatzen zaien informazioa eman beharko dute.

Ekintza zuzentzaileak eta prebentziozkoak

Sistemen administratzaileak detektatzen badu baliabideak gaizki erabili direla eta erabilera oker hori kanpoko langileen jardueretatik edo ekipotik badator, neurri hauetako edozein hartu ahalko du gainerako pertsona, sare edo ekiptoak babesteko.

- Gorabeheraren berri ematea kanpoko langileei, erakundeko arduradunari eta/edo Segurtasun arduradunari.
- Zerbitzuetan sartzea edo erabiltzea etetea edo murriztea, ikerketak dirauen bitartean. Etete hori AKSaren Kudeatzailetzaren aurrean errekurritu ahalko du kanpoko langileak.
- Segurtasun arduradunaren baimenarekin eta justifikazio (funtzional eta legal) egokiarekin, zerikusia duen kanpoko langilearen fitxategiak edo biltegitratze gailuak ikuskatzea.
- AKSaren Kudeatzailetzari gertatutakoaren berri ematea.

Kontratu neurriak

Beharrezkoa bada, Segurtasun arduradunak edo sistemen administratzaileak txostena egin ondoren, AKSaren Kudeatzailetzak kontratu izaerako neurriak hartu beharko ditu arau hau hautsi duten kanpoko langileen enpresekin, indarrean dagoen legerian ezarritakoaren arabera.