bai euskarari ziurtagiria | Zerbitzua euskaraz

Publikoa

oreka i.t.
corporate balance

Hornitzaileen araudia

OREKA IT

Bertsioa: 5
Arduraduna: OREKA IT
2025/03/03

ARABA · Zumar Hiribidea 1, IV Eraikina · 243 bulegoa · 01013 | Vitoria-Gasteiz · 945 067 219
BARTZELONA · Passeig Mossèn Jacint Verdaguer 40, 2.solairua · 08700 | Igualada · 938 053 767
BIZKAIA · Ibaiondo Plaza 1, 2.solairua · 207 bulegoa · 48940 | Leioa · 944 143 983
GIPUZKOA · Pillotegi Bidea 2, 3.solairua · 301 bulegoa · 20018 | Donostia · 943 065 922
NAFARROA · Mutiloako Industrialdea, E kalea 9, 1.A · 31192 | Mutilva · 948 151 286

orekait.com
orekait@orekait.com

SAP Gold Partner · salesforce · Microsoft Cloud Solution Provider

AURKIBIDEA

1. Xedea 4
2. Irismena 4
3. Jarraibide orokorrak 4
3.1. Zerbitzua ematea 4
3.2. Informazioaren konfidentzialtasuna 5
3.3. Jabetza intelektuala 6
3.4. Informazioa trukatzea 7
3.5. Baliabideen erabilera egokia 7
3.6. Erabiltzailearen erantzukizunak 9
3.7. Erabiltzailearen gailua 11
3.8. Hardware gailuen kudeaketa 12
4. Jarraibide espezifikoak 12
4.1. Aplikazio-eremua 12
4.2. Pertsonen antolaketa 14
4.3. Segurtasun-ikuskapena 15
4.4. Gertaeren jakinarazpena 15
4.5. Segurtasun fisikoa 15
4.6. Aktiboen kudeaketa 16
4.7. Segurtasun-arkitektura 17
4.8. Sistemen segurtasuna 17
4.9. Sareko segurtasuna 19
4.10. Sistemen erabileraren trazabilitatea 20
4.11. Identitateen eta sarbideen kontrola eta kudeaketa 20
4.12. Aldaketen kudeaketa 22
4.13. Aldaketen kudeaketa teknikoa 22
4.14. Segurtasuna Garapenean 23
4.15. Kontingentzien kudeaketa 24
5. Jarraipena eta kontrola 24

NORK EGINA	NORK BERRIKUSIA	NORK BERRIKUSIA	NORK ONARTUA
María Iturbe	Oier Ruiz de Loizaga	Jose Carasa	Iraitz Pérez de Goldarazena
KSren arduraduna	Sistemen arduraduna	Teknologiako zuzendaria	Zuzendari nagusia

BERRIKUSPENEN KONTROLA			
EDIZIOA	BERRIKUSPEN-DATA	OHARRAK	ONARTUA
1	2022/06/04	Dokumentazioa prestatzea	BAI
2	2023/01/24	KSren arduraduna aldatzea: Yolanda Vicentetik Koldo Ramari	BAI
3	2024/01/16	KSren arduraduna aldatzea: Koldo Ramatik Maria Iturberi	BAI
4	2024/12/10	KSren arduraduna aldatzea: Maria Iturbetik Mª Esperanza Oterori	BAI
5	2025/03/03	Oreka IT Plantilla berrian eguneratzea	BAI

1. Xedea

Dokumentu honen xedea da informazioaren segurtasunari buruzko arau-esparrua ezartzea Oreka IT hornitzen duten eta haren informazioa, informazio-sistemak edo baliabideak eskuratzen dituzten erakundeentzat, haien konfidentzialtasuna, osotasuna, eskuragarritasuna, benetakotasuna eta trazabilitatea babesteko.

Horretarako, erakunde hornitzaileak arduratzen dira Oreka ITri zerbitzua ematen dioten langileei eta azpikontratatuei informazioa emateaz.

2. Irismena

Erakunde hornitzaileek Oreka ITrentzat egiten dituzten jarduera guztiak, haren informazioa, informazio-sistemak edo baliabideak eskuratzen dituztenean.

“Jarraibide orokorrak” 3. atala edozein erakunde hornitzaileri aplika dakioke, ematen duen zerbitzua edozein dela ere.

“Jarraibide espezifikoak” 4. atala kasu bakoitzean adierazitako zerbitzu motarekin bat datozen zerbitzuak ematen dituzten erakunde hornitzaileei baino ez zaie aplikatuko, atalaren hasieran adierazten den bezala.

3. Jarraibide orokorrak

3.1. Zerbitzua ematea

Erakunde hornitzaileek dagokion zerbitzu-kontratuaren pean egiten diren jarduerak soilik egin ahal izango dituzte Oreka ITrentzat.

Erakunde hornitzaileak aldian-aldian emango dio Oreka ITri emandako zerbitzuari lotutako pertsonen, profilen, funtzioen eta erantzukizunen zerrenda, eta unean-unean emango dio harreman horretan gertatzen den edozein aldaketaren berri (alta, baja, ordezkapena edo funtzioen edo erantzukizunen aldaketa).

Zerbitzuak emateko kontratuari lotutako klausuletan ezarritakoaren arabera, Oreka IT enpresarentzat lan egiten duten kanpoko pertsona guztiek dokumentu honetan jasotako segurtasun-arauak bete beharko dituzte. Betebehar horietakoren bat bete ezean Oreka ITk beretzat gordetzen du arau-haustea egin duen pertsonari betoa jartzeko eskubidea, bai eta erakunde hornitzaileari dagokionez egokitzat jotzen diren zehapen-neurriak hartzeko eskubidea ere.

Erakunde hornitzaileak ziurtatu beharko du langile guztiek prestakuntza egokia dutela emandako zerbitzua garatzeko.

Oreka IT eta erakunde hornitzailearen artean gertatzen den informazio-truke oro zerbitzuak emateko kontratuak ezarritako esparruan egin dela ulertuko da; beraz, informazio hori ezingo da erabili esparru horretatik kanpo, ez eta beste helburu batzuetarako ere.

Sistemak taldeak Oreka ITren aktiboak babesteko ahalegin orokorrak zentralizatzen ditu.

Oro har, aktiboek honako hauek hartzen dituzte barne:

- Informazio babestua, hau da, pertsona fisikoak eta/edo juridikoak identifikatzeko aukera ematen duen informazioa, eta informazio-sistemen eta komunikazio-sareen konfigurazioari buruzkoa.

- Babestutako informazioa tratatzeko bestelakoak (softwarea, hardwarea, komunikazio-sareak, informazio-euskarriak, gailu osagarriak eta instalazioak).

3.2. Informazioaren konfidentzialtasuna

Oreka ITren informazioa eskura duten kanpoko pertsonek, informazio hori, besterik adierazi ezean, babestutzat jo beharko dute.

Informazio ez babestutzat joko da soilik Oreka ITk horretarako ezarritako hedabide publikoen bidez eskuratu ahal izan den informazioa.

Ez da informazioa zabaldu, aldatu, suntsitu edo gaizki erabiliko, dagoen euskarria edozein dela ere.

Erreserbarik handiena denbora mugagabez gordeko da, eta ez da informazio babesturik igorriko kanpora, behar bezala baimenduta dagoenean izan ezik.

Informazio babestua duten paper-formatuko txostenen kopurua minimizatu egingo da, eta leku seguruan eta hirugarren pertsonen eskueratik kanpo mantenduko dira.

Baldin eta, lanpostuarekin zuzenean lotutako arrazoiengatik, erakunde hornitzaileko langileak edozein euskarritan jasotako informazio babestua eskuratzen badu, jabetza hori aldi baterako baino ez dela ulertu beharko du, sekretua gordetzeko betebeharra duela, eta horrek ez diola inolako eskubiderik emango informazio horren edukitza, titulartasuna edo kopia izateko. Era berean, langileak aipatutako euskarria edo euskarriak itzuli beharko ditu, horiek aldi baterako erabiltzea eragin duten zereginak amaitu eta berehala, eta, nolanahi ere, bere enpresak Oreka IT enpresarekin duen harremana amaitu eta berehala.

Betebehar hauek guztiek indarrean jarraituko dute kanpoko pertsonek Oreka ITrako garatzen dituzten jarduerak amaitu ondoren.

Betebehar hauek ez betetzea sekretuak agerraraztearen delitua izan daiteke.

Datu pertsonalen segurtasuna bermatzeko, erakunde hornitzaileko pertsonek jarduera-arau hauek bete behar dituzte, aipatutako kontsiderazioetaz gain:

- Fitxategiak sortu ahal izango dituzte beren lana egiteko beharrezkoa denean bakarrik. Aldi baterako fitxategi hauek ez dira inoiz gordeko erabiltzaileen PCetako disko-unitate lokaletan, eta suntsitu egin beharko dira sortu ziren helbururako erabilgarriak izateari uzten diotenean.

- Ez da datu pertsonalik gordeko pertsona erabiltzailearen PC postuetako disko-unitate lokaletan.

- Euskarri eta dokumentuak (e-mailak bidaltzea barne) informazio hori kokatuta dagoen lokaletatik kanpo ateratzeko, Oreka ITk bakarrik baimendu ahal izango du eta definitutako prozeduraren arabera egingo da.

- Euskarriek eta dokumentuek aukera eman behar dute zer informazio-mota duten identifikatzeko, inbentarioa egiteko eta baimendutako pertsonek soilik erabiltzeko moduko leku batean gordetzeko.

- Bereziki babestutako datu pertsonalak transmititzea (adib. osasuna), telekomunikazio-sareen bidez (adib. posta elektronikoa) datu horiek zifratuz egingo da, edo beste edozein mekanismo erabiliz, hirugarren pertsonek informazioa ez dutela ulertuko edo manipulatuko bermatzeko.

3.3. Jabetza intelektuala

Jabetza intelektualaren araudiak babestutako materialaren erabilerari jarritako legezko murrizketak betetzen direla bermatuko da.

Erabiltzaileek Oreka ITk baimendutako materiala baino ezin izango dute erabili beren funtzioak betetzeko.

Erabat debekatuta dago programa informatikoak erabiltzea Oreka ITren informazio-sistemetan dagokion lizentzia gabe.

Era berean, debekatuta dago jabetza intelektualak babestutako edozein obra edo asmakuntza erabiltzea, erreproduzitzea, lagatzea, eraldatzea edo publikoki komunikatzea dagokion idatzizko baimenik gabe.

Oreka ITk berak ekoitzitako materiala edo titularrak baimendutako edo hornitutako materiala bakarrik erabiltzeko baimena emango du, adostutako baldintzen eta indarrean dagoen araudiaren arabera.

3.4. Informazioa trukatzea

Inork ezin izango du inoiz bere identitatea ezkutatu edo manipulatu.

Informazioa formatu elektronikoan edo fisikoan banatzeko, zerbitzuak emateko kontratuan horretarako zehaztutako baliabideak erabiliko dira, eta kontratu horri lotutako funtzioak errazteko helburu esklusiboa izango du. Oreka ITk beretzat gordetzen du, identifikatutako arriskuaren arabera, hedapen-baliabide horiei buruzko kontrol-, erregistro- eta auditoretza-neurriak ezartzea.

Zerbitzuak emateko kontratuaren esparruan informazioa trukatzeari dagokionez, ez dira baimendutzat joko hurrengo jarduerak:

- Egile-eskubideek babesten duten materiala transmititu edo jasotzea, Babes Intelektualaren Legea urratuz.
- Material pornografiko, sexu-izaera esplizituko, arraza-bereizkeriazko adierazpen eta iraingarri edo legez kanpoko gisa sailkatu daitekeen beste edozein adierazpen edo mezu mota transmititu edo jasotzea.
- Babestutako informazioa baimenik ez duten hirugarrenei transferitzea.
- Negozioarekin zerikusirik ez duten aplikazioak transmititu edo jasotzea.
- Interneteko jardueretan parte hartzea, hala nola, berri-taldeetan, jokoetan edo zerbitzua ematearekin zuzenean lotuta ez dauden beste batzuetan.

Oreka ITren irudia eta ospea kaltetu dezaketen jarduera guztiak debekatuta daude Interneten eta beste edozein lekutan.

3.5. Baliabideen erabilera egokia

Zerbitzua ematen duen erakundeak konpromisoa hartzen du Oreka ITri aldian-aldian zerbitzua eskaintzeko dituen aktiboen berri emateko.

Zerbitzua emateko ezarritako baliabideak erabiltzeko konpromisoa hartzen du erakunde hornitzaileak, diseinatu eta ezarri ziren baldintzen arabera.

Oreka ITk kanpoko pertsonen eskura jartzen dituen baliabideak, edozein motatakoak direla ere (informatikoak, datuak, softwarea, sareak, komunikazio-sistemak, etab.), eman ziren eragiketako betebeharrak eta helburuak betetzeko soilik erabil daitezke. Oreka ITk beretzat gordetzen du baliabide horien erabilera egokia egiaztatzen duten kontrol- eta auditoretza-mekanismoak ezartzeko eskubidea.

Oreka ITren produkzio-sarera konektatzen diren gailu guztiak marka eta modelo homologatuetakoak izango dira. Erakunde hornitzaileak Oreka ITren esku jarriko ditu gailu horiek, hark software homologatuaren instalazioa koordinatu eta behar bezala konfigura ditzan.

Oreka ITren sarean edo euskarri automatizatuen, Interneten, posta elektronikoaren edo beste edozein bitartekoren bidez konektatutako edozein gailutan sartutako fitxategiek arau hauetan ezarritako baldintzak bete beharko dituzte, eta, bereziki, jabetza intelektualari, datu pertsonalen babesari eta malwarearen kontrolari buruzkoak.

Oreka ITri aktibo guztiak itzuli beharko zaizkio, justifikaziorik gabeko atzerapenik gabe, kontratua amaitu ondoren. Oreka ITk softwarea instalatu dien ordenagailu pertsonal guztiak Oreka ITri eramango zaizkio, zerbitzua amaitutakoan disko gogorra formateatu dezan.

Espresuki debekatuta dago:

- Oreka ITek emandako baliabideak zerbitzuaren helburuarekin zerikusirik ez duten jardueretarako erabiltzea.
- Softwarearen edo baliabide informatiko propioen estandarren zati gisa zehaztuta ez dauden gailuak eta/edo aplikazioak Oreka ITren produkzio-sarera konektatzea.
- Oreka ITren informazio-sistemetan edo sare korporatiboan eduki lizunak, mehatxagarriak, immoralak edo iraingarriak sartzea.
- Oreka ITren sare korporatiboan edozein malware mota (birusak, harrak, troiarrak, programa espioiak, ransomwarea...), gailu logiko, gailu fisiko edo baliabide informatikoetan edozein aldaketa edo kalte eragiten duen edo eragin dezakeen beste edozein agindu mota borondatez sartzea. Oreka ITren sarera sarbidea duten pertsona guztiek malwareen aurkako programa eguneratuak erabiltzeko betebeharra izango dute.
- Baimen espliziturik gabe, Oreka ITk esleitu ez dituen beste eskubide edo sarbide batzuk lortzea.
- Oreka ITren informazio-sistemen eremu mugatuetara sartzea baimen espliziturik gabe.

- Oreka ITren informazio-sistemen “log” erregistroak distortsionatzea edo faltsutzea.
- Baimen espliziturik gabe gakoak, sistemak edo zifratze-algoritmoak eta Oreka ITren prozesu telematikoetan parte hartzen duen beste edozein segurtasun-elementu deszifratzea.
- Beste erabiltzaileen lana oztopa dezaketen programak eduki, garatu edo exekutatzea, eta Oreka ITren baliabide informatikoak kaltetu edo aldatzea.
- Informazio babestua duten datu, programa edo dokumentu elektronikoak suntsitzea, aldatzea, baliogabetzea edo beste edozein modutan kaltetzea (egintza horiek delitu izan daitezke).
- Erabiltzailearen PC postuetako disko unitate lokaletan informazio babestua edukitzea.

3.6. Erabiltzailearen erantzukizunak

Zerbitzu-hornitzaileek bermatu behar dute Oreka IT programaren barruan lan egiten duten pertsona guztiek oinarrizko printzipio hauek betetzen dituztela:

- Oreka ITko informazioa eskura dezakeen pertsona bakoitza bere erabiltzaile-identifikatzaileak eta hortik eratorritako guztiak garatutako jardueraren erantzulea da. Beraz, ezinbestekoa da pertsona bakoitzak bere erabiltzaile-identifikatzaileari lotutako autentifikazio-sistemak kontrolpean izatea, eta hari lotutako gakoa erabiltzaileak bakarrik ezagutzen duela bermatzea. Gainerako pertsonei ez zaie inola ere jakinarazi behar.
- Erabiltzaileek ez dute beste erabiltzaile baten identifikatzailerik erabiliko, nahiz eta jabearen baimena izan.
- Erabiltzaileek ezagutzen eta aplikatzen dituzte erabiltzen duten informazioaren inguruko baldintzak eta prozedurak.

Informazio babestua eskuratu dezakeen edozein pertsonak honako zuzentarau hauek bete beharko ditu pasahitzen kudeaketari dagokionez:

- Kalitatezko pasahitzak hautatzea, hau da, gainerako erabiltzaileek nekez asma ditzaketenak.
- Pasahitza aldatzeko eskatzea beste erabiltzaile batzuek horren berri badutela uste badute.

- Pasahitzak gutxienez 90 egunean behin aldatzea eta pasahitz zaharrak berrerabiltzea saihestea.

- Pasahitzak lehenetsiak eta aldi baterakoak aldatzea lehen saioaren hasieran (“login”).

- Saioa hasteko prozesu automatizatuetan pasahitzik ez sartzea (adib. nabigatzaileetan biltegiratutakoak).

- Pasahitzekin zerikusia duen edozein segurtasun-gorabehera jakinaraztea, hala nola, galera, lapurreta edo konfidentzialtasun-galeraren zantzua.

Informazio babestua eskuratu dezakeen edozein pertsonak zaindu beharko du gailuak babestuta geratzen direla arretarik gabe geratzen direnean.

Informazio babestua eskuratu dezakeen edozein pertsonak idazmahai garbiko hurrengo arauak errespetatu beharko ditu, gutxienez, paperezko dokumentuak, euskarri informatikoak eta biltegiratzeko gailu eramangarriak babesteko eta informazioa baimenik gabe eskuratzeak, galtzeak eta kaltetzeak dakartzan arriskuak murrizteko, bai lan-ordutegi arruntean, bai lan-ordutegitik kanpo:

- Paperezko dokumentuak eta baliabide informatikoak giltzapean gordetzea, erabiltzen ez direnean, batez ere lan-ordutegitik kanpo.

- Erabiltzailearen saioak blokeatu edo PCa itzali, zaindu gabe uztean.

- Informazioa jaso eta bidaltzeko guneak (posta, eskaner eta fax makinak) eta kopiak egiteko gailuak (fotokopiagailua, faxa eta eskanerra) babestea. Horrelako gailuekin informazioa erreproduzitzea edo bidaltzea erabiltzailearen erantzukizunpean egongo da.

- Inprimatu ondoren, babestutako edozein informazio erretiratzea, justifikaziorik gabeko atzerapenik gabe.

- Beharrezkoa izateari uzten dionean informazio babestua suntsitzea.

- Oreka ITko sistemetara eta/edo informaziora sarbidea duten pertsonek ez dute inoiz, idatzizko baimenik gabe, ustezko ahultasun-, gertaera- edo segurtasun-gorabeherak detektatzeko eta/edo ustiatzeko probarik egingo.

- Oreka ITko sistemetara eta/edo informaziora sarbidea duen inor ez da saiatuko, berariazko eta idatzizko baimena izan ezean, segurtasun-sistema eta baimenak hausten. Debekatuta dago erabiltzaileak sareko trafikoa atzitzea, idatziz baimendutako auditoretza-lanak egiten ari direnean izan ezik.

Informazio babestua eskuratzen duten pertsona guztiek jarduteko arau hauek bete beharko dituzte:

- Babestutako informazioa babestu baimenik gabeko errebelazio, aldaketa, suntsiketa edo erabilera desegoki orotatik, halabeharrezkoa izan edo ez.
- Informazio-sistema eta telekomunikazio-sare guztiak babestea baimendu gabeko sarbide edo erabileretatik, eragiketa-eteteetatik, suntsiketatik, erabilera okerretik edo lapurretatik.
- Beharrezkoa den baimena izatea informazio- eta/edo informazio-sistemetara sarbidea izateko.

3.7. Erabiltzailearen gailua

Zerbitzu-hornitzaileek ziurtatu beharko dute informazio babestua eskuratzeko erabiltzen den erabiltzailearen gailu informatiko guztiek arau hauek betetzen dituztela:

- Erabiltzailearen jarduerarik ez badago, gailua automatikoki blokeatu beharko da, gehienez 15 minutuan.
- Erabiltzailearen gailuek ez dute inolaz ere izango segurtasun-sistemak eta baimenak urra ditzakeen tresnarik.
- Erabiltzailearen gailuak ekoizlearen zehaztapenen arabera mantenduko dira.
- Erabiltzaile guztiek malwareen aurkako babes egokia izango dute:
  - Malwarearen aurkako softwarea ordenagailu pertsonal guztietan instalatu eta erabili beharko da, birusekin edo bestelako software maltzurrekin lotutako eragiketa-arriskua murrizteko.
  - Eguneratuta egongo dira eskuragarri dauden azken segurtasun-eguneratzeekin.
  - Malwarearen aurkako softwareak gaituta eta eguneratuta egon behar du beti.

Bereziki zainduko da informazio babestua duten edo informazio horretara nolabait sartzeko aukera ematen duten erabiltzailearen gailu mugikor guztien segurtasuna:

- Egiaztatu behar da ez dutela behar-beharrezkoa den informazioa baino gehiago.

- Informazio hori eskuratzeko kontrolak aplikatzen direla bermatuz.
- Emandako zerbitzuarekin zerikusirik ez duten pertsonen aurrean informazio horretarako sarbideak minimizatuz.
- Gailuak zorro, maleta edo antzeko ekipamenduetan garraiatuz, ingurumen-agenteen aurkako babes egokia dutenak.

3.8. Hardware gailuen kudeaketa

Zerbitzuak ematen dituzten erakundeek ziurtatu beharko dute Oreka ITk zerbitzuak emateko emandako gailu guztiak, edozein motatakoak direla ere, behar bezala kudeatzen direla. Horretarako, honako arau hauek bete beharko dituzte:

- Erakunde hornitzaileak zerrenda eguneratua eduki beharko du Oreka ITk emandako gailuekin eta aktibo horien erabiltzaileekin, edo lotutako arduradunekin, aktiboak pertsona bakarreko erabilerakoak ez badira. Zerrenda hori Oreka ITk eskatu ahal izango du.
- Erakunde hornitzaile batek informazio babestua eduki duen Oreka ITren ekiporen bat berresleitu nahi duen bakoitzean, aldi baterako itzuli beharko du, berresleitu aurretik beharrezkoak diren ezabatze seguruko prozedurak egin ahal izateko.
- Erakunde hornitzaile batek baja eman nahi badu Oreka IT-tik jasotako gailuen erlaziotik, beti itzuli beharko ditu, Oreka ITk baja hori modu egokian tratatu ahal izan dezan.
- Erakunde hornitzaile batek zerbitzua emateari uzten badio, Oreka ITri itzuli beharko dizkio jasotako gailu guztiak, zerbitzuak emateko kontratuek ezartzen duten bezala. Paperezko eta euskarri informatikoko dokumentuen kasuan soilik ezabatu ahal izango ditu erakunde hornitzaileak; kasu horretan, Oreka ITri jakinarazi beharko dio ezabatzearen gainean.

4. Jarraibide espezifikoak

4.1. Aplikazio-eremua

Erakunde hornitzaile guztiek, arau orokorrez gain, atal honetan jasotako berariazko arauak bete beharko dituzte, kasu bakoitzari dagozkionak, Oreka IT enpresari emandako zerbitzuaren ezaugarrien arabera.

Zerbitzu-tipologia hauek aurreikusten dira:

- Zerbitzua exekutatzeko tokia: Zerbitzuak garatzen diren leku nagusiaren arabera, bi kasu bereizten dira:
  - Oreka IT: Erakunde hornitzaileak zerbitzua, batez ere, Oreka ITren egoitzatik bertatik ematen du.
  - Urrutikoa: Erakunde hornitzaileak nagusiki bere bulegoetatik ematen du zerbitzua, nahiz eta jarduera puntualak egin daitezkeen Oreka ITren egoitzan.
- Erabilitako IKT azpiegituren jabetza: Zerbitzua emateko erabiltzen diren IKT azpiegitura nagusien (komunikazioak, erabiltzailearen gailuak, softwarea) jabea nor den kontuan hartuta, bi kasu bereizten dira:
  - Oreka IT.
  - Erakunde hornitzailea.
- Oreka ITren sistemetara sartzeko maila: Oreka ITren informazio-sistemetara sartzeko mailaren arabera hiru kasu bereizten dira:
  - Sarbide pribilegiatuarekin: Ematen den zerbitzuak Oreka ITren informazio-sistemetarako sarbide pribilegiatua eskatzen du, sistema horiek edota prozesatzen dituzten ekoizpen-datuak administratzeko gaitasunarekin.
  - Erabiltzaile-mailako sarbidearekin: Ematen den zerbitzuak Oreka ITren informazio-sistemak erabiltzea eskatzen du; hala, zerbitzua ematen duten pertsonek erabiltzaile-kontuak dituzte, eta, horien bidez, sistema horietakoren batera sar daitezke ohiko pribilegioekin.
  - Sarbiderik gabe: Ematen den zerbitzuak ez du Oreka ITren informazio-sistemak erabili beharrik; beraz, zerbitzua ematen duten pertsonek ez dute erabiltzaile-konturik sistema horietan.

Hiru kategorietako bakoitzaren arabera, zerbitzua non kokatzen den kontuan hartuta, erakunde hornitzaileak, segurtasun-arau orokorrez gain, taula honetako ataletan jasotako arau espezifikoak bete beharko ditu:

	LEKUA		INFRAESTRUKTURA		SARBIDEA		
	OREKA IT	Urrunetik	OREKA IT	Erakunde hornitzailea	Pribilegiatua	Normala	Sarbiderik gabe
Pertsonen aukeraketa	EZ	EZ	EZ	EZ	BAI	EZ	EZ
Segurtasun-ikuskapena	EZ	EZ	EZ	EZ	BAI	EZ	EZ
Gertaeren jakinarazpena	BAI	BAI	BAI	EZ	BAI	BAI	EZ
Segurtasun fisikoa	EZ	BAI	EZ	EZ	EZ	EZ	EZ
Aktiboen kudeaketa	EZ	EZ	EZ	BAI	EZ	EZ	EZ
Segurtasun-arkitektura	EZ	EZ	EZ	BAI	BAI	BAI	EZ
Sistemen segurtasuna	EZ	EZ	EZ	BAI	EZ	EZ	EZ
Sareko segurtasuna	EZ	EZ	EZ	BAI	EZ	EZ	EZ
Sistemen erabileraren trazabilitatea	EZ	EZ	EZ	BAI	BAI	EZ	EZ
Identitateen eta sarbideen kontrola eta kudeaketa	EZ	EZ	EZ	BAI	EZ	EZ	EZ
Aldaketen kudeaketa	EZ	EZ	EZ	BAI	BAI	BAI	EZ
Aldaketen kudeaketa teknikoa	EZ	EZ	EZ	EZ	BAI	EZ	EZ
Garapenean segurtasuna	EZ	EZ	EZ	EZ	BAI	BAI	EZ
Kontingentzien kudeaketa	EZ	EZ	EZ	BAI	EZ	EZ	EZ

4.2. Pertsonen antolaketa

Erakunde hornitzaileak egiaztatu egin beharko ditu zerbitzuari esleitutako pertsonen aurrekari profesionalak, eta Oreka ITri bermatu beharko dio iraganean ez duela zigorrik jaso lanbideko praxi txarragatik, eta ez duela izan tratatutako informazioaren konfidentzialtasunarekin lotutako gorabeherarik, eta ondorioz, ez zaiola zigorrik ezarri.

Erakunde hornitzaileak Oreka ITri bermatu beharko dio Oreka ITk beto-eskubidea erabili nahi duen edozein pertsonaren zerbitzura esleitutako pertsonei berehala baja emateko aukera, “3.1. Zerbitzua ematea” atalean ezarritako baldintzekin bat etorriz.

4.3. Segurtasun-ikuskapena

Erakunde hornitzaileak baimena eman behar dio Oreka ITri eskatutako segurtasun-ikuskapenak egiteko, ikuskapen-taldearekin elkarlanean arituz eta eskatzen zaizkion ebidentzia eta erregistro guztiak emanez.

Ikuskapen bakoitzaren irismena eta sakontasuna Oreka ITk ezarriko ditu berariaz kasu bakoitzean. Kasu bakoitzean zerbitzua ematen duen erakundearekin adostutako plangintzari jarraiki egingo dira ikuskapenak.

Oreka ITek aparteko auditoretza gehigarriak egiteko eskubidea du, baldin eta hori justifikatzen duten arrazoi espezifikoak badaude.

4.4. Gertaeren jakinarazpena

Informazioaren edozein ahultasun, gertaera edo/eta segurtasun-gorabehera detektatzen denean, berehala jakinarazi beharko zaio Oreka ITren posta elektronikoaren bidez (info@orekait.com) edo zuzenean Sistemak taldeari (sistemas@orekait.com).

Edozein erabiltzailek postontzi horren bidez jakinarazi ahal izango ditu informazioaren segurtasunarekin eta arau hauetan jasotako jarraibideekin zerikusia izan dezaketen gertaerak, iradokizunak, ahuleziak eta abar, baldin eta horien berri badu.

Aipatutako postontziaren bidez jakinarazi beharko da datu pertsonalen segurtasunari eragiten dion edo eragin diezaiokeen edozein gorabehera (adibidez, zerrendak eta/edo euskarri informatikoak galtzea, beste pertsona batzuek sarbide baimendua oker erabili dutelako susmoa, segurtasun-kopietako datuak berreskuratzea...).

Aipatutako postontziak zentralizatu egiten du jakinarazitako gorabeheren bilketa, analisia eta kudeaketa.

Postontzira sartzerik ez badago, zerbitzuan bertan ezarritako komunikazio-bideak erabili beharko dira, Oreka ITeko solaskideak eman dezan segurtasun-gorabeheraren berri.

4.5. Segurtasun fisikoa

Egoitzak itxita egon beharko du eta sarrera kontrolatzeko sistemaren bat izan beharko du.

Bisiten kontrolen bat egongo da, gutxienez, sarbide publikoko eremuetan eta/edo zamalanetakoetan.

Egoitzak suteak detektatzeko eta itzaltzeko sistema egokiak izan behar ditu gutxienez, eta uholdeei aurre egiteko erresistentzia nahikoa izateko moduan eraikita egon behar du.

Segurtasun-kopiaren bat izanez gero, informazio hori gordetzen eta/edo prozesatzen duten sistemek bereziki babestutako eremu batean egon behar dute, eta eremu horretan, gutxienez, honako segurtasun-neurri hauek hartu behar dira:

- Bereziki babestutako eremuak egoitzatik aparteko sarrera kontrolatzeko sistema izan beharko du.
- Bereziki babestutako eremuetan kanpoko pertsonak sartzea mugatuko da. Sarbide hau beharrezkoa denean eta baimenduta dagoenean baino ez da esleituko, eta, betiere, baimendutako pertsonen zaintzapean.
- Kanpoko pertsonen sarrera guztien erregistroa egingo da.
- Kanpoko pertsonek ezin izango dute egon edo lanik egin bereziki babestutako eremuetan, gainbegiralerik gabe.
- Bereziki babestutako gune hauetan elikagaiak edo edariak kontsumitzea debekatuta egongo da.
- Eremu horietan kokatutako sistemek elikadura-akatsen aurkako babesen bat izan beharko dute.

4.6. Aktiboen kudeaketa

Erakunde hornitzaileak aktiboen erregistro eguneratua eduki beharko du, zerbitzua emateko erabilitako aktiboak identifikatu ahal izateko.

Zerbitzua emateko erabiltzen diren aktibo guztiek arduradun bat izan beharko dute, eta hark ziurtatu beharko du aktibo horiek erakunde hornitzaileak ezarritako gutxieneko segurtasun-neurriak dituztela, eta, gutxienez, araudi honetan zehaztutakoak izan behar dutela.

Zerbitzua emateko erabilitako aktiboen bajak jakinarazi beharko dizkio erakunde hornitzaileak Oreka ITri. Aktibo horrek Oreka ITren beste jabetza bat badu (hardwarea, softwarea edo bestelako aktiboak), Oreka ITri eman beharko zaio baja eman aurretik, Oreka ITk bere jabetzako aktiboak ken ditzan.

Aktibo batek informazio babestua izan duen guztietan, erakunde hornitzaileak aktiboen bajak gauzatu beharko ditu, informazio hori modu seguruan ezabatzen dela bermatuz, ezabatze seguruko funtzioak aplikatuz edo aktiboa fisikoki suntsituz, izan duen informazioa berreskuragarria izan ez dadin.

4.7. Segurtasun-arkitektura

Zerbitzu-erakunde hornitzaileak Oreka ITrentzat garapen-lanak eta/edo aplikazio-frogak egiten dituenean edo informazio babestuarekin, jarduera horiek egiteko inguruneek bakartuta egon behar dute beren artean, bai eta informazio babestua ostatatzen edo prozesatzen den produkzio-inguruneetatik ere.

Informazio babestua duten edo prozesatzen duten informazio-sistemetarako sarbide guztiek babestuta egon behar dute, gutxienez, horietara konektatzeko ahalmena mugatzen duen suebaki baten bidez.

Bereziki sentikorra den informazioa gordetzen edo prozesatzen duten informazio-sistemak besteetatik isolatuta egon beharko dira.

4.8. Sistemen segurtasuna

Informazio babestua biltzen edo tratatzen duten informazio-sistemek funtzionamenduari buruzko gertaera garrantzitsuenak erregistratu beharko dituzte. Jarduera-erregistro horiek erakunde hornitzailearen segurtasun-kopien araudiaren barruan egongo dira.

Informazio babestua prozesatzen edo gordetzen duten erakunde hornitzailearen sistemetako erlojuak sinkronizatuta egongo dira elkarren artean eta ordu ofizialarekin.

Zerbitzuaren erakunde hornitzaileak bermatuko du informazio babestua gordetzen edo tratatzen duten informazio-sistemen ahalmena behar bezala kudeatzen dela, eta sistema horiek baliabide gehiegi izateagatik izan ditzaketen gelditzeak edo funtzionamendu txarrak saihestuko direla.

Informazio babestua duten edo prozesatzen duten informazio-sistemak behar bezala babestuta egongo dira software maltzurren aurrean, eta honako neurri hauek aplikatuko dira:

- Sistemak egunean mantenduko dira eskuragarri dauden azken segurtasun-eguneratzeekin, garapen-, froga- eta produkzio-inguruneetan.
- Malwarearen aurkako softwarea zerbitzari eta ordenagailu pertsonal guztietan instalatu eta erabili beharko da, software maltzurrari lotutako arriskua murrizteko.
- Malwarearen aurkako softwareak beti gaituta eta eguneratuta egon beharko du.

Erakunde hornitzaileak asteroko segurtasun-kopiei buruzko araudia ezarriko du, emandako zerbitzurako garrantzitsua den edozein datu edo informazio babestuta dagoela bermatzeko.

Ematen den zerbitzua dela-eta posta elektronikoa erabiltzen den guztietan, erakunde hornitzaileak honako premisa hauek errespetatu beharko ditu:

- Ezingo da posta elektroniko bidez informazio babestua transmititu, komunikazio elektronikoa zifratuta dagoenean eta bidalketa idatziz baimenduta dagoenean izan ezik.

- Ezingo da posta elektronikoz bidali bereziki babestutako datu pertsonalak dituen informazioa (adib. osasuna), komunikazio elektronikoa zifratuta dagoenean eta bidalketa idatziz baimenduta dagoenean izan ezik.

- Zerbitzua emateko Oreka ITen posta elektronikoa erabiltzen den guztietan, gutxienez, honako printzipio hauek errespetatu beharko dira:

    - Posta elektronikoa beste lan-tresna izango da, kontratatutako zerbitzuaren helburu esklusiboarekin emana. Horrek Oreka ITri ahalmena emango dio baliabide horren babesa eta erabilera egokia zaintzeko kontrol-sistemak ezartzeko. Ahalmen hau, hala ere, pertsonen duintasuna eta intimitate-eskubidea babestuz erabiliko da.

    - Oreka IT posta elektronikoaren sistema ez da erabili behar iruzurrezko mezuak, mezu lizunak, mehatxatzaileak edo antzeko komunikatuak bidaltzeko.

    - Erabiltzaileek ez dute sortu, bidali edo birbidali behar publizitate- edo piramide-mezurik (erabiltzaile askori zabaltzen zaizkien mezuak).

Informazio babestua biltzen edo prozesatzen duten informazio-sistemetara beti autentifikatuta sartu beharko da, gutxienez pertsona-identifikatzaile bat eta hari lotutako pasahitz bat erabiliz.

Informazio babestua duten edo prozesatzen duten informazio-sistemek sarbidea kontrolatzeko sistemak izan beharko dituzte, eta sistema horiek informazio horretarako sarbidea zerbitzuko pertsonei bakarrik mugatuko diete.

Babestutako informazioa biltzen edo prozesatzen duten informazio-sistemetara sartzeko saioak automatikoki blokeatu beharko dira erabiltzaileak denbora batez erabili gabe egon ondoren.

Oreka ITek emandako softwarea erabiltzen den guztietan, arau hauek bete behar dira:

- Oreka ITren informazio-sistemetara sartzen diren pertsona guztiek emandako software-bertsioak baino ez dituzte erabili behar, eta haien erabilera-arauei jarraitu behar diete.

- Pertsona guztiek debekatua dute edozein softwareren kopia ilegalak instalatzea.
- Debekatuta dago Oreka ITk baliozkotu gabeko softwarea erabiltzea.
- Era berean, debekatuta dago Oreka ITk instalatutako edozein programa desinstalatzea.

4.9. Sareko segurtasuna

Informazio babestua zirkulatzeko erabiltzen diren sareek behar bezala kudeatuta eta kontrolatuta egon behar dute, eta ziurtatu behar da ez dagoela kontrolatu gabeko sarbiderik, ez eta konexiorik ere, horien arriskuak erakunde hornitzaileak behar bezala kudeatu ez dituenik.

Informazio babestua zirkulatzen ari den sareetan eskuragarri dauden zerbitzuak mugatu egin beharko dira, ahal den neurrian.

Oreka ITren IKT azpiegitura erabiltzeko aukera ematen duten sareek behar bezala babestuta egon behar dute, eta honako premisa hauek bete behar dira:

- Urruneko erabiltzaileak Oreka IT sarera sartu ahal izateko, aldez aurretik identifikatu eta autentifikatzeko eta sarbidea baliozkotzeko prozedurak bete beharko dira.
- Konexio horiek denbora mugatu batez egingo dira, sare pribatu birtualak edo linea dedikatuak erabiliz.
- Konexio hauetan ez da inolako komunikazio gailurik onartuko (txartelak, modemak, etab.) kontrolatu gabeko konexio alternatiboak ahalbidetzen dituena.

Informazio babestua zirkulatzen ari den sareetarako sarbideak mugatuta egon beharko du.

Informazio babestua ibiltzen den sareetara konektatutako gailu guztiek behar bezala identifikatuta egon behar dute, sareko zirkulazioak identifikagarriak izan daitezen.

Telelana sare korporatibora kanpotik sartzea dela jotzen da, eta hurrengo araudia aplikatuta erregulatzen da:

- Ezin da Oreka ITk kontrolatu gabeko gailurik erabili telelaneko jardueretarako.
- Telelana baimentzeko irizpideak ezarriko dira, lanpostuaren premien arabera.
- Sare korporatibora modu seguruan konektatzeko behar diren neurriak ezarriko dira.

- Ezarritako konexioetarako monitorizazio- eta segurtasun-auditoretza sistemak ezarriko dira.

- Premialdi-epea amaitu ondoren sarbideen eskubideak baliogabetzen direla eta gailuak itzultzen direla kontrolatuko da.

Oreka ITk emandako Interneteko sarbidea erabiltzen den guztietan, honako arau hauek ere errespetatu beharko dira:

- Internet lan tresna da. Interneteko jarduera guztiek lan-zereginekin eta -jarduerekin lotuta egon behar dute. Erabiltzaileek ez dituzte bilatu edo bisitatu behar Oreka ITren negozio-helburuaren edo eguneroko lana betetzearen euskarri ez diren lekuak.

- Sare korporatibotik Internetera sartzea sarean sartutako kontrol-gailuen bidez mugatuko da. Beste konexio-bitarteko batzuen erabilera aldez aurretik baliozkotu beharko da, eta Interneten erabilerari buruzko aurreko gogoetak bete beharko ditu.

- Erabiltzaileek ez dute Oreka ITren izena, ikurra, logotipoa edo antzeko ikurrik erabili behar Interneteko inongo elementutan (posta elektronikoa, web orriak, etab.) lan-jarduera hutsengatik justifikatuta ez dagoena.

- Datuak Internetetik edo Internetera transferitzea baimenduko da soilik negozioaren jarduerekin zerikusia dutenean. Jarduera horiei buruzkoa ez den fitxategien transferentzia debekatuta egongo da (adib. programak, multimedia-fitxategiak eta abar deskargatzea).

4.10. Sistemen erabileraren trazabilitatea

Sarbide pribilegiatuak erregistratuko dira, eta erregistro horiek gorde egingo dira, Erakundearen segurtasun-kopiei buruzko araudiaren arabera.

Sarbide pribilegiatuak gauzatzeko erabilitako sistemen jarduera erregistratuko da, eta erregistro horiek Erakundearen segurtasun-kopiei buruzko araudiaren arabera kontserbatuko dira.

Sistemen jardueran erregistratutako akatsak eta hutsegiteak aztertu egingo dira, zuzentzeko beharrezkoak diren neurriak hartuz.

4.11. Identitateen eta sarbideen kontrola eta kudeaketa

Informazio-sistema batera sarbidea duten erabiltzaile guztiek sarbide-baimen bakarra izango dute, erabiltzailearen identifikatzailea eta pasahitza izango dituena.

Erabiltzaileak izango dira sarbide baimenduaren erabilerarekin zerikusia duen jarduera ororen erantzule.

Erabiltzaileek ez dute beste erabiltzaile baten sarbide baimendurik erabilko, nahiz eta jabearen baimena izan.

Erabiltzaileek ez diote inola ere beren identifikatzailea eta/edo pasahitza beste pertsona bati jakinaraziko, ezta idatziz agerian eduki ere, ez eta hirugarren pertsonen eskura ere.

Pasahitzak 6 karaktere izan behar ditu gutxienez, eta ez du izan behar erabiltzailearen izen-abizenik edo identifikatzailerik. 45 egunean behin aldatu beharko da, eta aurreko 8 pasahitzak, gutxienez, ez dira errepikatu beharko.

Era berean, konplexuak izan behar dute eta asmatzeko zailak; beraz, lehenengo 8 karaktereetan gutxienez 4 aukera hauetako 3 konbinatuz osatuta egongo dira:

- Maiuskulak
- Minuskulak.
- Zenbakiak
- Karaktere bereziak

Pasahitzak aukeratzeko, jarraibide hauek erabiltzea komeni da:

- Ez erabili hitz ezagunik, ezta norberarekin lotu daitekeen hitzik ere, adibidez, izena.

- Pasahitzak ez du ezagutu daitekeen inolako kontzeptu, objektu edo ideiarik aipatu behar. Beraz, pasahitzetan ez dira erabili behar data esanguratsuak, asteko egunak, urteko hilabeteak, pertsona-izenak, telefonoak...

- Gakoa ia asmaezina izan beharko litzateke. Baina, aldi berean, erabiltzaileak erraz gogoratu beharko luke. Adibide on bat esaldi edo esamolderen baten akronimoa erabiltzea da.

Erakunde hornitzaileak bermatu beharko du aldian-aldian egiaztatzen dela informazio babestua horretarako behar bezala baimendutako pertsonek baino ezin dutela eskuratu.

Oreka ITren informazio-sistemetara sartzen den kasuetan, gainera, honako araudi hau ere hartu beharko da kontuan:

- Erabiltzaileek ez dute Oreka IT sistemetara sartzeko identifikatzailerik jasoko indarrean dagoen segurtasun-araudia idatziz onartzen ez duten arte.

- Erabiltzaileek beren eginkizunak betetzeko behar dituzten datu eta baliabideetarako sarbide baimendua baino ez dute izango.

- Sistemak automatikoki eskatzen ez badu, erabiltzaileak behin-behineko pasahitza aldatu beharko du sistemara baliozko sarbidea egiten duen lehen aldian.

- Sistemak automatikoki eskatzen ez badu, erabiltzaileak pasahitza aldatu beharko du gutxienez 90 egunetik behin.

- Aldi baterako sarbide baimenduak aldi labur baterako konfiguratuko dira. Epe hori amaitutakoan, sistemetatik desaktibatuko dira.

- Datu pertsonalei dagokienez, horretarako baimena duten pertsonek bakarrik eman, aldatu edo baliogabetu ahal izango dute datu eta baliabideetarako sarbide baimendua, fitxategiaren arduradunak ezarritako irizpideen arabera.

- Erabiltzaile batek bere sarbide baimendua beste pertsona bat erabiltzen ari delaren susmoak baditu (pertsona erabiltzailearen identifikatzailea eta pasahitza), pasahitza aldatu beharko du eta Oreka ITren postontzi elektronikoan gertakaria jakinarazi beharko du.

4.12. Aldaketen kudeaketa

IKT azpiegituran egiten diren aldaketa guztiak kontrolatuta eta baimenduta egon beharko dira, eta bermatu beharko da ez direla kontrolatzen ez diren osagaiak.

Zerbitzua emateko erabiltzen den erakunde hornitzailearen IKT azpiegituran sartutako osagai berri guztiek behar bezala funtzionatzen dutela eta sartu zireneko helburuak betetzen dituztela egiaztatu beharko da.

4.13. Aldaketen kudeaketa teknikoa

Egiten diren aldaketa guztiak formalki ezarritako eta dokumentatutako prozedura bati jarraiki egin beharko dira, aldaketa egiteko urrats egokiak jarraitzen direla bermatzeko.

Aldaketak kudeatzeko prozedurak IKT azpiegituran ahalik eta aldaketa gutxien egitea bermatu beharko du, ezinbestekoak diren aldaketetara mugatuz.

Aldaketa guztiak frogatu beharko dira produkzio-ingurunean hedatu aurretik, IKT azpiegituraren funtzionamenduan eta segurtasunean albo-ondoriorik edo aurreikusi gabeko ondoriorik gertatzen ez dela egiaztatzeko.

Erakunde hornitzaileek eskaneatu eta arindu egin beharko dituzte zerbitzua emateko erabilitako azpiegiturek dituzten ahulezia teknikoak, eta osagai kritikoekin lotutako guztien berri eman beharko diote Oreka ITri.

4.14. Segurtasuna Garapenean

Kanporatutako softwarea garatzeko prozesu guztia Oreka ITk kontrolatu eta gainbegiratuko du.

Identifikatzeko, autentifikatzeko, sarbide-kontrolerako, auditoretzarako eta osotasunerako mekanismoak sartuko dira softwarearen diseinu-, garapen-, ezarpen- eta eragiketa-bizi-ziklo osoan.

Softwarearen zehaztapenek berariaz jaso beharko dituzte kasu bakoitzean bete beharreko segurtasun-baldintzak.

Garatzen den softwareak sarrerako datuen baliozkotzeak izan behar ditu, datuak zuzenak eta egokiak direla egiaztatzeko eta exekutatu daitekeen kodea sartzea saihesteko.

Aplikazioek garatutako barne-prozesuek beharrezko baliozkotze guztiak izan beharko dituzte, informazioaren usteltzea ez dagoela bermatzeko.

Beharrezkoa den guztietan, autentifikaziorako eta integritate-kontrolerako funtzioak gehitu beharko dira aplikazioen osagaien arteko komunikazioetan.

Aplikazioek eskaintzen duten irteera-informazioa mugatu beharko da, eta informazio egoki eta beharrezkoa soilik eskaintzen dela bermatu beharko da.

Aplikatiboen iturburu-koderako sarbidea zerbitzuko pertsonek baino ez dute izan behar.

Proben ingurunean datu errealak behar bezala disoziatu direnean soilik erabiliko dira, edo, bestela, aplikatutako segurtasun-neurriak ekoizpen-ingurunean daudenen baliokideak direla berma daitekeenean.

Aplikazioen probak egitean, egiaztatu behar da ez dagoela kontrolatu gabeko informazio-hutsunerik, eta ezarritako bideetatik aurreikusitako informazioa baino ez dela ematen.

Berariaz onartutako softwarea bakarrik transferituko da produkzio-ingurunera.

Web-zerbitzuei dagokienez, Owasp-en Top 10-aren kudeaketa hartuko da kontuan.

4.15. Kontingentzien kudeaketa

Zerbitzuak kontingentziak egonda ere zerbitzu hori ematea ahalbidetzen duen plana izan beharko du.

Aurreko plana garatu beharko da zerbitzuan etenak eragin ditzaketen gertaeren eta gertatzeko duten probabilitatearen arabera.

Erakunde hornitzaileak kontingentzia-plana bideragarria dela frogatzeko modua izan beharko du.

5. Jarraipena eta kontrola

Aipatutako baliabideak behar bezala erabiltzen direla zaintzeko, egokitzat jotzen diren mekanismo formal eta teknikoen bidez, Oreka ITek egiaztatuko du, bai aldian behin, bai segurtasun-edo zerbitzu-arrazoi espezifikoengatik komeni denean.

bai euskarari ziurtagiria | Zerbitzua euskaraz

oreka i.t.

corporate balance

ARABA · Zumar Hiribidea 1, IV Eraikina · 243 bulegoa · 01013 | Vitoria-Gasteiz · 945 067 219
BARTZELONA · Passeig Mossèn Jacint Verdaguer 40, 2.solairua · 08700 | Igualada · 938 053 767
BIZKAIA · Ibaiondo Plaza 1, 2.solairua · 207 bulegoa · 48940 | Leioa · 944 143 983
GIPUZKOA · Pillotegi Bidea 2, 3.solairua · 301 bulegoa · 20018 | Donostia · 943 065 922
NAFARROA · Mutiloako Industrialdea, E kalea 9, 1.A · 31192 | Mutilva · 948 151 286

orekait.com
orekait@orekait.com

SAP Gold Partner · salesforce · Microsoft Cloud Solution Provider