AURKIBIDEA

NORI BANATUA:					
Presidenteari	Zuzendari nagusiari	Eragiketa, Merkataritza, Logistika eta Zaintza Estrategikoko zuzendariari	Idazkari nagusiari	Talentu, Antolaketa eta Marketin Korporatiboko zuzendariari	Ekonomia eta Finantzetako zuzendariari eta Europako Funtsen Koordinazioari
Sailetako buruei	Dibisioetako buruei	Unitateetako buruei			
NORK EGINA: Zibersegurtasuneko arduradunak		NORK BERRIKUSIA: Eraldaketa Digitaleko buruak		NORK ONARTUA: Sistemak eta Kudeaketa Kontroleko buruak	

1.- HELBURUA ETA IRISMENA

Prozedura honen xedea hau da: bermatzea betetzen dela indarrean den informazioari buruzko segurtasun-araudia eta, horrekin batera, behar diren mekanismoak ezartzea BPAk kudeatzen duen informazioaren kalitatea eta eskaintzen diren zerbitzuen jarraitutasuna ziurtatzeko.

Informazioaren segurtasuna prozesu integraltzat hartzen da, informazio-sistemei dagozkien langileek eta elementu tekniko, material eta antolakuntzakoek osatua. Hori dela eta, hauei aplikatu behar zaie jarraibide hau:

- BPAren informazio- eta telekomunikazio-sistema guztiei.
- Administrazio elektronikoko prozesu guztiei.
- Herritarrei, erakundeei edo enpresei zerbitzu ematen dieten prozesu guztiei.
- Aipatutako prozesuekin loturaren bat duten BPAko eta hirugarrenetako langile guztiei.

Barne hartutako informazioaren segurtasunari buruzko arauketak eta estandarrak:

- Datu Pertsonalak Babesteko Legea.
- Araua ISO/IEC 27001.
- Araua ISO/IEC 27002.
- Datuak Babesteko Erregelamendu Orokorra.

2.- GARAPENA

2.1.- DEFINIZIOAK

- Euskarri informatikoak: Fitxategiak kudeatzeko prozesuetan kopiak edo tarteko urratsak egiteko erabiltzen diren datuak grabatzeko bitartekoak (diskoak, disketeak, CD-ROMak, DVDak, zintak, memoria ateragarriak, eramangarriak, etab.).
  Datuak transferitzeko euskarritzat hartuko dira edozein sare telematikoren bidez bidaltzen edo jasotzen diren mezuak eta haiek izan litzaketen eranskinak.

- Segurtasuneko Batzorde Korporatiboa: Talde horren osaera eta eginkizunak IGI 01.02/04 "Informazioaren segurtasuneko funtzioak eta obligazioak" jarraibideak deskribatzen ditu.

- Informazioaren segurtasunaren arduraduna (CISO): (Chief Information Security Officer: Informazioaren segurtasunaren ofizial nagusia). Informazioaren segurtasuna hobetzeko politika, prozedura eta jardueren planifikazio, garapen, kontrol eta kudeaketaren arduradun gorena da, eta konfidentzialtasuna, osotasuna eta eskuragarritasuna ditu bere jardueraren ardatz nagusi.

- Informazioaren arduraduna: Informazioaren segurtasun-mailak ezartzen dituena, Segurtasun Eskema nazionala (SEN) eta Datuak Babesteko Erregelamendu orokorra (DBEO) arautzeko indarrean den legediaren arabera.

- Zerbitzu-arduraduna: Zerbitzuen segurtasun-mailak ezartzen dituena, indarren den legediaren arabera.

- Informazio Sistemen arduraduna: (aurrerantzean, sistemaren arduraduna). Informazio-sistemak Segurtasun Politikaren irizpideetara etengabe egokituta edukitzearen arduraduna.

- Informazio Sistemen Segurtasunaren administratzaileak: (aurrerantzean, segurtasun-administratzaileak). Sistemaren segurtasuna administratzeko ardura dutenak.

- Erabiltzaileak: **BPA**ko langile guztiak.

- Fitxategia: Datuak antolatzeko multzo oro, edozein dela ere haiek sortzeko, biltegiratzeko, antolatzeko edo eskuratzeko modua edo modalitatea.

- Datu pertsonalak: Identifikatuta dauden edo identifika daitezkeen pertsona fisikoei buruzko informazio numeriko, alfabetiko, fotografiko, akustikoa edo bestelakoa.

- Informazioaren tratamendua: Datuak biltzeko, grabatzeko, gordetzeko, egiteko, aldatzeko, kontsultatzeko, erabiltzeko, blokeatzeko edo ezabatzeko edozein eragiketa edo prozedura tekniko.

- Aldaketa: Onespena, euskarri edo erreferentzia-lerro bat duen hardwarea, sarea, softwarea, ingurunea, sistema, lan-estazioa edo atxikitako dokumentazioa gehitzea, aldatzea edo ezabatzea.

- Aldaketen kontrola: Aldaketa guztiak kontrolatzen direla ziurtatzea, barne direla aldaketaren aurkezpena, azterketa, erabakitze-prozesua, onespena, inplementazioa eta inplementazioaren ondorena.

- Planifikatutako aldaketen zerrenda: Inplementatzeko onetsitako aldaketa guztien zerrenda, eta proposatutako datak.

- Aldaketa-erregistroa: Aldaketak eragiten dien konfigurazio-elementuen xehetasunak, aldaketaren xehetasunak eta baimena jasotzen dituen erregistroa.

- Aldaketa-eskaria: Zerbitzu edo azpiegituraren bateko edozein konfigurazio-elementutan aldaketaren bat egiteko eskariaren xehetasunen erregistroa.

- Informazioaren segurtasun-gorabeherak: Informazioaren segurtasuna xede duen osagaietakoren bati edo gehiagori eragiten dien gertakaria: benetakotasuna, konfidentzialtasuna, osotasuna, eskuragarritasuna eta trazabilitatea.

- Dagokiona edo interesduna: Tratatu beharreko datuen pertsona fisiko titularra.

- Bereizte-prozedura**:** Metodo horren bidez, lortzen den informazioa ezin zaio lotu identifikatu den edo identifika daitekeen pertsonari.

- Datuen blokeoa**:** Datuak identifikatzea eta gordetzea, trata ez daitezen.

- Interesdunaren baimena**:** Interesdunak bere datuak tratatzea baimentzeko egiten duen borondatezko adierazpen libre, garbi, espezifiko eta informatua.

2.2.- INFORMAZIOAREN SEGURTASUN-POLITIKAREN PRINTZIPIOAK

Hauek dira BPAko segurtasun-politikaren printzipioak:

- Babestuta egon behar dute informazioak eta zerbitzuek hauek galtzeko arriskutik: eskuragarritasuna, konfidentzialtasuna, osotasuna, benetakotasuna eta trazabilitatea
- Eskuragarri egon behar dute informazioak eta zerbitzuak, eta, behar den guztietan, utzi egin behar haiek eskuratzen eta erabiltzen, dagozkien baimenak tarteko direla.
- denon ardura da informazioaren segurtasuna. BPAren informazioa eskuragarri duten guztiek babestu egin behar dute; hori dela eta, dagokien trebakuntza eta kontzientziazioa jaso behar dute.
- Behar bezala babestu behar dira informazioa gordetzen, garraiatzen edo prozesatzen den aktibo guztiak (azpiegiturak, euskarriak, sistemak, komunikazioak eta abar).
- Ezartzen diren segurtasun-neurriek proportzionalak izan behar dute babesten duten informazioaren garrantziarekiko eta hari eragin dakizkiokeen kalte edo galerekiko. Une oro bete behar dira Segurtasun eskema Nazionalaren segurtasun-neurriak, gutxienez.
- Behar bezala jakinarazi eta tratatu behar dira segurtasun-gorabeherak.
- Etengabe kontrolatu behar da informazioaren segurtasuna eta, aldian behin, berrikusi.
- Bestalde, datu pertsonalen tratamenduak bat etorri behar du, beti, une bakoitzean aplikatzekoak diren legeekin eta BPAren jarraibide eta prozedurekin.
- Dagozkion neurriak hartu behar dira politika hori betearazteko.
- Politika alderdi interesdunen eskura jarriko da, posta elektroniko bidez.

2.3.- INFORMAZIOAREN SEGURTASUNA ANTOLATZEA

Segurtasuneko Batzorde Korporatiboak kudeatu behar du informazioaren segurtasuna.

Sistema batek jarraibideetan zehazten eta esleitzen ditu segurtasunari dagozkion funtzioak eta ardurak:

- IGI 01.02/04 "Informazioaren segurtasunari dagozkion funtzioak eta obligazioak"
- IGI 01.02/05 "Informazio-sistemen erabiltzaileen funtzioak"

Batzorde hori arduratuko da informazioaren segurtasunaren jarraipena egiteaz eta, horrela, kudeaketa-sistema hobetzeaz

Zibersegurtasuneko arduradunak beharrezko bitartekoak, baliabideak eta gaitasun teknikoak izango ditu gainbegiratzeko, egiaztatzeko, arriskuak aztertzeko, auditoria teknikoa egiteko eta gorabeherei erantzuteko eginkizunak behar bezala betetzeko, eta bere independentzia operatiboa bermatuko du, Segurtasun Eskema Nazionalean eta Informazioaren Segurtasuna Kudeatzeko Sisteman ezarritakoaren arabera.
Erakundeak ziurtatuko du eginkizun horrek funtzio horiek betetzeko beharrezkoak diren sarbide-, informazio- eta tresna teknikoen maila dituela, ISKSk ezarritako kontrolak, gainbegiratzea eta trazabilitatea alde batera utzi gabe.

2.4.- INFORMAZIOAREN SEGURTASUN-POLITIKAN SARTZEN DIREN PROZESUAK.

Prozesu horiek erakunde osoak jakinarazi, ulertu eta bete beharko ditu, informazioaren segurtasunari aplika dakizkiokeen baldintzak ba.

ARRISKUAK KUDEATZEA

Politika honen mendeko sistema guztiei arriskuak eta mehatxuak aztertzeko prozesu bat ezarri behar zaie. Azterketa errepikatu behar da:

- urtean behin, gutxienez
- erabiltzen ari den informazioa aldatzean
- ematen diren zerbitzuak aldatzean
- segurtasun-gorabehera larriren bat gertatzean
- kalteberatasun larriak hautematen direnean

Informazioaren Segurtasun Arduradunak (ISA) "Arriskuen azterketa- eta kudeaketa-txostena" prestatu behar du. **Segurtasuneko Batzorde Korporatiboak** onetsi behar du txostena, zeina aintzat hartu behar duten informazio- eta zerbitzu-arduradunek.

INFORMAZIOAREN SAILKAPENA

Sistema batek sailkatzen du BPAk kudeatzen duen informazioa, sentikortasunaren arabera, IGI 01.02/06 "Informazioaren sailkapena" jarraibidean.

INFORMAZIO-ATZIPENAREN KONTROLA

Informazio-sistemen erabiltzaileek beren jarduera profesionalerako behar dituzten informazioa eta funtzionalitateak bakarrik eskura ditzakete, IGI 01.02/07 "Informazio-atzipenaren kontrola"-ren arabera.

SEGURTASUNAREN PLANIFIKAZIOA

Jarraibide hauek arautzen dute:

- IGI 01.02/08 "Informazio-sistemen segurtasun fisikoa"
- IGI 01.02/09 "Informazio-sistemen segurtasun logikoa"
- IGI 01.02/14 "Segurtasun-kopiak eta euskarrien kudeaketa"

DATU PERTSONALEN BABESA

Jarraibide hauek arautzen dute:

- IGI 01.02/11 "Fitxategi pertsonalen kudeaketa"
- IGI 01.02/12 "Sarbide-kontroleko eta bidezaintzako datuen babesa"
- IGI 01.02/13 "Datuen babesa: eskubideak"

SOFTWARE-GARAPENA

Softwarea garatzeko prozedura bat ezarriko da, programa eta aplikazio informatikoak garatu, probatu eta jartzean ahalik eta arrisku gutxiena izateko.

IGI 01.02/10 "Software-garapena" jarraibideak arautzen du jarduera.

SEGURTASUN-GORABEHERAK KUDEATZEA

Informazioaren alorreko gorabeherak (zibergertakariak) detektatu, aztertu eta kudeatzeko prozedura bat ezarriko da, IGI 01.02/15 "Segurtasun-gorabeheren kudeaketa" jarraibidearen arabera.

JARRAITUTASUNAREN KUDEAKETA

IGI 01.02/16 "Jarraitutasunaren kudeaketa" jarraibidearen arabera.

2.5.- KONTROLA, BERRIKUSPENA ETA AUDITORETZA

Barne-auditoretzak egiten zaizkio Segurtasuna Kudeatzeko Sistemari, PGI 03.03 "Barne- eta kanpo-auditoretzak" jarraibidearen arabera.

2.6.- HELBURUAK EZARTZEA ETA ETENGABEKO HOBEKUNTZA

Informazioaren Segurtasuna Kudeatzeko Sistema (ISKS) etengabeko hobekuntzako ikuspegi baten arabera kudeatzen da, sistemaren eraginkortasuna eta bilakaera bermatzera bideratutako helburuen aldizkako definizioan, jarraipenean eta ebaluazioan oinarrituta, 01.03 PGIan "Helburuak ezartzea" ezarritakoaren arabera. Era berean, hobekuntza-ekintzen identifikazioa, kudeaketa eta jarraipena 04.01 "Hobekuntza-ekintzen kudeaketa" PGIaren arabera egiten da, sistemaren jarduna indartzeko eta erakundearen beharretara eta aplikatu beharreko eskakizunetara etengabe egokitzen dela bermatzeko

3.- ERREGISTROA ETA ARTXIBOA

KODEA	IZENA	ERREGISTROAREN ARDURADUNA	ARTXIBATZEKO METODOA	TOKIA	ZENBAT DENBORA GORDE BEHAR DEN
----------	Arriskuen azterketa- eta kudeaketa-txostena	CISO	Indarrean zegoen azkena	Sistema informatikoa	Iraunkorra

4.- ERREFERENTZIA-DOKUMENTUAK

Ez dagokio.