TOLOSALDEA

GOIMAILAKO L. H. INSTITUTUA

INFORMAZIO SISTEMA MODU EGOKIAN ERABILITZEKO PRAKTIKA ONEN ESKULIBURUA

BERTSIO KONTROLA				
Bertsioa	**Data**	**Egilea(k)**	**Berrikuspena**	**Oharrak**
000	08/08/07	ISSGunea	ISS Gunea eta Adigunea	Zirriborroa
001	10/09/07	issGunea	issGunea eta adigunea	
Onartua		ISS Gunea		

AURKIBIDEA

1 Sarrera

Hemen aurkezten den **Informazio Segurtasunaren Kudeaketarako Eskuliburuak**, erakundearen aktiboen eta prozesuen konfidentzialtasuna, osotasuna eta erabilgarritasuna bermatzeko ISKSren betebeharrak eta kontrolak ezartzen ditu.

Eskuliburuak honako helburuak ditu

- Segurtasunean gertatu daitezkeen intzidenteak aurrezaintzea.
- TGLHIren ikasle eta irakasleen segurtasuna mantentzea eta bermatzea.

1.1 Ezarpena

Hemen aurkezten den eskuliburuak, ISO 17799:2005 ezartzen dituen betekizun guztiak barneratzen ditu.

Eskuliburua, TGLHIn identifikatuak dauden **aktiboei** eta baita ere **ikasle eta kanpoko langile guztiei aplikatzen zaie**

Fisikoki, TGLHI barnean identifikatuak dauden aktiboen kokapenak eta zerbitzuak kudeatzen diren lekuak barneratuak daude eskuliburu honetan.

2 Erreferentziazko Araudiak

2.1 Araudi Orokorrak.

- ISO/IEC 17799:2005
- BS7799-2:2002 Information security management systems – Specification with guidance for use.
- Norma UNE 71502

2.2 Betebeharreko legeak

- Abenduaren 13ko 15/1999 Lege Organikoa, Izaera Pertsonaleko Datuak Babesteari buruzkoa
- 994/1999 Errege Dekretua, ekainaren 11koa; horren bitartez, datu pertsonalak dituzten fitxategi automatizatuen segurtasun-neurriak ezartzeko Erregelamendua onartu zen.
- Ekainaren 11ko 34/2002 Legea.

3 Datu pertsonalen babesa eta informazio segurtasunaren kudeaketa

3.1 Zertarako informazio segurtasuna kudeatzeko sistema bat?

1. Kalitatezko **zerbitzua bermatu**, informazioaren segurtasuna zutabeetako bat izanik, barne prozesuak hobetuz, Lanbide Heziketaren esparruan **erreferentzi bilakatzea Euskal Herrian eta Europan**.
2. Bezeroen **konfiantza** lantzen jarraitu, kudeaketa sistemak segurtasunez eskainiz

Hau lortu ahal izateko ezinbestekoa izango da erakundean, informazio aktiboen **konfidentzialtasuna**, **osotasuna** eta **erabilgarritasuna** bermatzea.

TGLHIak segurtasun helburu estrategiko bezala honako hauek sailkatu ditu:

1. **Segurtasuna kalitatearekin bat**, Erakundearen helburu estrategikoak lortzeko bide bezala hautatzea.
2. **Adigunearen konpromisoa** segurtasunarekiko nabarmentzea. ISS Guneari eskaintzen dion babesa eta laguntza agerian utziz.
3. Kontrol metodologikoak, teknikoak eta kudeaketarako beharrezkoak direnak definitzea, garatzea eta ezartzea, konfidentzialtasunaren, osotasunaren, eta erabilgarritasunaren maila **heldutasun egoki** batean izateko.
4. **Adostasun legalarekin** bat etortzea. Datu Pertsonalen Babeserako Lege Organiko, Jabetza Intelektualaren legea eta Informazio Gizartearen Zerbitzu Legea eta Segurtasunarekin bat doazen beste guztiak betetzea.

5. "**Segurtasunaren kultura**" sortu eta bultzatzea, bai barneko lankideekiko, bai bezero eta hornitzaileen aurrean. Horretarako, ISS Guneak segurtasunean etengabeko formazio kontzientzia garatuko du, formazio saioak antolatuz, barne eta kanpo segurtasun akordioak sinatuz eta manualak idatziz.
6. **Kanpoko erakundeekin**, (Teknika adibidez), segurtasun proiektuak eta ekimenak sustatuko ditu, besteak beste Informazioaren Gizartea garatzen laguntzeko.
7. Informazioaren Segurtasuna, **etengabeko hobekuntza** ereduarekin tratatzea.

TGLHIn ezarritako ISKS, politika orokorraz, barne araudiaz, prozedura teknikoaz eta argibide teknikoaz osatuta dago.

3.2 Eta LOPD?

LOPDren helburua, pertsona fisikoek bere **datu pertsonalekiko** dituen **eskubideak** defendatzea da. LOPDa erakunde juridiko guztiei aplikatzen zaie eta erakundeek hainbat zeregin izango dituzte legeak ezartzen dituen betebeharrak betearazteko.

- Pertsonek bere datuak kontrolatzeko eta datuen gainean erabakiak hartzeko eskubidea izango dute.
- 994/1999 Errege Dekretua, ekainaren 11koa; horren bitartez, datu pertsonalak dituzten fitxategi automatizatuen segurtasun-neurriak ezartzeko Erregelamendua onartu da. Erregelamendu honek hainbat segurtasun neurri ezartzen ditu, eta erakunde guztiek bete beharko dituzte.
- TGLHIk lehen aipatutako Erregelamendua betetzeko, Eusko jaurlaritzako Hezkuntza Sailari Segurtasun Dokumentua eskatu dio.
- TGLHIk legearekin ados egoteko, zure lankidetza behar du.

3.3 Gogoratu…

- TGLHIk Segurtasunari buruzko hainbat araudi garatu dituela. Zure zereginen barruan, **araudi hauek errespetatzea** egongo da.
- Segurtasun neurriak, politikak, araudiak eta prozedurak barneratzen dituen **dokumentazioa eskuragarri** duzula.
- Erakunde barruan tratatzen diren **datu pertsonalak sekretuak** direla eta modu horretan tratatu beharko direla.
- Edozein **intzidente** gertatzen baldin bada, ISS Guneari **komunikatu** behar zaiola. Komunikazioaren prozedura, TGLHIren intraneten barnean publikatuta dago.

4 Zure eskubide eta betebeharrak

4.1 Zure eskubideak

- Zure zereginak aurrera eramateko, **eskuragarri duzun informazioa** erabiltzea.
- Zure zereginekin erlazionatuta dauden segurtasunari buruzko **araudiak ezagutzea.**
- Zure eguneroko lana bete beharko duzu **intimitatea eta pribazitatea errespetatuz**.

4.2 Zure betebeharrak

- Segurtasunari buruz ezarritako **araudiak errespetatzea**.
- Erakundeak zure esku jartzen dituen **prozedurak betetzea**.

4.2.1 **Informazio Sistemen erabilera**

TGLHI izango da erabiltzaileak erabiltzen dituen **ordenagailuen jabea** eta honen ondorioz, informazio sistemen konfidentzialtasuna, osotasuna eta erabilgarritasuna bermatzeko ezarrita dauden neurri teknikoak errespetatu beharko dira.

Informazio sistemen erabilera eta ekoizpena kudeatu ahal izateko, TGLHIk informazio sistemen erabilera **ikuskatzeko eskubidea** izango du, beti ere erabiltzailearen intimitatea bermatuz.

TGLHIren baliabideak ezin dira erabili ilegalak edo irabazizkoak diren helburuekin

Ikasle, irakasle eta langile guztiek TGLHIn ezarrita dauden politika eta araudi guztiek jakin beharko dituzte.

Erabiltzaileek ezingo dute Sare Kudeatzailearen baimenik gabe bere ordenagailuaren **segurtasun neurririk desaktibatu**.

TGHLIko erabiltzaileek honako betebeharrak izango dituzte:

- "**Antibirus**"aren ezarpenerako eta eguneraketarako, Sare Kudeatzailearen argibideak jarraitzea.
- Gertatzen diren **intzidenteen komunikazioa** egitea.
- Laneguna bukatzerakoan ordenagailua behar bezala **itzaltzea**.

Hala ere, erabiltzaileek ezingo dituzte honako ekintzarik egin:

- TGLHIren ordenagailuak, ekipoak, programak, etab. **txikitzea**.
- Informazio sistemak gehiegi erabiltzeagatik, erabiltzaileen Informazio Sistemetarako sarrera **oztopatzea**,.
- Erabiltzaileak dituen **pribilegioak ugaritzea**.
- Ez baimendutako SW ezartzea.
- Legalak diren programak kentzea.
- Edozein ekipo edo ordenagailua baimenik gabe lekuz aldatzea.

4.2.2 **Pasahitzak**

- Zure pasahitzaren konfidentzialtasunaren arduraduna zu izango zara.
- Beste pertsona batek, zure pasahitza jakin duenaren susmoa baduzu, sare kudeatzaileari jakinarazi beharko diozu, zure pasahitza aldatu dezan.

- Pasahitzik ez idatzi ikus daitekeen lekuetan.
- Sistemara sartzen zaren lehen momentuan pasahitza aldatu beharko duzu.
- Pasahitz zailak erabili beharko dituzu.

4.2.3 **Informazioaren babespena eta klasifikapena**

TGLHIak eskura duen informazioa, nahiz erakundeak sortutakoa izan, nahiz kanpotik jasotakoa izan, bere konfidentzialtasunaren arabera babestuko du.

Berdin du ze euskarritan datorren, (papera, diskoan, etab.), ze sistemek prozesatzen duten (ordenagailuak, zerbitzariek, etab..) edo ze bide erabiltzen den hau zabaltzeko (hitza, posta elektronikoa, etab), informazioa neurri eraginkorren bitartez babestu behar da sortzen denetik deusezten den arte.

Barneko zein kanpoko informazioa 2 multzotan sailkatuko da:

Sailkapen Gida	
Id.	**Multzoa**
K	Konfidentziala
P	Publikoa

Informazio Konfidentziala: Kritikoa eta sarrera mugatua duen informazioa. Konfidentziala den informazioa galtzea edo publiko egiteak erakunderen gain eragin nabarmena izango luke.

Adibidez: Ikasle eta irakasleen espedienteak, Ikasleen notak eta ebaluaketak, sistema ezberdinetara sartzeko pasahitzen fitxategia, etab.

Informazio konfidentzialak segurtasun maila altuago bat eskatzen du.

Multzo honen barruan erakundearen prozesu kritikoei lotua doan informazioa sartuko genuke. Beraz, langile eta ikasleen txostenak, pasahitzak, barne informe eta memoriak, sistemen konfigurazioa, etab..

Sailkapen zehatzago bat dokumentu honen bukaeran aurki genezake

Informazio Publikoa: Multzo honetan, bestetik kanpo gelditzen den guztia sartzen da. Konfidentzialarekin duen diferentzia, honek duen eraginean datza. Hau kanporatzen bada, ez du barne prozesuetan kalterik sortuko.

Publikoa egin nahi den informazio guztia bertan sartzen da.

Eranskina I-ean informazioari ematen zaion tratamendua argi azaltzen da.

4.2.4 **Segurtasun kopiak eta euskarriak**

- ISS Guneak ordenagailuen memorian gordetako informazioa ez du bermatzen segurtasun kopien bitartez.
- Honen ondorioz erabiltzaileek informazio guztia sarean gordetzeaz arduratuko dira.

4.2.5 **Segurtasun fisikoa**

- Inprimagailuak, paper konfidentziala edo edozein beste informazio konfidentziala leku seguru batean gordeta egon beharko dira.
- Erabiltzaileak bere lekua uzterakoan, bermatu beharko du bere ordenagailua itzalita dagoela eta bere **mahai gainean** ez dagoela inolako informazio konfidentzialik.

4.2.6 **Gertakarien kudeaketa**

Erabiltzaileek, iTolosaldeak Mantenurako duen atalaren bitartez, komunikatuko ditu **gertakariak**.

Astean zehar eta lan ordutegian bada Intraneta erabiliko da, ordutegi horretatik kanpo bada, telefonoz komunikatuko da.

Nahiz eta erregistratzeko, Intraneta erabili behar, Segurtasun Arduradunak PR-8301 EZ-ADOSTASUN PROZEDIMENDUA martxan jarriko du.

Segurtasun gertakaria, informazioaren segurtasuna mehatxatzen duen edozer gauza izango da. Datuen konfidentzialtasunaren, osotasunaren, erabilgarritasunaren galera orokorrean.

Beraz, gertakari hauen aurrean jarrera, honen berri ematea izango da beti. Horrek gertakarien errepikapena saihestuko luke.

Gertakaria zehazki deskribatuko da Intraneteko formularioa erabiliz, eta hauen erregistroa mantenduko da.

4.2.7 **Kode maltzurra**

Zure informazio sistema zaintzeko birus, zizare, “troyano” edo beste edozein malwareren kontra, honako aspektuak kontutan hartu beharko dira.

- Erabiltzaile guztiek, ezezagun batetik jasotako mezu elektronikoetan **erantsita dauden artxiboekin**, kontu handia izan beharko dute. Kasu guztietan artxiboen garbitasuna egiaztatu beharko da.
- **Internetik, USBtik** edo beste euskarri batetik ordenagailura artxiboren bat pasatzen baldin bada, “antibirusa” pasatu beharko da.
- Edozein “**anomalia**” aurkitzen baldin bada, ekipoa itzali eta saretik deskonektatu eta intzidentzia, sare kudeatzaileari jakinarazi beharko zaio.

4.2.8 **Mezu elektronikoen erabilera**

- Mezu elektronikoa ez da guztiz segurua. Honen ondorioz erabiltzaileek kontutan hartu beharko dute mezu elektronikoen segurtasun falta.
- Mezu elektronikoetan konfidentzialtasun klausulak barneratu beharko dira. (Ikus e*ranskina II*).
- Mezu elektroniko baten barruan, informazio konfidentziala den fitxategi bat eransterakoan, honako neurriak kontutan hartu beharko dituzu:
    - Informazioaren jabeari baimena eskatu beharko diozu.

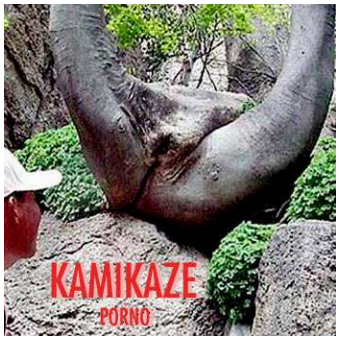
Orokorrean erabiltzaileek, honako aktibitateak ezingo dituzte egin:

- Ez eskatutako e-mail masiboak bidaltzea (***SPAM***).
- Mezu elektronikoak **faltsutzea**.
- **Baimenik gabe**, beste baten mezu elektronikoak irakurtzea, aldatzea, ezabatzea, etab.
- Lege kontrakoak, ospea kentzekoak, edo diskriminatzaileak diren mezuak bidaltzeak.
- Interneta erabiltzea jolasteko, apustuak egiteko, musika / pelikulak deskargatzea edo TGLHIrekin aktibitatea zerikusia ez duen aktibitateak egitea.

4.2.9 **Internetaren erabilera**

TGLHIren erabiltzaile bakoitzak sare publikoaren erabileraren ardura izango da.

- "Txat" tresnak erabiltzea debekatuta dago.
- Debekatuta dago lege kontrako, pornografia edo biolentziari buruzko Web orrietan sartzea.
- Internetik fitxategiak jaisterakoan, jabetza intelektual eta industriala errespetatu beharko da.
- TGLHIk, erakunde barruan egiten diren komunikazio elektroniko guztien berrikuspena egiteko eskubidea dauka, beti ere intimitate pertsonala errespetatuz.



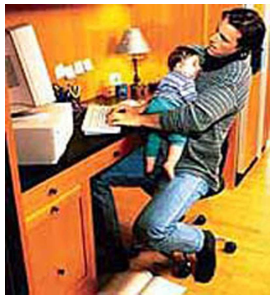
Interneten nabigatzerakoan, honako gomendioak jarraitu beharko dira:

- Web zerbitzariak erregistratu dezakete zuk bisitatutako web orriak zure profil bat ateratzeko.
- Ez seguruak diren hornitzaileetan, transakzio komertzialak ez egitea gomendatzen da.

4.2.10 **Telelana eta ordenagailu garraiagarriak**

TGLHIn dauden ordenagailu garraiagarriek, atzipen kontrolak ezarrita izan beharko dituzte, beti TGLHI barruan dagoen politikaren arabera.

- Gogoratu, TGLHIn dagoen informazio konfidentziala ezin dela erakundetik atera eta ateratzen baldin bada, ateratzen den euskarria zifratuta egon beharko dela.
- TGLHIra kanpotik informazioa sartzeko, beti erakundeak hornitutako sistemen bitartez egin beharko da.



4.3 Sare kudeatzailearen erantzukizunak eta betebeharrak

Sare kudeatzailearen zereginak hurrengoak dira:

- TGLHIren **informazio sistema babeste**a lapurreta eta min fisikoaren aurrean.
- HW eta SW ari buruzko **lizentzia** eta akordioak **errespetatzea**.
- Erakundearen informazio babesteko jarri behar diren **segurtasun neurriak** ezartzea eta kudeatzea, beti ere babestu behar den informazioa eta aktiboaren kritikotasuna kontutan hartuz.
- Zerbitzuen erabilerari buruzko **politikak** eta gomendioak zabaltzea.
- Informazio eta sistemen **berreskurapen** prozedurak bermatzea.
- Erakundeak onartutako segurtasun neurrien ezarpena aurrera eramatea.

5 Eranskinak.

5.1 Eranskina I.

MOTA	SARRERA BAIMENDUA	BILTEGIRATZEA	POSTAZ, POSTA ELEKTRONIKOZ, FAXEZ TASMISIOA	HITZEZ	DEUSEZTAPENA
KONFIDENTZIALA	a) ISS Gunea b) Adigunea c) Segurtasun Arduraduna d) Zuzendaria e) Alorburuak f) Langileak g) Konfidentzialtasun akordioa sinatu duten kanpokoek	• Papera: Parera edonola uztea ez da komenigarria. Eskuragarri egon behar ez duenean gordeta mantendu. • Euskarri elektronikoak: Atzipen kontrola erabiltzaile eta pasahitzetan oinarritua. .	Kanpora trasmisioa: • Fax: jaso behar duenak jasoko duenaren ziurtasuna eta zuzentzen zaionari iritsi zaionaren berma. • Posta: mezulari onartua • e-mail: Konfidentzialtasun klausulekin Barne trasmisioa: • Eskura edo posta elektroniko bitartez	Kanpoko bisitak daudenean, eta informazio konfidentziala hitzez tratatzen denean, ingurukoek entzun ez dezaten transmitituko da. Ahal bada ez da leku irekietan hitz egingo informazio konfidentzialari buruz. Bilera salak horretarako daude.	• Papera: Paper deuseztagailuak • Euskarri elektronikoak: Dagokion politikak ezartzen duena jarraituko du • Desegin ezin daitekeen euskarri fisikoa: Hautsi, deuseztatu.

MOTA	SARRERA BAIMENDUA	BILTEGIRATZEA	POSTAZ, POSTA ELEKTRONIKOZ, FAXEZ TASMISIOA	HITZEZ	DEUSEZTAPENA
PUBLIKOA	• Irakasleak • Ikasleak • Akordia sinatu behar izan ez duten kanpoek	Mugarik gabe	Mugarik gabe	Mugarik gabe	Mugarik gabe

5.2 Eranskina II: Mezu elektronikoetan barneratu behar den konfidentzialtasun klausula.

Posta elektroniko honen barruan doan informazioa, erantsita doazen osagai guztiak bezala, konfidentzialak dira. Posta honen hartzaile ez zaren kasuan, igorleari jakinaraztea erregutzen dizugu eta posta hau berehala deuseztatzea. Informazio honen irakurketa edo/eta erabilera aurretik aipatutako egoeran legez kanpokotzat joko da, honela legezko ekintza ezberdinak hartzeko baimenduta gelditzen da enpresa igorlea.

La información contenida en este mail, así como los archivos adjuntos, es CONFIDENCIAL. En el caso de que el destinatario del correo no sea usted, le rogamos envíe una notificación al remitente y lo destruya de forma inmediata. La lectura y/o manipulación de esta información en la situación señalada anteriormente será considerada ilegal, permitiendo a la empresa remitente realizar acciones legales de diferente envergadura.

The information contained in this e-mail is strictly confidential and for the use of the addressee only; it may also be legally privileged and or price sensitive. Notice is hereby given that any disclosure, use or copying of the information by anyone other than the intended recipient is prohibited and may be illegal. If you have received this message in error, please notify the sender immediately by return e-mail.