Informazioaren Segurtasunerako Politika (SEN)

Política de Seguridad de la Información (ENS)

sanmarkos
Mankomunitatea

DOKUMENTUEN KONTROLA			
Titulua:		INFORMAZIOAREN SEGURTASUNERAKO POLITIKA (ENS-SENa)	
Dokumentuaren kodea:		ENS_ORG1	
Sailkapena:		KONFIDENTZIALA	
Bertsioa		001	
Egilea[k]:	P3RSEUS CIBERSEGURIDAD S.L	Data:	
Onarlea:	San Marko Mankomunitatea	Data:	x

ALDAKETAREN DESKRIBAPENA		
Bertsioa	Data	Aldaketaren deskribapena

CONTROL DOCUMENTAL			
Título		POLÍTICA DE SEGURIDAD DE LA INFORAMACIÓN (ENS)	
Código documento:		ENS_ORG1	
Clasificación:		CONFIDENCIAL	
Versión		001	
Autor[es]:	P3RSEUS CIBERSEGURIDAD S.L	Fecha:	
Aprobador:	Mancomunidad de San Marcos	Fecha:	x

HISTORIAL DE CAMBIOS		
Versión	Fecha	Descripción del Cambio

Aurkibidea/Índice

1. SARRERA/INTRODUCCIÓN

Herritarrek Zerbitzu Publikoetan Sarbide Elektronikoa izateari buruzko ekainaren 22ko 11/2007 Legeak Segurtasun Eskema Nazionala ezarri zuen. Urtarrilaren 8ko 3/2010 Errege Dekretuaren bidez onartu zen Eskema hori, eta bere aplikazio-eremuan bitarteko elektronikoak erabiltzeko segurtasun-politika zehaztea du helburu. Eskema hori informazioa behar bezala babesteko oinarrizko printzipioek eta gutxieneko baldintzek osatuko dute. Geroago, urriaren 1eko 40/2015 Legeak, Sektore Publikoaren Araubide Juridikoarenak, Segurtasun Eskema Nazionala (SENa) jasotzen du 156. artikuluko 2. paragrafoan.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos.

2. XEDEA/OBJETO

Dokumentu honen xedea da San Marko Mankomunitatearen (aurrerantzean Mankomunitatea) segurtasun-politika zehaztea, lege horrek aipatzen dituen bitarteko elektronikoak erabiltzean aplikatu beharrekoa.

Este documento tiene por objeto determinar la Política de Seguridad de Mancomunidad de San Marcos (en adelante Mancomunidad) que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada Ley.

3. IRISMENA/ALCANCE

Urtarrilaren 8ko 3/2010 Errege Dekretuak, Administrazio Elektronikoaren eremuan Segurtasun Eskema Nazionala arautzen duenak, 12. artikuluan ezartzen duen bezala. "Segurtasun-prozesua antolatzea eta ezartzea":

Tal como se establece en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en su Artículo 12. “Organización e implantación del proceso de seguridad”:

Segurtasunak erakundeko kide guztiak konprometitu beharko ditu. Segurtasun-politikak, II. eranskineko 3.1 atalean zehazten denaren arabera, argi eta garbi identifikatu beharko ditu politika hori betetzen dela zaintzeko eta administrazio-antolamenduko kide guztiek horren berri izan dezaten.

La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

4. HELBURUAK ETA MISIOA/OBJETIVOS Y MISIÓN

Mankomunitate honek, bere interesak kudeatzeko eta bere eskumenen esparruan, herritarren beharrak eta nahiak asetzen laguntzen duten jarduera eta zerbitzu publikoak sustatzen ditu. Era berean,

Esta Mancomunidad, para la gestión de sus intereses y en el ámbito de sus competencias, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la ciudadanía.

Mankomunitatean eta herritarrentzako teknologia berrien erabilera bultzatu nahi da.

Asimismo, se desea potenciar el uso de las nuevas tecnologías tanto en la Mancomunidad como para la propia ciudadanía.

Horretarako, erakunde honen esku jartzen du online izapideak egitea, herritarrek gai publikoetan parte har dezaten bultzatzeko, partaidetza-demokraziaren garapena eta ekintza publikoaren eraginkortasuna bermatuko duten partaidetza-bide berriak ezarriz.

Para ello pone a disposición de ésta la realización de trámites online con el objetivo de impulsar la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la eficacia de la acción pública.

Hauek dira, besteak beste, lortu nahi diren helburu nagusiak:

- Herritarren harreman elektronikoa sustatzea.
- Herritarrekiko beharrezko konfiantza sortzea harreman horretan.

Los principales objetivos que se persiguen entre otros son:

- Fomentar la relación electrónica de la ciudadanía.
- Crear la confianza necesaria con el ciudadano en esta relación.

Mankomunitatearen eskumenak gauzatzeko, modu eraginkor eta efizientean babestu behar diren informazio-sistemak erabiltzen dira.

Para ejercer las competencias de la Mancomunidad se hace uso de sistemas de información que deben ser protegidos de una forma efectiva y eficiente.

4.1. Eskumenak/Competencias

Mankomunitateko Sail guztiek aplikatu beharko dute politika hori, eta nahitaez bete beharko dute. Sailtzat hartuko dira beren arloak eta Batzarrak, hala badagokio, sortzea erabakitzen dituen mendeko erakundeak, beren errekurtsoak eta ENS-SENek eta DBEOk eragindako prozesuak, hirugarrenekin egindako kontratu edo akordioen bidez erakundeari lotutakoak izan zein kanpokoak izan.

Esta Política será de aplicación y de obligado cumplimiento para todos los Departamentos de la Mancomunidad, entendiendo por Departamentos a sus Áreas y a entes dependientes que decida crear, en su caso, la Junta, a sus recursos y a los procesos afectados por el ENS y el RGPD, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Irismena bi ikuspuntutatik zehaztuko da: alde batetik, antolakuntzakoa, eta, bestetik, informazio-sistemei edo irismen funtzionalari buruzkoa.

Se determinará el alcance desde un doble punto de vista, el organizativo por un lado y el relativo a sistemas de información o alcance funcional.

Azken horri dagokionez, politika hau aplikatuko zaie eskubideak bitarteko elektronikoen bidez baliatzearekin, betebeharrak bitarteko elektronikoen bidez betetzearekin edo informaziorako edo administrazio-prozedurarako sarbidearekin zerikusia duten informazio-sistemei. Badira administrazioen eta herritarren arteko

En cuanto a este último, esta Política se aplicará a los sistemas de información que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo. Existen recursos que se utilizan para las relaciones

harremanetarako erabiltzen diren baliabideak, enpresa pribatuek sortu dituztenak eta oraindik mantentzen dituztenak. Haiei enkargatutako aplikazioak eta webguneak dira. Horiei dagokienez, ENS-SENaren eremuan sartu beharko dira, eta enpresa horiei jakinarazi beharko zaizkie Mankomunitatea arautzen duten segurtasun-irizpideak, baliabideak segurtasun-baldintza horietara egokitu ditzaten.

entre administraciones y ciudadanos que han sido creadas y siguen siendo mantenidas por empresas privadas. Son aplicaciones y páginas web cuyo desarrollo ha sido encargado a éstas. En lo que a éstos se refiere, se deberán incluir dentro del ámbito de la ENS, y se deberá notificar a estas empresas los criterios de seguridad por los que se rige la Mancomunidad, a fin de que adecuen los recursos a estos requisitos de seguridad.

5. ARAU-ESPARRUA/MARCO NORMATIVO

Mankomunitateak Informazioaren Segurtasun Politikaren esparruan egiten dituen jardueren arau-esparrua honako arau hauek osatzen dute:

El marco normativo de las actividades de la Mancomunidad en el ámbito de la Política de Seguridad de la Información está integrado por las siguientes normas:

- 7/1985 Legea, Toki Araubidearen Oinarriak arautzen dituena.
- Ley 7/1985, Reguladora de las Bases del Régimen Local.
- 2016/679 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari dagokionez pertsona fisikoen babesari eta datu horien zirkulazio askeari buruzkoa eta 95/46/EE Zuzentaraua indargabetzen duena.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- 34/2002 Legea, informazioaren gizartearen zerbitzuei eta merkataritza elektronikoari buruzkoa.
- Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico.
- 33/2003 Legea, Herri Administrazioen Ondareari buruzkoa.
- Ley 33/2003, del Patrimonio de las Administraciones Públicas.
- 5/2015 Legegintzako Errege Dekretua, urriaren 30ekoa, Enplegatu Publikoaren Oinarrizko Estatutuaren Legearen testu bategina onartzen duena.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público
- 59/2003 Legea, abenduaren 19koa, sinadura elektronikoari buruzkoa.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- 1553/2005 Errege Dekretua, abenduaren 23koa, nortasun-agiri nazionala eta sinadura elektronikoko ziurtagiriak arautzen dituena.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- 25/2007 Legea, komunikazio elektronikoei eta komunikazio-sare publikoei buruzko datuak kontserbatzeari buruzkoa.
- Ley 25/2007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- 57/2003 Legea, abenduaren 16koa, tokiko
- Ley 57/2003, de 16 de diciembre, de

gobernua modernizatzeko neurriei buruzkoa.	medidas para la modernización del gobierno local.
• 3/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoaren eremuan Segurtasun Eskema Nazionala arautzen duena.	• Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
• 951/2015 Errege Dekretua, urriaren 23koa, honako hau aldatzen duena: 3/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoaren eremuan Segurtasun Eskema Nazionala arautzen duena.	• Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
• 4/2010 Errege Dekretua, Administrazio Elektronikoaren eremuan Elkarreragingarritasun Eskema Nazionala arautzen duena.	• Real Decreto 4/2010, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
• 9/2017 Legea, azaroaren 8koa, Sektore Publikoko Kontratuei buruzkoa.	• Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
• 19/2013 Legea, gardentasunari, informazio publikoa eskuratzeko bideari eta gobernu onari buruzkoa.	• Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno.
• 27/2013 Legea, Toki Administrazioaren Arrazionalizazio eta Iraunkortasunari buruzkoa.	• Ley 27/2013, de Racionalización y Sostenibilidad de la Administración Local.
• 9/2014 Lege Orokorra, Telekomunikazioei buruzkoa.	• Ley 9/2014, General de Telecomunicaciones.
• 8/2014 Errege Dekretua, hazkunderako, lehiakortasunerako eta eraginkortasunerako premiazko neurriak onartzen dituena.	• Real Decreto 8/2014, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
• 18/2014 Legea, hazkunderako, lehiakortasunerako eta eraginkortasunerako premiazko neurriak onartzen dituena.	• Ley 18/2014, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
• 39/2015 Legea, Administrazio Publikoen Administrazio Prozedura Erkidearena.	• Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas.
• 40/2015 Legea, Sektore Publikoaren Araubide Juridikoarena.	• Ley 40/2015, de Régimen Jurídico del Sector Público.
Era berean, Mankomunitatearen jarduera erregulatzen duten beste arau guztiak aplikatuko dira bere eskumenen esparruan, bai eta Mankomunitateak bere eskumenak erabiliz kudeatzen dituen bitarteko elektronikoetan erabilitako datu, informazio eta zerbitzuen eskuragarritasuna, osotasuna, erabilgarritasuna, benetakotasuna, konfidentzialtasuna, trazabilitatea eta	Asimismo, resultarán de aplicación cuantas otras normas regulen la actividad de la Mancomunidad en el ámbito de sus competencias y aquellas otras dirigidas a asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos gestionados por la Mancomunidad

kontserbazioa ziurtatzera bideratutakoak ere.

igualmente en el ejercicio de sus competencias.

6. SEGURTASUNAREN ANTOLAKETA/ORGANIZACIÓN DE LA SEGURIDAD

Mankomunitatearen jarduerako informazio-sistemen segurtasuna kudeatzeko –definizioa, ezarpena eta mantentzea –, Segurtasunaren Antolakuntza bat ezarri behar da. Antolaketa horrek zehaztasunez ezartzen ditu erakundea osatzen duten eragileak, haien funtzioak eta erantzukizunak, bai eta horiek oinarrituko dituen egitura bat ezartzea ere.

La gestión de la seguridad de los sistemas de información actividad de la Mancomunidad, -definición, implantación y mantenimiento- exige establecer una Organización de la Seguridad. Tal organización determina con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte.

3/2010 Errege dekretuko 10. artikulua. ***Segurtasuna funtzio bereizi gisa***
Informazio-sistemetan, informazioaren arduraduna, zerbitzuaren arduraduna eta segurtasunaren arduraduna bereiziko dira.

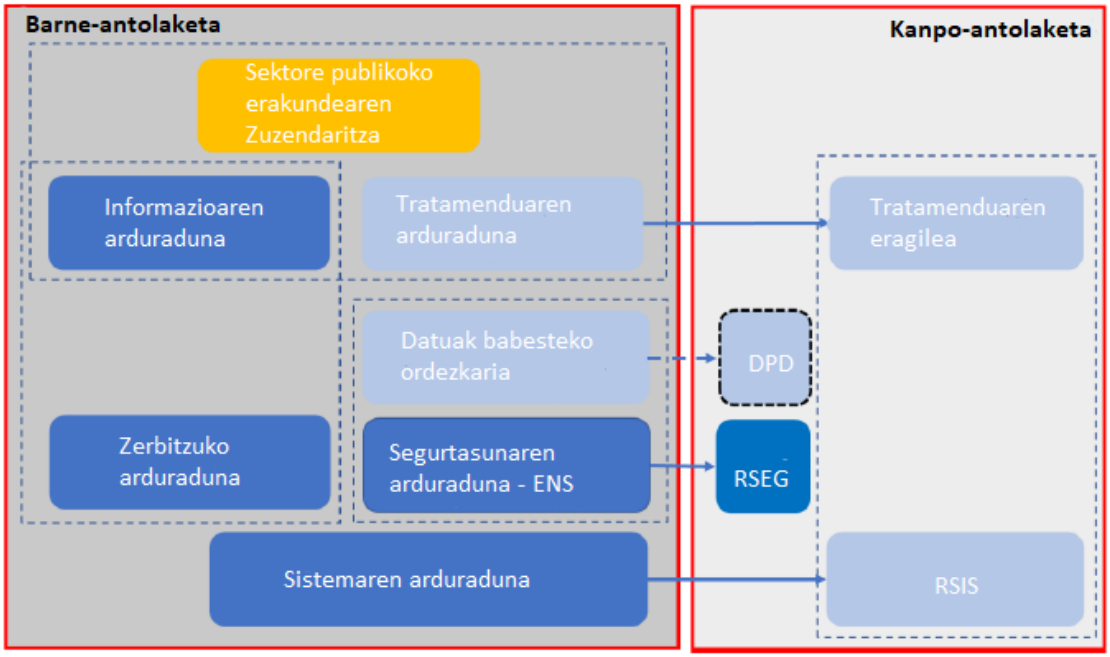
Informazioaren arduradunak zehaztuko ditu tratatutako informazioaren betekizunak; zerbitzuaren arduradunak zehaztuko ditu emandako zerbitzuen betekizunak; eta segurtasun-arduradunak zehaztuko ditu informazioaren eta zerbitzuen segurtasun-eskakizunak betetzeko erabakiak.

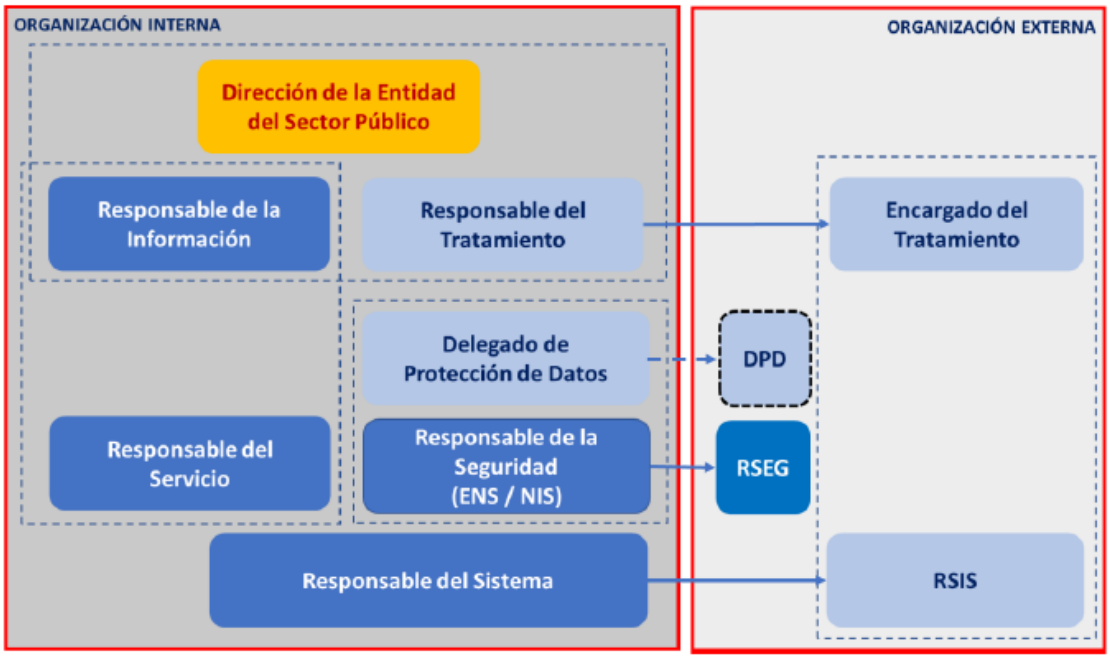
Informazio-sistemen segurtasunaren erantzukizuna zerbitzuak emateko erantzukizunetik bereizita egongo da.

Artículo 10 del Real Decreto 3/2010. ***La seguridad como función diferenciada***
En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.
El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

Mankomunitatean honako segurtasun-rol hauek ezartzen dira:

En la Mancomunidad se establecen los siguientes roles de seguridad que a continuación se describen:





Dokumentu honek Segurtasun Eskema Nazionalari dagozkion rolak baino ez ditu jasotzen. "Betetze-gida" dokumentuak DBEO/DBEDBLO betetzeari lotutako rolak deskribatzen ditu.

Este documento únicamente recoge los roles relativos al Esquema Nacional de Seguridad. El documento “Guía cumplimiento” describe los roles relacionados con el cumplimiento de RGPD/LOPDGDD.

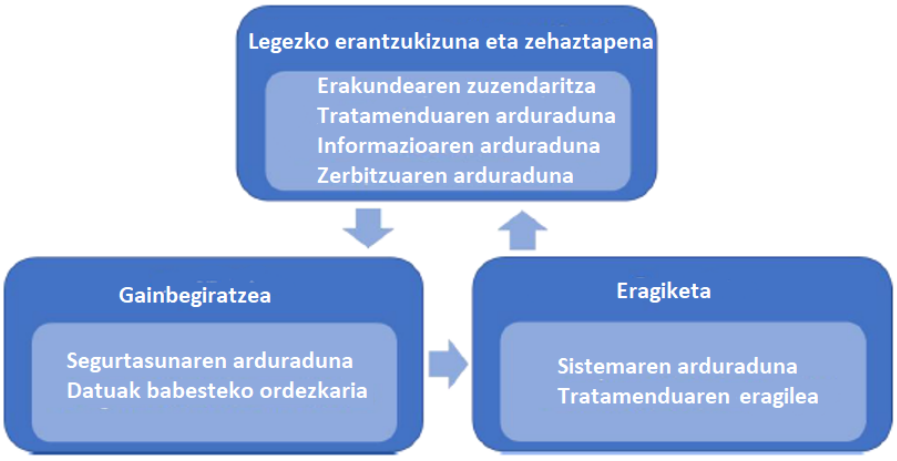
6.1. Erantzukizun-blokeak/Bloques de responsabilidad

Mankomunitate honek hiru erantzukizun-bloke handi ezartzen ditu:

1. Mankomunitateko Batzarrari eta tratamenduaren, informazioaren eta zerbitzuaren arduradunei dagozkien **legezko erantzukizuna** eta behar edo betekizunen zehaztapena.
2. **Ikuskapena**, segurtasunaren arduradunari eta datuak babesteko ordezkariari dagokiena, bakoitzak bere eremuan.
3. **Informazio-sistemaren eragiketa**, sistemaren arduradunari dagokiona.

La presente Mancomunidad establece tres grandes bloques de responsabilidad:

1. **La responsabilidad legal** y la especificación de las necesidades o requisitos, que corresponde a la Junta de la Mancomunidad y a los responsables del tratamiento, de la información y del servicio.
2. **La supervisión**, que corresponde al Responsable de la Seguridad y al Delegado de Protección de Datos, en sus respectivos ámbitos.
3. **La operación del sistema de información**, que corresponde al Responsable del Sistema.



Erantzukizun-blokeak

Bloques de responsabilidad

6.2. Mankomunitateko Batzarra/Junta de la Mancomunidad

- **Legezko kokapena:**
  - 40/2015 Legea aplikatzetik eratorritakoa
- **Funtzioak, ezaugarriak edo erreferentziak:**
  - ENS-SENaren aplikazio-eremuko sektore publikoko erakundeak, zeinen titularrak erantzukizun nagusia baitu Mankomunitatearen eskumenak garatzean, informazioaren segurtasunari buruzkoak barne, 40/2015 Legean eta gainerako ordenamendu juridikoan xedatutakoaren arabera. ENS-SEN-arean ezarpenaren arduradun nagusia da.

- **Ubicación legal:**
  - La derivada de la aplicación de la Ley 40/2015
- **Funciones, Características o Referencias:**
  - Entidades del Sector Público del ámbito de aplicación del ENS, cuyo titular ostenta la máxima responsabilidad en el desarrollo de las competencias de la Mancomunidad, incluyendo las de seguridad de la información, de conformidad con lo dispuesto en la Ley 40/2015 y en el resto del ordenamiento jurídico. Es el máximo responsable de la implantación del ENS.

6.3. Informazioaren arduraduna/Responsable de Información

- **Legezko kokapena:**
  - ENS-SENa, 10 art.
- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Tratatutako informazioaren betekizunak (segurtasunekoak) zehazten ditu, ENS-SENaren I. eranskineko parametroen arabera. Pertsona fisiko berezia edo kide anitzeko organoa izan daiteke, eta Informazioaren Segurtasun Batzordeko kide izan daiteke. Segurtasuna erakunde publikoen berezko jarduketa-printzipioa denez, informazioaren segurtasun-mailak onartzea ere eskuordetu ezin den jarduera da.

- **Ubicación legal:**
  - ENS, art. 10
- **Funciones, características o referencias:**
  - Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o un órgano colegiado, formando parte del Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de la información constituye asimismo una actividad indelegable.

- **Legezko kokapena:**
  - ENS-SENa, 43 art.
- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Informazioaren segurtasunaren gaineko inpaktu negatibo baten ondorioak baloratzeko, kontuan hartuko dira organizazioak bere helburuak lortzeko duen gaitasunean duen eragina, bere aktiboak babestea, zerbitzu-betebeharrak betetzea, eta legezkotasuna eta herritarren eskubideak errespetatzea.

- **Ubicación legal:**
  - ENS, art. 43
- **Funciones, características o referencias:**
  - La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

6.4. Zerbitzuaren arduraduna/ Responsable del Servicio

- **Legezko kokapena:**
  - ENS-SENa, 10 art.
- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Emandako zerbitzuen betekizunak (segurtasunekoak) zehazten ditu, ENS-SENaren I. eranskineko parametroen arabera.
  - Pertsona fisiko berezia edo kide anitzeko organoa izan daiteke, eta Informazioaren Segurtasunerako Batzordeko kide izan daiteke.
  - Segurtasuna erakunde publikoen berezko jarduketa-printzipioa denez, zerbitzuen segurtasun-mailak onartzea ere eskuordetu ezin den jarduera da.

- **Ubicación legal:**
  - ENS, art. 10
- **Funciones, características o referencias:**
  - Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.
  - Puede tratarse de una persona física singular o un órgano colegiado, formando parte del Comité de Seguridad de la Información.
  - Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de los servicios constituye asimismo una actividad indelegable.

- **Legezko kokapena:**
  - ENS-SENa, 39 art.
- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Zerbitzuen eta sistemen bizi-zikloko segurtasun-zehaztapenak sartu behar ditu, dagozkion kontrol-prozedurekin batera.

- **Ubicación legal:**
  - ENS, art. 39
- **Funciones, características o referencias:**
  - Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

- **Legezko kokapena:**
  - ENS-SENa, 43 art.
- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Zerbitzuen segurtasunaren gaineko inpaktu negatibo baten ondorioak baloratzeko, kontuan hartuko dira organizazioak bere helburuak lortzeko duen gaitasunean duen eragina, bere aktiboak babestea, zerbitzu-betebeharrak betetzea, eta legezkotasuna eta herritarren eskubideak errespetatzea.

- **Ubicación legal:**
  - ENS, art. 43
- **Funciones, características o referencias:**
  - La valoración de las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

6.5. Segurtasunaren arduraduna/Responsable de la Seguridad

- **Legezko kokapena:**
  - ENS-SENa, 10 art.

- **Ubicación legal:**
  - ENS, art. 10

- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Informazioaren eta zerbitzuen arduradunek ezarritako baldintzak

- **Funciones, características o referencias:**
  - Determina las decisiones de seguridad pertinentes para satisfacer los

betetzeko segurtasun-erabaki egokiak zehazten ditu.

- Pertsona fisikoa da, sistemaren arduradunarengandik hierarkikoki independentea.

Oharra: kanpora ateratako zerbitzuen kasuan, azken erantzukizuna Mankomunitateak du beti, zerbitzuen hartzaile gisa, nahiz eta berehalako erantzukizuna (kontratu, hitzarmen, gomendio eta abarren bidez) zerbitzua ematen duen erakundeari dagokion.

- **Legezko kokapena:**
  - ENS-SENa, 15.3 art.

- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Mankomunitateak exijituko du, modu objektibo eta ez-diskriminatzailean, segurtasun-zerbitzuak ematen dizkieten erakundeek profesional kualifikatuak eta emandako zerbitzuetan kudeaketa- eta heldutasun-maila egokiak izatea.

- **Legezko kokapena:**
  - ENS-SENa, 18. art.

- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Informazioaren eta komunikazioaren teknologien segurtasun-produktuak eskuratzeko, sistemaren kategoriaren eta segurtasun-mailaren arabera, produktu horiek eskuratzeko xedearekin lotutako segurtasun-funtzionaltasuna ziurtatuta dutenak erabiliko dira, hartutako arriskuei dagokienez proportzionaltasun-eskakizunek justifikatzen ez dutenean izan ezik, Segurtasunaren arduradunaren iritziz.

- **Legezko kokapena:**
  - ENS-SENa, 27.3, 27.4 eta 27.5 art.

- **Funtzioak, ezaugarriak edo erreferentziak:**
  - ENS-SENaren II. eranskineko neurriak, bai eta datu pertsonalen tratamendu

requisitos establecidos por los responsables de la información y de los servicios.

- Es una persona física, jerárquicamente independiente del Responsable del Sistema.

Nota: En caso de servicios externalizados, la responsabilidad última la tiene siempre la Mancomunidad como destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, convenio, encomienda, etc.) a la organización prestataria del servicio.

- **Ubicación legal:**
  - ENS, art.15.3

- **Funciones, características o referencias:**
  - La Mancomunidad exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

- **Ubicación legal:**
  - ENS, art 18

- **Funciones, características o referencias:**
  - En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de la Seguridad.

- **Ubicación legal:**
  - ENS, arts.27.3, 27.4 y 27.5

- **Funciones, características o referencias:**
  - Las medidas del Anexo II del ENS, así como aquellas otras necesarias para

egokia bermatzeko beharrezkoak direnak ere, zabaldu ahal izango dira, aipatutako konkurrentzia edo sistemaren segurtasunaren arduradunaren borondate zuhurra dela-eta, teknologiaren egoera, emandako zerbitzuen eta erabilitako informazioaren izaera eta arriskuak kontuan hartuta.

- II. eranskinean hautatutako neurrien zerrenda Aplikagarritasun-adierazpena izeneko dokumentu batean formalizatuko da, eta segurtasunaren arduradunak sinatuko du.
- II. eranskinean aipatutako segurtasun-neurriak beste konpentsazio-neurri batzuekin ordeztu ahal izango dira, betiere dokumentu bidez justifikatzen bada aktiboen gaineko arriskua berdin edo hobeto babesten dutela (I. eranskina) eta errege-dekretuaren II. eta III. kapituluetan aurreikusitako oinarrizko printzipioak eta gutxieneko baldintzak betetzen badira.
- Aplikagarritasun-adierazpenaren zati integral gisa, zehatz-mehatz adieraziko da ezarritako konpentsazio-neurrien eta II. eranskineko konpentsazio-neurrien arteko egokitasuna, eta segurtasunaren arduradunak formalki onartuko du multzoa.

garantizar el adecuado tratamiento de datos personales podrán ser ampliadas por causa de la concurrencia indicada o del prudente arbitrio del Responsable de la Seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

- La relación de medidas seleccionadas del Anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el Responsable de la Seguridad.
- Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto.
- Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de la seguridad.

- **Legezko kokapena:**
  - ENS-SENa, 28 art.

- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Administrazio Publikoetan onartutako azpiegitura eta zerbitzu erkideak erabiltzeak SENean eskatutako oinarrizko printzipioak eta gutxieneko baldintzak eraginkortasun hobeko baldintzetan betetzea erraztuko du. Azpiegitura eta zerbitzu komun horiek erabiltzeko kasu zehatzak administrazio bakoitzak zehaztuko ditu.

- **Ubicación legal:**
  - ENS, art. 28

- **Funciones, características o referencias:**
  - La utilización de infraestructuras y servicios comunes reconocidos en las Administraciones Públicas facilitará el cumplimiento de los principios básicos y los requisitos mínimos exigidos en el ENS en condiciones de mejor eficiencia. Los supuestos concretos de utilización de estas infraestructuras y servicios comunes serán determinados por cada Administración.

- **Legezko kokapena:**
  - ENS-SENa , 34.6 art. eta III. Eranskina
- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Autoebaluazio-txostenak eta/edo auditoretza-txostenak segurtasun-arduradun eskudunak aztertuko ditu, eta ondorioak Sistemaren arduradunari helaraziko dizkio, neurri zuzentzaile egokiak har ditzan.

- **Ubicación legal:**
  - ENS, art. 34.6 y Anexo III
- **Funciones, características o referencias:**
  - Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.

6.6. Informazio sistemen arduraduna/Responsable del Sistema (de información)

- **Legezko kokapena:**
  - ENS-SENa
- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Informazio-sistemaren eragiketaz arduratzen da, segurtasunaren arduradunak zehaztutako segurtasun-neurriak kontuan hartuta.

- **Legezko kokapena:**
  - 40/2015 Legea aplikatzetik eratorritakoa
- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Erakundearen barruan dago haren erantzukizuna (sistema propioak erabiltzea), edo hurbileko erantzukizun baten (erakundearena berarena) eta berehalako erantzukizun baten (hirugarrenena, publikoa zein pribatua) artean zatituta, informazio-sistemak kanpora aterata daudenean.

- **Legezko kokapena:**
  - ENS-SENa, 34.6 eta 34.7 art.
- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Autoebaluazio-txostenak eta/edo auditoretza-txostenak segurtasun-arduradun eskudunak aztertuko ditu, eta ondorioak Sistemaren arduradunari helaraziko dizkio, neurri zuzentzaile egokiak har ditzan.

- **Ubicación legal:**
  - ENS
- **Funciones, características o referencias:**
  - Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.

- **Ubicación legal:**
  - La derivada de la aplicación de la Ley 40/2015
- **Funciones, características o referencias:**
  - Su responsabilidad está situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados.

- **Ubicación legal:**
  - ENS, art.34.6 y 34.7
- **Funciones, características o referencias:**
  - Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas

correctoras adecuadas.

6.7. Segurtasun Batzordea/Comité de Seguridad

Sektore publikoko erakundeetan informazioaren segurtasuna koordinatzea bereziki garrantzitsua da gastua arrazionalizatzea eskatzen delako eta informazio-sistemetan puntu ahulek eragindako segurtasun-arrailak sortzea eragiten duten disfuntzioak saihesteko, ustekabeko gorabeherak edo, are gehiago, zibererasoak ahalbidetzen dituztenak.

La coordinación de la seguridad de la información en las entidades del Sector Público es especialmente importante por exigencia de racionalización del gasto y para evitar disfunciones que propicien la aparición de brechas de seguridad provocadas por puntos débiles en los sistemas de información que posibiliten incidentes accidentales o, incluso, ciberataques.

Informazioaren Segurtasunerako Batzordeak Mankomunitateko informazioaren segurtasuna koordinatzen du, eta segurtasunaren arduradunak (informazioaren arduradunak) eta eragindako erakundeko beste arlo batzuetako ordezkariek osatuko dute. Saio bakoitzaren osaera zehaztuko da, adierazitako rolez gain, haren helburuari ekarpena egiten dioten barneko eta/edo kanpoko rolen arabera.

El Comité de Seguridad de la Información coordina la seguridad de la información en la Mancomunidad, y estará formado por el Responsable de la Seguridad (de la Información) y por representantes de otras áreas de la organización afectadas. La composición de cada sesión se determinará, además de por los roles señalados, por cualesquiera que se consideren, tanto internos y/o externos que aporten al objetivo de esta.

Informazioaren Segurtasunerako Batzordearen ohiko eginkizunak dira:

Son funciones típicas del Comité de Seguridad de la Información:

- Mankomunitateko Batzarraren eta sailen kezkei erantzutea.
- Atender las inquietudes de la Junta de la Mancomunidad y de los diferentes departamentos.
- Informazioaren segurtasunaren egoeraren berri ematea aldizka Zuzendaritza Nagusiari.
- Informar regularmente del estado de la seguridad de la información a la Dirección General.
- Informazioaren segurtasuna kudeatzeko sistemaren etengabeko hobekuntza sustatzea.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Erakundearen bilakaera-estrategia prestatzea, informazioaren segurtasunari dagokionez.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Informazioaren segurtasunaren arloko arloen ahaleginak koordinatzea, bermatzeko ahaleginak sendoak direla, eta gai horretan erabakitako estrategiarekin bat datozela, bikoiztasunak saihestuz.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Informazioaren Segurtasun Politika egitea (eta aldizka berrikustea), Zuzendaritza Nagusiak onar dezan.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección General.
- Informazioaren segurtasunari buruzko
- Aprobar la Normativa de Seguridad de la

araudia onartzea.

- Administratzaile, operadore eta erabiltzaileen prestakuntza- eta kalifikazio-betekizunak prestatzea eta onartzea, informazioaren segurtasunaren ikuspegitik.
- Erakundeak bere gain hartutako hondar-arrisku nagusiak monitorizatzea eta egin daitezkeen jarduerak gomendatzea.
- Segurtasun-intzidenteak kudeatzeko prozesuen jarduna monitorizatzea eta horiei dagokienez egin daitezkeen jarduketak gomendatzea. Bereziki, gorabehera horien kudeaketan segurtasun-arloak koordinatzen direla zaintzea.
- Erakundeak segurtasunaren arloan dituen betebeharrak betetzen direla egiaztatzeko aukera ematen duten aldizkako auditoriak egin daitezen sustatzea.
- Erakundearen informazioaren segurtasuna hobetzeko planak onartzea. Bereziki, hainbat arlotan egin daitezkeen planen koordinazioa zainduko du.
- Segurtasun-arloko jarduerak lehenestea, baliabideak mugatuak direnean.
- IKT proiektu guztietan informazioaren segurtasuna kontuan hartzen dela zaintzea, hasierako zehaztapenetik abian jarri arte.

información.

- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación.

Bereziki, zerbitzu horizontalak sortzen eta erabiltzen direla zaindu beharko du, bikoiztasunak murrizteko eta IKT sistema guztien funtzionamendu homogeneoa bultzatzeko.

En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

Arduradunen eta/edo erakundeko arloen artean ager daitezkeen erantzukizun-gatazkak konpontzea, eta erabakiak hartzeko autoritate nahikorik ez duten kasuak areagotzea.

Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

San Marko Mankomunitateak erabaki du, bere tamaina txikia dela eta, gaur egun ez duela segurtasun-batzorde baten figura behar; era berean, batzordearen funtzioak

La Mancomunidad de San Marcos ha decidido que, debido a su pequeña dimensión, no requiere actualmente la figura de un comité de seguridad, asimismo, las

figura anizkoitz batek xurgatuko ditu (ikus 6.9 atala).

funciones del comité serán absorbidas por una figura múltiple (ver apartado 6.9).

6.8. Datuak Babesteko Ordezkaria/Delegado de Protección de Datos

- **Legezko kokapena:**
  - DBLO
- **Funtzioak, ezaugarriak edo erreferentziak:**
  - Arduradunari, arduradunari eta enplegatuei informazioa eta aholkularitza ematea.
  - Betetzea gainbegiratzea, erantzukizunak esleitzea, kontzientziazioa eta prestakuntza pertsonala barne.
  - Eraginaren ebaluazioari buruzko aholkularitza ematea eta horren aplikazioa gainbegiratzea.
  - Kontrol-agintaritzarekin lankidetzan aritzea.
  - Harremanetarako gune gisa jardutea datuen tratamenduari buruzko gaietan, aurretiazko kontsultak barne.

- **Ubicación legal:**
  - LOPDGDD
- **Funciones, Características o Referencias:**
  - Informar y asesorar al responsable, al encargado y empleados.
  - Supervisar el cumplimiento incluyendo asignación de responsabilidades, concienciación y formación personal.
  - Asesorar acerca de la evaluación de impacto y supervisar su aplicación.
  - Cooperar con la autoridad de control.
  - Actuar como punto de contacto en cuestiones relativas al tratamiento de los datos, incluyendo las consultas previas.

- **Legezko kokapena:**
  - DBEOren 4. atala eta 39. Artikulua

- **Ubicación legal:**
  - Sección 4 y artículo 39 del RGPD

6.9. Izendatzeko prozedura/Procedimiento de designación

Mankomunitateko Batzarraren eginkizuna da honako hauek izendatzea:

- Informazioaren arduradunari; pertsona bakarreko kargua edo kide anitzeko organoa izan daiteke (normalean, Informazioaren Segurtasun Batzordean integratzen da.
- Zerbitzuaren arduradunari; informazioaren arduraduna bera izan daiteke, eta pertsona bakarreko kargua edo kide anitzeko organoa ere izan daiteke (normalean, Informazioaren Segurtasun Batzordean integratzen da).
- Segurtasunaren arduraduna, zuzenean Zuzendaritza Nagusiari eta Informazioaren Segurtasun Batzordeari jakinarazi behar diena.
- Sistemaren arduradunari, zeinak segurtasunaren arloko informazioa emango baitio segurtasunaren arduradunari.

Es función de la Junta de la Mancomunidad designar:

- Al Responsable de la Información, que puede ser un cargo unipersonal o un órgano colegiado (integrado, habitualmente, en Comité de Seguridad de la Información).
- Al Responsable del Servicio, que, pudiendo ser el mismo que el Responsable de la Información, también puede ser un cargo unipersonal o un órgano colegiado (integrado, habitualmente, en Comité de Seguridad de la Información).
- Al Responsable de la Seguridad, que debe reportar directamente a la Dirección General y a al Comité de Seguridad de la Información.
- Al Responsable del Sistema, que, en materia de seguridad, reportará al Responsable de la Seguridad.

- Datuak babesteko ordezkariari.

CCN-STIC 803: "Erantzukizunak" delakoaren segurtasun-gidak ezartzen duenez, dimentsio txikiko organismoetan, politika honetan identifikatutako rolak eta erantzukizunak honako gutxieneko egitura honetara murriztu daitezke, bi roletara murriztuta:

1. Tokiko zuzendaritza edo Batzarra: figura bat, honako eginkizun hauek dituena:

- Tratamenduaren arduraduna.
- Informazioaren arduraduna.
- Zerbitzuaren arduraduna.
- Segurtasunaren arduraduna.

Eginkizun horiek mankomunitateko Lehendakariari dagozkio.

2. Eragiketa: figura bat, zuzendaritzara edo Batzarrera bidalita, eta honako eginkizun hauek barne hartuta:

- Sistemaren arduraduna
- Segurtasun-administratzailea

Eginkizun hauek eta Segurtasun Batzordearenak (ikus 6.7) Mankomunitateko Zuzendari Kudeatzaileari dagozkio, eta, zehazki, segurtasun-administratzailearen eginkizunak mankomunitateko informatika-arduradunari eskuordetu ahal izango zaizkio, halakorik balego, edo mankomunitateko sistema informatikoak mantentzeaz arduratzen den enpresari.
Segurtasun Batzordeari egiten zaizkion aipamen guztiak Zuzendari Kudeatzaileari egindakotzat hartuko dira.

- Al Delegado de Protección de datos.

La Guía de seguridad del CCN-STIC 803: “responsabilidades”, establece que, en los organismos de pequeña dimensión, los roles y responsabilidades identificadas en esta política pueden reducirse a la siguiente estructura mínima reducida a 2 roles:

1. Dirección o Junta local: una figura integrando las siguientes funciones:

- Responsable del tratamiento.
- Responsable de la información.
- Responsable del servicio.
- Responsable de la seguridad.

Estas funciones recaerán en la Presidencia de la Mancomunidad.

2. Operación: una figura, reportando a Dirección o a Junta, e integrando las siguientes funciones:

- Responsable del sistema
- Administrador de seguridad

Estas funciones y las del Comité de Seguridad (ver 6.7) recaerán en la Directora-Gerente de la Mancomunidad, y en concreto las funciones de administrador de seguridad se podrán delegar bien al responsable de informática de la Mancomunidad, si lo hubiera, o bien a la empresa encargada de mantener los sistemas informáticos de la Mancomunidad.
Todas las menciones hechas al Comité de Seguridad deben entenderse realizadas a la Directora-Gerente.

7. FORMAZIOA ETA KONTZIENTZIAZIOA/FORMACIÓN Y CONCIENCIACIÓN

Informazioaren segurtasunak Mankomunitateko kide guztiei eta garatzen diren jarduera guztiei eragiten diela erabat jabetzeko helburuarekin, ENS-SENaren 5. artikuluan jasotako Segurtasun Integralaren printzipioarekin bat etorriz, eta prozesuan esku hartzen duten pertsona guztiek eta horien arduradun hierarkikoek arriskuekiko sentsibilitatea izan dezaten beharrezkoak

Con el objetivo de lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de la Mancomunidad y a todas las actividades que se desarrollan, de acuerdo con el principio de Seguridad Integral recogido en el artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus

diren baliabideak artikulatzeko helburuarekin.

responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Ahalik eta arreta handiena jarriko da segurtasun-prozesuan esku hartzen duten pertsonen eta horien arduradun hierarkikoen kontzientziazioan, informazio-sistemen segurtasunerako arrisku-iturri izan ez daitezen ezjakintasuna, antolaketa- eta koordinazio-falta eta jarraibide desegokiak.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso de seguridad y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad de los sistemas de información.

Informazioarekin eta sistemekin zerikusia duten langile guztiei prestakuntza eta informazioa eman beharko zaizkie segurtasun-arloan dituzten betebehar eta betebeharrei buruz. Haien jarduerak gainbegiratu egin behar dira, ezarritako segurtasun-prozedurak betetzen direla egiaztatzeko.

Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos de seguridad establecidos.

Mankomunitateko langileek beharrezko prestakuntza eta informazio espezifikoa jasoko dute, ematen diren sistemei eta zerbitzuei aplika dakizkiekeen informazioaren teknologien segurtasuna bermatzeko.

El personal de la Mancomunidad recibirá la formación e información específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios que se prestan.

Etengabeko kontzientziazio-programa bat ezarriko da Mankomunitateko kide guztientzat, bereziki sartu berri direnentzat.
Sistemen segurtasuna langile kualifikatuek, dedikatuek eta trebatuek zaindu, berrikusi eta ikuskatuko dute beren bizi-zikloaren fase guztietan: instalazioan, mantentze-lanetan, gorabeheren kudeaketan eta desegitean.

Se establecerá un programa de concienciación continua dirigido a todos los miembros de la Mancomunidad, en particular a los de nueva incorporación.
La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

8. ARRISKUEN KUDEAKETA/GESTIÓN DE RIESGOS

Politika honen mendeko sistema guztien gainean arriskuen analisi bat egiten da, eta horien eraginpean dauden mehatxuak eta arriskuak ebaluatzen dira. MAGERIT metodologia jarraitzen da (arriskuak aztertzeko eta kudeatzeko metodologia, Administrazio Elektronikoaren Kontseilu Nagusiak egina, arriskuen kudeaketa gobernu onaren gidetan giltzarria dela uste duena). 2012an eguneratua, 3. bertsioan).

Sobre todos los sistemas sujetos a esta Política se realiza un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Se sigue la metodología MAGERIT (metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. Actualizada en 2012 en su versión 3).

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/

pae_Metodolog/
pae_Magerit.html#.WD2otn0bhQM

Azterketa hori errepikatu egingo da:

- Aldizka, urtean behin gutxienez.
- Maneiatutako informazioa aldatzen denean.
- Emandako zerbitzuak aldatzen direnean.
- Segurtasun-gorabehera larriren bat gertatzen denean.
- Kalteberatasun larriak daudenean.

Arriskuen analisiak harmonizatzeko, Segurtasun Batzordeak erreferentziazko balorazio bat ezarriko du maneiatutako informazio motetarako eta emandako zerbitzuetarako. Segurtasun Batzordeak segurtasun-beharrei erantzuteko baliabideen eskuragarritasuna dinamizatuko du, inbertsio horizontalak sustatuz.

pae_Metodolog/
pae_Magerit.html#.WD2otn0bhQM

Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad, promoviendo inversiones de carácter horizontal.

9. INFORMAZIOAREN SEGURTASUN-POLITIKA GARATZEA/ DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Politika hori honako dokumentu hauen bidez garatzen da, alderdi espezifikoei aurre eginez:

- Segurtasun-arauak.
- Segurtasun-prozedurak.
- Sinadura elektronikoko politika.
- Informazio-sistema baloratzea.

Esta Política se desarrolla por medio de los siguientes documentos, que afrontan aspectos específicos:

- Normas de Seguridad.
- Procedimientos de Seguridad.
- Política de firma electrónica.
- Valoración del Sistema de Información.

Era berean, baliabideak (ekipoak, baliabideak eta instalazioak) erabiltzeko araudia ezagutu behar duten erakundeko kide guztien eskura dago, bereziki Mankomunitateko informazio- eta komunikazio-sistemekin lan egin, erabiltzen edo administratzen dituztenen eskura.

Asimismo, la normativa de uso de recursos (equipos, recursos e instalaciones) está a disposición de todos los miembros de la entidad que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones de la Mancomunidad.

10.LANGILEEN BETEBEHARRAK/OBLIGACIONES DEL PERSONAL

Mankomunitateko kide guztiek dute informazioaren segurtasun-politika eta segurtasun-araudia ezagutzeko eta betetzeko betebeharra, eta Segurtasun Batzordearen

Todos los miembros de la Mancomunidad tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo

ardura da informazioa eraginpekoei helarazteko behar diren bitartekoak jartzea.

responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Mankomunitateko kide guztiek segurtasunari buruzko kontzientziazio-saio bat egingo dute gutxienez urtean behin. Etengabeko kontzientziazio-programa bat ezarriko da Mankomunitateko kide guztiei arreta emateko, bereziki sartu berriei.

Todos los miembros de la Mancomunidad atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Mancomunidad, en particular a los de nueva incorporación.

IKT sistemen erabileran, eragiketan edo administrazioan erantzukizuna duten pertsonek sistemak segurtasunez erabiltzeko prestakuntza jasoko dute, beren lana egiteko behar duten neurrian. Prestakuntza nahitaezkoa izango da ardura bat bere gain hartu aurretik, bai lehen esleipena bada, bai lanpostuz edo arduraz aldatzen bada.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11.HIRUGARRENAK/TERCERAS PARTES

Mankomunitateak beste erakunde batzuei zerbitzuak ematen dizkienean edo beste erakunde batzuen informazioa erabiltzen duenean, Informazioaren Segurtasunerako Politika horren partaide egingo dira, IKTen Segurtasun Batzordeak informatzeko eta koordinatzeko kanalak ezarriko dira eta segurtasun-gorabeheren aurrean erantzuteko jarduketa-prozedurak ezarriko dira.

Cuando la Mancomunidad preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Mankomunitateak hirugarrenen zerbitzuak erabiltzen dituenean edo hirugarrenei informazioa ematen dienean, zerbitzu edo informazio horiei eragiten dien segurtasun-politika eta segurtasun-araudia jakinaraziko zaie. Hirugarren hori araudi horretan ezarritako betebeharren mende geratuko da, eta araudi hori betetzeko bere prozedura operatiboak garatu ahal izango ditu. Gorabeherak jakinarazteko eta konpontzeko prozedura espezifikoak ezarriko dira. Bermatuko da hirugarrenetako langileak behar bezala kontzientziatuta daudela segurtasunaren arloan, gutxienez politika honetan ezarritako maila berean.

Cuando la Mancomunidad utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Aurreko paragrafoetan eskatzen denaren

Cuando algún aspecto de la Política no pueda

arabera, politikaren alderdiren bat heren batek ezin badu bete, segurtasun-arduradunaren txosten bat beharko da, arriskuak eta horiek tratatzeko modua zehazteko. Informazioaren arduradunek eta eragindako zerbitzuek txosten hori onartu beharko dute aurrera jarraitu aurretik.

ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

12.ONARTZEA ETA INDARREAN SARTZEA/ APROBACIÓN Y ENTRADA EN VIGOR

Informazioaren Segurtasunerako Politika hau eraginkorra da Mankomunitateko Batzarrak onartzen duen datatik, eta politika berri batek ordezten duen arte.

Esta Política de Seguridad de la Información es efectiva desde la fecha que se apruebe en la Junta de la Mancomunidad y hasta que sea reemplazada por una nueva Política.

13.BERRIKUSPEN PROZEDURA/ PROCEDIMIENTO DE REVISIÓN

Zuzendari-Kudeatzailearen egitekoa izango da informazioaren segurtasun-politika hori urtero berrikustea eta hura berrikusteko edo mantentzeko proposamena egitea.
Politika honen berrikuspenak Mankomunitateko Batzarrak onartuko ditu eta zabalduko da, eragindako alderdi guztiek ezagutu dezaten.

Será misión de la Directora-Gerente la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta.
Las revisiones de esta Política serán aprobada por la Junta y difundida para que la conozcan todas las partes afectadas.

14.DATU PERTSONALAK/ DATOS DE CARÁCTER PERSONAL

Mankomunitate honek datu pertsonalak tratatzen ditu. Tratamendu-jardueren erregistroak horiek eta horien helburua jasotzen ditu. Mankomunitateko informazio-sistema guztiak ezarritako arrisku-irizpideen, izaeraren eta helburuaren arabera babestuko dira, Datuak Babesteko Politikan adierazten den bezala.

Esta Mancomunidad trata datos de carácter personal. El Registro de Actividades de Tratamiento recoge éstos y su finalidad. Todos los sistemas de información de la Mancomunidad se protegerán en función de los criterios de riesgo establecidos, su naturaleza y finalidad, tal y como se indica en su Política de Protección de Datos.

Eranskina. Rolak eta erantzukizunak

CCS – Segurtasun Batzordea.
RINFO – Informazioaren arduraduna.
RSERV – Zerbitzuaren arduraduna.
RSEG – Segurtasunaren arduraduna.
RSIS – Sistemaren arduraduna.
ASS – SSII administratzaileak.

ZEREGINA	ARDURADUNA
Dimentsio bakoitzean eskatzen diren segurtasun-mailak zehaztea	CCS
Sistemaren kategoria zehaztea	CCS
Arriskuen analisia	RSEG
Aplikagarritasun-aitorpena	RSEG
Segurtasun-neurri gehigarriak	RSEG
Segurtasun-konfigurazioa	egilea: RSEG aplikatzailea: ASS
Segurtasun-neurriak ezartzea	ASS
Hondar-arriskua onartzea	RINFO + RSERV
Sistemaren segurtasunari buruzko dokumentazioa	RSEG
Segurtasun-politika	egilea: CCS oneslea: Zuzendaritza nagusia
Segurtasun-araudia	egilea: RSEG oneslea: CCS
Segurtasuneko prozedura operatiboak	egilea: RSIS oneslea: RSEG aplikatzailea: ASS
Sistemaren segurtasunaren egoera	begiralea: ASS Erreportaria: RSEG
Segurtasuna hobetzeko planak	egileak: RSIS + RSEG oneslea: CCS
Kontzientziazio- eta prestakuntza-planak	egilea: RSEG oneslea: CCS
Jarraipen-planak	egilea: RSIS Balidatzailea: RSEG Koordinatzailea eta oneslea: CCS Ariketak: RSIS
Zerbitzua aldi baterako etetea	RSIS
Bizi-zikloa: espezifikazioa, arkitektura, garapena, eragiketa, aldaketak	egilea: RSIS oneslea: RSEG

Anexo. Roles y responsabilidades

CCS – Comité de Seguridad
RINFO – Responsable de la Información
RSERV – Responsable del Servicio
RSEG – Responsable de la Seguridad
RSIS – Responsable del Sistema
ASS – Administradores de SSII

TAREA	RESPONSABLE
Determinación de los niveles de seguridad requeridos en cada dimensión	CCS
Determinación de la categoría del sistema	CCS
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	elabora: RSEG aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	RSEG
Política de seguridad	elabora: CCS aprueba: Dirección General
Normativa de seguridad	elabora: RSEG aprueba: CCS
Procedimientos operativos de seguridad	elabora: RSIS aprueba: RSEG aplica: ASS
Estado de la seguridad del sistema	monitoriza: ASS reporta: RSEG
Planes de mejora de la seguridad	elaboran: RSIS + RSEG aprueba: CCS
Planes de concienciación y formación	elabora: RSEG aprueba: CCS
Planes de continuidad	elabora: RSIS valida: RSEG coordina y aprueba: CCS ejercicios: RSIS
Suspensión temporal del servicio	RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS aprueba: RSEG