IV. ERANSKINA
SEGURATSUNARI BURUZKO AGIRIAK

DATU PERTSONALEN BABESAren

arloko Jardunbide Egokien Eskuliburua Euskal

Autonomia Erkidegoko toki erakundeetarako

ANEXO IV
DOCUMENTOS RELACIONADOS CON LA SEGURIDAD

Manual de Buenas Prácticas para entidades locales de

la Comunidad Autónoma del País Vasco en materia de

PROTECCIÓN DE DATOS PERSONALES

Jardunbide Egokien Eskuliburu hau egiten parte hartu dute:

Ana Novoa Carbarllido, Vitoria-Gasteizko Udala
Enrique Pascual Antxia, Basauriko Udala
José Antonio Fernández Celada, Ermuko Udala
Javier Aramberri Miranda, Getxoko Udala
José Luis Irigoien Martínez, Eibarko Udala
Julen Urteaga Legarra, Beasaingo Udala
Iñaki Galdeano Larizgoitia, EUDEL
Ignacio Alonso Errazti, EUDEL
Pedro Alberto González González, DBEB
Pablo Lakuntza Amiano, DBEB
Edurne Barañano Etxebarria, DBEB
Aintzane Osa Alberdi, Euskarazko itzulpena, DBEB
Simón Mesanza Legarda, DBEB

Ale kopurua: 1500 ale

Argitaratzailea: **EUDEL. Euskadiko Udalen Elkartea**
Internet: www.eudel.net
Inprimaketa: GRAFILUR S.A.
L.G.: BI-1239-08

En la elaboración de este **Manual de Buenas Prácticas** han colaborado las siguientes personas:

Ana Novoa Carbarllido, Ayuntamiento de Vitoria-Gasteiz
Enrique Pascual Antxia, Ayuntamiento de Basauri
José Antonio Fernández Celada, Ayuntamiento de Ermua
Javier Aramberri Miranda, Ayuntamiento de Getxo
José Luis Irigoien Martínez, Ayuntamiento de Eibar
Julen Urteaga Legarra, Ayuntamiento de Beasain
Iñaki Galdeano Larizgoitia, EUDEL
Ignacio Alonso Errazti, EUDEL
Pedro Alberto González González, AVPD
Pablo Lakuntza Amiano, AVPD
Edurne Barañano Etxebarria, AVPD
Aintzane Osa Alberdi, traducción al euskera, AVPD
Simón Mesanza Legarda, AVPD

Tirada: 1500 ejemplares

Edita: **EUDEL. Asociación de Municipios Vascos**
Internet: www.eudel.net
Impresión: GRAFILUR S.A.
D.L.: BI-1239-08

AURKIBIDEA / ÍNDICE

ERANSKINA
ANEXO

IV

EREDUAK ETA DOKUMENTUEN ADIBIDEAK

MODELOS Y DOCUMENTOS TIPO

Segurtasun agiri bat zehaztu behar dugu. Segurtasun agiri honek 3 ale izango ditu. Hona hemen:

1. alea edo Arauak: ale honetan giza baliabideen antolaketaren gaineko segurtasun politika zehaztuko da, DPen fitxategietarako sarbidearen ikuspuntutik, eta erabiltzaile profil bakoitzaren eginkizunak eta erantzukizunak finkatuko dira.

2. alea edo Prozedurak: ale honetan kopiak eta berreskuratzeak egiteko prozedurak, segurtasun-gorabeheretarako prozedurak eta abar zehaztuko dira.

3. alea edo Eranskinak: ale honek fitxategien benetako egoera, baimenak eta abar islatzen ditu. Ale hau da gehien aldatu beharko duguna benetako egoera islatzeko. Ale hau barne erabilerarako da eta argitaratuta egon daiteke ala ez, oso aldakorra delako erakunde handietan eta ez delako hainbeste aldatzen txikietan.

Beraz, horregatik, gerta daiteke informazio guzti hau erakundean dauden inprimakietan bilduta egotea edo kudeaketarako aplikazio batean jasota egotea. Edozelan ere, kontrol agintaritzak edozein unetan eska dezakeenez, ezinbestekoa da nahi denean erraz eta azkar eskuratzeko moduan izatea.

Lehendabiziko ale biak bakar batean bildu ahal izango dira edo hemen proposatutako eskema mantendu ahal izango da, toki erakunde bakoitzaren antolaketaren arabera.

Definimos un modelo de Documento de Seguridad según el cual dividimos el Documento de Seguridad en 3 volúmenes:

Volumen 1 o Normas: en este volumen se define la política de seguridad en lo referente a la organización de los recursos humanos desde el punto de vista del acceso a los ficheros con DCP y las funciones y responsabilidades de los diferentes perfiles de usuario/a.

Volumen 2 o Procedimientos: en este volumen se definen cómo se realizan concretamente los procedimientos de copias y recuperación, incidencias, etc.

Volumen 3 o Anexos: este volumen refleja la información real de ficheros, permisos, etc., en cada momento. Este es el volumen que más frecuentemente hemos de modificar para reflejar la situación real. Este volumen es de uso interno y además puede estar o no publicado, ya que en organizaciones grandes es muy variable, y es bastante estable en organizaciones pequeñas.

Lo anterior conlleva que esta información pueda estar soportada en base a formularios existentes en la organización, o pueda estar soportada por una aplicación de gestión; en cualquier caso y dado que esta información puede ser solicitada por las autoridades de control, debe ser obtenible de una manera ágil y precisa en cualquier momento.

En función de la organización de cada entidad local, ésta podrá decidir aglutinar los 2 primeros volúmenes en uno sólo, o mantener el esquema aquí propuesto.

1. ALEA. ARAUAK

1. SARRERA

2. EZARPEN EREMUA

3. ARAUAK

- Segurtasun-gorabeheren erregistroa
- Identifikazioa eta autentifikazioa- Erabiltzaileen administrazioa
- Datuetarako sarbide kontrola
- Euskarrien kudeaketa eta banaketa
- Babes kopiak eta berreskuratzea
- Segurtasun arduraduna
- Auditoria
- Sarbide fisikoaren kontrola
- Probak benetako datuekin
- Telekomunikazioak

4. GIZA BALIABIDEEN KUDEAKETA

- Tratamendu kontrolatzailea
- Segurtasun arduraduna
- Tratamenduaren arduraduna
- Sistema informatikoen erabiltzaileak

5. EGINKIZUNAK ETA BETEBEHARRAK

- Tratamendu kontrolatzailearen fitxategia

- Segurtasun arduradunaren eginkizunak

- Tratamendu arduradunaren eginkizunak

- Erabiltzaile guztien betebeharrak:

  - Hw baliabideak
  - Sw baliabideak
  - Identifikazioa eta autentifikazioa
  - Segurtasun gorabeheren kudeaketa
  - Euskarrien kudeaketa
  - Sekretua gorde beharra

6. DP-EN FITXATEGIEN EGITURA

7. TERMINOEN ZERRENDA

VOLUMEN 1. NORMAS

1. INTRODUCCIÓN

2. ÁMBITO DE APLICACIÓN

3. NORMAS

- Registro de incidencias
- Identificación y autenticación - Administración de usuarios/as
- Control de acceso a datos
- Gestión y distribución de soportes
- Copias de respaldo y recuperación
- Responsable de Seguridad
- Auditoría
- Control de acceso físico
- Pruebas con datos reales
- Telecomunicaciones

4. ORGANIZACIÓN DE RECURSOS HUMANOS

- Responsable de los Ficheros
- Responsable de Seguridad
- Persona encargada del Tratamiento
- Usuarios/as de SSII

5. FUNCIONES Y OBLIGACIONES

- Funciones de la persona Responsable de Ficheros
- Funciones de la persona Responsable de Seguridad
- Funciones de la persona Encargada del Tratamiento
- Obligaciones que afectan a todo el personal usuario:

  - Recursos Hw
  - Recursos Sw
  - Identificación y autenticación
  - Gestión de incidencias
  - Gestión de soportes
  - Deber de Secreto

6. ESTRUCTURA DE LOS FICHEROS DCP

7. GLOSARIO DE TÉRMINOS

2. ALEA - PROZEDURAK

- Jakinarazpen, kudeaketa eta erantzun prozedura, gorabeheraren bat dagoenerako
- Erabiltzaileak kudeatzeko prozedura
- Baimenak kudeatzeko prozedura
- Euskarriak kudeatzeko prozedura
- Kopiak eta datu berreskuratzeak kudeatzeko prozedura
- Segurtasun agiria eguneratzeko prozedura

VOLUMEN 2. PROCEDIMIENTOS

- Procedimiento de notificación, gestión y respuesta ante las incidencias
- Procedimiento de gestión de usuarios/as
- Procedimiento de gestión de permisos
- Procedimiento de gestión de soportes
- Procedimiento de gestión de copias y de recuperación de datos
- Procedimiento de actualización del Documento de Seguridad

3. ALEA - ERANSKINAK

- 1.1. Eranskina.- DPdun fitxategiak eta horien segurtasun arduradunak
- 1.2. Eranskina.- Aplikazioak
- 1.3. Eranskina.- Ekipo informatiko pertsonalak
- 1.4. Eranskina.- Zerbitzariak eta sistema eragilearen eta komunikazio sistemaren ingurunea
- 1.5. Eranskina.- Tratamendu zentroak
- 1.6. Eranskina.- Erabiltzaileak

VOLUMEN 3. ANEXOS

- Anexo 1.1.- Ficheros con DCP y sus responsables de seguridad
- Anexo 1.2.- Aplicaciones
- Anexo 1.3.- Equipos informáticos personales
- Anexo 1.4.- Servidores y el entorno de sistema operativo y de comunicaciones

- Anexo 1.5.- Centros de tratamiento
- Anexo 1.6.- Usuarios/as

SEGURTASUN AGIRIA – ARAUAK

DOCUMENTO DE SEGURIDAD - NORMAS

1. HITZAURREA

Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoaren (DBLO) 9. artikuluko 1. paragrafoak honakoa xedatzen du: Tratamendu kontrolatzaileak eta, hala badagokio, tratamendu arduradunak datu pertsonalak babestuta daudela eta datu horiek ez direla aldatuko eta galduko, eta baimendu gabeko tratamendurik edo atzipenik ez dela egingo bermatzen dituzten neurri teknikoak eta antolaketakoak hartu beharko dituzte, teknologiaren egoera, bildutako datuen ezaugarriak eta datu horiek dauzkaten arriskuak kontuan hartuta. Arriskuak gizakiaren jardueretatik edo ingurune fisiko eta naturaletik etor daitezke.

Artikulu bereko 2. paragrafoak dio fitxategietan ez dela datu pertsonalik erregistratuko, baldin eta fitxategiek eta tratamendu zentro, lokal, ekipo, sistemena eta programek ez badituzte betetzen osotasunari eta segurtasunari buruz erregelamendu bidez ezarritako baldintzak. Era berean, 3. paragrafoak xedatzen du Erregelamendu baten bidez ezarriko direla bereziki babestutako datuen tratamenduan parte hartzen duten pertsonek eta fitxategiek bete beharreko betekizunak eta baldintzak.

Datu pertsonalak babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatzeko Erregelamendua onartzen duen abenduaren 21eko 1720/2007 Errege Dekretuak eta erregelamenduaren 88. artikuluak xedatzen dute segurtasun agiria egin eta ezarri behar dela eta agiria nahitaez bete behar dutela komunikazio sistemak eta automatizatutako datu pertsonalak atzitu ditzaketen langileek.

DBLO garatzen duen Erregelamenduaren 5. artikuluak datuen tratamendu automatizatuaren arloko zenbait kontzeptu definitzen ditu. Segurtasun agiri honetarako kontzeptu eta definizio horiexek erabiliko ditugu. Hona hemen:

1. INTRODUCCIÓN

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), establece en su punto 1 que *"la persona Responsable del Fichero, y, en su caso, las personas encargadas del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana, del medio físico o natural."*

El mismo artículo en el punto 2 añade que *"no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas"*; y en el punto 3 remite a un Reglamento posterior el establecimiento de los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos especialmente protegidos.

El Real Decreto 1720/2007, de 21 de diciembre, aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y el artículo 88 de dicho Reglamento especifica la necesidad de elaborar e implantar el Documento de Seguridad siendo éste un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de comunicación.

El artículo 5 del Reglamento de desarrollo de la LOPD define una serie de conceptos en el ámbito del tratamiento automatizado de datos; conceptos y definiciones que adoptaremos en el ámbito de este Documento de Seguridad. En consecuencia, se entenderá por:

- Ukitua edo interesduna: tratatu beharreko datu pertsonalen titularra den pertsona fisikoa.

- Ezereztea: prozedura honen eraginez, arduradunak datuak erabiltzeari uzten dio. Ezerezteak datuak blokeatzea dakar, hau da, datu horiek identifikatzea eta gordetzea dakar, tratamendurik egon ez dadin. Izan ere, egon daitekeen tratamendu bakarra da datuak administrazio publikoen eta epaile eta epaitegien eskura uztea, tratamenduaren ondorioz sor daitezkeen erantzukizunei erantzun ahal izateko, baina beti ere erantzukizunaren preskripzio epearen barruan. Preskripzio epea igaro ondoren, datuak ezabatu egin beharko dira.

- Datuak lagatzea edokomunikatzea: interesduna ez den beste pertsona bati datuen berri ematea dakarren tratamendua.

- Interesdunaren adostasuna: interesdunaren borondate-adierazpen askea, argia, berariazkoa eta informatua da, berari buruzko datu pertsonalak tratatzeko adostasuna adierazteko.

- Datu disoziatua: ukitua edo interesduna identifikatzen uzten ez duen datua.

- Datu pertsonalak: pertsona fisiko identifikatu edo identifikagarriei buruzko edozein informazio (zenbakizkoa, alfabetikoa, grafikoa, fotografikoa, akustikoa edo beste edozein motatakoa).

- Osasunarekin zerikusia duten datu pertsonalak: norbanakoaren osasun fisikoari edo buru osasunari buruzko lehengo, oraingo eta etorkizuneko informazioa. Pertsonen osasunari buruzko datu pertsonaltzat jotzen dira batez ere norbanakoaren ezgaitasun portzentajea eta norbanakoaren informazio genetikoa.

- Afectado/a o interesado/a: Persona física titular de los datos que sean objeto del tratamiento.

- Cancelación: Procedimiento en virtud del cual la persona responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces o Juezas y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

- Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta de la persona interesada.

- Consentimiento de la persona interesada: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que la persona interesada consienta el tratamiento de datos personales que le conciernen.

- Dato disociado: aquél que no permite la identificación de una persona afectada o interesada.

- Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

- Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

- Hartzailea edo lagapen-hartzailea: datu transferentzia jasotzen duen pertsona fisikoa edo juridikoa, publikoa edo pribatua ala administrazio organoa. Nortasun juridikorik ez duten enteak ere hartzaile izan daitezke, baldin eta subjektu berezitu moduan jarduten badute trafikoan.

- Destinatario/a o cesionario/a: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- Tratamendu arduraduna: pertsona fisikoa nahiz juridikoa, agintari publikoa nahiz pribatua edo administrazio organoa da, bakarrik nahiz beste batzuekin batera datuak tratatzen dituena tratamendu kontrolatzailearen edo fitxategiaren erantzulearen kontura, harreman juridiko bat dagoelako tratamendu kontrolatzailearekin edo fitxategiaren erantzulearekin lotzen duena eta zerbitzua emateko jardute eremua mugatzen diona.
Nortasun juridikorik ez duten enteak ere tratamendu arduradun izan daitezke, baldin eta subjektu berezitu moduan jarduten badute trafikoan.

- Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta de la persona Responsable del tratamiento o de la persona Responsable del Fichero, como consecuencia de la existencia de una relación jurídica que le vincula con la misma y delimita el ámbito de su actuación para la prestación de un servicio.
Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciado.

- Datu pertsonalen esportatzailea: Espainian kokatuta dagoen pertsona fisikoa edo juridikoa, publikoa edo pribatua ala administrazio organoa, Erregelamendu honetan xedatutakoa kontuan hartuta, hirugarren herrialde batera datu pertsonalen transferentzia bat egiten duena.

- Exportadora de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

- Fitxategia: datu pertsonalei buruzko informazio-multzo egituratua, irizpide jakin batzuk erabilita datuak atzitzen uzten duena, edozein dela ere sortzeko, biltegiratzeko, antolatzeko eta atzitzeko era edo modalitatea.

- Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma
o modalidad de su creación, almacenamiento, organización y acceso.

- Titulartasun pribatuko fitxategiak: zuzenbide pribatuko enpresa edo entitateen edo pertsonen erantzukizunpean dauden fitxategiak dira, alde batera utzita horien kapitalaren edo baliabide ekonomikoen titularra nor den. Horiez gain, zuzenbide publikoko korporazioen erantzukizunpeko fitxategiak ere titulartasun pribatuko fitxategiak dira, baldin eta fitxategi horiek ez badaude erabat lotuta korporazioen berariazko araudiak esleitutako zuzenbide publikoko ahalei.

- Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

- Titulartasun publikoko fitxategiak: Estatuko organo konstituzionalen edo konstituzio mailako organoen erantzukizunpeko fitxategiak, antzeko eginkizunak dauzkaten erakunde autonomiadunen erantzukizunpeko fitxategiak, lurraldeetako administrazio publikoen erantzukizunpekoak eta horiei lotutako edo horien menpeko entitate edo erakundeen erantzukizunpekoak, eta zuzenbide publikoko korporazioen erantzukizunpekoak, baldin eta haien helburua zuzenbide publikoko ahalez baliatzea bada.

- Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

- Fitxategi ez automatizatu: datu pertsonalei buruzko informazio multzoa da, modu ez automatizatuan antolatua eta pertsona fisikoei buruzko irizpide jakin batzuen arabera egituratua, pertsona horien datuak ahalegin berezirik egin gabe atzitzeko aukera ematen duena; eta zentralizatuta ala deszentralizatuta edo modu funtzionalean edo geografikoan banatuta egon daiteke.

- Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.

- Datu pertsonalen inportatzailea: hirugarren herrialde batera egiten den datu transferentzietan datuak jasotzen dituen pertsona fisikoa edo juridikoa, publikoa edo pribatua ala administrazio organoa. Tratamendu kontrolatzailea, tratamenduaren arduraduna nahiz hirugarrena izan daiteke.

- Importadora de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

- Pertsona identifikagarria: zuzenean edo zeharka, nor den jakin daitekeen pertsona fisikoa, bereziki bere nortasun fisiko, psikiko, ekonomiko, kultural edo sozialari dagozkion ezaugarri bat edo gehiago erabiliz. Pertsona fisiko bat ez da joko identifikagarritzat identifikaziorako neurriz kanpoko epeak edo jarduerak behar badira.

- Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

- Disoziazio prozedura: Datu pertsonalen tratamendu oro, datu disoziatuak lortzeko.

- Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

- Fitxategiaren erantzulea edo tratamendu kontrolatzailea: pertsona fisikoa nahiz juridikoa, publikoa nahiz pribatua edo administrazio organoa da, eta bakarrik edo beste batzuekin batera erabakitzen du zein den tratamenduaren helburua, edukia eta erabilera, nahiz eta berak ez gauzatu tratamendua. Nortasun juridikorik ez duten enteak ere tratamendu kontrolatzaile izan daitezke, baldin eta subjektu berezitu moduan jarduten badute trafikoan.

- Responsable del Fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también Responsables del Fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- Hirugarrena: pertsona fisikoa nahiz juridikoa, agintari publikoa nahiz pribatua edo administrazio organoa da, ondoko hauetako bat ez dena: ukitua edo interesduna, tratamendu kontrolatzailea edo fitxategiaren erantzulea, tratamendu kontrolatzailearen edo tratamenduaren arduradunaren zuzeneko ardurapean datuak tratatzeko baimena duen pertsona.

Nortasun juridikorik ez duten enteak ere hirugarren izan daitezke, baldin eta subjektu berezitu moduan jarduten badute trafikoan.

- Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinto del afectado o interesado, del responsable del tratamiento, del Responsable del Fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa de la persona responsable del tratamiento o de la persona del tratamiento.
Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

- Nazioarteko datu-transferentziak: Europako Esparru Ekonomikotik kanpora datu transmisioa egitea dakarren tratamendua da. Datu lagatzea edo datu komunikazioa izan daiteke edo Espainian kokatuta dagoen tratamendu kontrolatzailearen kontura egiten den datu tratamendu bat izan daiteke.

- Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta de la persona Responsable del Fichero establecido en territorio español.

- Datuen tratamendua: modu automatizatuan edo ez automatizatuan egiten diren operazio edo prozedura teknikoak dira, eta datuak jaso, grabatu, gorde, landu, aldatu, kontsultatu, erabili ezereztu, blokeatu eta ezabatzea ahalbideratzen dute, bai eta komunikazio, kontsulta, interkonexio eta transferentzietatik etorritako datu lagatzeak egitea ere.

- Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Erregelamendu honetako VIII. tituluan (datu pertsonalen tratamendurako segurtasun neurriei buruzkoa) kontuan hartuta:

En particular, en relación con lo dispuesto en el título VIII (de las medidas de seguridad en el tratamiento de datos de carácter personal) de este reglamento se entenderá por:

- Baimendutako atzipenak: erabiltzaile bati emandako baimenak, zenbait baliabide erabil ditzan. Hala badagokio, tratamendu kontrolatzaileak edo segurtasun arduradunak erabiltzaile bati eskuordetutako baimenak edo eginkizunak ere bai.

- Accesos autorizados: autorizaciones concedidas a un usuario o usuaria para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario o usuaria por delegación de la persona Responsable del Fichero o tratamiento o de la persona Responsable de Seguridad.

- Autentifikazioa: erabiltzaile baten identitatea egiaztatzeko ezagutze prozedura.

- Autenticación: procedimiento de comprobación de la identidad de un usuario o usuaria.

- Pasahitza: erabiltzaile bat autentifikatzeko edo baliabide bat atzitzeko erabil daitekeen isilpeko informazioa, karaktere-kate batez osatuta egon ohi dena.

- Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

- Sarbide kontrola: erabiltzailearen identitatea autentifikatu eta identifikatu ondoren datuak edo baliabideak atzitzen uzten duen mekanismoa.

- Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

- Babes kopia: fitxategi automatizatu bateko datuak kopiatzea datu horiek berreskuratzeko aukera ematen duen euskarri batean.

- Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

- Agiria: informazio sistema baten barruan ale berezitu moduan tratatu daitekeen idazki, grafiko, soinu edo irudi oro nahiz bestelako edozein informazio mota.

- Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

- Fitxategi iragankor: erabiltzaileek edo prozesuek sortutako fitxategiak. Beharrezkoak izan ohi dira noizbehinkako tratamenduetarako edo tratamendu baten barruko urrats moduan.

- Ficheros temporales: ficheros de trabajo creados por usuarios/as o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

- Identifikazioa: erabiltzaile baten identitatea jakiteko ezagutze prozedura.

- Identificación: procedimiento de reconocimiento de la identidad de un usuario.

- Segurtasun gorabehera: datuen segurtasunari eragiten dion edo eragin diezaiokeen edozein irregulartasun.

- Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

- Erabiltzaile profila: erabiltzaile multzo bati baimendutako atzipenak.

- Perfil de usuario/a: accesos autorizados a un grupo de usuarios/as.

- Baliabidea: informazio sistema baten edozein osagai.

- Segurtasun arduraduna: tratamenduaren kontrolatzaileak izendatutako pertsona edo pertsonak, aplikatu beharreko segurtasun neurriak koordinatu eta kontrolatzeko.

- Informazio sistemak: datu pertsonalak tratatzeko erabili ohi diren fitxategiak, tratamenduak, programak, euskarriak eta, hala badagokio, bai eta ekipoak ere.

- Tratamendu sistemak: informazio sistema bat antolatzeko edo erabiltzeko modua. Tratamenduaren sistema kontuan hartuta, informazio sistemak automatizatuak, ez automatizatuak edo zati batean automatizatuak izan daitezke.

- Euskarria: datuak edo dokumentuak biltegiratzen edo jasotzen dituen objektu fisikoa, edo informazio sistema batean tratatzeko modukoa den objektua. Bertan datuak grabatu eta berreskuratu ahal dira.

- Dokumentu transmisioa: bertan jasotako informazioa garraiatzea, jakinaraztea, bidaltzea, ematea edo hedatzea.

- Erabiltzailea: datuak edo baliabideak erabiltzeko baimena duen pertsona edo prozesua. Erabiltzailetzat joko dira identifikaziorik gabe erabiltzaile fisiko baten datuak edo baliabideak atzitzen uzten duten prozesuak.

- Recurso: cualquier parte componente de un sistema de información.

- Responsable de Seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

- Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

- Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

- Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

- Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

- Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un/a usuario/a físico/a.

2. EZARPEN EREMUA

Agiri hau ondoko toki entitatearen erantzukizunpean dauden datu pertsonalen fitxategiei ezarriko zaie: [toki entitea]; datu pertsonalen fitxategiak modu eraginkorrean babesteko, datu pertsonalen fitxategi horietara sarbidea erraztu dezaketen bestelako baliabideak ere kontrolatu behar dira. Beraz, horiek ere segurtasun agiri honen ezarpen eremuan sartzen dira:

2. ÁMBITO DE APLICACIÓN

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de [entidad local]; del mismo modo la protección efectiva de los ficheros con DCP se debe realizar mediante el control de todos los recursos por los que se puede tener acceso a dichos ficheros con datos de carácter personal, por lo que también se incluyen en el ámbito de este Documento de Seguridad:

- DPen fitxategietara sarbidea duten **aplikazioak**.
- Fitxategi horietara sarbidea izan dezaketen **ekipo informatikoak**, tokikoak nahiz urrutikoak.
- Fitxategi horiek kokatuta dauden **zerbitzariak** eta sistema eragilearen eta komunikazio sistemaren ingurunea.
- Zerbitzari horiek kokatuta dauden **instalazioak** edo tratamendu zentroak edo lokalak, bai eta DPen fitxategiak biltegiratzen dituzten bestelako tokiak ere.

- Datu pertsonalak atzitu ditzaketen **erabiltzaileak**.

- Las **aplicaciones** con acceso a dichos ficheros con DCP.
- Los **equipos informáticos**, locales o remotos, desde los que se puede tener acceso a los ficheros.
- Los **servidores** y el entorno de sistema operativo y de comunicaciones en el que se encuentran ubicados los ficheros.
- Las **instalaciones** o centros de tratamiento y locales donde se encuentran ubicados dichos servidores y también aquellos en los que se almacenan los soportes que contengan ficheros con DCP.
- Los/as **usuarios/as** que puedan acceder a datos de carácter personal.

Baliabide fisikoen, baliabide logikoen eta giza baliabideen inbentarioa segurtasun agiri honen eranskinetan dago islatuta.

Hona hemen:

- 1. ERANSKINA Datu pertsonalen fitxategiak.
- 2. ERANSKINA Aplikazioak.
- 3. ERANSKINA Instalazioak.
- 4. ERANSKINA Zerbitzariak.
- 5. ERANSKINA Ordenagailu pertsonalak (mahai gainekoak, eramangarriak eta abar)
- 6. ERANSKINA Erabiltzaileak.

El inventario de cada uno de estos recursos físicos, lógicos y humanos se refleja en los anexos correspondientes del Documento Seguridad.
A saber:

- ANEXO 1 Ficheros con DCP.
- ANEXO 2 Aplicaciones.
- ANEXO 3 Instalaciones.
- ANEXO 4 Servidores.
- ANEXO 5 Ordenadores personales (sobremesa, portátiles, etc.)
- ANEXO 6 Usuarios/as.

3. ARAUAK

3.1 Segurtasun gorabeheren erregistroa

Segurtasun gorabeheratzat joko da datuen segurtasunari eragiten dion edo eragin ahal dion edozein irregulartasun. Udal honek [toki entitea] segurtasun gorabeheren erregistro bat dauka eta bertan honako informazioa gordetzen du:

- Segurtasun gorabehera mota.
- Segurtasun gorabeheraren data eta ordua.
- Nork atzeman duen segurtasun gorabehera.
- Nori jakinarazi zaion.
-Segurtasun gorabeheraren ondorioak.

3. NORMAS

3.1. Registro de incidencias

Entendiendo como incidencia cualquier anomalía que afecta o pudiera afectar a la seguridad de los datos, [entidad local] dispone de un registro de incidencias que guarda la siguiente información:

- Tipo de la incidencia.
- Fecha y hora de la incidencia.
- Persona que la detecta.
- Persona a quien se notifica.
- Efectos de la incidencia.

Segurtasun gorabeheraren ondorioz, segurtasun kopiaren bateko datuak berreskuratu beharra badago, datu horiek berreskuratzeko ezarrita dagoen prozedura bete beharko da, eta guzti horiez gain, honako informazioa ere jaso beharko da segurtasun gorabeheren erregistroan:

- Nork gauzatu zuen prozesua.
- Zeintzuk datu berreskuratu ziren, eta halakorik gertatuz gero, bai eta eskuz zeintzuk datu grabatu ziren ere.

Gorabeheren jakinarazpen, kudeaketa eta erantzun prozeduran dago zehaztuta segurtasun gorabeheren erregistro honen eta bertako prozesuen ezarpena.

Si la incidencia supusiera la necesidad de recuperar datos de alguna copia de seguridad, ésta se realizará siguiendo el procedimiento de recuperación de datos correspondiente y en el registro de incidencias se almacenará, además de lo anterior, la siguiente información:

- Persona que ejecutó el proceso.
- Qué datos se restauraron, y si ha sido necesario, cuáles se han grabado manualmente.

La implementación de este registro de incidencias y sus procedimientos asociados viene especificada en el Procedimiento de notificación, gestión y respuesta ante incidencias.

3.2. Identifikazioa eta autentifikazioa - Erabiltzaileen administrazioa

Udal honetako [toki erakundearen izena] informazio sistemetara sarbidea duen edonor identifikatu eta autentifikatu egin beharko da sistemara sartu nahi badu. Sistemak pasahitz bidez egingo du autentifikazioa eta erabiltzaileak kudeatzeko prozedura bat egongo da pasahitz horien kudeaketa-mekanismoa inplementatzeko.
Erabiltzaileen kudeaketa prozedura horrek honako arauak inplementatuko ditu:

a.Informazio sistema batera sarbidea duten erabiltzaileek atzipen baimen bakarra izango dute, pertsonala eta beste inorena ez dena, eta erabiltzailearen identifikatzailearekin eta pasahitzarekin osatuta egongo da.
b.Pasahitzak bost karaktere edo gehiagoko luzera izango du eta karaktere alfabetikoz eta zenbakikoz osatuta egongo da.

c.Pasahitzen konfidentzialtasuna bermatzeko asmoz, sistemak enkriptatze-algoritmo bidez biltegiratuko ditu.

d.Pasahitza esleitzeko arduradunak (tratamenduaren ardura duen entitateko tratamendu kontrolatzaileak hautatua) pertsonalki jakinaraziko dizkie erabiltzaileei Informazio sistemetan sartzeko pasahitzak.

e.Erabiltzaileak lehengo aldiz saioa hazten duenean aldatu beharko du esleitu dioten pasahitza, eta hortik aurrera nahi duen guztietan aldatu ahal izango du sarbide pasahitza.

3.2. Identificación y autenticación - Administración de usuarios/as

Toda persona que acceda a alguno de los SSII de [entidad local] deberá identificarse y autenticarse para acceder al sistema; la autenticación el sistema se realizará mediante contraseña, existirá un Procedimiento de gestión de usuarios y usuarias que implementará el mecanismo de gestión de dichas contraseñas.
Este procedimiento de gestión de usuarios/as implementará las siguientes reglas:

a.Todos los usuarios y usuarias con acceso a un sistema de información dispondrán de una única autorización de acceso personal y exclusiva compuesta de identificador de usuario o usuaria y contraseña.
b.La longitud de la contraseña será de cinco o más caracteres y estará constituida por una combinación de caracteres alfabéticos y numéricos.
c.El sistema almacenará las contraseñas mediante algoritmos de cifrado, al objeto de garantizar la confidencialidad de las mismas.
d.Las contraseñas de acceso a los sistemas de información serán comunicadas personalmente a los/las usuarios y usuarias por la persona encargada de realizar la asignación de la contraseña (designada por la persona Responsable del Fichero de la entidad encargada del tratamiento).
e.El usuario o usuaria deberá cambiar la contraseña que se le ha asignado en el primer inicio de sesión y a partir de ahí podrá cambiar su contraseña de acceso en cualquier momento.

3.3 Datuetarako sarbide kontrola

Udal honetan [toki entitatearen izena] martxan dabiltzan datu pertsonalen fitxategietan sarbidea duten aplikazio guztiek sarbide kontroleko sistema bat izango dute inplementatuta, eta sistemaren oinarrian erabiltzailea/pasahitza bidezko autentifikazioa egongo da. Gainera, datu pertsonalen fitxategietara sarbidea duen aplikazio bakoitzeko bi erabiltzaile profil egongo dira: bata kontsultarako eta bestea aldaketak egiteko eskubidea duena. Horrela, toki erakunde honetako informazio sistemen erabiltzaile guztiek profil bat eta bakarra izango dute esleituta sarbidea baimenduta duten aplikazio bakoitzerako.

Sarbideak kudeatzeko sistema bat egongo da eta, Erabiltzaileen Erregistroko datuak kontuan hartuta, baimendu ala ukatuko egin ahal izango zaio erabiltzaileari aplikazio baterako sarbidea.

Erabiltzaileen Erregistroak honela funtzionatu behar du:

1. Bertan ematen diren altak, bajak edo aldaketak Baimenen Kudeaketako Prozeduratik etorritako eskaera baten ondorio izango dira.

2. Erabiltzaileen erregistroak aukera eman behar du aplikazio bakoitzean sarbidea duten erabiltzaile guztien zerrenda eskura izateko nahi den guztietan. Era berean, toki erakunde honetako tratamendu kontrolatzaileak edonoiz eskatu ahal izango dio segurtasun arduradunari aplikazio guztietarako sartzeko baimenen historia eta erabiltzaile guztiena, gutxienez azken bi urtetakoa. Horretarako, erabiltzaileen erregistroak honako informazioa izan behar du gutxienez:

- Erabiltzailearen izen-abizenak.
- Erabiltzailearen identifikatzailea.
- Erabiltzailearen helbidea edo unitate funtzionala.
- Sarbidea duen aplikazio bakoitzeko.
- Aplikazioaren identifikatiboa.
- Baimen mota: alta, baja ala aldaketa.
- Erabiltzailearen profila: esleitutako profila, alta edo aldaketa bada.
- Aldaketaren data.

3.3. Control de acceso a datos

Todas las aplicaciones con acceso a ficheros con DCP en funcionamiento en [entidad local] tendrán implementado un sistema de control de acceso basado en la autenticación mediante usuario/a/contraseña y para cada aplicación con acceso ficheros con DCP existirá un perfil de usuario/a de consulta de la aplicación y un perfil de usuario/a con derecho de modificación; de este modo, todos los usuarios y usuarias de los SSII de [entidad local] tendrán asignado uno y sólo un perfil para cada aplicación para la que tengan acceso autorizado.

Existirá un Sistema de Gestión de Accesos que autorice/desautorice el acceso a una aplicación a un usuario o usuaria basándose en la información existente en el Registro de Usuarios y Usuarias.

El Registro de Usuarios y Usuarias debe funcionar del siguiente modo:

1. Las altas, bajas o modificaciones en el mismo serán efecto de una petición proveniente del Procedimiento de gestión de permisos.

2. El Registro de Usuarios y Usuarias debe permitir conocer en todo momento cuál es la lista de usuarios y usuarias con acceso a las diferentes aplicaciones, y del mismo modo, la persona Responsable del Fichero de [entidad local] podrá solicitar en cualquier momento a la persona Responsable de Seguridad el historial de permisos de acceso de todas las aplicaciones y de todos los usuarios y usuarias hasta un mínimo de dos años. Para ello, el Registro de Usuarios y Usuarias debe contemplar por lo menos la siguiente información:

- Nombre y apellidos del usuario o usuaria.
- Identificador de usuario o usuaria.
- Dirección o Unidad funcional del usuario o usuaria.
- Para cada aplicación a la que tenga acceso.
- Identificativo de la aplicación.
- Tipo de permiso: alta, baja, modificación.
- Perfil de usuario o usuaria: en caso de alta o modificación, cuál es el perfil asignado.
- Fecha de la modificación.

Atzipenak kudeatzeko sistemak kudeatuko du atzipen erregistroa. Atzipen erregistroak goi-mailako datu pertsonalen fitxategiekin lan egiten duten aplikazioetan sartzeko egin diren atzipen saio guztien gaineko informazioa gordeko du, saioak arrakasta izan ala ez.

El Sistema de Gestión de Accesos gestionará el Registro de Accesos. El Registro de Accesos guardará información de los intentos de acceso tanto exitosos como infructuosos a las aplicaciones que trabajen con ficheros con DCP de nivel alto.

Saioak ez badu arrakastarik izan, erabiltzailearen identifikazioa eta saiakera egin zeneko data eta ordua gordeko dira.

En el caso de un intento de acceso fallido se guardará la identificación del usuario o usuaria y la fecha, hora en que se intentó el acceso.

Saioak arrakasta izan badu, atzipen erregistroan gordeko dira erabiltzailearen identifikazioa, saiakeraren data eta ordua, atzitu den fitxategiaren erregistroa eta egin den atzipen mota (aldaketa edo kontsulta). Informazio hori gutxienez bi urtez gorde beharko da eta tratamendu kontrolatzailearen eskura egon beharko du, eskatu egin baitezake.

En el caso de un acceso exitoso se guardará en el Registro de Accesos la identificación del usuario o usuaria, la fecha y hora, el registro del fichero que se ha accedido y el tipo de acceso que se ha realizado (modificación o consulta). Esta información se debe almacenar por un período mínimo de dos años y debe estar a disposición de la persona Responsable del Fichero en caso de que la solicite.

3.4 Euskarrien kudeaketa eta banaketa

3.4. Gestión y distribución de soportes

Datu pertsonalen fitxategiak dituzten euskarriak jaso eta bidaltzeko eta euskarriak baztertzeko edo berriz erabiltzeko baimena duten langileen zerrenda bat egon beharko da. Langile horiek tratamendu kontrolatzailearen baimena izango dute eta informazio hori guztia eguneratuta egon beharko da erabiltzaileen erregistroan.

Existirá una relación de personal autorizado a realizar tanto Entradas como Salidas de soportes con ficheros con DCP y a desecharlos o reutilizarlos. Este personal estará autorizado por la persona Responsable del Fichero y esta información deberá estar actualizada en el Registro de Usuarios y Usuarias.

Datu pertsonalen fitxategiak dauzkaten euskarrien erregistro bat egon beharko da. Erregistro horri esker jakingo da zenbat sarrera eta irteera egon diren eta zeintzuk euskarri baztertu edo berrerabili diren. Erregistroak honako eremuak izango ditu:

Existirá un Registro de soportes con ficheros con DCP. Este Registro permitirá conocer tanto todos las Entradas y Salidas que se han producido como los soportes que se han desechado y los que se han reutilizado. Este registro contendrá los siguientes campos:

- Fitxategiaren izena eta euskarriak daukan informazioaren deskripzio laburra.
- Euskarrian dauden datu pertsonalen maila, Datuak Babesteari buruzko Legearen arabera.
- Euskarri mota.
- Euskarriaren identifikatzailea.
- Mugimendu mota.
- Data eta ordua.
- Euskarriak emateko arduraduna (euskarrien bidaltzailea): irteera baimendu duen pertsonaren izena, helbidea eta entitatea/organoa.

- Nombre del fichero y breve descripción de la información que contiene el soporte.
- Nivel LOPD (Ley Orgánica de Protección de Datos) de los datos personales contenidos en el soporte.
- Tipo de soporte.
- Identificador del soporte.
- Tipo de movimiento.
- Fecha y hora.
- Responsable de la entrega (emisor/a de soportes): entidad/órgano, dirección postal y nombre de la persona que autorizó la salida.

- Euskarriak jasotzeko arduraduna (euskarrien jasotzailea): euskarrien hartzailearen izena, helbidea eta entitatea/organoa.
- Bidalketa-mota, euskarri bat irteten bada.

- Erabilitako metodoa: euskarri bat baztertu bada edo berriz erabili bada.
- Euskarria zein egoeratan geratu den (jatorrira itzuli den, berriz erabili den, baztertua izan den ala inbentariatuta eta gordeta dagoen.

- Euskarria toki entitate honetan geratzen bada [toki entitatearen izena] bere inbentarioko datuak izan behar ditugu kontrolerako, biltegiratzeko eta lokalizatzeko.

- Responsable de la recepción (destinatario/a de los soportes): entidad/órgano, dirección postal y nombre de la persona destinataria de los soportes.
- Forma de envío si es una salida del soporte.
- Método utilizado: si desecho o reutilización.
- Estado en que queda el soporte (devuelto a origen, reutilizado, desechado o inventariado y guardado).

- Si el soporte se queda en [entidad local] tenemos que tener sus datos de inventario para control, almacenamiento y localización.

Datu pertsonalen fitxategiak dauzkaten euskarrien erregistroko mekanismoak modu unibokoan identifikatu beharko du euskarrien sarrera, baztertze edo berrerabiltze bakoitza, eta egindako erregistroen gaineko datuak aldatzeko edo ezabatzeko saiakerak eragotzi edo atzeman beharko ditu.

El mecanismo de Registro de soportes con ficheros con DCP identificará de manera unívoca cada entrada, salida, desecho o reutilización de soportes, impidiendo o detectando la alteración, modificación o eliminación de los datos de los registros realizados.

Tratamendu kontrolatzailearen baimena beharko da datu pertsonalak dauzkaten fitxategien euskarriak atera ahal izateko fitxategia kokatuta dagoen lokaletatik, eta berdin dio nork egiten duen euskarriaren bidalketa: toki entitateak [toki entitatearen izena] ala toki entitate horretako tratamendu arduradunak. Gainera, goi-mailako segurtasun neurriak behar dituzten datuak badira, informazioa enkriptatuta egon beharko da, ezinezkoa izan dadin informazioa bidean atzematea eta manipulatzea.

La salida y distribución de soportes informáticos que contengan ficheros con DCP, fuera de los locales en los que está ubicado el fichero, será autorizada por la persona Responsable del Fichero tanto si el envío del soporte lo realiza [entidad local] como si lo realiza directamente la persona encargada del tratamiento de [entidad local], y en caso de contener datos cuyo nivel de seguridad sea alto la información irá cifrada con el objeto de que la información no pueda ser interceptada ni manipulada.

Ordenagailu eramangarri batetik datu pertsonalak ateratzeko ere tratamendu kontrolatzailearen baimena beharko da eta datu pertsonalak dauzkan euskarri informatiko bati ematen zaion tratamendu bera emango zaio erregistroaren ondorioetarako.

La salida de datos de carácter personal en un PC portátil deberá ser también autorizada por la persona Responsable del Fichero y se le dará el mismo tratamiento que a una salida de soporte informático con datos de carácter personal, a efectos de registro.

Edozein arrazoirengatik baztertu ala berrerabili behar diren euskarriak lehendabizi tratatu egin beharko dira, lehendik zegoen informazioa berreskuratzea ezinezkoa izan dadin. Horrez gain, euskarriaren egoera aldaketa ere jaso egin beharko da inbentarioan.

Araudi hau inplementatzeko Euskarri Informatikoen Kudeaketa Prozedura beteko da.

Datu pertsonalen fitxategiak dauzkaten euskarriak armairu ignifugoetan eta giltzapean biltegiratuko dira erabiltzen ez direnean edo lan orduetatik kanpo.

Toki entitatean [toki entitatearen izena] tratamendu arduradun bat badago, arduradun horrek datu pertsonalen fitxategiak dauzkaten euskarriak biltegiratzeari eta kudeatzeari buruzko araudia bete beharko du fitxategi horiekin egiten dituen tratamendu guztietan, toki entitateak berak egingo balu bezala.

3.5. Babes kopiak

Fitxategien zerbitzarien sare-unitateetan biltegiratutako datu guztien babes kopiak (backup) egingo dira bai ofimatikaren arloan bai postu anitzeko aplikazioetatik eskuragarriak diren fitxategien arloan.

- Ingurune ofimatikoko fitxategien zerbitzarietan egunero egingo dira segurtasun kopiak, eta hilabetez gordeko dira; horrela, hilabete horretan ingurune ofimatikoko datu pertsonalen edozein fitxategi berreskuratzeko aukera egongo da.

- Postu anitzeko aplikazioetatik eskuragarriak diren datuak dauzkaten zerbitzarietan dauden datu pertsonalen fitxategien segurtasun kopiak bermatu beharko du datuak galdu edo suntsitu zirenean zeuden bezala, egoera berean, berreskuratu ahal izango direla.

Los soportes que por cualquier motivo vayan a ser desechados o reutilizados serán previamente tratados de modo que la recuperación de la información previamente existente no sea posible. Además de lo anterior la modificación de estado del soporte se debe reflej ar en el inventario.

Para implementar esta normativa seguiremos el Procedimiento de Gestión de Soportes informáticos.

Los soportes con ficheros con DCP se almacenarán en un armario ignífugo y bajo llave, mientras estén fuera de uso o en horario no laboral.

Si existe una persona encargada del tratamiento de [entidad local] deberá cumplir con toda la normativa relativa al almacenamieanto y gestión de soportes con ficheros con DCP, para los tratamientos que efectúe a dichos ficheros como si fuera la misma entidad local.

3.5 Copias de seguridad

Se realizarán copias de respaldo (backup) de todos los datos almacenados en las unidades de red de los servidores de ficheros tanto en el ámbito de la ofimática como de los ficheros accesibles desde aplicaciones multipuesto.

- La copia de seguridad de los servidores de ficheros para entorno ofimático será diaria, y se conservará durante 1 mes de modo que durante ese período será posible la recuperación de cualquier fichero con DCP del entorno ofimático.

- La copia de seguridad de los ficheros con DCP alojados en servidores de datos con acceso a los mismos desde aplicaciones multipuesto se realizará garantizando su reconstrucción en el estado en que se encontraban los datos al tiempo de producirse la pérdida o destrucción.

Segurtasun kopien planak bermatu beharko du astero egiten direla babes kopia bat eta datuak berreskuratzeko prozeduren kopia bat. Babes kopia ez da gordeko ekoizpeneko fitxategiak dauden toki berean, hau da, datuak prozesatzeko zentroan (DPZ) bertan.

El plan de copias de seguridad debe garantizar la existencia semanal de una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente del CPD en el que se hallan los ficheros de producción.

Tratamendu arduradunak egindako segurtasun kopiek toki entitatearen eskura egon beharko dute, toki entitateak eskatzen duen unean bertan datuak berreskuratu ahal izateko.
Datu berreskuratzerik egiten bada, datuak berreskuratzeko erregistroan jaso beharko da, eta honako informazioa gordeko da: data, ordua, berreskuratutako fitxategiak eta abar.

Las copias de seguridad realizadas por la persona encargada del tratamiento estarán a disposición de [entidad local] para la recuperación de los datos en cualquier momento en que ésta lo solicite. La realización de un proceso de recuperación de datos quedará reflejada en el Registro de recuperación de datos que guardará información sobre la fecha, hora, ficheros recuperados, etc.

Babes kopien prozeduran dago adierazita arau honen inplementazioa, bai eta kopiak nola egin, nola biltegiratu eta nola berreskuratu ere.

La implementación de esta norma viene especificada en el Procedimiento de copias de respaldo que incluye la realización, el almacenamiento y la recuperación de las mismas.

3.6 Segurtasun arduraduna

3.6. Responsable de Seguridad

Maila ertaineko edo goi-mailako segurtasun neurriak behar dituen fitxategi bakoitzak segurtasun arduradun bat izango du, eta horren gaineko informazioa “1. ERANSKINA Datu pertsonalen fitxategiak” izeneko agirian eguneratuta egon beharko du; izan ere, agiri horretan adierazi behar da fitxategi bakoitzaren segurtasun arduraduna nor den.

Existirá una persona Responsable de Seguridad para cada fichero con nivel de seguridad medio o alto; esta información estará actualizada en el documento ANEXO 1 Ficheros con DCP en el que se especifica quién es la persona Responsable de Seguridad para cada fichero.

3.7. Auditoria

3.7 Auditoría

Auditoria bat egin beharko da gutxienez bi urtean behin. Auditoriaren helburua da segurtasun agirian jasota dauden arau eta prozedurak egokiak direla eta aplikatzen direla egiaztatzea. Hortik auditoria-txosten bat aterako da eta segurtasun arduradunek aztertu beharko dute. Txostenak honakoak jaso beharko ditu gutxienez:

Con una periodicidad máxima de dos años, se realizará una auditoría cuyo objetivo será verificar la adecuación y aplicación de las Normas y Procedimientos contemplados en este Documento de Seguridad. Dicha auditoría dará lugar a un informe de auditoría que será analizado por las personas Responsables de Seguridad y contemplará, al menos, los siguientes aspectos:

- Informazio sistemetan sartzeko identifikazio eta autentifikazio sistema.
- Sarbide logikoaren kontrol sistema.
- Sarbide fisikoaren sistema.
- Euskarriak kudeatzeko prozedurak.
- Babes kopien eta datu berreskuratzeen prozedurak.
- Segurtasun gorabeheren jakinarazpenak eta kudeaketak.

- Sistema de identificación y autenticación de accesos a los sistemas de información.
- Sistema de control de acceso lógico.
- Sistema de acceso físico.
- Procedimientos de gestión de soportes.
- Procedimientos de copias de respaldo y recuperación de datos.
- Notificación y gestión de incidencias.

Auditorien edukia segurtasun arduradunak aztertuko du eta ateratzen dituen ondorioak tratamendu kontrolatzaileari jakinaraziko dizkio, eta tratamendu kontrolatzaileak neurri zuzentzaileak hartuko ditu, beharrezkoak badira.

El contenido de las auditorías será analizado por la persona Responsable de Seguridad, que elevará las conclusiones a la persona Responsable del Fichero, la cual, en su caso, tomará las medidas correctoras oportunas.

3.8. Sarbide fisikoaren kontrola

Informazio sistemak dauden bulego guztietan sartzeko, baldin eta datu pertsonalak dauzkaten fitxategiak badaude bertan, sarbide fisikoaren kontrol sistema bat ezarri beharko da. Sarbide fisikoaren kontrolak honako araudia bete beharko du:

1. Baimendutako langileak bakarrik sartu eta egon ahal izango dira bulego horietan.

2. Datuak prozesatzeko zentroan (DPZ) sartzeko ateak itxita egon beharko dute beti. Ez baldin badago txartel bidez kontrolatutako sarbiderik, atea itxita dagoela ziurtatu beharko da, datuak prozesatzeko zentroan behar bezala baimendutako pertsonak bakar-bakarrik sartu daitezen.

3. Datuak prozesatzeko zentroan sartzeko baimena duten pertsona kopurua behar bestekoa izango da, baina egin beharrekoak egiteko behar den kopururik txikiena.

4. Datuak prozesatzeko zentroan sartzeko baimenik behar ez duten pertsonei lehenbailehen kenduko zaie hor sartzeko baimena, nahiz eta lehen baimenduta egon. Norbaiti baliogabetzen bazaio datuak prozesatzeko zentro batean sartzeko baimena, sarbide txartela itzuli beharko du, edo, hala badagokio, datuak prozesatzeko zentroan sartzeko atea irekitzeko giltza.

5. Datuak prozesatzeko zentroetan sartzeko baimena duten pertsonen zerrenda bat egon beharko da beti toki entitateko [toki entitatearen izena] tratamendu kontrolatzailearen eskura, eskatu egin dezakeelako.

6. Datuak prozesatzeko zentroan baimenik gabeko pertsona bat atzematen bada edo sumatzen bada baten bat sartu dela baimenik gabe, gertaera hori segurtasun gorabeheratzat joko da eta jaso egingo da.

3.8. Control de acceso físico

Se establecerá un sistema de control de acceso físico a todas las dependencias en las que existan SSII con ficheros con DCP. El control de acceso físico deberá cumplir la siguiente normativa:

1. Sólo el personal autorizado podrá acceder y permanecer en dichas dependencias.

2. Las puertas de acceso al CPD deberán estar permanentemente cerradas. En caso de que no se disponga de control de acceso por tarjetas, deberá controlarse que la puerta está cerrada, al objeto de que sólo puedan acceder a las dependencias del CPD personas debidamente autorizadas.

3. El número de personas autorizadas para acceder al CPD debe ser suficiente, pero el mínimo necesario para realizar las funciones correspondientes.

4. Se tendrá especial diligencia en anular con prontitud las autorizaciones de acceso a las dependencias de los CPD a las personas que, habiendo estado autorizadas, ya no necesiten el acceso al mismo. Cuando a una persona se le anule la autorización para acceder al CPD, deberá devolver la tarjeta de acceso o, en su caso, la llave de apertura de la puerta de acceso al CPD.

5. Una relación actualizada de personas autorizadas para acceder al CPD estará a disposición de la persona Responsable del Fichero de [entidad local] en todo momento, si ésta lo solicita.

6. Cuando se detecte la presencia, en las dependencias del CPD, de una persona no autorizada o indicios de que se ha producido un acceso no autorizado, se hará constar este hecho como una incidencia de seguridad.

3.9. Probak benetako datuekin

Arau orokor bezala, probak egiteko inguruneetan egiten diren programen eta prozesuen probetarako, benetakoak ez diren datuak erabili beharko dira. Hala ere, probak egiteko, ustiapen-datuak hartu ahal izango dira, baina tratamendu arduradunak baimentzen badu eta honako segurtasun neurriekin:

1. Ustiapenetik datozen benetako datuek datu-disoziazio prozesu bat igaro beharko dute, ezinezkoa izan dadin lortutako informazioa pertsona identifikatu edo identifikagarri batekin lotzea.

2. Datuak ez badira disoziatzen, erabili behar diren datuei dagokien segurtasun maila ziurtatu beharko da.

3.9 Pruebas con datos reales

Como regla general, en los entornos de pruebas y desarrollo se deberán realizar las pruebas de los programas y procesos utilizando bases de datos y ficheros con datos ficticios. No obstante podrán tomarse datos de explotación para la realización de pruebas, siempre que lo autorice la persona Responsable del Fichero, adoptando las siguientes medidas de seguridad:

1. Los datos reales provenientes de explotación serán sometidos a un proceso que permita la disociación de los datos, de tal modo que se imposibilite la asociación de la información obtenida con una persona identificada o identificable.
2. Si los datos no se disocian, deberá asegurarse el nivel de seguridad correspondiente a la naturaleza de los datos que se van a manejar.

3.10. Telekomunikazioak

Prozesatu, kopiatu, atzitu eta abarretarako telekomunikazio-sareak erabili behar badira, sare horiek toki erakundearen [toki entitatearen izena] instalazioetan lan egiten denean bezalako segurtasun maila izan beharko dute. Beraz, datu pertsonalen fitxategien transmisioak egiteko, informazioa enkriptatu egin beharko da beti. Arau hau beti bete beharko da, bai toki erakundeko informazio sistemetan ekipo eramangarrietatik sartzeko, bai urrutiko backups-etara informazioa bidali edo kopiatzeko.

3.10. Telecomunicaciones

La utilización de redes de telecomunicaciones para el proceso, copiado, acceso, etc., debe mantener el nivel de seguridad del mismo modo que si se estuviera trabajando en las propias instalaciones de [entidad local], por lo que la transmisión de ficheros con DCP se realizará siempre cifrando la información. Esto se debe respetar tanto para cualquier acceso a los SSII de [entidad local] desde equipos portátiles, como para el envío o copiado de información para backups remotos.

4. GIZA BALIABIDEEN KUDEAKETA

Hona hemen gure erakundean egongo diren figurak eta bakoitzaren eginkizunak eta betebeharrak:

- Tratamendu kontrolatzailea.
- Segurtasun arduraduna.
- Informatika Saila.
- Informazio sistemen (IS) erabiltzeak.

4. ORGANIZACIÓN DE RECURSOS HUMANOS

A estos efectos identificamos en nuestra organización las siguientes figuras con sus respectivas funciones y obligaciones:

- Responsable del Fichero.
- Responsable de Seguridad.
- Departamento de Informática.
- Usuarios/as de SSII.

4.1 Tratamendu kontrolatzailea

Tratamendu kontrolatzailea toki entitatearen [toki entitatearen izena] titularra da, administrazio organo horri atxikita baitago fitxategia, eta berak erabakitzen baitu zein den informazioaren helburua, edukia eta erabilera.

Segurtasun arduradunak emandako aholkuak kontuan hartuta arituko da tratamendu kontrolatzailea, baina aholku emateak ez du esan segurtasun arduradunak bere erantzukizunak eskuordetzen dituenik, datuak babestearen arloko erantzukizuna legez baitagokio segurtasun arduradunari, hala xedatzen baitu 1720/2007 Errege Dekretuak onartu zuen segurtasun-neurriak ezartzeko Erregelamenduaren 95. artikuluak.

4.2. Segurtasun arduraduna

Tratamenduaren kontrolatzaileak izendatutako pertsona da (edo pertsonak) eta aplikatu beharreko segurtasun neurriak koordinatu eta kontrolatu behar ditu.

4.3 Informatika Saila

Informazio sistemak sortzeko, abian jartzeko eta mantentzeko ardura duen zerbitzua da. Zenbait erakundetan zerbitzu honen eginkizunak tratamendu arduradunak hartzen ditu bere gain. Tratamendu arduraduna da bere aldetik edo beste batzuekin batera, administrazio interesdunaren kontura datu pertsonalak tratatzen dituen pertsona fisiko nahiz juridikoa, agintari publikoa, zerbitzua nahiz bestelako erakundea.

4.4. Informazio sistemen (IS) erabiltzaileak

Atal honetan biltzen ditugu toki erakundearen [toki entitatearen izena] sistema informatikoak erabiltzen dituzten langile guztiak, berdin dio toki entitate horrekin duten kontratu harremana: plantillako funtzionarioak, bitarteko funtzionarioak, aldi baterako lan-kontratudunak, bekadunak nahiz beste edozein egoera administratiboan daudenak. Hau da, toki administrazioaren informazio sistemen erabiltzailetzat joko da toki administrazio horretako edozein informazio sistematan sartzeko erabiltzaile baimena duen edonor.

4.1 Responsable del Fichero

La persona Responsable del Fichero es la titular de [entidad local] ya que éste es el órgano administrativo al que está adscrito el fichero, y es el que decide sobre la finalidad, contenido y uso del tratamiento de la información.

La persona Responsable del Fichero actuará asesorada por la persona Responsable de Seguridad, sin embargo, este asesoramiento no supone en ningún caso una delegación de las responsabilidades, que en materia de seguridad de datos de carácter personal corresponden legalmente a la persona Responsable del Fichero o al encargado del tratamiento tal y como lo especifica el artículo 95 del Reglamento de Medidas de desarrollo de la LOPD aprobado por el R.D. 1720/2007.

4.2 Responsable de Seguridad

Es la persona o personas a las que la persona Responsable del Fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

4.3. Departamento de Informática

Es el servicio encargado de la generación, puesta en marcha y mantenimiento de los SSII. En algunas organizaciones todas o alguna de sus funciones las puede realizar el Encargado o la Encargada del Tratamiento que *"será aquella persona física o jurídica, autoridad pública o privada, servicio o cualquier otro organismo que, sólo o conjuntamente con otros trate datos personales por cuenta de la persona Responsable del Fichero"*.

4.4 Usuarios/as de SSII

En este apartado incluimos a todo el personal que utiliza los Sistemas Informáticos de [entidad local] independientemente de cuál sea la relación contractual que le une con dicha entidad local: personal de plantilla funcionario, interino, contratado temporal, becario o personal en cualquier otra situación administrativa existente; es decir, toda persona que tenga en un momento un usuario o usuaria de acceso autorizado en alguno de los SSII de [entidad local] será considerado usuario/a de los SSII de la entidad local.

5. EGINKIZUNAK ETA BETEBEHARRAK

Datu pertsonalen fitxategietan sar daitezkeen langile guztiek dute indarrean dagoen legedia jakiteko eta betetzeko obligazioa, bereziki haien laneko eginkizunei eragiten badie. Gainera, denek gorde beharko dute lan egitean jakiten dituzten datu pertsonalen gaineko lanbide sekretua.

5.1 Tratamendu kontrolatzailearen eginkizunak

1. Goi-mailako edo maila ertaineko segurtasuna dagokien DPen fitxategi bakoitzaren segurtasun arduraduna izendatzea. Izendapen hau Segurtasun Agiriaren Eranskinen 3. alean jasoko da.

2. Informazio sistemen erabiltzaile guztiek izan behar dute indarrean dagoen segurtasun araudiaren berri, bereziki haien zereginei eragiten badie, bai eta araudia bete ezean, jasan ditzaketen ondorioen berri ere; eta hori lortzeko, egoki ikusten diren neurri guztiak hartu beharko ditu. Hala badagokio, zeregin honetan segurtasun arduradunaren laguntza izango du.

3. Segurtasun agiria egitea eta eguneratuta izatea, eta behar duen zabalkundea ematea.

4. Datu pertsonalak berreskuratzeko prozedurak gauzatzeko baimenak ematea, behar besteko bermearekin. Baimena emateko, behar duen adina informazio osagarri eskatu ahal izango dio segurtasun arduradunari.

5. Datu pertsonalen fitxategiak erabiltzen dituzten erabiltzaileentzat aplikazioetara sartzeko altak, bajak eta aldaketak eskatzea, erabiltzaileak kudeatzeko prozeduran eta baimenak kudeatzeko prozeduran ezarritakoaren arabera.

6. Datu pertsonalak dauzkaten euskarri informatikoak fitxategia dagoen lokaletik atera ahal izateko baimena ematea, horretarako ezarrita dagoen prozedura kontuan hartuta.

5. FUNCIONES Y OBLIGACIONES

Todo el personal que acceda a ficheros con datos de carácter personal está obligado a conocer y observar la normativa en vigor que afecte a las funciones que desarrolla; además todas las personas deberán guardar secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

5.1 Funciones de la persona Responsable del Fichero

1. Designar a la persona Responsable de Seguridad para cada uno de los ficheros con DCP con nivel de seguridad medio o alto. Esta designación queda reflejada en el Anexo correspondiente del volumen de Anexos del Documento de Seguridad.

2. Adoptar las medidas necesarias para que los usuarios y usuarias de sistemas de información conozcan la normativa de seguridad en vigor que afecta al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento; tarea que realizará, en su caso, con la colaboración de la persona Responsable de Seguridad.

3. Elaborar y mantener actualizado el Documento de Seguridad, dándole la oportuna difusión.

4. Autorizar, con las debidas garantías, la ejecución de los procedimientos de recuperación de datos de carácter personal, solicitando a la persona Responsable de Seguridad toda la información adicional que necesite para otorgar la autorización.

5. Solicitar las altas, bajas y modificaciones de acceso de los usuarios y usuarias a las aplicaciones que manejan datos de carácter personal según lo establecido en el Procedimientos de gestión de usuarios/as y en el Procedimiento de gestión de permisos.

6. Autorizar la salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales donde se ubica el fichero, de acuerdo con el procedimiento establecido al efecto.

7. Datu pertsonalak dauzkaten euskarriak identifikatu, inbentariatu, berrerabili, baztertu, bidali eta jasotzeko baimena duten pertsonak zehaztea eta baimendutako pertsonen zerrenda eguneratuta mantentzea.
8. Aldizka egiten diren auditorietan atzematen diren datuen segurtasunaren arloko akatsak konpontzeko neurri zuzentzaileak hartzea.

9. Baimenak ematea datuen jabeek, hau da, titularrek eskatzen dituzten atzipenak, aldaketak eta ezabatzeak egiteko datu pertsonalen fitxategietan.

10. Ahaleginak egitea datuen titularrek datuen babesaren inguruan izan behar duten informazio guztia jasota egon dadin datu pertsonalak jasotzeko erabiltzen diren formulario, agiri eta inprimakietan. Horrez gain, zerbitzuak emateko kontratuek datu pertsonalak atzitzea badakarte berekin, ahalegina egin beharko du kontratistaren betebeharrak ezartzen dituzten baldintzen artean segurtasunaren eta babesaren arloko betebeharrak ere jasota egon daitezen.
11. Datu pertsonalen fitxategi automatizatuak sortu, aldatu eta ezerezten badira, Datuak Babesteko Euskal Bulegoari jakinaraztea, erregistroan jaso dezan. Baina, lehendabizi, dagokion lurralde historikoko aldizkari ofizialean argitaratu beharko da.
12. Bere ardurapeko fitxategiak dauden lokaletan sartzeko baimena ematea horretarako baimena eskatzen duten langileei. Baimendutako langileek nahitaez bete beharko dituzte lokalen titularrek bertan sarbide fisikoa izateko ezarrita dauzkaten prozedurak eta arauak.

7. Determinar las personas autorizadas para identificar, inventariar, reutilizar, desechar, emitir y recibir soportes que contengan datos de carácter personal, manteniendo actualizada la relación de personas autorizadas.
8. Adoptar las medidas correctoras pertinentes para solventar las deficiencias que, en materia de seguridad de datos de carácter personal, se detecten tras la realización de las auditorías periódicas.
9. Autorizar los accesos, modificaciones y supresiones, solicitadas por los/as propietarios/as titulares de los datos (afectados/as-interesados/as), en los ficheros de datos de carácter personal.
10. Procurar la inclusión en los formularios, documentos e impresos de recogida de datos de carácter personal, de toda la información que debe conocer la persona titular de dichos datos respecto a la protección de éstos; asimismo, procurará que, en los contratos de prestación de servicios que impliquen acceso a datos de carácter personal, se incluyan las cláusulas que establezcan las obligaciones de la parte contratista en la seguridad y protección de estos datos.
11. Notificar, para su inscripción en la Agencia Vasca de Protección de Datos, la creación, modificación y cancelación de ficheros automatizados que contengan datos de carácter personal. Todo ello, previa publicación en el Boletín Oficial del Territorio Histórico correspondiente.
12. Autorizar al personal que lo requiera el acceso a las dependencias en las cuales están ubicados los ficheros objeto de su responsabilidad. Este personal previamente autorizado deberá cumplir en todo caso los procedimientos y normativas establecidas para el acceso físico a locales por los/las titulares de los mismos.

5.2 Segurtasun arduradunaren eginkizunak

1. Eguneratuta mantentzea bere erantzukizunpeko datu pertsonalen fitxategien inbentarioa.

5.2. Funciones de la persona Responsable de Seguridad

1. Mantener actualizado el inventario de ficheros con datos de carácter personal de los que es Responsable de Seguridad.

2. Datu pertsonalak erabiliko dituzten aplikazio berriak sortzen badira, tratamendu kontrolatzailearekin batera identifikatzea aplikazio horiek inplementatu behar dituzten segurtasun neurriak, bertan dauden fitxategien segurtasun maila kontuan hartuta.

3. Erabiltzaile profilak definitzea tratamendu kontrolatzailearekin lankidetzan. Profil horiek honakoak ezarriko dituzte: fitxategiak tratatzen dituen aplikazioetarako eskatzen den sarbide mota (eguneratzeko ala kontsultak egiteko) eta baimendutako sarbideen aukerak.

4. Erabiltzaileek adierazitako premietatik ondorioztatutako administrazio eskabideak betetzeko behar diren datu teknikoak eta administratiboak zehaztea.

5. Erabiltzaileen sarbide eskabideetarako baimenak eskatzea tratamendu kontrolatzaileari, eta erabiltzaileen administrazio eskabideak egitea.

6. Datu pertsonalak dauzkaten fitxategiak bidaltzeko nahitaez behar den baimena eskatzea tratamendu kontrolatzaileari. Euskarrien sarrera eta irteeren aldizkako kontrola egitea (baimena, erregistroa eta inbentarioa).

7. Datu pertsonalak berreskuratzeko prozesuetan, beste ezer baino lehen, erabiltzaileen premiei erantzun beharko die; eta datuak berreskuratzeko beharraren berri eman behar dio tratamendu kontrolatzaileari, berreskuratzeko baimena eman dezan; eta baimena emateko behar duen informazio guztia ere eman beharko dio.

8. Hartu beharreko neurriak hartzea, fitxategiko datu pertsonalak atzitzeko aukera duten pertsona guztiak gai izan daitezen datuen titularrei datuak atzitu, zuzendu, ezereztu eta aurka egiteko eskubideez baliatzeko bete behar duten prozedurari buruzko informazioa emateko.

2. Para cada aplicación de nueva creación que vaya a manejar datos de carácter personal, identificar, junto con la persona Responsable del Fichero, las medidas de seguridad que debe implementar la aplicación en función del nivel de seguridad de los ficheros implicados en la misma.

3. Colaborar con la persona Responsable del Fichero en la definición de perfiles de usuario/a, donde se especifiquen las opciones de acceso permitido y el tipo de acceso requerido (actualización o consulta) a las aplicaciones que trata el fichero.

4. Concretar los datos técnicos y administrativos para cumplimentar las peticiones de administración de usuarios o usuarias derivadas de las necesidades manifestadas por los usuarios o usuarias.

5. Solicitar a la persona Responsable del Fichero las autorizaciones para las peticiones de acceso de usuarios y usuarias, así como realizar las correspondientes peticiones de administración de usuarios y usuarias.

6. Solicitar a la persona Responsable del Fichero la preceptiva autorización para la salida de soportes que contengan datos de carácter personal. Realizar el control periódico de las entradas y salidas de soportes (autorización, registro e inventario).

7. En los procesos de recuperación de datos de carácter personal, atiende, en primera instancia, las necesidades provenientes de los usuarios y usuarias y comunica, a la persona Responsable del Fichero, para obtener la oportuna autorización, la necesidad de recuperación de datos, facilitándole toda la información que precise para otorgar dicha autorización.

8. Adoptar las medidas oportunas para garantizar que todas las personas que tienen acceso a los datos de carácter personal del fichero, puedan informar, a la persona titular de los mismos, del procedimiento a seguir para que pueda ejercer sus derechos de acceso, rectificación, cancelación y oposición.

9. Agiri honetan ezarritakoa betetzen dela egiaztatzea eta betetzeari buruzko txostenak egitea.
10. Goi-mailako segurtasun neurriak badaude tartean, erabiltzaileek egindako sarbideen gaineko kontrol-informazioa gainbegiratzea aldian-aldian. Horrez gain, egindako berrikusketei buruzko eta atzemandako arazoei buruzko txosten bat egin beharko du hilean behin.
11. Segurtasun-neurriak ezartzeko Erregelamenduarekin (1720/2007 ED) zerikusia duten segurtasun auditorietan kolaboratzea. Auditoria txostenak aztertzea eta tratamendu kontrolatzaileari bidaltzea.

12. Segurtasun gorabeherak gainbegiratzea eta aztertzea aldian-aldian, larriak izan daitezkeen gorabeheren gaineko txosten bat egitea eta segurtasun gorabeherak gutxitzeko neurriak proposatzea.
13. Datu pertsonalen fitxategiak sortu, aldatu edo ezabatzen badira, horien gainean Datuak Babesteko Euskal Bulegoari egiten zaizkion jakinarazpenak eta dagokion lurralde historikoaren aldizkari ofizialean egiten diren argitalpenak gainbegiratzea; jakinarazpenak eta argitaratzeak egiteko ardura tratamendu kontrolatzailearena da.
14. Tratamendu kontrolatzailearekin batera segurtasun agiria eta agiriaren eguneratzeak egitea, datu pertsonalen fitxategiek dituzten xehetasunak definituz bere arloan. Horrez gain, arauak, prozedurak eta segurtasun neurriak egokitzea ere bere eginkizuna izango da.
15. Bere erantzukizunpean dauden fitxategiak kokatu eta prozesatzen diren lokaletako Sarbide Fisikoen Erregistroa kontrolatzea.
16. Goi-mailako datu pertsonalak enkriptatzeko mekanismoak eta prozedurak gainbegiratzea beharrezkoa den guztietan, hardware nahiz software izan.

9. Verificar el cumplimiento de lo dispuesto en este documento y elaborar los informes oportunos al respecto.
10. En el caso de medidas de seguridad de nivel alto, revisar periódicamente la información de control registrada sobre los accesos de usuarios y usuarias y elaborar, al menos una vez al mes, un informe de las revisiones realizadas y los problemas detectados.
11. Colaborar en las auditorías de seguridad relacionadas con el Reglamento de desarrollo de la LOPD (R. D. 1720/2007). Analizar los informes de auditoría y remitirlos a la persona Responsable del Fichero.
12. Supervisar y analizar, periódicamente, las incidencias de seguridad producidas, elaborar un informe explicativo de aquellas que tengan una cierta gravedad y proponer medidas para aminorar las incidencias.

13. Supervisar la publicación en el Boletín Oficial del Territorio Histórico correspondiente y las declaraciones que se dirijan a la propia Agencia Vasca de Protección de Datos, en cuanto se refiere a la creación, modificación y supresión de ficheros con DCP, que serán, respectivamente, dispuestas y notificadas por la persona Responsable del Fichero.
14. Colaborar con la persona Responsable del Fichero en la elaboración y actualización del Documento de Seguridad, definiendo las particularidades de los Ficheros con DCP en su ámbito, así como la adecuación de las normas, procedimientos y medidas de seguridad.
15. Controlar el Registro de Accesos Físicos a locales en que se procesen y alberguen ficheros con DCP, en su ámbito de responsabilidad.
16. Supervisar los mecanismos y procedimientos de cifrado de DCP de nivel alto cuando esto sea necesario, ya sean hardware o software.

5.3 Informatika Sailaren eginkizunak

Datuen administrazioarekin eta segurtasunarekin lotutako eginkizun hauek esleitzen zaizkio Informatika Sailari:

1. Datu atzipeneko segurtasunaren administrazioa. Datu pertsonalak atzitzeko baimenak aktibatzeaz eta desaktibatzeaz arduratuko diren langileak egongo dira, tratamendu kontrolatzailearen jarraibideak gauzatuko dituzte eta profil horiek definitzeko segurtasun arduradunaren laguntza eta eskabidea izango dituzte.

2. Segurtasun gorabeheren kudeaketa. Datu pertsonalen segurtasunari eragiten dieten segurtasun gorabeheren erregistroa mantetzeko lanez eta segurtasun gorabeheren kudeaketaz arduratzen diren langileak egongo dira.

3. Babes kopien kudeaketa. Babes kopiez eta datu berreskuratzeaz arduratuko diren langileak egongo dira. Hori egiteko toki erakundeko Segurtasun Agiriko prozedurei buruzko alean ezarritako prozedura bete beharko da.

4. Informazio sistemetarako sarbide fisikoak. Informatika Saileko Ustiapen arduraduna da datu pertsonalak gordetzen edo prozesatzen diren lokalen edo instalazioen arduraduna. Beraz, berak zehaztu beharko du eta martxan jarri beharko du informazio sistemetako sarbide fisikoaren kontrola.

Toki entitateak [toki entitatearen izena] Tratamenduaren arduradun batekin kontratatuta dauzkan eginkizunak dagokion kontratuan jasota egon beharko dira.

5.3. Funciones del Departamento de Informática

Al Departamento de Informática se le encomiendan las siguientes funciones relacionadas con la administración y seguridad de los datos:

1. Administración de la seguridad del acceso a los datos. Existirá personal que se ocupará de activar y desactivar los permisos de acceso a los DCP, ejecutando las instrucciones dadas por la persona Responsable del Fichero, con la colaboración y solicitud de la persona Responsable de Seguridad en la definición de dichos perfiles.

2. Gestión de incidencias. Existirá personal que se ocupe de la gestión de incidencias y del mantenimiento del registro de incidencias de seguridad que afecten a datos de carácter personal.

3. Gestión de copias de respaldo. Existirá personal que se ocupe de la gestión de copias de respaldo y de recuperación de datos, que serán ejecutados conforme al Procedimiento correspondiente especificado en el Documento de Seguridad [entidad local] (volumen II).

4. Accesos físicos a los Sistemas de Información. La persona Responsable de Explotación del Departamento de Informática es la persona responsable de la sala o instalación donde se procesan o albergan DCP y como tal debe definir y poner en práctica el control de acceso físico a los SSII.

Aquellas funciones que [entidad local] tenga contratadas con un ET, deberán ser reflejadas en el contrato correspondiente y soportadas por el mismo.

5.4 Erabiltzaile guztiei eragiten dieten betebeharrak

Informazio sistemen erabiltzaileek segurtasun agiri honen edukiaren berri izan beharko dute eta bere egin beharko dute; erabiltzaile guztiek izan beharko dute agiriaren kopia eta agirian ezarritakoa betez egin beharko dituzte esleituta dauzkaten eginkizunak.

Erabiltzaileek dute haien eskura jartzen diren datuen, aplikazioen eta gainontzeko baliabide informatikoen erantzukizuna, hau da, sortu eta ezarri zirenean zeuzkaten helburuak betetzeko bakar-bakarrik erabiltzen direla ziurtatu beharko dute.

Datu pertsonalen segurtasuna bermatzeko, erabiltzaileek honako arauak bete beharko dituzte ondoko jarduera eremuetako bakoitzean:

a. Hw baliabideak
b. Sw baliabideak
c. Identifikazioa eta autentifikazioa
d.Segurtasun gorabeheren kudeaketa
e. Euskarrien kudeaketa
f. Sekretua gorde beharra

a. Hw baliabideak

Hardware baliabidetzat joko ditugu datuak prozesatzea edo biltegiratzea ahalbideratzen duten elementuen artean datuak biltegiratzea, sartzea, irtetea edo eskualdatzea ahalbideratzen duten elementu fisiko guztiak.

1.Erabiltzaileentzako ekipo informatiko bakoitza baimendutako erabiltzaile baten ardurapean egongo da, eta bere ardura izango da ahal duen neurrian datu pertsonalen konfidentzialtasuna babestea, baimenik gabeko jakinarazterik edo bidegabeko manipulazioari edo erabilerarik gertatu ez dadin.

5.4 Obligaciones que afectan a todos los usuarios y usuarias

Los usuarios y usuarias de sistemas de información deberán conocer y asumir el contenido de este documento de seguridad; todos ellos/as podrán acceder a una copia del mismo y desempeñarán las funciones que se les encomienden de conformidad con lo dispuesto en este documento.

Los usuarios y usuarias son responsables, de asegurar que los datos, las aplicaciones y demás recursos informáticos puestos a su disposición, sean usados únicamente para el desarrollo de la operativa propia para la que fueron creados e implantados.

Para garantizar la seguridad de los datos de carácter personal, los usuarios y usuarias estarán obligados/as a observar las siguientes normas de actuación en los siguientes ámbitos de actuación:

a. Recursos Hw
b. Recursos Sw
c. Identificación y autenticación
d. Gestión de incidencias
e. Gestión de soportes
f. Deber de secreto

a. Recursos Hw

Consideramos recursos Hardware todos los elementos físicos que permitan el almacenamiento, la entrada, salida o transmisión de datos entre elementos que permitan el procesamiento o el almacenamiento de datos.

1. Cada equipo informático de usuario/a estará bajo la responsabilidad de algún usuario/a autorizado/a que tratará de proteger, en la medida de sus posibilidades, la confidencialidad de los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o cualquier otra manipulación o uso indebido.

2. Ekipo informatiko baten arduradunak ekipoa bakarrik uzten badu denbora tarte batean, babestutako datuak ez ikusteko moduan utzi beharko du, hau da, pantaila-babesle bat ipinita adibidez. Berriz lanean hasteko, dagokion pasahitza sartu beharko da pantalla-babestekoa desaktibatzeko. Ekipoa uzten bada lanaldia bukatu delako, orduan erabiltzaileak erabat itxi beharko du sistemaren sesioa.

3. Ezin izango da datu pertsonalak dauzkan fitxategirik gorde ordenagailuen disko gogorrean.

4. Datu babestuak dauzkaten agiriak jaso egin beharko dira inprimagailuetatik eta gainontzeko perifekoetatik atera ahala. Era berean, datu pertsonalak dauzkaten txosten kopurua ere ahalik eta txikiena izan beharko da.

5. Erabiltzaileek ezin izango dute konektatu baliabide informatikoetara sare korporatibora konektatzea ahalbideratzen duen komunikazio ekiporik, horretarako baimenik ez badute.

2. Cuando la persona responsable de un equipo informático lo abandone temporalmente deberá dejarlo en un estado que impida la visualización de los datos protegidos, por ejemplo, a través de un protector de pantalla. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente. Si el abandono del equipo se produjera debido a la finalización de su turno de trabajo, el usuario o usuaria procederá al cierre completo de la sesión del sistema.

3. No se deberán guardar ficheros que contengan datos de carácter personal en discos locales de los PCs.

4. Se deben retirar de las impresoras y demás periféricos de salida todos los documentos que contengan datos protegidos conforme se vayan imprimiendo. Del mismo modo se debe minimizar el número de informes que contenga DCP.

5. Ningún usuario o usuaria debe conectar, a ninguno de los recursos informáticos, ningún tipo de equipo de comunicaciones que posibilite la conexión a la red corporativa, sin la oportuna autorización.

b. Sw baliabideak

1.Toki erakundearen [toki erakundearen izena] informazio sistemen erabiltzaileek toki erakundeak utzitako software bertsioak bakarrik erabili ahal izango dituzte eta toki erakundeak emandako arauak bete beharko dituzte. Ezin izango dute, inolaz ere, programen legez kanpoko kopiarik instalatu, ez eta legez instalatutako programarik ezabatu ere.

2. Era berean, erabiltzaileek ezin izango dute beste erabiltzaile batzuen lana eragotzi ditzaketen edo baliabide informatikoak kaltetu edo hondatu ditzaketen programak instalatu edo exekutatu.

b. Recursos Sw

1. Los usuarios y usuarias de los SSII de [entidad local] deben utilizar únicamente las versiones de software facilitadas por [entidad local] y siempre siguiendo sus normas de utilización. En ningún caso podrán instalar copias ilegales o irregulares de programas, ni borrar ninguno de los programas instalados legalmente.

2. Del mismo modo ningún usuario o usuaria debe instalar ni ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios o usuarias, ni dañar o alterar cualquiera de los recursos informáticos.

c. Identifikazioa eta autentifikazioa

1. Informazio sistema batean sarbidea izateko, erabiltzaileek identifikatzaile baten bidez identifikatu beharko dute euren burua eta pasahitz baten bidez autentifikatu. Pasahitzak honako baldintzak bete beharko ditu:

c. Identificación y autenticación

1. Para acceder a un SSII todo usuario y usuaria se identificará mediante un identificador de usuario o usuaria y se autenticará mediante una contraseña que deberá cumplir una serie de requisitos:

- Pasahitzak gutxienez bost karaktere izango ditu (zenbakizko karaktereak eta karaktere alfabetikoak nahastuz). Pasahitza ezin izango da jakinarazi, ezin izango da idatziz jaso eta ezin izango da hirugarren pertsonek ikusteko moduan utzi.
- Erabiltzaileak uste badu beste pertsona bat ari dela erabiltzen edo erabil dezakeela berea den baimendutako sarbidea, nahitaez aldatu beharko du bere pasahitza eta segurtasun arduradunarekin harremanetan jarri beharko da gertatutakoaren berri emateko.
- Ezin izango da erabili beste erabiltzaile baten baimendutako sarbiderik, nahiz eta jabeak erabiltzeko baimena eman.

2. Erabiltzaileek ez dute euren edo hirugarren pertsonen informazio sistemetako gune murriztuetara sartzeko ahaleginik egin behar, ez bada haiei esleitutako gunea.

3. Erabiltzaileek ez dute koderik, sistemarik edo enkriptatze-algoritmorik edo prozesu telematikoetan parte hartzen duen bestelako segurtasun elementurik deszifratzeko ahaleginik egingo.

4. Sare korporatibora konektatzeko, entitateak [toki entitatearen izena] zehaztutako bitartekoak bakarrik erabili ahal izango dituzte erabiltzaileek.

d.Segurtasun gorabeheren kudeaketa

Erabiltzaileek datu pertsonalen segurtasunari eragiten dion edo eragin diezaiokeen segurtasun gorabeheraren bat atzematen badute (zerrendak edo disketeak galtzea, baimendutako atzipenaren erabilera oker baten susmoa izatea, datuak berreskuratzea eta abar), segurtasun arduradunari eman beharko diote horren berri. Erabiltzaile batek segurtasun gorabehera baten berri badu, baina ez badu horren berri ematen, segurtasunaren aurkako hutsegitetzat joko da.

- La contraseña estará compuesta por un mínimo de cinco caracteres, (combinando caracteres alfabéticos y numéricos) y no se deberá revelar mediante ningún concepto, ni se deberá mantener por escrito o a la vista de terceras personas.
- Si un usuario o usuaria tiene sospecha fundada de que su acceso autorizado está siendo o puede ser utilizado por otra persona, estará obligado a cambiar su contraseña y contactará con la persona Responsable de Seguridad, para comunicar la incidencia.
- No se podrá utilizar ningún acceso autorizado de otro usuario o usuaria, aunque lo autorice la persona propietaria.

2. Ningún usuario o usuaria debe intentar acceder a áreas restringidas de los sistemas de información propios o de terceras personas, distintos de los que le hayan sido asignados.

3. Ningún usuario o usuaria debe intentar descifrar claves, sistemas o algoritmos de cifrado o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

4. Ningún usuario o usuaria debe conectar a la red corporativa a través de otros medios que no sean los definidos por [entidad local].

d. Gestión de incidencias

Todo usuario y usuaria deberá notificar a la persona Responsable de Seguridad cualquier incidencia que detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal (pérdida de listados o disquetes; sospecha de uso indebido del acceso autorizado, por otras personas; recuperación de datos, etc.).El conocimiento y la no notificación de una incidencia por parte de un usuario o usuaria será considerado como una falta contra la seguridad por parte de ese usuario o usuaria.

e. Euskarrien kudeaketa

1. Erabiltzaileek nahitaez itzuli beharko dituzte datu pertsonalak dauzkaten euskarriak, euskarri horiek aldi baterako erabili beharra ekarri duten eginkizunak bukatu bezain pronto.

2. Era berean, datu pertsonalak dauzkaten euskarriak leku seguruan eta giltzapean gorde beharko dituzte erabili behar ez direnean, bereziki lanalditik kanpoko denboran.
3. Datu pertsonalak dauzkaten euskarriak oso ondo identifikatuta egon beharko dute. Horretarako kanpoaldean etiketa bat izango dute (zeharka edo zuzenean) adieraziz zein fitxategi den, zeintzuk datu mota dituen, zein prozesuk sortu dituen eta sortze data.

f. Sekretua gorde beharra

1. Informazio sistemen erabiltzaileek betiko gorde beharko dute sekretua eta ezin izango dituzte datu pertsonalak kanpora jaulki, edozein dela ere euskarria, ez bada horretarako behar bezalako baimen dutela. Era berean, ezin izango dute, zuzenean nahiz zeharka, erabili erakundearekin harremana izandako denboran atzitutako datu pertsonalak eta gainontzeko informazioa. Betebehar horrek iraun egingo du nahiz eta erakundearekin izandako harremana iraungi.

2. Lanpostuarekin zerikusia duten arrazoiak direla eta, erabiltzaileak informazio konfidentziala eskuratzen badu, edozein izanik euskarria eta edozein izanik lortzeko modua, ulertu beharko da aldi baterako baino ez duela eskuratu eta sekretua gorde beharra dagoela. Eta informazioa eskuratu izanak ez du esan nahi informazioaren jabea izateko, titularra izateko, kopia bat eskuratzeko edo banatu ahal izateko eskubiderik dagoenik.

e. Gestión de soportes

1. Los usuarios y usuarias están obligados/as a devolver los soportes que contienen datos de carácter personal inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.
2. Igualmente deberán guardar los soportes que contengan datos de carácter personal en lugar seguro y siempre bajo llave cuando no sean usados, especialmente fuera de la jornada laboral.
3. Los soportes que contengan datos de carácter personal deberán estar claramente identificados con una etiqueta externa que indique (directa o indirectamente) de qué fichero se trata, qué tipo de datos contiene, proceso que los ha originado y fecha de creación.

f. Deber de secreto

1. Los usuarios y usuarias de los SSII deberán guardar, por tiempo indefinido, la máxima reserva y no deberán emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte, salvo que esté debidamente autorizado. Del mismo modo, no podrán utilizar directa o indirectamente, los datos de carácter personal y demás información a la que tengan acceso durante su vinculación con la organización. Esta obligación continuará vigente incluso después de la extinción de las relaciones con dicha organización.
2. En el caso en que por motivos relacionados con el puesto de trabajo, el usuario o usuaria entre en posesión de información confidencial contenida en cualquier tipo de soporte y a través de cualquier medio, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello otorgue derecho alguno de posesión, titularidad, copia o distribución sobre dicha información.

6. DP-EN FITXATEGIEN EGITURA

Toki entitatean [toki entitatearen izena] aitortutako datu pertsonalen fitxategi bakoitzeko ondoko informazioa adieraziko da Eskuliburuaren Eranskinei buruzko alean dagokion eranskinean:

- Fitxategiaren izena.
- Fitxategiaren deskribapena.
- Zein xedapen orokorren bidez argitaratu zen.
- Fitxategiaren segurtasun maila.
- Segurtasun arduraduna.
- Zeintzuk pertsona edo kolektibori buruzko datu pertsonalak gordetzen diren.
- Datu lagatzeak eta komunikazioak.
- Fitxategiaren helburua.
- Datuen jatorria.
- Datuak biltzeko prozedura.

- Erabilitako euskarria.
- Fitxategia tratatzen duten aplikazio informatikoak (edo tresnak). Aplikazio edo tresna horiek fitxategiari dagozkion mailaren araberako segurtasun neurriak jaso beharko dituzte.
- Nazioarteko datu transferentziak.

- Datu pertsonalen egitura. Oinarrizko egituran jasota dauden datu pertsonal motak adierazteko, honako sailkapena eta sinboloak erabiliko dira:

  - **ID:** Identifikaziokoak.
  - **EP:** Ezaugarri pertsonalak.
  - **EF:** Ekonomiko-finantzarioak.
  - **AH:** Arau-hauste administratiboak edo penalak.
  - **BB:** Bereziki babestuak (erlijioa, osasuna, bizitza sexuala eta abar.)

Segurtasun agiriak eranskin bat izan behar du toki entiatea dagoen datu pertsonalen fitxategi bakoitzeko.

6. ESTRUCTURA DE LOS FICHEROS DCP

Por cada fichero con DCP declarado en [entidad local] se especifica en el Anexo correspondiente del volumen de anexos la siguiente información:

- El nombre del fichero.
- Descripción del fichero.
- Disposición general de publicación.

- El nivel de seguridad del fichero.
- La persona Responsable de Seguridad.
- Las personas o colectivos sobre los que se guardan los DCP.
- Las cesiones y comunicaciones de datos.
- La finalidad del fichero.
- La procedencia de los datos.
- El procedimiento de recogida de los datos.
- Soporte utilizado.
- Las aplicaciones informáticas (o herramientas) que tratan ese fichero, las cuales deberán incluir las medidas de seguridad correspondientes al nivel de seguridad del fichero.
- Las transferencias internacionales de datos.
- La estructura de datos de carácter personal. Para indicar los tipos de datos de carácter personal, contenidos en la estructura básica, se utilizará la siguiente clasificación y su correspondiente simbología:
  - **ID:** Carácter identificativo.
  - **PE:** Características personales.
  - **EF:** Económico-financieros.
  - **IN:** Infracciones administrativas o penales.
  - **PR:** Especialmente protegidos (religión, salud, vida sexual, etc.)

El Documento de Seguridad incluye un anexo por cada fichero con DCP existente en la entidad local.

7. TERMINOEN ZERRENDA		7. GLOSARIO DE TÉRMINOS	
DPZ	Datuak Prozesatzeko Zentroa	CPD	Centro de Proceso de Datos
DP	Datu pertsonalak	DCP	Datos de Carácter Personal
SA	Segurtasun Agiria	DS	Documento de Seguridad
TA	Tratamendu arduraduna	ET	Encargado/a del Tratamiento
Hw	Hardware-a	Hw	Hardware
DBLO	Datu Pertsonalak Babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa.	LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
PC	Ordenagailu pertsonala (ingelesez, Personal Computer)	PC	Ordenador Personal (en inglés, Personal Computer)
TK	Tratamendu kontrolatzailea.	RF	Responsable del Fichero
BDLOED	DBLO garatzeko Erregelamandua onartzen duen abenduaren 21eko 1720/2007 Errege Dekretua	RDLOPD	Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la LOPD
SA	Segurtasun arduraduna	RS	Responsable de Seguridad
SE	Sistema Eragilea	SO	Sistema Operativo
IS	Informazio sistemak	SSII	Sistemas de Información
Sw	Software-a	Sw	Software

SEGURTASUN AGIRIA – PROZEDURAK

DOCUMENTO DE SEGURIDAD - PROCEDIMIENTOS

1. PROZEDURAK

1.1. Segurtasun gorabeheraren bat dagoenerako jakinarazpen, kudeaketa eta erantzun prozedura.

Segurtasun gorabeheratzat joko da datuen segurtasunari eragiten dion edo eragin diezaiokeen edozein irregulartasun.

Prozeduraren jarduerak:

1.1.1. Segurtasun gorabeheraren identifikazioa

Segurtasun gorabehera atzematen duen pertsonak Informatika Sailari jakinarazi beharko dio dagokion bitarteko elektroniko edo fisikoaren bidez bidaliko dion Segurtasun Gorabeheraren Jakinarazpenaren bidez.

1.1.2. Segurtasun gorabeheraren erregistroa

Abisua jasotakoan, gertaera Segurtasun Gorabeheren Erregistroan jaso beharko da. Gorabehera Informatika Sailean atzematen bada, jakinarazpen beharrik gabe jasoko da Erregistroan.

Erregistroko mekanismoak modu unibokoan identifikatu beharko du segurtasun gorabehera bakoitza, eta erregistratutako datuak hondatu, aldatu edo desagertu daitezkeela atzemateko eta horrelakorik ez gertatzeko gaitasuna izango du.
Erregistroko ondorioetarako, segurtasun gorabehera hauek bereizten dira:

a. Pasahitza ahaztea.
b. Sarbide murriztua bidegabe erabiltzen dela susmatzea.
c.Datu pertsonalen euskarri informatikoak galtzea.
d. Baimenik gabeko sarbideak datu pertsonalen informazio sistemak dauzkaten bulegoetan.
e. Datu pertsonalak berreskuratzeko eskabidea.
f. Bestelakoak (kode pribatua galtzea eta abar.)

1. PROCEDIMIENTOS

1.1. Procedimiento de notificación, gestión y respuesta ante las incidencias

Se entiende por incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Actividades del procedimiento:

1.1.1. Identificación de la incidencia

La persona que detecte la incidencia, la comunica al Departamento de Informática por medio de una Notificación de la Incidencia a través del medio electrónico o físico correspondiente.

1.1.2. Registro de la incidencia

Se anotará el suceso en un Registro de Incidencias una vez recibido el aviso, o bien a su propia iniciativa, siempre que la incidencia se detecte en el Departamento de Informática.

El mecanismo de registro deberá identificar de manera unívoca cada incidencia acaecida, impidiendo o detectando la alteración, modificación o eliminación de los datos registrados.

A los efectos de su registro, se distinguen los siguientes tipos de incidencias:

a. Olvido de contraseña.
b. Sospecha de uso indebido del acceso restringido.
c. Pérdida de soportes informáticos con datos de carácter personal.
d. Accesos no autorizados a dependencias que contienen sistemas de información con datos de carácter personal.
e. Petición de recuperación de datos de carácter personal.
f. Otras (pérdida de clave privada, etc.)

1.1.3. Segurtasun gorabeherak aztertzea eta neurriak aplikatzea

Segurtasun arduradunak gainbegiratu eta aztertu beharko ditu fitxategiarekin gertatu diren gorabeherak. Gertaerarekin zerikusia duten pertsona guztiak sartuko ditu eginkizun horretan, eta egin den kaltea gutxitzeko edo konpontzeko egokien iruditzen zaizkion neurriak proposatuko ditu, etorkizunean gauza bera gertatu ez dadin.

Segurtasun arduradunak bere erantzukizunpeko fitxategien segurtasunari eragiten dieten segurtasun gorabeheren gaineko oinarrizko informazioa jaso ahal izango du Segurtasun Gorabeheren Erregistroaren bidez, eta berdin dio zein organotan edo organismotan gertatu edo atzeman den segurtasun gorabehera.

Gertatu den segurtasun gorabehera segurtasun sistemaren akats larri batengatik gertatu bada, segurtasun arduradunak segurtasun-gorabeheraren gaineko txostenaren kopia bat tratamendu kontrolatzaileari bidali beharko dio eta beste kopia bat artxibatu, behar den guztietan txostena eskura izateko, bai segurtasun gorabeherak aztertu ahal izateko bai hobetzeko proposamena egin ahal izateko.

1.1.3. Análisis de las incidencias y aplicación de medidas

La persona Responsable de Seguridad supervisará y analizará las incidencias acaecidas en relación con el fichero, involucrando en ello a todas las personas que considere implicadas, y proponiendo las medidas que estime oportunas para eliminar o aminorar el daño que pudiera haberse ocasionado y de esta forma evitar su repetición en el futuro.

La persona Responsable de Seguridad podrá obtener la información básica de las incidencias que afecten a los ficheros de cuya seguridad es responsable, sea cual sea el órgano u organismo en que se hayan producido o detectado, a través del Registro de Incidencias.

Si la incidencia acaecida supone un fallo grave en los sistemas de seguridad, la persona Responsable de Seguridad confeccionará un informe detallado de la incidencia que concrete las medidas adoptadas. Enviará una copia la persona Responsable del Fichero y otra la archivará adecuadamente para poder recurrir a ese informe siempre que sea necesario para analizar las incidencias y proponer soluciones de mejora.

1.2 Erabiltzaileak kudeatzeko prozedura

Toki erakundearen [toki erakundearen izena] zerbitzuan ari den langile baten alta edo baja gertatzen den bakoitzean honako prozedura jarri beharko da abian.
Prozeduraren jarduerak:

1.2.1. Erabiltzailea sortzeko / bajan emateko eskabidea

Toki Erakundearen [toki erakundearen izena] Langileen Sailak badaki zeintzuk diren langileen inkorporazio eta kargu-uzte datak. Beraz, zerbitzu horri dagokio prozedura hastea. Horretarako, Informatika Sailari jakinarazi beharko dio erabiltzailea sortu edo aldatu beharra dagoela, eta horretarako inprimaki eredu hau erabiliko du: **Erabiltzailea sortzeko/bajan emateko eskabidea.**

1.2. Procedimiento de gestión de usuarios y usuarias

Cada vez que se produzca un alta o una baja de personal al servicio de [entidad local] se pondrá en marcha este procedimiento.

Actividades del procedimiento:

1.2.1. Solicitud de creación/baja de usuario o usuaria

El Departamento de Personal de [entidad local] conoce las fechas de incorporaciones y ceses de personal en la [entidad local], por tanto es éste servicio el que inicia el procedimiento,haciendo saber al Departamento de Informática la necesidad de creación o modificación de usuario o usuaria mediante el formulario correspondiente: **Solicitud de alta/baja de usuario o usuaria.**

1.2.2. Pertsona erabiltzailea sortzea eta baimenak kudeatzeko prozedura abian jartzea.

Eskabidea erabiltzaile bat bajan emateko bada, pertsonari baja emateaz gain, **Baimenak kudeatzeko prozedura** jarriko da abian, pertsona erabiltzaile horrek zeuzkan aplikazioetara eta zerbitzuetara sartzeko baimenak ezeztatzeko. Ezeztapena egin ondoren, Informatika Sailari jakinaraziko zaio, eta Informatika Sailak izango du baja izan dela eta benetan bajan eman dutela egiaztatzeko erantzukizuna.

Eskabide bati alta eman behar bazaio eta **Aplikazioetan sartzeko baimen eskabide batekin batera badator**, tratamendu arduradunaren erakundeko erabiltzaileak atenditzeko zerbitzuak emango du altan erabiltzailea eta **Baimenak kudeatzeko prozedura abian jarriko du**.

Eskabidea alta bat egiteko bada, baina eskabidearekin batera ez bada **Aplikazioetan sartzeko baimen eskabiderik** aurkeztu, erabiltzaileari sisteman baino ez zaio emango altan.

Edozelan ere, Erabiltzaileen Erregistroak beti egon beharko du eguneratuta. Erregistroko informazioa Informatika Sailari jakinarazi beharko zaio eta Informatika Sailak izango du erabiltzaileari jakinarazteko ardura eta erabiltzailearekin batera egin beharko ditu egiaztapenak.

1.3 Baimenak kudeatzeko prozedura

Prozedura honek Erabiltzaileen Erregistroan sartzeko baimenen altak, bajak eta aldaketak arautzen ditu.

Prozeduraren jarduerak:

1.2.2. Creación de la persona usuaria y arranque del Procedimiento de gestión de permisos.

Si la petición es una baja de usuario o usuaria, además de dar de baja a la persona se iniciará el **Procedimiento de gestión de permisos** con el fin de revocar todos los permisos de acceso a aplicaciones y servicios para esta persona usuaria. Una vez realizado, lo notificará al Departamento de Informática que será el responsable de comprobar si efectivamente se ha dado de baja en el caso de una baja.

Si la petición es un alta y viene acompañada de la **Solicitud de permiso de acceso** a aplicaciones, el servicio de atención a personas usuarias de la entidad encargada del tratamiento dará de alta la persona usuaria y arrancará el **Procedimiento de gestión de permisos**.

Si la petición es un alta pero no viene acompañada de la **Solicitud de permiso de acceso a aplicaciones**, solamente dará de alta a la persona usuaria en el sistema.

En todos los casos se actualizará el Registro de Usuarios y Usuarias con la información correspondiente y se notificará al Departamento de Informática que será el responsable de notificarlo a la persona usuaria y realizar con el mismo las comprobaciones oportunas.

1.3 Procedimiento de gestión de permisos

Este procedimiento regula las altas, bajas y modificaciones de permisos de accesos en el Registro de Usuarios y Usuarias.

Actividades del procedimiento:

1.3.1. Sarbide baimenen aldaketak identifikatzea

Sarbide baimenak aldatzeko premia bi eratara atzeman ahal izango da:

1. Langile batek toki erakundean [toki entitatearen izena] egiten zuen jarduera uzten badu, Langile Sailak izango du horren berri eta berak jakinarazi beharko dio Informatika Sailari.
2. Baimenak gehitu edo aldatu behar badira, langilea atxikita dagoen administrazio unitateak identifikatu beharko du premia eta berak jakinarazi beharko dio Informatika Sailari.

1.3.2. Baimenak aldatzeko eskabidea

Toki erakundeko [toki entitatearen izena] erabiltzaile batek kargua uzten badu, Langile Sailak jaulkitako baja eskabideak esan nahi du pertsona erabiltzaile horrek zeuzkan aplikazioetarako eta zerbitzuetarako baimenak kentzeko eskabidea ere egiten dela.

Erabiltzaile bati aplikazio batean alta emateko edo erabiltzaile horren sarbide baimenen bat aldatzeko eskabidea bada, langilea atxikita dagoen administrazio unitateko arduradunak **Aplikazioetan sartzeko baimena** bidali beharko du Informatika Sailera.

1.3.3. Sarbide baimenak aldatzea

Informatika Sailak gauzatuko du eskabidea, dena delako baimenak emanez edo kenduz eta Erabiltzaileen Erregistroan eguneratu beharko du.

1.3.1. Identificación de la modificación de permisos de acceso

La necesidad de la modificación de los permisos de acceso podrá ser detectada de dos modos diferentes:
1. En el caso del cese de la actividad de un trabajador o trabajadora en [entidad local] será el Departamento de Personal quien tendrá conocimiento de ello y lo notifique al Departamento de Informática.
2. En el caso de una incorporación o una modificación de permisos, la unidad administrativa a la que está adscrito el trabajador o trabajadora será la que identifica la necesidad y lo notifique al Departamento de Informática.

1.3.2. Solicitud de modificación de permisos

Si se produce el cese de una persona usuaria en [entidad local] la solicitud de baja de la persona usuaria lanzada por el Departamento de Personal incluye explícitamente la solicitud de retirada de los permisos de todas las aplicaciones y servicios para esa persona usuaria.

En los casos en los que suponga un alta de una persona usuaria para una aplicación o una modificación en los permisos de acceso la persona responsable de la unidad administrativa a la que está adscrito/a el trabajador o trabajadora, cursará al Departamento. de Informática la **Solicitud de permiso de acceso** correspondiente.

1.3.3. Modificación de los permisos de acceso

El Departamento de Informática ejecutará la solicitud, dando
o quitando los permisos correspondientes y actualizando el Registro de Usuarios y Usuarias.

1.4 Euskarriak kudeatzeko prozedura

Euskarriak kudeatzeko prozedurak euskarrien sarrerak eta irteerak kudeatzen ditu, bai eta hondakinak eta berrerabilerak ere, honakoen bidez:

- Euskarrien sarrera-prozedura
- Euskarrien irteera-prozedura
- Euskarriak baztertzeko eta berrerabiltzeko prozedura

1.4.1. Euskarrien sarrera prozedura

Toki erakundean euskarri bat jasotzea eta erregistratzea

Datu pertsonalak dauzkan euskarri bat heltzen bada eta horrelako euskarri bati sarrera emateko baimenik ez duen pertsona batek jasotzen badu, pertsona horrek berehala jarri beharko du euskarria baimena duen pertsonaren esku edo tratamendu kontrolatzailearen esku, azken horrek baimendutako pertsona bati helarazi diezaion.

Baimendutako pertsona batek hartzen duenean euskarria, Euskarrien Sarrera eta Irteeren Erregistroan sinatu beharko du eta euskarriaren sarrera erregistratu beharko du Datu pertsonalen fitxategiak dauzkaten euskarrien erregistroan.

Euskarria aztertzean ikusten bada bertan jasotako datuak ez direla toki erakundean [toki entitatearen izena] prozesatu behar, euskarria jatorrira itzuli beharko da. Horretarako, **Euskarrien irteera prozedura** bete beharko da.

Datuak kargatzea eta datu tratamendua

Datuak toki erakundeak [toki entitatearen izena] tratatzekoak badira, euskarria norako den ikusi eta gero, administrazio unitate horretako arduradunari bidaliko zaio, eta berak izango du datuak sisteman kargatzeko eta euskarria erregistrora itzultzeko ardura. Bestalde, datu horiek erakundeko tratamendu arduradunak tratatzekoak badira, euskarria berari bidaliko zaio **Euskarrien irteera prozedura betez**.

1.4 Procedimiento de gestión de soportes

El procedimiento de gestión de soportes regula las Entradas y Salidas de los soportes y los desechos o reutilizaciones de los mismos a través de:

- Procedimiento de entrada de soportes.
- Procedimiento de salida de soportes.
- Procedimiento de desecho, reutili zación de soportes.

1.4.1. Procedimiento de entrada de soportes

Recepción y registro de un soporte en la entidad local

Si un soporte que contiene datos de carácter personal llega a una persona que no está autorizada a dar una entrada de este tipo de soportes, inmediatamente pondrá el soporte a disposición de una persona autorizada o de la persona Responsable del Fichero quien lo pondrá a disposición de una persona autorizada.

Una vez recibido el soporte por una persona autorizada, procederá firmar un Justificante de E/S de soportes y a registrar la entrada del mismo en el Registro de soportes con ficheros con DCP. Si el soporte no posee un código identificador, se le asignará una codificación al mismo.

Si, examinado el soporte, se comprueba que los datos contenidos en el mismo no deben ser procesados en [entidad local], se devolverá a su origen, siguiendo el **Procedimiento de Salida de soportes.**

Carga y tratamiento de datos

Si los datos han de ser tratados en [entidad local] se entregará el soporte a la persona responsable de la unidad administrativa a la que el soporte va dirigido y ésta se encargará de cargar los datos en el sistema y devolver el soporte al registro y si los datos deben ser tratados por la persona encargada del tratamiento de la entidad local, se enviará el soporte al mismo siguiendo el **Procedimiento de Salida de soportes.**

Euskarria biltegiratzea edo itzultzea

Datu tratamendua bukatu ostean, datu pertsonalen fitxategiak dauzkaten euskarrien erregistroaren ardura daukan pertsonak beheko aukeren arteko bat hautatu beharko du eta erregistroan jaso beharko du nola geratu den euskarria:

1. Jatorrira itzuli, euskarrien irteera prozedura kontuan hartuta.
2. Inbentariatu eta gorde.
3. Berrerabili ala suntsitu.

1.4.2. Euskarrien irteera prozedura

Baimena

Datu pertsonalen fitxategiak dauzkaten euskarriak bidaltzeko baimena daukan pertsonak prestatuko du euskarria, etiketa jarriz eta tratamendu kontrolatzaileari bidalketa egiteko baimena eskatuz.

Euskarriak ematea eta erregistratzea

Euskarriak bidaltzeko baimena jasotakoan, euskarriak bidaltzeko ardura daukan pertsonak **Euskarrien sarrera eta irteeren frogagiriaren** jakinarazpen bat eman beharko dio garraiolariari, eta frogagiriaren kopietako bat, garraiolariak izenpetua, toki erakundean [toki entitatearen izena] gorde beharko da.

Euskarria, ahal bada, itxita dagoen eta zigilua duen kartazal edo edukiontzi batean bidaliko zaio hartzaileari, eta euskarriak bidaltzeko ardura daukan erabiltzaileak bidaliko du.

Euskarria hartzaileari bidaltzeko prest dagoenean, baimena daukan pertsonak **Euskarriak irteteko erregistroan** erregistratuko du irteera,identifikazio kode bat eman ondoren.

Almacenamiento o devolución del soporte

Finalizado el tratamiento de los datos, la persona encargada del Registro de soportes con ficheros con DCP adoptará una de las opciones siguientes y registrará, en el registro, la situación en que queda el soporte:

1. Devolverlo a su origen, siguiendo el procedimiento de salida de soportes.
2. Inventariarlo y guardarlo.
3. Reutilizarlo o destruirlo.

1.4.2. Procedimiento de salida de soportes

Autorización

La persona autorizada para realizar el envío de soportes con ficheros con DCP realizará la preparación del soporte, etiquetándolo y solicitando la autorización del envío a la persona Responsable del Fichero.

Entrega y registro

Una vez obtenida la autorización para el envío de soportes, la persona Encargada de la emisión de soportes facilita al/a la transportista una notificación de **Justificante de E/S de soportes**, una de cuyas copias, firmada por el o la transportista, se guarda en [entidad local].

El soporte se entrega a la persona destinataria en un sobre o contenedor cerrado y sellado, siempre que el tipo de soporte lo permita, por medio del usuario o usuaria Encargado/a de Emisión de Soportes.

Una vez entregado el soporte para el envío a la persona destinataria, la persona autorizada registra la salida en el **Registro de salida de soportes**, previa asignación de un código identificador.

1.4.3. Euskarriak baztertzeko eta berrerabiltzeko prozedura

Baimena

Datu pertsonalen fitxategiak dauzkan euskarri bat baztertu edo berreskuratu ahal izateko, tratamendu kontrolatzaileak horretarako baimena eman beharko dio Euskarrien erregistroaren arduradunari.

Gauzatzea eta erregistratzea

Euskarria baztertzeko edo berrerabiltzeko baimena daukan pertsonak euskarria baztertu edo berrerabiliko du, erregistroan jasoz eta euskarria baztertuz edo biltegiratuz, gauzatzen den aukeraren arabera, leku batean edo bestean gordez.

1.4.3. Procedimiento de desecho, reutilización de soportes

Autorización

Para proceder al desecho o reutilización de un soporte con ficheros con DCP, la persona Responsable del Fichero deberá dar la autorización correspondiente a la persona encargada del Registro de soportes.

Actuación y registro

La persona autorizada realizará la actuación necesaria para el desecho o la reutilización del soporte, reflejándolo en el registro y deshaciéndose del soporte o almacenándolo donde proceda según cada caso.

1.5. Kopiak kudeatzeko eta datuak berreskuratzeko prozedura

1.5.1. Kopiak kudeatzeko prozedura

1.5.1.1. Segurtasun kopiak egitea

Informatika Sailak babes kopiak antolatu beharko ditu, eta horretarako kontuan hartu beharko du gauza bat dela sistema berreskuratzea eta beste bat informazioa berreskuratzea eta berreskuratzeko erak ezberdinak eta bata bestearengandik independienteak izan behar dutela. Segurtasun gorabehera bat badago, babes kopiek aukera eman beharko dute segurtasun gorabehera gertatu aurreko egoera berean berreskuratu ahal izateko informazioa. Beraz, berreskuratze leihoa erabakitzeko, erakundearen premiak hartu beharko dira kontuan.

Zentzu horretan, gogoan izan behar da datu pertsonalak babestearen arloan indarrean dagoen legediak agintzen duela astero egin behar direla babes kopiak, eta ez dela astero egin beharrik izango, epealdi horretan ez bada datuen eguneratzerik egon.

1.5. Procedimiento de gestión de copias y de recuperación de datos

1.5.1. Procedimiento de gestión de copias

1.5.1.1. Realización de las copias de seguridad

El Departamento de Informática deberá organizar las copias de respaldo de manera que sea posible la recuperación del sistema y de la información de manera separada e independiente. Ante una incidencia, las copias de seguridad deberán permitir la recuperación de la información al mismo estado en que se encontrara en el instante anterior a la incidencia, por lo que se debe acordar la ventana de recuperación necesaria de acuerdo a las necesidades de la organización.

En este punto, se tendrá en cuenta que la legislación vigente en materia de protección de datos de carácter personal exige que se realicen copias de seguridad, al menos semanalmente, salvo que en dicho periodo no se hubiera producido ninguna actualización de los datos.

Babes kopiak modu automatizatuan egin beharko dira, aldizkako programazioaren bidez.

La realización de las copias de seguridad se deberá automatizar mediante su programación periódica.

1.5.1.2. Babes kopiak gordetzea eta suntsitzea

Tratamendu kontrolatzaileak finkatu beharko ditu babes kopietako informazioa gordetzeko irizpideak, indarrean dagoen legediak ezartzen dituen epeak eta premia operatiboak kontuan hartuta, eta informazioa gordetzeko denbora tarte hori ahalik eta laburrena izanik.

1.5.1.2. Conservación y destrucción de las copias de seguridad

La persona Responsable del Fichero deberá determinar los criterios de retención de información en las copias de seguridad durante los plazos determinados por la legislación vigente y las necesidades operativas, minimizando los tiempos de retención.

Goi-mailako informazioa badute, babes kopiak eta berreskuratzeko prozedurak ezin izango dira egon datuak tratatzen dituzten ekipo informatikoak dauden toki berean, eta edozelan ere, segurtasun neurriak bete beharko dira.

Siempre que alojen información de nivel alto, las copias de seguridad y los procedimientos de recuperación de los datos deberán conservarse en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad.

Datu pertsonalen fitxategiak dauzkaten euskarrien irteerek tratamendu kontrolatzailearen baimena beharko dute.

La salida de los soportes de las copias de seguridad que contengan datos de carácter personal será autorizada por la persona Responsable del Fichero.

Babes kopien euskarriak aldizka birziklatu beharko dira, ezinezkoa izan dadin bertan gordetako informazioa berreskuratzea.

Los soportes de las copias de seguridad serán reciclados periódicamente de forma que no sea posible la recuperación de la información guardada.

1.5.2. Datuak berreskuratzeko prozedura

1.5.2. Procedimiento de recuperación de datos

1.5.2.1. Datuak berreskuratzeko eskabidea

Datuak berreskuratzeko eskabidea segurtasun gorabehera baten ondorioa izan ohi da; segurtasun-gorabeherak eragindako erabiltzaileak fitxategi bateko datuak berreskuratzeko eskabidea aurkeztu behar du Informatika Sailean, zein datako informazioa behar duen adieraziz.

1.5.2.1. Solicitud de recuperación de datos

Una solicitud de recuperación de datos es el resultado de alguna incidencia; el usuario o la usuaria afectada por la incidencia, hace una solicitud de recuperación de datos de un fichero al Departamento de Informática, indicando la fecha a la que se quiere retrotraer la información

1.5.2.2. Baimena

Informatika Sailak segurtasun arduradunari eskatu beharko dio baimena. Baina, goi-mailako eta maila ertaineko fitxategiak badira, tratamendu kontrolatzaileari eskatuko beharko dio datuak berreskuratzeko baimena.

Babes kopien bitartez informazioa berreskuratu ahal izateko, tratamendu kontrolatzailearen baimena beharko da. Informazioa goi-mailakoa edo maila ertaineko bada, honakoak erregistratu beharko dira: datuak berreskuratzeko gauzatu diren prozedurak zehatz-mehatz, berreskuratzea egin zuen profesionala nor izan zen, zeintzuk datu berreskuratu ziren eta zergatik berreskuratu behar izan ziren datu horiek.

Berreskuratzea egin ahal izateko, berreskuratu den informazioa ustiatu ohi duten pertsonen onarpena ere beharko da.

Informatika Sailak fitxategiaren segurtasun arduradunari eskatu beharko dio baimena tratamendu arduradunari eskatu ahal izateko datu horiek berreskuratzeko.

1.5.2.3. Babes kopietako informazioa berreskuratzea

Dena delako fitxategiaren segurtasun arduraduna den pertsonak adostasuna agertu ondoren, datuak berreskuratu egingo dira eta honakoak erregistratu beharko dira: datuak berreskuratzeko gauzatu diren prozedurak zehatz-mehatz, berreskuratzea egin zuen profesionala nor izan zen, zeintzuk datu berreskuratu ziren eta zergatik berreskuratu behar izan ziren datu horiek.

Berreskuratzea egin ahal izateko, berreskuratu den informazioa ustiatu ohi duten pertsonen onarpena ere beharko da.

1.5.2.2. Autorización

El Departamento de Informática solicita autorización a la persona Responsable de Seguridad o a la persona Responsable del Fichero en los ficheros de nivel medio y alto para realizar la recuperación de esos datos.

La recuperación de información a partir de copias de respaldo deberá ser autorizada por la persona Responsable del Fichero, en el caso de que ésta sea de nivel medio y alto, registrándose en detalle los procedimientos llevados a cabo para la recuperación de los datos, el o la profesional que la realizó, los datos restaurados y el motivo que hizo necesaria la operación.

La recuperación deberá incluir la aceptación por parte de los usuarios y usuarias que explotan habitualmente la información recuperada.

El Departamento de Informática solicita autorización a la persona Responsable de Seguridad del fichero para solicitar la recuperación de esos datos a la persona encargada del tratamiento.

1.5.2.3. Recuperación de información de las copias de seguridad

Una vez obtenida la conformidad de la persona Responsable de Seguridad del fichero afectado, se ejecuta la recuperación de los datos registrándose en detalle los procedimientos llevados a cabo para la recuperación de los datos, el o la profesional que la realizó, los datos restaurados y el motivo que hizo necesaria la operación.

La recuperación deberá incluir la aceptación por parte de los usuarios y usuarias que explotan habitualmente la información recuperada.

1.6. Segurtasun agiria eguneratzeko prozedura

1. Segurtasun agiria arrazoi askorengatik eguneratu daiteke: kanpoko gertaera batek eraginda, aurreko prozedura horietako bat gauzatu delako edo toki erakundeko [toki erakundearen izena] tratamendu kontrolatzaileak eskatu duelako. Eguneratze mota kontuan hartuta, gerta daiteke Eranskinak bakarrik eguneratu behar izatea edo, kontrakoa, hau da, Araudi berria onartu behar izatea, edo prozeduraren bat eguneratu behar izatea.
2. Eguneratze prozedura hasteko arrazoiak:

1. Datu pertsonalen fitxategiak sortu, ezabatu edo aldatzea.

2. Segurtasunaren antolaketan aldaketak egotea.
3. Araudietan edo prozeduretan aldaketak egotea.
4. Lege-xedapenetan aldaketak egotea.
5. Ekipamendu informatikoa erostea, aldatzea edo kentzea.
6. Datu pertsonalen fitxategiak atzitzen dituzten aplikazioen ekoizpenak abian jartzea edo geldiaraztea.
7. Aldaketak fitxategien zerbitzarietan.

8. Erabiltzaileak kudeatzeko prozedura gauzatzea.
9. Baimenak kudeatzeko prozedura gauzatzea.

1.6.1. Aldatzeko proposamena

1, 2, 3 eta 4 kasuak badira, tratamendu kontrolatzaileak aldaketa proposamena egin beharko dio Informatika Sailari.

6. kasuan aldaketak baimenen kudeaketaren arlokoak dira; beraz, eguneratze prozedura abian jarri beharko da.
7. kasuan Informatika Sailak eguneratu beharko du segurtasun agiria.

8 eta 9. kasuetan prozedura horiek gauzatzean berez dator prozedura hau hasi beharra.

1.6. Procedimiento de actualización del Documento de Seguridad

1. El procedimiento de actualización del Documento de Seguridad puede ser motivado por un hecho externo, por la ejecución de alguno de los procedimientos anteriores, o puede ser iniciado a demanda por la persona Responsable del Fichero de [entidad local]. En función de la modificación es posible que sólo debamos actualizar los Anexos, o por el contrario aprobar una nueva Normativa o actualizar algún Procedimiento.
2. Causas que inician el procedimiento de actualización:

1. Creación, supresión o modificación de ficheros que contienen datos de carácter personal.
2. Cambios en la organización de la seguridad.
3. Cambios en las normativas o procedimientos.
4. Cambios en las disposiciones legales.
5. Adquisición, sustitución o retirada de equipamiento informático.
6. Puesta en funcionamiento o retirada de producción de aplicaciones con acceso a ficheros con DCP.
7. Modificaciones en los servidores de ficheros.
8. La ejecución del procedimiento de gestión de usuarios y usuarias.
9. La ejecución del procedimiento de gestión de permisos.

1.6.1. Propuesta de cambio

En los casos 1, 2, 3 y 4 la persona Responsable del Fichero lanza una propuesta de cambio al Departamento de Informática.
En el caso 6 se producen cambios en la gestión de permisos, con lo que se arranca el procedimiento de actualización.

En el caso 7 el Departamento de Informática es que actualiza el Documento de Seguridad.
En los casos 8 y 9 la ejecución de los procedimientos conlleva automáticamente la iniciación de este procedimiento.

1.6.2. Segurtasun agiria eguneratzea

Informatika Sailak egingo du. Aldaketak araudia aldatzea edo prozedura aldatzea badakar, tratamendu kontrolatzaileak onartu beharko du.

1.6.2. Actualización del Documento de Seguridad

El Departamento de Informática realizará las acciones pertinentes. En el caso de que la modificación suponga un cambio de Normativa o una modificación de Procedimiento, deberá ser aprobada por la persona Responsable del Fichero.

1.6.3. Segurtasun agiria onartzea eta agiriaren zabalkundea egitea

Tratamendu kontrolatzaileak onartu behar du agiria eta bera arduratuko da agiriaren zabalkundea egiteaz toki erakundean [toki erakundearen izena].

1.6.3. Aprobación y difusión del Documento de Seguridad

La persona Responsable del Fichero aprueba el documento y se encarga de la difusión del mismo en [entidad local].

1. ERANSKINA – DP-EN FITXATEGIAK / ANEXO 1 – FICHEROS CON DCP

Agiria Documento	**Izena** Nombre	**Segurtasun maila** Nivel de Seguridad	**Segurtasun Arduraduna** Responsable de Seguridad
1.1 Eranskina Anexo 1.1			
1.2 Eranskina Anexo 1.2			
1.n Eranskina Anexo 1.n			

1.1. ERANSKINA – 1 FITXATEGIA / ANEXO 1.1 – FICHEROS 1

Deskribapena
Descripción

Xedapen orokorra
Disposición General

Segurtasun maila
Nivel de seguridad

Helburua
Finalidad

Kolektiboak
Colectivos

Datu lagatzeak eta komunikazioak
Cesiones y comunicaciones de datos

Datuen jatorria
Procedencia de los datos

Datuen bilketaren prozedura
Procedimiento de recogida

Erabilitako euskarria
Soporte utilizado

Nazioarteko datu-transferentziak
Transferencias internacionales de datos

Datu pertsonalen egitura
La estructura de datos de carácter personal

Izaera identifikatzailea
Carácter identificativo

Ezaugarri pertsonalak
Características personales

Ekonomiko-Finantzarioak
Económico-Financieros

Arau-hauste administratiboak
Infracciones administrativas

Bereziki babestuak
Especialmente protegidos

Fitxategi hau tratatzen duten aplikazio informatikoen zerrenda

Relación de aplicaciones informáticas que tratan este fichero

2. ERANSKINA – APLIKAZIOAK / ANEXO 2 – APLICACIONES

Agiria Documento	**Aplikazioa** Aplicación	**Deskribapena** Descripción
2.1 Eranskina Anexo 2.1		
2.2 Eranskina Anexo 2.2		
2.n Eranskina Anexo 2.n		

2.1. ERANSKINA – 1 FITXATEGIA / ANEXO 2.1 – FICHEROS 1

Aplikazioa
Aplicación

Aplikazioaren kodea
Código aplicación

Deskribapena
Descripción

Autentifikazio sistema
Sistema autenticación

Zerbitzaria
Servidor

Aplikazio honetan tratatzen diren DPen fitxategien zerrenda

Relación de ficheros con DCP que se tratan en esta aplicación

3. ERANSKINA – ORDENAGAILU PERTSONALAK
ANEXO 3 – ORDENADORES PERSONALES

Agiria Documento	**Etiketa** Etiqueta	**Deskribapena** Descripción
3.1 Eranskina Anexo 3.1		
3.2 Eranskina Anexo 3.2		
3.n Eranskina Anexo 3.n		

3.1. ERANSKINA – 1 ORDENAGAILUA / ANEXO 3.1 – PC 1

Etiketa
Etiqueta

Deskribapena
Descripción

Mota
Tipo

Serie zenbakia
Número de serie

Sistema eragilea
Sistema operativo

Kokapena
Ubicación

4. ERANSKINA – ZERBITZARIAK / ANEXO 4 – SERVIDORES

Agiria Documento	**Zerbitzaria** Servidor	**Deskribapena** Descripción
4.1 Eranskina Anexo 4.1		
4.2 Eranskina Anexo 4.2		
4.n Eranskina Anexo 4.n		

4.1. ERANSKINA – 1 ZERBITZARIA / ANEXO 4.1 – SERVIDOR 1

Zerbitzariaren izena
Nombre servidor

Sistema eragilea
Sistema operativo

Bertsioa
Versión

Kokapena
Ubicación

Zerbitzari honetan dauden datu pertsonalen fitxategien zerrenda

Relación de ficheros con DCP que se albergan este servidor

5. ERANSKINA – INTALAZIOAK / ANEXO 5 – INSTALACIONES

Agiria Documento	**Izena** Nombre	**Deskribapena** Descripción
5.1 Eranskina Anexo 5.1		
5.2 Eranskina Anexo 5.2		
5.n Eranskina Anexo 5.n		

5.1. ERANSKINA – 1 INSTALAZIOA / ANEXO 5.1 – INSTALACIÓN 1

Izena
Nombre

Helbidea
Dirección

Instalazio hauetako bakoitzean kokatua dauden zerbitzarien zerrenda

Relación de servidores ubicados en cada una de estas instalaciones

6. ERANSKINA – ERABILTZAILEAK / ANEXO 6 – USUARIOS

Agiria Documento	**Erabiltzailea** Usuario	**Deskribapena** Descripción
6.1 Eranskina Anexo 6.1		
6.2 Eranskina Anexo 6.2		
6.n Eranskina Anexo 6.n		

6.1. ERANSKINA – 1 ERABILTZAILEA / ANEXO 6.1 – USUARIO/A 1

Izena
Nombre

Identifikatiboa
Identificativo

Baimenen bat duen aplikazioen zerrenda
Relación de aplicaciones en las que tiene alguna autorización

Baimen mota
Tipo de autorización

	OINARRIZKO MAILA: Datu pertsonalen fitxategiak edo tratamenduak.		
	MAILA ERTAINA: Arau-hauste administratiboei edo penalei buruzko fitxategiak, ondare eta kreditu kaudimenari buruzko zerbitzuen informazioa ematen duten fitxategiak, Zerga Administrazioen fitxategiak, finantza zerbitzuetako fitxategiak, Gizarte Segurantzako Erakunde Kudeatzaileen eta Zerbitzu Orokorren fitxategiak, laneko istripuen mutualitateen fitxategiak eta nortasuna ebaluatzea ahalbideratzen duten fitxategiak.		
	GOI-MAILA: Ideologiari, sindikatu afiliazioari, erlijioari, sinesmenei, arrazari, osasunari edo bizitza sexualari buruzko datu pertsonalen fitxategiak edo tratamenduak eta polizia helburuetarako pertsonen adostasun beharrik gabe bildutako datuen eta genero indarkeriaren ondoriozko datuen fitxategiak edo tratamenduak.		
SEGURTASUN AGIRIA	• Segurtasun arloko araudia ezartzen du eta honakoak zehazten ditu: ezarpen eremua, neurriak, arauak, segurtasuneko prozedurak eta ereduak, langileen eginkizunak eta betebeharrak, fitxategien eta informazio sistemen deskribapenak eta segurtasun gorabeherak, euskarriak eta agiriak eta segurtasun kopiak kudeatzeko prozedurak. • Euskarriak eta dokumentuak garraiatzeko, berriz erabiltzeko edo baztertzeko hartu beharreko neurriak ezartzen ditu. • Tratamendu arduraduna eta ukitutako fitxategiak identifikatzen ditu, eta hori SAn eta kontratuan jasotzen da. • Eguneratuta egon behar da bai erakundeari dagokionez bai indarrean dagoen legediari dagokionez.	• Segurtasun arduraduna edo arduradunak identifikatzen ditu. • Agiria betetzen dela egiaztatzeko aldizkako kontrolak ezartzen ditu.	
SEGURTASUN ARDURADUNA		• Dokumentuaren segurtasun neurriak koordinatu eta kontrolatzeko arduraduna da. • Horrek ez dakar tratamendu kontrolatzaileak bere erantzukizunetatik azkatzea.	
AUDITORIA		• Barneko edo kanpoko bat, gutxienez 2 urtean behin, Informazio Sistemetan (IS) funtsezko aldaketak agiten direnean. • Hortik auditoria txosten bat aterako da neurrien egokitasunari eta atzemandako akatsei buruzkoa eta neurri zuzentzaileak proposatuko ditu. • Segurtasun arduradunak aztertu behar du. • BDEBren esku geratuko da.	
LANGILEAK	• Segurtasun agiriak argi eta era dokumentatuan zehaztu beharko ditu eginkizunak eta betebeharrak.	• Langileei azaldu beharko zaie zeintzuk arau bete behar dituzten eta zeintzuk diren ez betetzearen ondorioak.	
IDENTIFIKAZIOA ETA AUTENTIFIKAZIOA	• Erabiltzaileak identifikatzeko eta autentifikatzeko neurriak egon beharko dira. • Erabiltzaile bakoitza modu unibokoan eta pertsonalki identifikatu beharko da. • Pasahitzak kudeatzeko, biltegiratzeko eta banatzeko prozedura bat egon beharko da. • Pasahitzen iraungitzea kontrolatzeko eta pasahitzak era irakurtezinean biltegiratzeko prozedura bat egon beharko da.	• Baimenik gabe behin eta berriz egiten diren atzipen saiakerak mugatzeko mekanismoak ezarri beharko dira.	
SARBIDE KONTROLA ETA ATZIPEN ERREGISTROA	• Erabiltzaile bakoitzak bere eginkizunak gauzatzeko behar dituen datu eta baliabideak bakarrik atzitu ahal izango ditu. • Baimendutako erabiltzaileen, erabiltzaile-profilen eta atzipenen zerrenda eguneratu bat egon beharko da. • Baliabideak zeintzuk eskubiderekin atzitzen diren kontrolatzeko mekanismoak egon beharko dute. • Segurtasun agirian baimendutako langileentzako sarbide baimenak kudeatzen dituzten mekanismoak egon beharko dute.	• Sarbide fisikoa kontrolatu beharko da informazio sistemak dauden lokaletan sartzeko.	• Atzipen saiakera bakoitzari buruzko datuak erregistratuko dira. • Datuak bi urtez gordeko dira. • Segurtasun arduradunaren kontrolpean egon beharko da. • Segurtasun arduradunak txosten bat egingo du hilero. • Salbuespen bat dago: pertsona fisikoa eta pertsona bakarraren atzipena.
EUSKARRIEN ETA DOKUMENTUEN KUDEAKETA ETA GARRAIOA	• Bertan dagoen informazio mota identifikatu beharko da. • Inbentario bat egon beharko da. • Sarbide murriztuarekin biltegiratu beharko dira. • Tratamendu kontrolatzaileak baimendu beharko du euskarrien irteera. • Neurriak hartuko dira, euskarriak baztertzen direnerako.	• Euskarrien sarrera eta irteeren erregistro bat egon beharko da uneoro jakiteko zein euskarri edo dokumentu mota den, sarrera edo irteeraren data eta ordua, bidaltzailea eta hartzailea nortzuk diren, informazio mota, euskarria bidaltzeko era eta arduraduna.	• Etiketatze sistema bat egon beharko da, baimendutako erabiltzaileek bakarrik uler dezaketena. • Datuak enkriptatu egingo dira, euskarriak garraiatu behar badira edo eramangarrietan jaso behar badira.
BABES KOPIAK ETA BERRESKURATZEAK	• Babes kopietarako eta datuak berreskuratzeko prozedura bat egon beharko da. • Prozedurak bermatu beharko du datuak galdu edo suntsitu zirenean bezala, egoera berean, berregingo direla. • Babes kopia bat egingo da, gutxienez, astean behin.	• Tratamendu kontrolatzaileak sei hilean behin egiaztatu egin beharko ditu kopiak egiteko prozedurak. • Benetako datuekin lan egin ahal izango da, tratatzen den fitxategiari dagokion segurtasun maila ziurtatzen bada eta kopia bat egin bada.	• Babes kopia bat eta berreskuratze prozeduren kopia bat egon beharko dira, baina ez ekipoak dauden toki berean, beste batean baizik.
SEGURTASUN GORABEHEREN ERREGISTROA	• Erregistratu egin beharko da zein gorabehera mota gertatu den, noiz gertatu den, zein pertsonari jakinarazi zaion eta zeintzuk ondorio eragin dituen.	• Erregistratu egin beharko da datuak berreskuratzeko zein prozedura erabili den, nork gauzatu duen prozedura, zeintzuk datu berreskuratu diren eta zeintzuk grabatu diren eskuz. • Tratamendu kontrolatzaileak eman beharko du datu berreskuratzeetarako prozedurak gauzatzeko baimena.	
TELEKOMU-NIKAZIOAK	• Komunikazio sareen bidez egiten diren atzipenei eskatu behar zaizkien segurtasun neurriak tokian bertan egiten diren atzipenen segurtasun neurrien parekoak izan beharko dira.		• Sare publikoen edo hari gabeko sareen bidez egiten diren datu transmisioak enkriptatu egin beharko dira.

	NIVEL BÁSICO: Ficheros o tratamientos de datos de carácter personal.		
	NIVEL MEDIO: Ficheros o tratamientos de datos relativos a infracciones administrativas o penales, los que informen de servicios de solvencia patrimonial y crédito, los que sean de Administraciones tributarias, los de prestación de servicios financieros, los de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, los de las mutuas de accidentes de trabajo y los que permitan evaluar la personalidad.		
	NIVEL ALTO: Ficheros o tratamientos de datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas y los que contengan datos derivados de actos de violencia de género.		
DOCUMENTO DE SEGURIDAD	• Implanta la normativa de seguridad concretando el ámbito de aplicación, del mismo, las medidas, normas, procedimientos y estándares de seguridad, las funciones y obligaciones del personal, la descripción de los ficheros y de los SSII y los procedimientos de gestión de incidencias, soportes y documentos y copias de seguridad. • Establece las medidas a adoptar en caso de transporte, reutilización o desecho de soportes y documentos. • Identifica a la persona encargada del tratamiento y los ficheros afectados y esto se expresa en el DS y en el contrato. • Se debe mantener actualizado tanto en lo relativo a la organización como a la legislación vigente.	• Identifica al o los responsables de seguridad. • Establece los controles periódicos de cumplimiento del documento.	
RESPONSABLE DE SEGURIDAD		• Es el encargado de coordinar y controlar las medidas de seguridad del documento. • Esto no supone exoneración de responsabilidad del responsable del fichero.	
AUDITORÍA		• Una interna o externa al menos cada 2 años o cuando se realicen cambios sustanciales en los SSII. • Da lugar a un informe de auditoría sobre la adecuación a las medidas, las deficiencias identificadas y propone medidas correctoras. • Es analizado por el responsable de seguridad. • Queda a disposición de la AVPD.	
PERSONAL	• El Documento de Seguridad especifica las funciones y obligaciones de un modo claro y documentado.	• Se difunden entre el personal las normas que les afecten y las consecuencias por incumplimiento.	
IDENTIFICACIÓN Y AUTENTICACIÓN	• Existen medidas para la identificación y autenticación de los usuarios. • Se identifica unívoca y personalmente a cada usuario. • Existe un procedimiento de gestión, almacenamiento y distribución de contraseñas. • Existen procedimientos para controlar la caducidad de contraseñas y el almacenamiento ininteligible de las mismas.	• Se establece un mecanismo que limite el número de intentos reiterados de acceso no autorizado.	
CONTROL Y REGISTRO DE ACCESOS	• Cada usuario accede únicamente a los datos y recursos necesarios para el desarrollo de sus funciones. • Existe una relación actualizada de usuarios, perfiles y accesos autorizados. • Existen mecanismos para controlar los derechos con que se accede a los recursos. • Existen mecanismos que gestionen la concesión de permisos de acceso sólo por personal autorizado en el Documento de Seguridad.	• Se realiza un control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	• Se registran los datos de cada intento de acceso. • Los datos se conservan 2 años. • Está bajo control del responsable de seguridad. • La persona responsable de seguridad realiza un informe mensual. • Existe una excepción: persona física y acceso unipersonal.
GESTIÓN Y DISTRIBUCIÓN DE SOPORTES Y DOCUMENTOS	• Se identifica el tipo de información que contienen. • Se mantiene un inventario. • Se almacenan con acceso restringido. • La persona responsable del fichero autoriza la salida de soportes. • Se adoptan medidas en caso de desecho de soportes.	• Existe un registro de entrada y salida de soportes que permite conocer el tipo de soporte o documento, la fecha y hora, el emisor o receptor, el tipo de información, la forma de envío y la persona responsable.	• Existe un sistema de etiquetado solo comprensible para los usuarios autorizados. • Se cifran los datos en la distribución de soportes y en los dispositivos portátiles.
COPIAS DE RESPALDO Y RECUPERACIÓN	• Debe existir un procedimiento de copias de respaldo y recuperación de datos. • El procedimiento garantiza la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción. • Se realiza una copia de respaldo, al menos semanal.	• El responsable del fichero verifica semestralmente los procedimientos de copia. • Se trabaja sólo con datos reales si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado y se ha hecho una copia.	• Debe existir una copia de respaldo y de los procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
REGISTRO DE INCIDENCIAS	• Se debe registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados.	• Se debe registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente. • La persona responsable del fichero autoriza la ejecución de los procedimientos de recuperación de datos.	
TELECOMUNI-CACIONES	• Las medidas de seguridad exigibles a los accesos a través de redes de comunicaciones deben garantizar un nivel de seguridad equivalente a los accesos en modo local.		• La transmisión de datos a través de redes públicas o de redes inalámbricas debe ser cifrada.

	OINARRIZKO MAILA: Datu pertsonalen fitxategiak edo tratamenduak.		
	MAILA ERTAINA: Arau-hauste administratiboei edo penalei buruzko fitxategiak, ondare eta kreditu kaudimenari buruzko zerbitzuen informazioa ematen duten fitxategiak, Zerga Administrazioen fitxategiak, finantza zerbitzuetako fitxategiak, Gizarte Segurantzako Erakunde Kudeatzaileen eta Zerbitzu Orokorren fitxategiak, laneko istripuen mutualitateen fitxategiak eta nortasuna ebaluatzea ahalbideratzen duten fitxategiak.		
	GOI-MAILA: Ideologiari, sindikatu afiliazioari, erlijioari, sinesmenei, arrazari, osasunari edo bizitza sexualari buruzko datu pertsonalen fitxategiak edo tratamenduak eta polizia helburuetarako pertsonen adostasun beharrik gabe bildutako datuen eta genero indarkeriaren ondoriozko datuen fitxategiak edo tratamenduak.		
SEGURTASUN ARDURADUNA		• Dokumentuaren segurtasun neurriak koordinatu eta kontrolatzeko arduraduna da. • Horrek ez dakar tratamendu kontrolatzailea bere erantzukizunetatik askatzea.	
AUDITORIA		• Barneko edo kanpoko bat, gutxienez 2 urtean behin, Informazio Sistemetan (IS) funtsezko aldaketak egiten direnean. • Hortik auditoria txosten bat aterako da neurrien egokitasunari eta atzemandako akatsei buruzkoa eta neurri zuzentzaileak proposatuko ditu. • Segurtasun arduradunak aztertu behar du. • BDEBren esku geratuko da.	
INFORMAZIOA BILTEGIRATZEA			• Babestutako guneetako artxiboak giltzapean edo antzeko sistema batekin.
KOPIA EDO ERREPRODUKZIOA			• SAk baimendutako langileak bakarrik. • Baztertutako kopiak suntsitu egin beharko dira.
DOKUMENTAZIOA ATZITZEA			• Baimendutako langileak bakarrik. • Atzipenak identifikatzeko mekanismoak daude. • Baimendu gabeko atzipenen erregistroa dago.
DOKUMENTAZIOA GARRAIATZEA			• Neurriak hartuko dira atzipenik edo manipulaziorik egon ez dadin.
SEGURTASUN AGIRIA	• Segurtasun araudia ezartzen du eta honakoak zehazten ditu: ezarpen eremua, neurriak, arauak, segurtasuneko prozedurak eta ereduak, langileen eginkizunak eta betebeharrak, fitxategien eta informazio sistemen deskribapenak eta segurtasun gorabeherak, euskarriak eta agiriak eta segurtasun kopiak kudeatzeko prozedurak. • Euskarriak eta dokumentuak garraiatzeko, berriz erabiltzeko edo baztertzeko hartu beharreko neurriak ezartzen ditu.	• Tratamendu arduraduna eta ukitutako fitxategiak identifikatzen ditu, eta hori SAn eta kontratuan jasotzen da. • Eguneratuta egon behar da bai erakundeari dagokionez bai indarrean dagoen legediari dagokionez.	
LANGILEAK	• Segurtasun agiriak argi eta era dokumentatuan zehaztu beharko ditu eginkizunak eta betebeharrak.	• Langileei azaldu beharko zaie zeintzuk arau bete behar dituzten eta zeintzuk diren ez betetzearen ondorioak.	
SEGURTASUN GORABEHEREN ERREGISTROA	• Erregistratu egin beharko da zein gorabehera mota gertatu den, noiz gertatu den, zein pertsonari jakinarazi zaion eta zeintzuk ondorio eragin dituen.		
SARBIDE KONTROLA ETA ATZIPEN ERREGISTROA	• Erabiltzaile bakoitzak bere eginkizunak gauzatzeko behar dituen datu eta baliabideak bakarrik atzitu ahal izango ditu. • Baimendutako erabiltzaileen, erabiltzaile-profilen eta atzipenen zerrenda eguneratu bat egon beharko da.	• Baliabideak zeintzuk eskubiderekin atzitzen diren kontrolatzeko mekanismoak egon beharko dute. • Segurtasun agirian baimendutako langileentzako sarbide baimenak kudeatzen dituzten mekanismoak egon beharko dute.	
EUSKARRIEN ETA AGIRIEN KUDEAKETA	• Bertan dagoen informazio mota identifikatu beharko da. • Inbentario bat egon beharko da. • Sarbide murriztuarekin biltegiratu beharko dira.	• Tratamendu kontrolatzaileak baimendu beharko du euskarrien irteera. • Neurriak hartuko dira, euskarriak baztertzen direnerako.	
ARTXIBATZEKO IRIZPIDEAK	• Dokumentuak behar bezala gordeko dira, erraz aurkitu eta kontsultatzeko moduan eta AZETA eskubideak erraztasunez erabiltzeko moduan.		
BILTEGIRATZEKO GAILUAK	• Irekitzeko trabak jartzen dituzten gailuak izan beharko dituzte.		
EUSKARRIAK ZAINTZEA	• Dokumentazioa zaintzapean eduki beharko da biltegiratze gailuetan artxibatuta ez dagoenean.		

	NIVEL BÁSICO: Ficheros o tratamientos de datos de carácter personal.		
	NIVEL MEDIO: Ficheros o tratamientos de datos relativos a infracciones administrativas o penales, los que informen de servicios de solvencia patrimonial y crédito, los que sean de Administraciones tributarias, los de prestación de servicios financieros, los de las Entidades Gestoras y Servicios Comunes de la Seguridad Social, los de las mutuas de accidentes de trabajo y los que permitan evaluar la personalidad.		
	NIVEL ALTO: Ficheros o tratamientos de datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas y los que contengan datos derivados de actos de violencia de género.		
DOCUMENTO DE SEGURIDAD	• Implanta la normativa de seguridad concretando el ámbito de aplicación del mismo, las medidas, normas, procedimientos y estándares de seguridad, las funciones y obligaciones del personal, la descripción de los ficheros y de los SSII y los procedimientos de gestión de incidencias, soportes y documentos y copias de seguridad. • Establece las medidas a adoptar en caso de transporte, reutilización o desecho de soportes y documentos.	• Identifica al o los responsables de seguridad del tratamiento y los ficheros afectados y esto se expresa en el DS y en el contrato. • Se debe mantener actualizado tanto en lo relativo a la organización como a la legislación vigente.	
PERSONAL	• El Documento de Seguridad especifica las funciones y obligaciones de un modo claro y documentado.	• Se difunden entre el personal las normas que les afecten y las consecuencias por incumplimiento.	
REGISTRO DE INCIDENCIAS	• Se debe registrar tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados.		
CONTROL Y REGISTRO DE ACCESOS	• Cada usuario accede únicamente a los datos y recursos necesarios para el desarrollo de sus funciones. • Existe una relación actualizada de usuarios, perfiles y accesos autorizados.	• Existen mecanismos para controlar los derechos con que se accede a los recursos. • Existen mecanismos que gestionen la concesión de permisos de acceso sólo por personal autorizado en el Documento de Seguridad.	
GESTIÓN DE SOPORTES Y DOCUMENTOS	• Se identifica el tipo de información que contienen. • Se mantiene un inventario. • Se almacenan con acceso restringido.	• El responsable del fichero autoriza la salida de soportes. • Se adoptan medidas en caso de desecho de soportes.	
CRITERIOS DE ARCHIVO	• Se debe garantizar la correcta conservación, localización y consulta de los documentos y posibilitar el ejercicio de los derechos ARCO.		
DISPOSITIVOS DE ALMACENAMIENTO	• Deben disponer de mecanismos que obstaculicen su apertura.		
CUSTODIA DE SOPORTES	• Se debe custodiar la documentación cuando no se encuentre archivada en los dispositivos de almacenamiento.		
RESPONSABLE DE SEGURIDAD		• Es el encargado de coordinar y controlar las medidas de seguridad del documento. • Esto no supone exoneración de la responsabilidad del responsable del fichero.	
AUDITORIA		• Una interna o externa al menos cada 2 años o cuando se realicen cambios sustanciales en los SSII. • Da lugar a un informe de auditoría sobre la adecuación a las medidas, las deficiencias identificadas y propone medidas correctoras. • Es analizado por el responsable de seguridad • Queda a disposición de la AVPD.	
ALMACENAMIENTO DE LA INFORMACIÓN			• Archivadores en áreas de acceso protegido con llave u otro sistema equivalente.
COPIA O REPRODUCCIÓN			• Sólo personal autorizado en el DS. • Las copias desechadas se deben destruir.
ACCESO A DOCUMENTACIÓN			• Sólo personal autorizado. • Existen mecanismos de identificación de accesos. • Existe un registro de accesos no autorizados.
TRASLADO DE DOCUMENTACIÓN			• Se adoptan medidas para impedir el acceso o manipulación.