Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

BOE, nº 151, de 25 de junio, pág. 24241

El art. 18.4 de la Constitución Española establece que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, prevé en su art. 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas 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 estén expuestos, ya provengan de la acción humana o del medio físico o natural, estableciéndose en el art. 43.3.h) que mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen constituye infracción grave en los términos previstos en la propia Ley.

Sin embargo, la falta de desarrollo reglamentario ha impedido disponer de un marco de referencia para que los responsables promovieran las adecuadas medidas de seguridad y, en consencuencia, ha determinado la imposibilidad de hacer cumplir uno de los más importantes principios de la Ley Orgánica.

El presente Reglamento tiene por objeto el desarrollo de lo dispuesto en los arts. 9 y 43.3.h) de la Ley Orgánica 5/1992.

El Reglamento determina las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas de seguridad que se establecen se configuran como las básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal, sin perjuicio de establecer medidas especiales para aquellos ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigen un grado de protección mayor.

En su virtud, a propuesta de la Ministra de Justicia, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 11 de junio de 1999,

DISPONGO:

994/1999 Errege Dekretua, ekainaren 11koa; horren bitartez, datu pertsonalak dituzten fitxategi automatizatuen segurtasun-neurriak ezartzeko Erregelamendua onartu da.

EAO,151 zk., ekainaren 25ekoa, 24241 or.

Espainiako Konstituzioaren 18.4 artikuluak ezartzen duenez, “legeak informatikaren erabilera mugatuko du, herritarren ohorea, eta norberaren nahiz senitartekoen bizitza pribatua, eta horien guztien eskubideen egikaritza osoa bermatzeko”.

Datu pertsonalen tratamendu automatizatua arautzen duen urriaren 29ko 5/1992 Lege Organikoaren 9. artikuluan ezartzen denez, fitxategiaren arduradunak datu pertsonalen segurtasuna bermatzeko eta datuok alteratu, galdu, edo baimendu gabeko tratamendu edo hedapena saihesteko neurri tekniko eta antolaketazkoak hartu beharko ditu, teknologiaren egoera, gordetako datuen izaera eta giza ekintzaren, ingurune fisikoaren zein naturaren ekintzatik datorren zer arriskuren mende dauden kontuan izanda; bestela, 43.3.h) artikuluan ezarritakoaren arabera, eta legeak berak arlo horretan jasotakoari jarraituz, arau-hauste larria egingo da, baldin eta, datu pertsonalak dauzkaten fitxategiak, lokalak, programak edo ekipoak izanda, erregelamendu bidez ezarritako beharrezko segurtasun-neurriak jartzen ez badira.

Hala ere, Legea arauen bitartez garatu ez denez, ezinezkoa izan da orain arte erreferentzia-esparrurik izatea, era horretara, arduradunek segurtasun-neurri egokiak sustatzeko modua izan zezaten, eta, horrenbestez, orain arte ezinezkoa izan da Lege Organikoaren oinarri eta abiaburu garrantzitsuenetako bat betearaztea.

Erregelamendu honen bidez, 5/1992 Lege Organikoaren 9. eta 43.3.h) artikuluetan ezarritakoa garatu nahi da; horixe du xede.

Erregelamendu honek neurriak ezartzen ditu, antolamenduari zein arlo teknikoari dagokienez, informazioa isilpean eta ondo babestuta egongo dela bermatzeko, era horretara zainduko baitira gizakien zein familien ohorea eta intimitatea, baita eskubide pertsonalak erabat baliatzeko aukera ere, datuak aldatu, galdu edo baimenik gabe jakinarazi zein erabiltzeko bidea itxita.

Hemen ezarritako segurtasun-neurriak oinarri-oinarrizkoak dira segurtasun-arloan, eta datu pertsonalak dituzten fitxategi guztietan errespetatu beharko dira; dena dela, oinarrizko neurriez gainera, neurri bereziak ere jarri beharko dira, fitxategiko datuek izaera berezia dutelako edo datuek eurek dituzten ezaugarriak halakoxeak direlako babes-maila handiagoa ezartzea komeni denean.

Horrenbestez, Justizia Ministro andreak halaxe proposatuta, Estatu Kontseiluarekin bat, eta Ministroen Kontseiluak 1999ko ekainaren 11n izandako bileran gaia eztabaidatu ondoren,

XEDATU DUT:

Artículo único. Aprobación del Reglamento

Se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, cuyo texto se inserta a continuación.

Disposición final única.

Entrada en vigor

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE MEDIDAS DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS QUE CONTENGAN DATOS DE CARACTER PERSONAL

CAPITULO PRIMERO

DISPOSICIONES GENERALES

Artículo 1. Ambito de aplicación y fines

El presente Reglamento tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Artículo 2. Definiciones

A efectos de este Reglamento, se entenderá por:

Sistemas de información:

conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Usuario:

sujeto o proceso autorizado para acceder a datos o recursos.

Recurso:

cualquier parte componente de un sistema de información.

Accesos autorizados:

autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

Identificación:

procedimiento de reconocimiento de la identidad de un usuario.

Autenticación:

procedimiento de comprobación de la identidad de un usuario.

Control de acceso:

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

Contraseña:

información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

Artikulu bakarra.Erregelamendua onartzea

Datu pertsonalak dituzten fitxategi automatizatuen segurtasun-neurriak ezartzeko Erregelamendua onartu da, ondoren erantsitako testuaren arabera.

Azken xedapen bakarra.

Indarrean sartzea

Errege Dekretu hau Estatuko Aldizkari Ofizialean argitaratu eta hurrengo egunean jarriko da indarrean.

DATU PERTSONALAK DITUZTEN FITXATEGI AUTOMATIZATUEN SEGURTASUN-NEURRIAK EZARTZEKO ERREGELAMENDUA

LEHEN KAPITULUA

XEDAPEN OROKORRAK

1. artikulua.- Aplikazio-eremua eta xedeak

Honako Erregelamendu honek beharrezko diren neurri tekniko eta antolaketazkoak ezarri nahi ditu, datu pertsonalen tratamendu automatizatua arautzen duen urriaren 29ko 5/1992 Lege Organikoaren erregimenari lotuta daudela, datu pertsonalen tratamendu automatizatuan parte hartzen duten fitxategi automatizatuak, tratamendu-zentroak, lokalak, ekipoak, sistemak, programak eta pertsonak errespetatu behar duten segurtasuna bermatuta egon dadin.

2. artikulua.- Definizioak

Erregelamendu honen ondorioetarako, definizio hauek hartuko dira oinarri:

Informazio-sistemak:

datu pertsonalak biltzeko eta tratatzeko erabiltzen diren fitxategi automatizatuak, programak, euskarriak eta tresneriak.

Erabiltzailea:

datuak edo baliabideak erabiltzeko baimena duen pertsona edo prozedura.

Baliabidea:

informazio-sistema baten osagai den edozein zati.

Baimendutako sarbideak:

erabiltzaile bati, zenbait baliabide erabili ahal izateko, eman zaizkion baimenak.

Identifikazioa:

erabiltzaile baten identitatea zein den ezagutzeko prozedura.

Autentifikazioa:

erabiltzaile baten identitatea zein den egiaztatzeko prozedura.

Sarbide-kontrola:

identitatea egiaztatutakoan, datuak edo baliabideak atzitzeko baimena ematen duen mekanismoa.

Pasahitza:

Isilpeko informazioa, erabiltzaile baten identitatearen autentifikazioa egiteko erabiltzen dena; karaktere-katea izaten da askotan.

Incidencia:

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

Soporte:

objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

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.

Copia del respaldo:

copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Artículo 3. Niveles de seguridad

Las medidas de seguridad exigibles se clasifican en tres niveles:

básico, medio y alto.

Dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Artículo 4. Aplicación de los niveles de seguridad

Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el art. 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.

Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los arts. 17, 18, 19 y 20.

Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.

Artículo 5. Acceso a datos a través de redes de comunicaciones

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Intzidentzia:

datuen segurtasunean eragiten duen edo eragin dezakeen edozein irregulartasun.

Euskarria:

objektu fisikoa, informazio-sistema batean erabilgarri den edo izan litekeena, eta datuak grabatzeko edo berreskuratzeko balio duena.

Segurtasun-arduraduna:

fitxategi-arduradunak formalki halaxe eman diolako, aplikatu beharreko segurtasun-neurriak koordinatzeko eta kontrolatzeko eginkizuna bere gain duen pertsona (edo pertsonak).

Babes-kopia:

fitxategi automatizatu bateko datuen kopia egitea, datuak berreskuratzeko moduko euskarri batean.

3. artikulua.- Segurtasun-mailak

Eskatu beharreko segurtasun-neurrien sailkapenak hiru maila ditu:

oinarrizko maila, maila ertaina eta goi-maila.

Maila horietatik bat ezarriko da, erabilitako informazioa nolakoa den, informazioa isilpean eta ondo babestuta gordetzeko beharra handiagoa edo txikiagoa den kontuan izanda.

4. artikulua.- Segurtasun-mailak aplikatzea

Izaera pertsonaleko datuak dituzten fitxategi guztietan oinarrizko mailakotzat jotako segurtasun-neurriak bete beharko dira.

Oinarrizko mailako neurriez gainera, maila ertainekoak ere bete beharko dira, baldin eta, 5/1992 Lege Organikoaren 28. artikuluaren arabera funtzionatzen duten fitxategietako datuak badira, Herri Ogasuneko edo finantza-zerbitzuetako datuak badira, edo administrazio-arloko zein arlo penaleko arau-hausteei dagozkienak gordetzen badira fitxategian.

Baldin eta fitxategietan ideologia, erlijioa, sinesmenak, arraza-jatorria, osasuna edo bizitza sexuala xede dituzten datuak gordetzen badira, edota, dagokien pertsonen baimenik gabe, polizia-xedeetarako bildutako datuak gordetzen badira, oinarrizko eta maila ertaineko neurriez gain, goi-mailako segurtasun-neurriak ere bete beharko dira.

Fitxategietan jasotako datu pertsonalen multzoak pertsona baten nortasunari buruzko ebaluazioa lortzeko besteko informazioa ematen badu, 17., 18., 19. eta 20. artikuluetan ezarritako maila ertaineko neurriak bermatu beharko dira.

Arestian azaldutako mailetako bakoitza gutxienez eskatu beharreko maila da, betiere, legeen eta erregelamenduen bidez indarrean dauden xedapenei kalterik egin gabe.

5. artikulua.- Komunikazio-sareen bitartez datuak atzitzea

Datu pertsonalak komunikazio-sareen bitartez atzitzeko orduan eskatu behar diren segurtasun-neurriak, datuak sare lokalaren bidez atzitzeko eskatzen den segurtasun-mailari dagozkion neurrien parekoak izango dira.

Artículo 6. Régimen de trabajo fuera de los locales de la ubicación del fichero

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Artículo 7. Ficheros temporales

Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el presente Reglamento.

Todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPITULO II

MEDIDAS DE SEGURIDAD DE NIVEL BASICO

Artículo 8. Documento de seguridad

El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ambito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.

c) Funciones y obligaciones del personal.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Artículo 9. Funciones y obligaciones del personal

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas, de acuerdo con lo previsto en el art. 8.2.c).

El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que

6. artikulua.- Fitxategia kokatuta dagoeneko egoitzez kanpoko lan-araubidea

Izaera pertsonaleko datuak fitxategia kokatuta dagoeneko egoitzaz kanpo tratatu behar badira, fitxategiaren arduradunak horretarako baimena eman beharko du berariaz, eta, nolanahi den ere, dena delako fitxategi-motari dagokion segurtasun-maila bermatu beharko da beti.

7. artikulua.- Fitxategi iragankorrak

Erregelamendu honetan ezarritako irizpideen arabera fitxategi bakoitzari dagokion segurtasun-maila bete beharko dute fitxategi iragankorrek.

Fitxategi iragankor oro ezabatu egin behar da, sortu zuten horretarako eta bere xedeak betetzeko beharrezko izateari uzten dionean.

II. KAPITULUA

OINARRIZKO MAILAKO SEGURTASUN-NEURRIAK

8. artikulua.- Segurtasun-dokumentua

Fitxategiaren arduradunak segurtasun-arautegia sortu eta ezarriko du agiri baten bidez, izaera pertsonaleko datu automatizatuak eta informazio-sistemak atzitzeko modua duten langile guztiek nahitaez bete dezaten.

Agiri horrek, gutxienez, honako argibide hauek bilduko ditu bere baitan:

a) Agiriaren aplikazio-eremua; babestutako baliabideak zein diren azaldu behar da zehatz.

b) Erregelamendu honetan eskatutako segurtasun-maila bermatzeko ezarriko diren neurriak, arauak, prozedurak, jarraibideak eta estandarrak.

c) Langileen betekizunak eta betebeharrak.

d) Datu pertsonalak biltzen dituzten fitxategien egitura eta datu horiek tratatzen dituzten informazio-sistemen deskribapena.

e) Intzidentziei buruzko jakinarazpen-, kudeaketa- eta erantzun-prozedura.

f) Datuei buruzko babes- eta berreskurapen-kopiak egiteko prozedurak.

Agiria eguneratuta egon beharko da beti eta uneoro, eta, informazio-sisteman edo antolamenduan kontuan hartzeko moduko aldaketak gertatzen diren bakoitzean, berrikusi egin beharko da beti.

Agiriaren edukia egokitu egin beharko zaie, beti eta uneoro, izaera pertsonaleko datuen segurtasun-arloan unean-unean indarrean dauden xedapenei.

9. artikulua.- Langileen betekizunak eta betebeharrak

Izaera pertsonaleko datuak eta informazio-sistemak atzitzeko modua duten pertsonetako bakoitzak izango dituen betekizunak eta betebeharrak argi azalduta eta dokumentatuta egongo dira, betiere, 8.2.c) artikuluan ezarritakoaren arabera.

Fitxategiaren arduradunak hartu beharreko neurri guztiak hartuko ditu langileek segurtasun-neurriak ondo ezagut ditzaten, batez ere, bakoitzak bete beharreko betekizunei dagokienez, eta, neurriok bete

pudiera incurrir en caso de incumplimiento.

Artículo 10. Registro de incidencias

El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

Artículo 11. Identificación y autenticación

El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Artículo 12. Control de acceso

Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

La relación de usuarios a la que se refiere el art. 11.1 de este Reglamento contendrá el acceso autorizado para cada uno de ellos.

Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

Artículo 13. Gestión de soportes

Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

Artículo 14. Copias de respaldo y recuperación

El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos

ezean, izan ditzaketen ondorioen berri izan dezaten.

10. artikulua.- Intzidentzien erregistroa

Intzidentziei buruzko jakinarazpen- eta kudeaketa-prozedurak erregistroa izango du nahitaez, eta honako hauek jaso beharko dira bertan: intzidentzia nolakoa izan den, noiz gertatu den, jakinarazpena nork egin duen, jakinarazpena nori egin zaion, eta intzidentziaren ondorioak.

11. artikulua.- Identifikazioa eta autentifikazioa

Fitxategiaren arduradunak eguneratuta izan behar du informazio-sisteman sartzeko baimena duten erabiltzaileen zerrenda bat, eta sarbidean erabiltzaile horiek erabili beharreko identifikazio- eta autentifikazio-prozedurak ere ezarri behar ditu.

Autentifikazio-mekanismo hori pasahitzetan oinarritzen denean, pasahitz horiek esleitzeko, banatzeko eta biltzeko prozedura bat ere ezarri behar da, pasahitzak ondo babestuta eta isilpean gordeta egon daitezen.

Pasahitzak aldian-aldian aldatu behar dira, segurtasun-agirian horretarako ematen diren epeak errespetatuta, eta, indarrean dauden bitartean, inork ez ulertzeko moduko sistema batean egongo dira jasota.

12. artikulua.- Sarbide-kontrola

Erabiltzaileek beren zereginak betetzeko behar dituzten datuak eta baliabideak atzitzeko, horretarako bakarrik balio izan behar du sarbide-baimenak.

Fitxategiaren arduradunak mekanismoak ezarri behar ditu, erabiltzaile batek baimenduta dituenez bestelako daturik edo baliabiderik erabiltzeko modurik izan ez dezan.

Erabiltzaileetako bakoitzari emandako sarbide-baimena ere jakinarazi behar da, Erregelamendu honetako 11.1 artikuluan adierazitako erabiltzaile-zerrenda horretan.

Segurtasun-agirian berariaz horretarako baimena duten langileek eta horiek bakarrik izango dute datuei eta baliabideei buruzko sarbide-baimena emateko, aldatzeko edo kentzeko ahalmena, betiere, fitxategiaren arduradunak ezarritako jarraibideen arabera.

13. artikulua.- Euskarrien kudeaketa

Datu pertsonalak jasota dituzten euskarri informatikoek beti eman behar dute beren informazio-mota identifikatu eta datuak inbentarioan jaso ahal izateko aukera; era berean, segurtasun-agiriaren arabera baimena duten langileentzat bakarrik, sarbide murriztua duen leku batean egon behar dute gordeta.

Datu pertsonalak jasota dituzten euskarri informatikoak fitxategiaren kokagune den egoitzaz kanpora atera ahal izateko, fitxategiaren arduradunak eta berak bakarrik eman beharko du horretarako baimena.

14. artikulua.- Babes- eta berreskurapen-kopiak

Fitxategiaren arduradunak egiaztatu beharko du ea datuei buruzko babes- eta berreskurapen-kopiak

de realización de copias de respaldo y de recuperación de los datos.

Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

CAPITULO III

MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 15. Documento de seguridad

El documento de seguridad deberá contener, además de lo dispuesto en el art. 8 del presente Reglamento, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

Artículo 16. Responsable de seguridad

El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad.

En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento.

Artículo 17. Auditoría

Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.

Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

Artículo 18. Identificación y autenticación

El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y

egiteko prozedurak ondo definituta dauden eta ea modu egokian aplikatzen diren.

Datuei buruzko babes-kopiak egiteko eta datuak berreskuratzeko ezarrita dauden prozedurek bermatu egin behar dute datuak galdu edo suntsitu aurre-aurreko unean zeuden hartantxe utziko dituztela berriz ere.

Gutxienez, astean behin egin beharko dira babes-kopiak; salbuespen izango da denbora-tarte horretan inongo daturik eguneratzen ez bada.

III. KAPITULUA

MAILA ERTAINEKO SEGURTASUN-NEURRIAK

15. artikulua.- Segurtasun-agiria

Segurtasun-agiriak, Erregelamendu honetako 8. artikuluan ezarritakoaz gainera, hauek ere jaso beharko ditu bere baitan: segurtasun-arduradunaren edo -arduradunen identifikazioa; agirian ezarritakoa modu egokian betetzen ari dela egiaztatzeko aldian behin egin beharreko kontrolak; eta euskarri bat suntsitu edo berrerabili behar denerako aintzakotzat hartu beharreko neurriak.

16. artikulua.- Segurtasun-arduraduna

Fitxategiaren arduradunak segurtasun-arduradun bat edo batzuk izendatuko ditu, segurtasun-agirian zehaztutako neurriak koordinatzeko eta kontrolatzeko.

Izendapen horrek, ordea, ez du inola ere esan nahi Erregelamendu honen arabera fitxategiaren arduradunari dagokion ardura beste inoren eskuetan uzten denik.

17. artikulua.- Auditoretza

Gutxienez bi urtean behin, kanpo zein barne-auditoretza egin beharko da datuei buruzko informazio-sistemak eta tratamendu-instalazioak aztertzeko, era horretara, egiaztatuta gera dadin Erregelamendu hau, eta datu-segurtasunaren arloan indarrean diren jarraibideak zein prozedurak betetzen direla.

Auditoretzak egindako txostenak irizpena eman behar du erabilitako neurriak eta kontrolak Erregelamendu honi egokitzen zaizkion, akatsak eta hutsuneak antzeman behar ditu, eta egoera zuzentzeko edo osatzeko beharrezko diren neurriak proposatu behar ditu.

Era berean, txostenak datuak, gertakariak eta oharrak ere jakinarazi behar ditu, emandako irizpenak eta egindako proposamenak zertan oinarritzen diren erakusteko.

Horretarako eskumena duen segurtasun-arduradunak aztertu behar ditu auditoretzaren txostenak, eta, ondoren, fitxategiaren arduradunari jakinaraziko dizkio ondorioak, egoera zuzentzeko hartu beharreko neurriak har ditzan; Datuak Babesteko Bulegoak eskuragarri izango ditu txosten horiek.

18. artikulua.- Identifikazioa eta autentifikazioa

Fitxategiaren arduradunak mekanismoren bat ezarriko du informazio-sisteman sartzen ahalegindu

personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 19. Control de acceso físico

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Artículo 20. Gestión de soportes

Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

Artículo 21. Registro de incidencias

En el registro regulado en el art. 10 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Artículo 22. Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

CAPITULO IV

MEDIDAS DE SEGURIDAD DE NIVEL ALTO

den erabiltzaile oro inolako zalantzarik gabe eta modu pertsonalizatuan identifikatu ahal izateko, eta, erabiltzaileak sartzeko baimena izanez gero, hori egiaztatu ahal izateko.

Informazio-sisteman, baimenik izan gabe, behin eta berriz sartzen ahalegintzeko aukera ere murriztu egin behar da.

19. artikulua.- Sarbide fisikorako kontrola

Segurtasun-agiriaren arabera baimena duten langileak, horiek bakarrik sartu ahal izango dira datu pertsonalak jasota dituzten informazio-sistemak kokatuta daudeneko egoitzetan.

20. artikulua.- Euskarrien kudeaketa

Euskarri informatikoen sarrera-erregistroa osatzeko sistema bat ezarri behar da, era horretara, zuzenean zein zeharka, honako argibide hauen berri izan ahal izateko: euskarri-mota, eguna eta ordua, igorlea, euskarri-kopurua, beren baitako informazio-mota, igorpen-mota, eta, behar bezalako baimena duela, euskarria jasotzeaz arduratuko den pertsona.

Modu berean, euskarri informatikoen irteera-erregistroa osatzeko sistema bat ezarri behar da, era horretara, zuzenean zein zeharka, honako argibide hauen berri izan ahal izateko: euskarri-mota, eguna eta ordua, jasotzailea, euskarri-kopurua, beren baitako informazio-mota, igorpen-mota, eta, behar bezalako baimena duela, euskarria igortzeaz arduratuko den pertsona.

Euskarri bat suntsitu edo berrerabili behar denean, zerrendatik behin-betiko kendu aurretik, hartu beharreko neurri guztiak hartuko dira, euskarri horretan jasotako informazioa geroago inork berreskuratzea erabat ezinezkoa izan dadin.

Euskarriak, mantentze-lanak direla-eta, fitxategiak kokatuta daudeneko egoitzetatik kanpora atera behar badira, hartu beharreko neurri guztiak hartuko dira, euskarri horietan jasotako informazioa geroago inork bidegabe berreskuratzea erabat ezinezkoa izan dadin.

21. artikulua.- Intzidentzien erregistroa

Horrez gainera, 10. artikuluan araututako erregistroan, datuak berreskuratzeko jarraitutako prozedurak ere jaso behar dira, honako hauek adierazita: prozedura burutu zuen pertsona, berreskuratutako datuak, eta, hala badagokio, berreskurapen-prozeduran eskuz grabatu behar izan diren datuak.

Beharrezkoa izango da fitxategiaren arduradunak idatziz baimena ematea, datuak berreskuratzeko prozedurak burutu ahal izateko.

22. artikulua.- Probak nola egin

Datu pertsonalak jasota dituzten fitxategiak badira, informazio-sistemak ezarri edo aldatu aurretik egiten diren probetan ez da benetako daturik erabiliko; salbuespena egin liteke tratatutako fitxategi-mota horri dagokion segurtasun-maila bermatuta badago.

IV. KAPITULUA

GOI-MAILAKO SEGURTASUN-NEURRIAK

Artículo 23. Distribución de soportes

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Artículo 24. Registro de accesos

De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos.

El período mínimo de conservación de los datos registrados será de dos años.

El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

Artículo 25. Copias de respaldo y recuperación

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

Artículo 26. Telecomunicaciones

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPITULO V

INFRACCIONES Y SANCIONES

Artículo 27. Infracciones y sanciones

El incumplimiento de las medidas de seguridad descritas en el presente Reglamento será sancionado de acuerdo con lo establecido en los arts. 43 y 44 de la Ley Orgánica 5/1992, cuando se trate de ficheros de titularidad privada.

El procedimiento a seguir para la imposición de la sanción a la que se refiere el párrafo anterior será el establecido en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones,

23. artikulua.- Euskarrien banaketa

Datu pertsonalak dituzten euskarriak banatu behar direnean, datu horiek enkriptatu egin beharko dira, edo, bestela, beste edozein mekanismo erabili beharko da, garraio-denboran informazio hori inork ulertzeko edo manipulatzeko modurik izan ez dezan.

24. artikulua.- Sarbideen erregistroa

Atzipen bakoitzetik, gutxienez, argibide hauek gordeko dira: erabiltzailearen identifikazioa, atzipen-eguna eta –ordua, atzitutako fitxategia, atzipen-mota, eta atzipena baimendu edo ukatu egin den.

Atzipena baimendutakoa izan bada, beharrezkoa izango da atzitutako erregistroa identifikatzeko besteko informazioa gordetzea.

Aurreko paragrafoetan zehaztutako datuen erregistroa bideratzeko mekanismoak zuzenean kontrolpean izango ditu beti horretan eskumena duen segurtasun-arduradunak; ez da inoiz utzi behar, inola ere ez, mekanismo horiek indargabetzen.

Erregistroan jasotako datuak gordetzeko epea, gutxienez, bi urtekoa izango da.

Horretarako eskumena duen segurtasun-arduradunak aldian behin aztertu beharko ditu erregistroan jasotako kontrol-informazioa, eta txostena egingo du azterketa horietaz eta antzemandako arazoez, gutxienez, hilean behin.

25. artikulua.- Babes- eta berreskurapen-kopiak

Babes-kopia bat eta datuak berreskuratzeko prozeduren kopia bat gorde beharko dira, datuen tratamendurako tresneria informatikoak daudeneko lekuan ez, beste nonbait, eta, nolanahi den ere, Erregelamendu honetan agindutako segurtasun-neurriak bete beharko dira beti.

26. artikulua.- Telekomunikazioak

Telekomunikazio-sareen bitartez datu pertsonalak transmititu behar direnean, datu horiek enkriptatu egin beharko dira, edo, bestela, beste edozein mekanismo erabili beharko da, informazio hori beste inork ulertzeko edo manipulatzeko modurik izan ez dezan.

V. KAPITULUA

ARAU-HAUSTEAK ETA ZEHAPENAK

27. artikulua.- Arau-hausteak eta zehapenak

Erregelamendu honetan adierazitako segurtasun-neurriak bete gabe utziz gero, titulartasun pribatuko fitxategiak direnean, zehapena ezarriko da, 5/1992 Lege Organikoaren 43. eta 44. artikuluetan ezarritakoaren arabera.

Aurreko lerrokadan adierazitako zehapenak ezartzeko jarraitu behar den prozedura ekainaren 20ko 1332/1994 Errege Dekretuan dago jasota; izan ere, Errege Dekretu horren bitartez garatu ziren datu pertsonalen tratamendu automatizatua arautzen duen urriaren 29ko 5/1992 Lege Organikoaren zenbait alderdi.

Herri Administrazioen ardurapean dauden fitxategiak direnean, prozedurari eta zehapenei dagokienez, 5/1992 Lege Organikoaren 45. artikuluan ezarritakoa

a lo dispuesto en el art. 45 de la Ley Orgánica 5/1992.

Artículo 28. Responsables

Los responsables de los ficheros, sujetos al régimen sancionador de la Ley Orgánica 5/1992, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal en los términos establecidos en el presente Reglamento.

CAPITULO VI

COMPETENCIAS DEL DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS

Artículo 29. Competencias del Director de la Agencia de Protección de Datos

El Director de la Agencia de Protección de Datos podrá, de conformidad con lo establecido en el art. 36 de la Ley Orgánica 5/1992:

Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica 5/1992.

Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros cuando no se cumplan las medidas de seguridad previstas en el presente Reglamento.

DISPOSICION TRANSITORIA

Disposición Transitoria Unica. Plazos de implantación de las medidas

En el caso de sistemas de información que se encuentren en funcionamiento a la entrada en vigor del presente Reglamento, las medidas de seguridad de nivel básico previstas en el presente Reglamento deberán implantarse en el plazo de seis meses desde su entrada en vigor, las de nivel medio en el plazo de un año y las de nivel alto en el plazo de dos años.

Cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de alguna de las medidas de seguridad previstas en el presente Reglamento, la adecuación de dichos sistemas y la implantación de las medidas de seguridad deberán realizarse en el plazo máximo de tres años a contar desde la entrada en vigor del presente Reglamento.

hartuko da oinarri.

28. artikulua.- Arduradunak

Fitxategi-arduradunek, baldin eta 5/1992 Lege Organikoaren zehapen-erregimenari lotuta badaude, beharrezko diren neurri guztiak hartu beharko dituzte antolamendu zein teknika aldetik, Erregelamendu honetan ezarritakoaren arabera datu pertsonalen segurtasuna erabat bermatuta egon dadin.

VI. KAPITULUA

DATUAK BABESTEKO BULEGOKO ZUZENDARIAREN ESKUMENAK

29. artikulua.- Datuak Babesteko Bulegoko zuzendariaren eskumenak

Datuak Babesteko Bulegoko zuzendariak eskumen hauek izango ditu, 5/1992 Lege Organikoaren 36. artikuluan ezarritakoari jarraituz:

Hala dagokionean, datuen tratamendu automatizatuak 5/1992 Lege Organikoaren printzipioei egokitzeko beharrezko diren jarraibideak emateko eskumena, betiere, beste erakunde batzuen eskumenei ezer kendu gabe.

Datu pertsonalen tratamenduaren amaiera eta fitxategien deuseztapena agintzeko eskumena, Erregelamendu honetan jasotako segurtasun-neurriak betetzen ez direnean.

XEDAPEN IRAGANKORRA

Xedapen Iragankor Bakarra. Neurriak ezartzeko epeak

Erregelamendu hau indarrean sartzen denerako martxan dauden informazio-sistemak badira, Erregelamendu honetan jasotako segurtasun-neurriak, oinarrizko mailakoak, sei hilabeteko epean jarri beharko dira martxan; maila ertainekoak, berriz, urtebeteko epean; eta goi-mailako segurtasun-neurriak, azkenik, bi urteko epean abiarazi beharko dira.

Erregelamendu hau indarrean sartu orduko martxan dauden informazio-sistemak diren modukoak direlako, Erregelamendu honetan jasotako segurtasun-neurrietakoren bat ezartzea teknologia aldetik ezinezkoa denean, sistema horiek egokitzeko eta segurtasun-neurriak ezartzeko epea, gehienez ere, hiru urtekoa izango da, Erregelamendu hau indarrean sartzen denetik kontatzen hasita.