“REGULAMENTO MUNICIPAL DE SEGURIDADE PARA A PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL

Aprobado inicialmente por acordo do Pleno do Concello de Santiago de Compostela do 28 de xullo de 2005. Publicada no BOP de A Coruña do 15 de outubro de 2005.

1. OBXECTO

2. DEFINICIÓNS

3. ÁMBITO DE APLICACIÓN DO DOCUMENTO

3.1. Ficheiros de datos de carácter persoal.
3.2. Aplicacións informáticas que manexan datos de carácter persoal.
3.3. Centros onde se atopan estes ficheiros.
3.4. Equipos nos que se almacenan ou tratan estes ficheiros.
3.5. Soportes lóxicos nos que residen os ficheiros.

4. NIVEIS DE SEGURIDADE

5. MEDIDAS E NORMAS GARANTES DO NIVEL DE SEGURIDADE ADOPTADAS POLA ORGANIZACIÓN

5.1. Rexistro Municipal de Protección de Datos
5.2. Responsable Municipal de Protección de Datos
5.3. Responsable do ficheiro
5.4. Responsable de seguridade
5.5. Xestión de ficheiros que conteñan datos de carácter persoal
5.6. Xestión de usuarios. Identificación e autenticación.
5.7. Xestión de soportes.
5.8. Distribución de soportes.
5.9. Normas de uso dos equipos informáticos e servicios de comunicacións.
5.10. Acceso restrinxido ós locais.
5.11. Acceso a datos a través de redes de comunicacións.
5.12. Integridade e dispoñibilidade da información.
5.13. Controis periódicos e auditoría de seguridade.
5.14. Cesión de datos e tratamento de datos por conta de terceiros.
5.15. Procedemento de acceso, oposición, rectificación e cancelación.
5.16. Difusión de información sobre as medidas de seguridade e protección de datos.

6. FUNCIÓNS E OBRIGAS DO PERSOAL

6.1. Funcións do persoal.
6.2. Obrigas do persoal.

7. ESTRUCTURA DOS FICHEIROS CON DATOS DE CARÁCTER PERSOAL E DESCRICIÓN DOS SISTEMAS DE INFORMACIÓN

8. PROCEDEMENTO DE NOTIFICACIÓN, XESTIÓN E RESPOSTA ANTE INCIDENCIAS

8.1. Procedemento de notificación e resposta a seguir fronte a incidencias.
8.2. Rexistro de incidencias.

9. PROCEDEMENTO DE COPIA DE RESPALDO E RECUPERACIÓN DE DATOS

9.1.Copia de respaldo.

9.2.Recuperación de datos

10. PROCEDEMENTO DE APROBACIÓN E MODIFICACIÓN DO REGULAMENTO DE SEGURIDADE

11. ANEXOS

ANEXO I:
Modelos de documentación e formularios

I.1. Modelos de solicitude de alta / baixa / modificación de ficheiros.
I.2. Modelos de solicitude de alta / baixa / modificación de usuarios.
I.3. Modelo de inventario de soportes.
I.4. Modelo de rexistro de entrada de soportes.
I.5. Modelo de rexistro de saída de soportes.
I.6. Modelo de rexistro de accesos.
I.7. Modelo de rexistro de incidencias.
I.8. Modelo de solicitude de xeración de soporte informático
I.9. Modelo de autorización xenérica de recuperación de datos
I.10. Modelo de autorización de transporte de información de carácter persoal
I.11. Modelo de autorización de cesión de datos
I.12. Modelo de cláusula para os formularios de solicitude de información de carácter persoal

1. OBXECTO

O presente regulamento ten por obxecto establecer as medidas de índole técnica e organizativas necesarias para garantir a seguridade dos ficheiros, centros de tratamento, locais, equipos, sistemas, programas e persoas que interveñan no tratamento de datos de carácter persoal dependentes do Concello de Santiago de Compostela suxeitos ó réxime da Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal.

Este Regulamento establécese en cumprimento do artigo 8.1 do Real Decreto 994/1999, de 11 de xuño, polo que se aproba o Regulamento de medidas de seguridade dos ficheiros automatizados que conteñan datos de carácter persoal, e constitúe, xunto co Rexistro Municipal de Protección de Datos, o Documento Municipal de Seguridade, que é documento de seguridade ó que se refire o devandito Real Decreto.

O Regulamento ten carácter obrigatorio para todo o persoal con acceso a datos de carácter persoal e ós sistemas de información municipais, e debe ser coñecido e asumido polos responsables dos ficheiros no momento da creación das bases de datos.

2. DEFINICIÓNS

A efectos de este Regulamento, entenderase por:

1. **Accesos autorizados:** Autorizacións concedidas a un usuario para a utilización dos diversos recursos.
2. **Afectado ou interesado:** Persoa física titular dos datos que sexan obxecto do tratamento.
3. **Autenticación:** Procedemento de comprobación da identidade dun usuario.
4. **Bloqueo de datos:** A identificación e reserva dos datos co fin de impedir o seu tratamento.
5. **Comunicación ou cesión de datos:** Toda revelación de datos realizada a unha persoa distinta do interesado.
6. **Consentimento do interesado:** Toda manifestación de vontade, libre, inequívoca, específica e informada, mediante a que o interesado consinta o tratamento de datos persoais que lle concirnen.
7. **Contrasinal:** Información confidencial, frecuentemente constituída por unha cadea de carácteres, que pode ser usada na autenticación dun usuario.
8. **Control de acceso:** Mecanismo que en función da identificación xa autenticada permite acceder a datos ou recursos.
9. **Copia de respaldo:** Copia de datos dun ficheiro nun soporte que posibilite a súa recuperación.

10. **Datos de carácter persoal:** Toda información numérica, alfabética, gráfica, fotográfica, acústica ou de calquera outro tipo, susceptible de recollida, rexistro, tratamento ou transmisión, concernente a persoas físicas identificadas ou identificables.
11. **Declarante:** Persoa física que cumprimenta a solicitude de inscrición e actúa como mediador entre a Axencia e o titular ou responsable do ficheiro.
12. **Encargado do tratamento:** Persoa física ou xurídica, autoridade pública, servicio ou calquera outro organismo que, só ou conxuntamente con outros, trate os datos persoais por conta do responsable do tratamento.
13. **Ficheiro:** Todo conxunto organizado de datos de carácter persoal, calquera que fose a forma ou modalidade da súa creación, almacenamento, organización e acceso.
14. **Fontes accesibles ó público:** Aqueles ficheiros a consulta dos cales pode ser realizada por calquera persoa, non impedida por unha norma limitativa, ou sen máis esixencia que, se fose o caso, o aboamento dunha contraprestación. Teñen a consideración de fontes de acceso publico, exclusivamente, o censo patrimonial, os repertorios telefónicos nos termos previstos pola súa normativa específica e as listas de persoas pertencentes a grupos profesionais que conteñan unicamente os datos de nome, título, profesión, actividade, grado académico, enderezo e indicación da súa pertenza ó grupo. Así mesmo, teñen o carácter de fontes de acceso público, os Diarios e Boletíns oficiais e os medios de comunicación.
15. **Identificación:** Procedemento de recoñecemento da identidade dun usuario.
16. **Identificación do afectado:** Calquera elemento que permita determinar directa ou indirectamente a identidade física, fisiolóxica, psíquica, económica, cultural ou social da persoa afectada.
17. **Incidencia:** Calquera anomalía que afecta ou puidera afectar á seguridade dos datos.
18. **Procedemento de disociación:** Todo tratamento de datos persoais de modo que a información que se obteña non poida asociarse a persoa identificada ou identificable.
19. **Recurso:** Calquera parte compoñente dun sistema de información.
20. **Responsable de ficheiro ou tratamento:** Persoa física ou xurídica, de natureza pública ou privada, ou órgano administrativo, que decida sobre finalidade, contido e uso do tratamento.
21. **Responsable de seguridade:** Persoa ou persoas ás que o responsable do ficheiro asignou formalmente a función de coordinar e controlar as medidas de seguridade aplicables.
22. **Seguridade da información:** Cumprimento das condicións esixibles de confidencialidade, dispoñibilidade e integridade da información.
23. **Sistemas de información:** Conxunto de ficheiros automatizados, programas, soportes e equipos empregados para o almacenamento e tratamento de datos de carácter persoal.
24. **Soporte:** Obxecto físico susceptible de ser tratado nun sistema de información e sobre o cal se poden gravar ou recuperar datos.
25. **Transferencia de datos:** O transporte dos datos entre sistemas informáticos por calquera medio de transmisión, así como o transporte de soportes de datos por correo ou por calquera outro medio convencional.
26. **Tratamento de datos:** Operacións e procedementos técnicos de carácter automatizado ou non, que permitan a recollida, gravación, conservación, elaboración, modificación, bloqueo e cancelación, así como as cesións de datos que resulten de comunicacións, consultas, interconexións e transferencias.
27. **Usuario:** suxeito ou proceso autorizado para acceder a datos ou recursos.

3. ÁMBITO DE APLICACIÓN DO REGULAMENTO

O presente Regulamento é de aplicación a todos os recursos protexidos deste Concello, entendendo como tales todos os sistemas de información empregados para o tratamento e almacenamento de datos de carácter persoal.

Forman parte do alcance deste Regulamento todos os ficheiros que conteñan datos de carácter persoal, automatizados ou non, e independentemente do soporte utilizado (electrónico, papel, vídeo, audio, etc.)

No caso de que as medidas indicadas neste Regulamento non resulten axeitadas por estar orientadas á utilización cun formato ou soporte determinado, estableceranse mecanismos alternativos adaptados ás características concretas do soporte e formato do ficheiro a protexer e que garantan o mesmo nivel de seguridade

O Rexistro Municipal de Protección de Datos conterá unha descrición detallada e actualizada dos recursos protexidos e os sistemas de información que os soportan.

3.1. FICHEIROS QUE CONTEÑEN DATOS DE CARÁCTER PERSOAL.

O Rexistro Municipal de Protección de Datos conterá unha relación detallada dos ficheiros que conteñan datos de carácter persoal utilizados polo Concello, proceda ou non a súa inscrición no Rexistro Xeral de Protección de Datos xestionado pola Axencia Española de Protección de Datos.

De existir algún ficheiro que conteña datos de carácter persoal e non estea incluído nesta relación, aplicaranse igualmente as medidas de seguridade correspondentes segundo o establecido neste Regulamento.

No caso de que existan ficheiros non rexistrados nin declarados á Axencia de Protección de Datos, seguirase o procedemento establecido máis adiante neste Regulamento para a creación de ficheiros, co fin de regularizar canto antes a súa situación.

3.2. APLICACIÓNS INFORMÁTICAS QUE MANEXAN DATOS DE CARÁCTER PERSOAL.

O Rexistro Municipal de Protección de Datos incluirá, para cada ficheiro inscrito, información detallada sobre as aplicacións de xestión principais que os utilizan.

En todo caso, aplicaranse as medidas de seguridade expostas neste Regulamento a todas as aplicacións que fagan uso de datos de carácter persoal.

3.3. CENTROS NOS QUE SE ATOPAN OS FICHEIROS E OS EQUIPOS DESDE OS QUE SE ACCEDE.

O Rexistro Municipal de Protección de Datos incluirá, para cada ficheiro inscrito, o listado de centros nos que se atopan os equipos servidores que os albergan, así como os centros nos que se atopan os postos de traballo desde os que se utilizan.

3.4. EQUIPOS NOS QUE SE ALMACENAN OU TRATAN ESTES FICHEIROS.

O Rexistro Municipal de Protección de Datos incluirá, para cada ficheiro inscrito, información sobre os equipos servidores que os albergan, así como os equipos cliente que se atopan nos postos de traballo desde os que se utilizan.

3.5. SOPORTES LÓXICOS ONDE RESIDEN OS FICHEIROS.

O Rexistro Municipal de Protección de Datos incluirá, para cada ficheiro inscrito, información sobre os soportes lóxicos nos que se atopan e os formatos de almacenamento.

Identificaranse para cada ficheiro as bases de datos almacenadas con axuda dun xestor de base de datos, os servicios de disco en rede ou en disco local, e calquera outro soporte que almacene un conxunto de datos ou sexa utilizado para o seu tratamento.

4. NIVEIS DE SEGURIDADE

Consonte o Real Decreto 994/1999 establécense tres niveis de seguridade baseados principalmente na natureza da información en relación coa esixencia de asegurar a súa confidencialidade e integridade:

a. Todos os ficheiros que conteñan datos de carácter persoal deberán adoptar as medidas de seguridade cualificadas de nivel básico.

b. Os ficheiros que conteñan datos relativos á comisión de infraccións administrativas ou penais, Facenda Pública, servicios financeiros e aqueles ficheiros cun funcionamento que veña rexido polo artigo 29 da Lei Orgánica 15/1999, así como os que conteñan datos que permitan obter unha avaliación da personalidade do individuo, deberán reunir, ademais das medidas de nivel básico, as cualificadas como de nivel medio.

c. Os ficheiros que conteñan datos de ideoloxía, relixión, crenzas, orixe racial, saúde ou vida sexual así como os que conteñan datos obtidos para fins policiais sen consentimento das persoas afectadas deberán reunir, ademais das medidas de nivel básico e medio, as cualificadas como de nivel alto.

Todo o persoal que teña acceso e realice algún tipo de tratamento sobre datos de carácter persoal deberá coñecer e aplicar as medidas de seguridade que o Real Decreto 994/1999 e este Regulamento establecen para cada un dos niveis identificados.

Co fin de facilitar a xestión e incrementar o nivel de seguridade xeral, recoméndase aplicar a todos os ficheiros que conteñan datos de carácter persoal de nivel básico as medidas de seguridade esixidas polo Real Decreto 994/1999 para os datos de nivel medio.

No caso de que un ficheiro conteña datos de carácter persoal considerados de nivel alto, teranse en conta ademais as medidas especificadas para este nivel.

5. MEDIDAS E NORMAS GARANTES DO NIVEL DE SEGURIDADE ADOPTADAS POLA ORGANIZACIÓN.

As medidas e normas establecidas neste Regulamento están orientadas a garantir a seguridade da información, entendendo como tal a garantía de que se cumpren as seguintes condicións:

a) Confidencialidade: Accesibilidade ós datos só por quen conte cos permisos correspondentes, é dicir, estea autorizado.

b) Dispoñibilidade: Recepción a tempo por parte dos que deban ser os destinatarios autorizados, así como posibilidade de acceso por aqueles que estean autorizados cando a necesiten.

c) Integridade: Mantemento de datos exactos, completos, actualizados e fiables.

5.1. REXISTRO MUNICIPAL DE PROTECCIÓN DE DATOS.

Crearase un Rexistro Municipal de Protección de Datos, o cal consistirá nun inventario centralizado con información sobre os ficheiros que conteñen datos de carácter persoal, proceda ou non declaralos á Axencia Española de Protección de Datos.

Neste Rexistro constará, para cada ficheiro inscrito, o responsable do ficheiro, o responsable de seguridade, o nivel de seguridade, e toda a información que o Real Decreto 994/1999, do 11 de xuño, polo que se aproba o Regulamento de medidas de seguridade dos ficheiros automatizados que conteñan datos de carácter persoal establece como de obrigada inclusión no documento de seguridade.

Non se poderán crear ou utilizar ficheiros nin realizar tratamentos de datos de carácter persoal non inscritos no Rexistro Municipal de Protección de Datos.

O creación do rexistro incluirá un proceso de revisión que permita verificar e adaptar, se é o caso, a información existente sobre ficheiros que conteñan datos de carácter persoal á situación real. Utilizarase como punto de partida o inventario de ficheiros inscritos no Rexistro Xeral de Protección de Datos xestionado pola Axencia Española de Protección de Datos.

O Rexistro Municipal de Protección de Datos, por tratarse dunha parte do Documento Municipal de Seguridade, recibirá o mesmo tratamento que este Regulamento no tocante á súa actualización, posibilidade de acceso e publicidade.

A súa xestión corresponde ó Responsable Municipal de Protección de Datos.

5.2. RESPONSABLE MUNICIPAL DE PROTECCIÓN DE DATOS

O Concello nomeará un Responsable Municipal de Protección de Datos que será o encargado de centralizar a xestión da protección de datos de carácter persoal mantendo o Documento Municipal de Seguridade, coordinando as actuacións dos distintos responsables de seguridade e homoxeneizando criterios co fin de optimizar o uso dos recursos na implantación das medidas de seguridade, e actuando

como interlocutor coa Axencia Española de Protección de Datos para o mantemento do seu Rexistro Xeral de Protección de Datos.

5.3. RESPONSABLE DO FICHEIRO

O responsable do ficheiro será o Alcalde ou o Órgano no que delegue.

5.4. RESPONSABLE DE SEGURIDADE.

O responsable do ficheiro, cando este conteña datos de nivel medio, designará formalmente un ou varios responsables de seguridade encargados de coordinar e controlar as medidas de seguridade. En ningún caso a designación pode supoñer unha delegación da responsabilidade que corresponde ó responsable do ficheiro ou tratamento.

De non designarse outro responsable de seguridade no momento de creación do ficheiro, será o Responsable Municipal de Protección de Datos quen asuma esta función, o que constará por escrito na solicitude.

Independentemente do responsable de seguridade designado en cada caso, a creación, supresión e modificación do ficheiro realizarase segundo o procedemento establecido neste Regulamento, co obxectivo de que o Responsable Municipal de Protección de Datos poida manter o Rexistro Municipal de Protección de Datos actualizado.

5.5. XESTIÓN DE FICHEIROS QUE CONTEÑAN DATOS DE CARÁCTER PERSOAL

Procedemento de alta de ficheiro

A creación do ficheiro só poderá facerse mediante disposición xeral publicada no Boletín Oficial do Estado, no Diario Oficial de Galicia, ou no Boletín Oficial da Provincia en cumprimento do artigo 20 da Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal.

A solicitude de alta do ficheiro será enviada ó Responsable Municipal de Protección de Datos, acompañada de:

a. Impreso de notificación á Axencia Española de Protección de Datos cumprimentado, para que o Responsable Municipal de Protección de Datos proceda á súa xestión e, se é o caso envío á Axencia.
b. Proposta de designación de responsable ou responsables de seguridade.

O Responsable Municipal de Protección de Datos, recibida a solicitude, será o responsable de:

1. Realizar o informe previo á correspondente proposta de creación de ficheiro.
2. Unha vez publicada a correspondente disposición xeral no Boletín Oficial, notificar o cambio á Axencia Española de Protección de Datos,
3. Actualizar o Rexistro Municipal de Protección de Datos.
4. Notificar a aceptación ou denegación de creación de ficheiro ó solicitante.

Só se fará efectiva a creación física do ficheiro unha vez recibida a correspondente notificación de aprobación.

A creación de ficheiros temporais, intermedios ou de proba, proceda ou non declaralos á Axencia Española de Protección de Datos, seguirán o mesmo procedemento e quedarán igualmente rexistrados no Rexistro Municipal de Protección de Datos xunto co período de validez previsto.

Para os ficheiros temporais que pasen a ter carácter definitivo seguirase desde o inicio o procedemento de alta previsto para os ficheiros permanentes.

Procedemento de baixa de ficheiro

A supresión do ficheiro só poderá facerse mediante disposición xeral publicada no Boletín Oficial do Estado, no Diario Oficial de Galicia, ou no Boletín Oficial da Provincia, en cumprimento do artigo 20 da Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal.

A solicitude de baixa do ficheiro será enviada ó Responsable Municipal de Protección de Datos, acompañada de:

a. Impreso de notificación á Axencia Española de Protección de Datos cumprimentado, para que o Responsable Municipal de Protección de Datos proceda á súa xestión e envío.

O Responsable Municipal de Protección de Datos, recibida a solicitude, será o responsable de:

1. Realizar o informe previo á correspondente proposta de supresión de ficheiro.
2. Unha vez publicada a correspondente disposición xeral no Boletín Oficial, notificar o cambio á Axencia Española de Protección de Datos.
3. Actualizar o Rexistro Municipal de Protección de Datos.
4. Notificar a aceptación ou denegación de supresión de ficheiro ó solicitante.

Só se fará efectiva a supresión física do ficheiro unha vez recibida a correspondente notificación de aprobación.

Para a supresión do ficheiro seguiranse os pasos seguintes:

- Realización das correspondentes copias de respaldo aplicando as medidas previstas neste Regulamento. Estas copias almacenaranse por un período mínimo de cinco anos
- Supresión física e permanente do ficheiro no entorno de producción.

Procedemento de modificación do ficheiro

A modificación do ficheiro só poderá facerse mediante disposición xeral publicada no Boletín Oficial do Estado, no Diario Oficial de Galicia, ou no Boletín Oficial da Provincia, en cumprimento do artigo 20 da Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal.

A solicitude de modificación do ficheiro será enviada ó Responsable Municipal de Protección de Datos, acompañada de:

a. Impreso de notificación á Axencia Española de Protección de Datos cumprimentado, para que o Responsable Municipal de Protección de Datos proceda á súa xestión e envío.

O Responsable Municipal de Protección de Datos, recibida a solicitude, será o responsable de:

1. Realizar o informe previo á correspondente proposta de modificación de ficheiro.
2. Unha vez publicada a correspondente disposición xeral no Boletín Oficial, notificar o cambio á Axencia Española de Protección de Datos,
3. Actualizar o Rexistro Municipal de Protección de Datos.
4. Notificar a aceptación ou denegación de creación de ficheiro ó solicitante.

Só se fará efectiva a modificación física do ficheiro unha vez recibida a correspondente notificación de aprobación.

5.6. XESTIÓN DE USUARIOS. IDENTIFICACIÓN E AUTENTICACIÓN.

Acceso á rede informática do Concello.

O acceso ós ordenadores da rede do Concello estará restrinxido ós usuarios autorizados. O mecanismo de autenticación basearase na asignación de contrasinais individuais.

Estes contrasinais serán persoais e cada usuario farase responsable de mantelas en secreto así como de todos os accesos que se fagan ó sistema baixo a súa identidade. No impreso de solicitude de alta de novos

usuarios, que o propio interesado deberá asinar co consentimento do xefe da unidade, reflectiranse estas e outras consideracións.

Os devanditos contrasinais actualizaranse periodicamente e terán unha vixencia non superior a doce meses. Será o propio usuario o encargado de actualizala cando, transcorrido o devandito prazo, o sistema llo solicite de xeito automático, negando o acceso ó sistema informático de non levarse a cabo a modificación. Poderase establecer unha vixencia máxima inferior de considerarse necesario e incluso establecer períodos de vixencia diferentes para distintas contas de usuario se as condicións e características o recomendan.

O sistema estará configurado para gardar un historial das derradeiras cinco palabras de acceso de cada usuario, de tal xeito que sexa imposible repetir unha contrasinal introducida anteriormente.

Estableceranse unha serie de requisitos mínimos para os contrasinais no tocante a número e tipo de carácteres e publicaranse recomendacións sobre a selección e mantemento de contrasinais. En calquera caso, formarán parte dos requisitos mínimos os seguintes:

- Terán unha lonxitude mínima de seis carácteres
- Os contrasinais non consistirán en teléfonos, matrículas de coches, nomes de persoas, nomes da organización, productos comerciais ou similares, repetición de carácteres seguidos, palabras do diccionario, conta de usuario e noutros elementos facilmente deducibles. Utilizaranse no seu lugar outros sistemas como frases, iniciais das palabras dunha frase, combinacións de números e letras, combinacións de maiúsculas e minúsculas, inclusión de carácteres de puntuación, e outros métodos similares.
- Os contrasinais utilizados nas contas do sistema de información do Concello non serán utilizados noutros contornos tales como contas de correo particulares, servicios bancarios telemáticos, etc.
- Non se utilizará a opción “Lembrar contrasinal” do sistema operativo e as aplicacións informáticas.

Permitirase a conexión á rede do Concello só durante o horario de traballo previsto en cada caso, para o que se incluirá esta información no formulario de alta dos novos usuarios.

Aplicaranse e faranse públicas aqueloutras medidas de carácter restrictivo que os sistemas operativos e de telecomunicacións permitan.

Os contrasinais, usuarios, directivas e, en xeral, as políticas de seguridade, serán almacenadas e xestionadas polo propio sistema operativo, gardando esta información na base de datos SAM, que non será accesible ós usuarios nin ós administradores. A devandita base de datos residirá en servidores redundantes, garantindo así a posibilidade de acceso seguro ó sistema en calquera momento.

O número de intentos de acceso frustrados permitidos non será superior a cinco, bloqueándose a conta do usuario no caso de superar este número ata que o persoal da unidade de Sistemas da Sección de Informática lle habilite de novo o acceso.

Auditarase de xeito automático tanto o comezo coma o fin da sesión, o acceso a ficheiros e obxectos que conteñan datos de nivel alto, e o uso erróneo dos dereitos de usuarios. As mensaxes xeradas polas auditorías revisaranse periodicamente para comprobar o grado de seguridade do sistema.

As baixas de usuarios comunicaranse obrigatoriamente a través dos formularios definidos a tal fin, co obxectivo de inhabilitar as contas de usuario correspondentes.

Non estarán permitidas as contas de contas de carácter xenérico con posibilidade de acceso a datos de carácter persoal.

As contas de superusuario só poderán ser utilizadas nas consolas dos equipos servidores.

Evitarase en todo o caso o uso das contas de superusuario, para o que o persoal que o necesite terá habilitados este tipo de privilexios na conta persoal.

Implantaranse mecanismos de autenticación máis seguros, como pode ser o uso de tarxetas físicas, sistemas de control biométrico ou sistemas de cifrado asimétrico e certificados dixitais, onde se considere necesario e especialmente cando se realice un tratamento de datos de nivel alto.

Acceso ós ficheiros que conteñan datos de carácter persoal.

A posibilidade de acceso a un recurso determinado por parte dun usuario conectado á rede de datos dependerá das autorizacións particulares dese usuario e dos grupos ós que pertence.

Os dereitos de acceso dos usuarios serán os imprescindibles para poder realizar o seu traballo dun xeito eficiente e seguro.

As aplicacións de xestión que traten con información de carácter persoal contarán cun mecanismo de control de acceso, xeralmente baseado nunha combinación usuario-contrasinal. Este sistema poderá estar integrado ou non co sistema de control de acceso da rede do Concello.

O esquemas de seguridade das aplicacións permitirán a creación de diversos perfiles de usuario ós que se poderán asignar privilexios de distinto tipo (consultas, altas, modificacións, copias, etc.) sobre toda a base de datos ou sobre elementos de información concretos.

As aplicacións que fagan uso do xestor de base de datos corporativo (Oracle) ou de calquera outro xestor departamental para o almacenamento da información, utilizarán no posible o esquema de seguridade do devandito xestor co fin de facilitar a implementación de auditorías de seguridade.

As aplicacións que traten datos de carácter persoal de nivel alto incorporarán a capacidade de rexistro de operacións de tal xeito que sexa posible facer un seguimento dos accesos para lectura ou escritura.

Estas funcionalidades formarán parte das esixencias incluídas nos Pregos de Prescricións Técnicas para a adquisición de novas aplicacións.

A posibilidade acceso directo ós ficheiros, sen o uso das aplicacións de xestión, estará limitada polos mecanismos de protección de ficheiros e directorios dos sistemas operativos, mediante o establecemento dos correspondentes permisos de lectura, escritura e execución para usuarios finais, grupos de usuarios ou listas de acceso.

Isto será así aínda cando o acceso habitual a esta información se realice a través de aplicacións que conten con mecanismos propios de control de acceso.

O acceso directo ós datos mediante o uso de utilidades do xestor de bases de datos, sen o encapsulamento do control das aplicacións, estará reservado ós administradores das bases de datos, sempre persoal da Sección de Informática.

Os postos de traballo con sistema operativo Windows 9x serán substituídos paulatinamente por equipos con Windows 2000 Professional ou superior co fin de limitar o acceso ós discos locais, impedir a instalación de aplicacións e reducir as posibilidade de acceso ó contorno informático.

Poderase polo tanto chegar a establecer ata tres puntos de control de acceso ós datos:

1. control de acceso a nivel da aplicación de xestión mediante a que se tratan os datos
2. control de acceso a nivel de xestor de base de datos no que se almacena a información
3. control de acceso a nivel de sistema de ficheiros e servicios de disco da rede de datos, mediante a control de inicio de sesión do sistema operativo.

Estes puntos de control poderán estar integrados de tal xeito que a combinación usuario-contrasinal sexa a mesma nos tres casos, sempre que isto non ocasione problemas de seguridade. Isto non impedirá que a combinación usuario-contrasinal se solicite cantas veces sexa necesario segundo o tipo de acceso que se pretenda realizar en cada momento durante a sesión de traballo.

O sistema informático municipal evolucionará cara unha única base de datos corporativa que permita centralizar a información e facilitar a xestión da seguridade dos datos de carácter persoal no tocante a restriccións de acceso, accesibilidade e integridade.

Acceso a través das redes de telecomunicacións.

No posible utilizaranse medios de comunicación propios, especialmente fibra óptica, para a conexión entre os distintos edificios do Concello, o que facilitará a xestión da seguridade posto que a tecnoloxía utilizada será a mesma independentemente de que os postos de traballo se atopen nos edificios principais ou en edificios remotos.

No caso de recorrer á contratación de servicios de transmisión de datos a través dun provedor, requiriráselle a este o compromiso por escrito do cumprimento das medidas de seguridade establecidas pola lexislación en materia de protección de datos, así como un informe detallado das medidas de seguridade aplicadas.

Para os casos de transmisión de datos de nivel alto de seguridade a través de redes externas, habilitarase un sistema de cifrado.

Asignación de permisos de acceso.

O xefe de cada unidade do Concello será o responsable de determinar os permisos de acceso para cada servicio de rede que se lle teña asignado, sen prexuízo de que cada responsable de ficheiro estableza os mecanismos e privilexios de acceso dos ficheiros que conteñan datos de carácter persoal que conteña.

As modificacións sobre os permisos de acceso ós datos ou recursos protexidos poden ser realizadas unicamente polos membros da Unidade de sistemas da Sección de Informática, previa autorización por escrito do responsable do ficheiro.

En situacións especiais que así o requiran, outros membros da Sección de Informática poderán levar a cabo esta tarefa no seu lugar, circunstancia que quedará convenientemente documentada.

Rexistro de accesos.

Para os datos de nivel alto de seguridade, habilítase un rexistro de accesos que gardará a seguinte información para cada acceso:

- Identificación do usuario que intenta acceder.
- Data e hora do acceso.
- Ficheiro ó que se accede.
- Tipo de acceso.
- Acceso autorizado ou denegado.
- Información accedida no caso de acceso autorizado.

Os mecanismos que permiten o funcionamento deste rexistro terán que estar sempre activos e baixo control directo do responsable de seguridade.

O contido deste rexistro conservarase por un tempo mínimo de dous anos. O responsable de seguridade elaborará un informe mensual das revisións efectuadas periodicamente e dos problemas detectados.

A este rexistro poderán acceder os usuarios autorizados a través da aplicación correspondente publicada na Intranet do Concello.

Método de obtención dos usuarios do sistema.

O Responsable Municipal de Protección de Datos terá acceso en todo momento a unha relación actualizada de usuarios, que permitirá coñecer a información que se indica de seguido:

- Nome do usuario (nome completo e identificador)
- Posto de traballo

- Servicio ó que está adscrito
- Relación de recursos (ficheiros, programas) ós que ten acceso e tipo de permisos cos que conta (alta, baixa, consulta, modificación).

A través das utilidades de administración dos equipos servidores, do xestor de bases de datos, de aplicacións deseñadas con este fin, ou das propias aplicacións de xestión que fagan uso dos datos de carácter persoal, poderase obter en calquera momento listados de usuarios e os seus correspondentes privilexios de acceso.

5.7. XESTIÓN DE SOPORTES.

Os datos de carácter persoal só se poderán almacenar en soportes externos ó equipo informático onde residen para facer copias de seguridade periódicas ou puntuais ou para transferir a información a outras entidades.

Os ficheiros temporais que conteñan datos de carácter persoal serán eliminados inmediatamente despois de cumprir a súa función, para o que se seguirá o procedemento previsto neste Regulamento.

Non se utilizarán datos reais para realizar probas de aplicacións sen as medidas de seguridade correspondente segundo o tipo de datos persoais obxecto de tratamento.

A execución de tratamento de datos de carácter persoal fóra dos locais de ubicación do ficheiro deberá ser autorizada expresamente polo responsable do ficheiro e, de ser o caso, deberá garantir o nivel de seguridade correspondente ó tipo de ficheiro tratado.

Identificación de soportes

Os soportes que inclúan datos de carácter persoal estarán etiquetados externamente de xeito recoñecible. A etiqueta interna (etiqueta lóxica do volume) dependerá da aplicación concreta utilizada para facer a copia.

Os soportes destinados a copias de seguridade periódicas dos sistemas informáticos, tanto completas como incrementais, identificarán:

- Equipo do que se fai copia
- Tipo de copia que se realiza
- Período de copia que contén
- Etiqueta interna que proporciona a utilidade de copia, no caso de dispor dela.
- Clave do inventario de soportes

Os soportes destinados a copias puntuais dun conxunto de ficheiros, realizadas como consecuencia de tarefas de mantemento das aplicacións ou dos datos, identificarán externamente:

- Equipo do que se fai copia
- Identificación do conxunto de ficheiros (directorio que se copia, patrón de busca dos nomes de ficheiro, etc.)
- Data da copia
- Clave do inventario de soportes

Os soportes destinados ó intercambio de datos con outras entidades identificarán:

- Entidade orixe (Concello de Santiago de Compostela)
- Entidade destino
- Descrición do contido
- Formato do contido
- Instruccións para cargar a información(comando de recuperación)
- Data de creación do soporte
- Clave do rexistro de saída de soportes

Inventario de soportes.

Cada soporte que conteña información de tipo persoal estará inventariado dentro do rexistro de soportes informáticos do Concello. Os campos do rexistro de inventario son os seguintes:

- Clave do soporte no inventario
- Etiqueta lóxica (se ten)
- Descrición
- Equipo do que se fai copia
- Tipo de copia (backup periódico, copia de seguridade puntual, traspaso de datos)
- Tipo de soporte(Streamer, 8mm, 4mm, disquete, CD, papel, etc.)
- Data da copia
- Período de vixencia (data de caducidade)

Este inventario actualizarase cada vez que se cree unha nova copia cos datos de carácter persoal. Farase unha revisión periódica das cintas que teñan que ser dadas de baixa do inventario e borradas fisicamente.

A este inventario poderán acceder os usuarios autorizados a través da aplicación correspondente publicada na Intranet do Concello.

Almacenamento de soportes.

Todos os soportes que conteñan unha copia de seguridade total ou parcial dos datos de carácter persoal almacenados nos servidores estarán almacenados nas seguintes localizacións:

- Nos locais de Informática, no Pazo de Raxoi (Praza do Obradoiro s/n).
- Nos locais de Informática, no edificio de Área Económica (Galeras, 5).

Quedarán excluídos os soportes que permanecen continuamente nas unidades de copia, necesarios para a realización automática das copias de seguridade. Estes soportes atoparanse protexidos fisicamente coas mesmas garantías que os propios datos contidos nos discos duros dos sistemas.

Todo soporte que teña que ser reparado deberá manterse “in-situ”, tendo que ser así establecido no contrato de mantemento dos soportes.

Soamente terá acceso a este lugar o persoal da Sección de Informática. O Responsable Municipal de Protección de Datos poderá permitir o acceso ó lugar a outro persoal lexitimamente autorizado, deixando constancia deste feito.

Os soportes dos departamentos encargados da xestión que conteñan datos de carácter persoal permanecerán, cando non sexan utilizados, en lugar seguro con acceso restrinxido e acondicionado para elo segundo as medidas establecidas neste Regulamento.

Reutilización e eliminación de soportes.

Unha vez transcorrido o tempo de vixencia dun soporte informático este será destruído ou borrado completamente para permitir a súa reutilización, utilizando o comando adecuado ó sistema de ficheiros e sistema operativo do que se trate.

Estarán dispoñibles para os usuarios aplicacións que permitan o borrado físico dos datos dun soporte informático sen posibilidade de recuperación.

5.8. DISTRIBUCIÓN DE SOPORTES.

A saída de soportes que conteñan datos de carácter persoal terá que ser autorizada por escrito polo responsable do ficheiro.

No caso de conter datos de nivel alto, estes serán cifrados para a súa distribución ou para a transmisión por medio de redes de transmisión de datos externas ó Concello.

O sistema de cifrado utilizado será o aportado polas aplicacións de xestión adquiridas a terceiros ou polas aplicacións ofimáticas mediante o uso de identificadores dixitais. Adicionalmente, estarán a disposición do persoal do Concello aplicacións de cifrado como PGP (Pretty Good Privacy).

Rexistro de saída de soportes informáticos.

As saídas do Concello de soportes informáticos que conteñan datos de carácter persoal reflectiranse nun rexistro de saída instrumentado para tal fin.

A información contida nese rexistro será a seguinte:

- Identificación do soporte (clave única do inventario)
- Tipo de soporte (diskette, CD, cinta, transmisión por rede, cartucho, etc.)
- Número de soportes (volumes)
- Date e hora do envío
- Destinatario
- Información que contén
- Forma de envío
- Responsable autorizado da entrega

A este rexistro poderán acceder os usuarios autorizados a través da aplicación correspondente publicada na Intranet do Concello.

Rexistro de entrada de soportes informáticos.

Reflectirase nun rexistro de entrada instrumentado para tal fin a entrada no Concello de soportes que conteñan datos de carácter persoal.

A información contida nese rexistro será a seguinte:

- Identificación do soporte (se ten)
- Tipo de soporte (diskette, CD, cinta, transmisión por rede, cartucho, etc.)
- Número de soportes (volumes)
- Date e hora da recepción
- Emisor
- Información que contén
- Forma de envío
- Responsable autorizado da recepción

A este rexistro poderán acceder os usuarios autorizados a través da aplicación correspondente publicada na Intranet do Concello.

5.9. NORMAS DE USO DOS EQUIPOS INFORMÁTICOS E SERVICIOS DE COMUNICACIÓNS.

Configuración e mantemento dos equipos informáticos

1. Existirá un inventario exhaustivo e actualizado de equipos informáticos e de telecomunicacións propiedade do Concello que permita coñecer en calquera momento o seu estado, uso, localización e configuración.

2. A conexión ó sistema informático do Concello de equipos non inventariados ou alleos só poderá ser realizada de xeito temporal, previa solicitude xustificada, e unha vez verificado o cumprimento das características de seguridade esixibles, adaptando, se é o caso, a súa configuración.

3. Non se levará a cabo a adquisición de ningún material informático sen o informe previo do Responsable Municipal de Protección de Datos ou de quen este determine. En todo caso, non pasará a formar parte do sistema informático do Concello a efectos de explotación e mantemento ningún equipo que non cumpra coas características mínimas para asegurar un funcionamento óptimo e seguro.

4. Establecerase unha configuración básica e estándar para os equipos informáticos do Concello, deseñada para optimizar o mantemento e control da seguridade dos equipos. A utilización dunha configuración alternativa deberá ser convenientemente xustificada e aprobada.

5. Os cambios na configuración dos equipos informáticos serán realizados única e exclusivamente polo persoal do departamento de Informática.

6. Establecerase unha relación de aplicacións informáticas admitidas. A utilización de aplicacións alternativas deberá ser convenientemente xustificada e aprobada.

7. Calquera instalación de aplicacións informáticas, a cal deberá estar convenientemente xustificada, será realizada polo persoal de Informática ou, en todo caso, baixo o seu control.

8. Establecerase unha relación de formatos de ficheiro e tipos de soporte admitidos para intercambio de información interna e externa. O envío ou recepción de ficheiros nun formato diferente deberá ser convenientemente xustificada e aprobada.

O correo electrónico e outros sistemas de intercambio de información

1. Establecerase e difundirase unha normativa específica de utilización que incluirá, entre outras, as normas que se indican neste apartado.

2. Os sistemas de intercambio de información serán utilizados única e exclusivamente como ferramenta de traballo.

3. A posibilidade de uso de unidades de lectura ou gravación de soportes de almacenamento ou de envío de ficheiros adxuntos mediante correo electrónico restrinxirase o máximo posible. O inventario de equipos informáticos permitirá coñecer en todo momento qué postos de traballo teñen activada esta función.

4. Non se utilizará o correo electrónico nin calquera outro servicio de intercambio para o envío ou recepción de mensaxes que acheguen ficheiros ou programas que poidan supoñer un risco para o sistema informático, sobre todo cando a procedencia sexa descoñecida.

5. No caso de recibir correos electrónicos con ficheiros adxuntos, só se descargarán ou executarán cando se coñeza a súa procedencia e se teña a seguridade de que non supoñen un risco para o sistema.

6. O envío de correos electrónicos a múltiples destinatarios utilizando os campos "PARA:" ou "CC" supón unha infracción da Lei 15/1999, de 13 de decembro, de Protección de datos de carácter persoal, ó facer públicos enderezos electrónicos entre os devanditos destinatarios, polo que se utilizará no seu lugar o campo "CCO".

7. Non se descargarán ficheiros desde sitios web, servidores FTP e outros servicios que poidan non resultar seguros.

8. Sempre que sexa posible, utilizaranse aplicacións de verificación baseadas en sistemas de sinatura electrónica para a descarga de programas.

5.10. ACCESO RESTRINXIDO ÓS LOCAIS.

Os servidores informáticos onde residen os ficheiros con datos de carácter persoal atoparanse en locais dedicados de xeito exclusivo e acondicionados para este uso.

O acceso estará restrinxido a persoal da Sección de Informática. Existirá un procedemento para facilitar o acceso en caso de emerxencia a persoal autorizado: Servicio de Extinción de Incendios, Policía Local, etc.

Os soportes físicos de copia de seguridade dos datos que se atopan nestes servidores almacenaranse en armarios ignífugos e con cerre de seguridade. Só terá acceso á chave o persoal da Sección de Informática.

As copias repartiranse entre os locais de Informática dos dous edificios principais (Pazo de Raxoi e Galeras-5) co fin de evitar a perda total no caso de desastre.

As salas de ordenadores contarán con portas de seguridade con acceso restrinxido e estarán controladas por un sistema que permita a identificación da persoa. Instalaranse medidas adicionais de protección como blindaxes, vixiantes, cámaras, e sistemas de limitación de acceso físico fóra de horarios salvo casos de emerxencia.

O equipamento de seguridade será revisado de xeito regular de acordo coas instruccións do fabricante.

5.11. ACCESO A DATOS A TRAVÉS DAS REDES DE TELECOMUNICACIÓNS.

As redes de comunicación deberán garantir un nivel de seguridade equivalente ós accesos locais, impedindo ós usuarios remotos comprometer a seguridade das mesmas.

O provedor de servicios de rede deberá proporcionar ós responsables dos ficheiros un informe en detalle da seguridade dos servicios contratados, así como un compromiso explícito de cumprimento das esixencias de seguridade establecidas pola lexislación vixente.

5.12. INTEGRIDADE E DISPOÑIBILIDADE DA INFORMACIÓN.

Estableceranse os mecanismos que permitan garantir a continuidade do servicio e a posibilidade de recuperación no caso de caída o antes posible e, en todo caso, que a interrupción do servicio ó cidadán non resulte significativa.

Equipamento do centro de proceso de datos

Co fin de facilitar a xestión dos sistemas e o mantemento de medidas de seguridade, e poder garantir a integridade e dispoñibilidade da información, tenderase no posible a crear un núcleo central de servidores accedidos mediante unha rede corporativa que abarque todas as sés do Concello.

En particular, e como mínimo, tomaranse as seguintes medidas:

a) Equipos servidores:

- Disporase de equipos servidores redundantes, a se posible formando estructuras en cluster, para cada un dos tipos de servicio: servicio de disco, de aplicacións, de base de datos, de controladores de dominio, de correo electrónico, de DNS, de DHCP, etc.
- Estes servidores contarán no posible con compoñentes redundantes (fontes de alimentación, tarxetas de rede, etc.)
- Os servidores contarán con sistemas de disco que ofrezan garantías de recuperación fronte a fallos. Polo xeral, seguirase este esquema ou ben outro equivalente:
    - Discos en espello para o almacenamento do sistema operativo, aplicacións e configuración, mantendo nun disco aparte unha última configuración válida para substitución en caso de imposibilidade de iniciar o equipo.
    - Discos en RAID 5 ou similar para o almacenamento de datos.
- Cada servidor contará cun sistema de almacenamento para a realización de copias de seguridade segundo o especificado no apartado correspondente deste Regulamento, podendo utilizar mecanismos que permitan a compartición dun mesmo dispositivo entre varios equipos.
- Buscarase no posible a homoxeneidade nas configuracións e sistemas operativos dos equipos servidores co fin de facilitar a integración e mantemento.
- Os servidores definidos como de apoio en caso de continxencia ou destinados á realización de probas non poderán ser utilizados como equipos de producción para a prestación de ningún servicio.

b) Sistema de telecomunicacións:

- O armario principal de telecomunicacións contará con activos de rede redundantes e un conxunto suficiente de conversores e adaptadores que permitan garantir un funcionamento continuo en caso de fallo.
- Para os armarios secundarios contarase con un ou dous activos de rede que permitan a substitución dalgún equipo en producción que presente fallos.
- Estableceranse VLANS e outros mecanismos que permitan manter a independencia das distintas redes que compartan os recursos de telecomunicacións do Concello (rede administrativa, rede de telefonía, redes de empresas municipais, redes de aulas de informática, rede de bibliotecas, etc.)
- Contarase cun sistema centralizado de xestión dos equipos activos de rede.

c) Subministro eléctrico:

- Implantaranse sistemas que garantan un subministro eléctrico continuado e estable a través da instalación de sistemas de alimentación ininterrompida para os equipos servidores e os armarios de comunicacións.
- A ser posible, estenderase o uso de subministro eléctrico a través de sistemas de alimentación ininterrompida ós ordenadores persoais dos postos de traballo e, en todo caso, tomaranse medidas para que este subministro sexa estable.
- Contarase con liñas de subministro alternativas co fin de que impresoras, fotocopiadoras, electrodomésticos e outros equipos non utilicen os mesmos sistemas de alimentación ininterrompida.

d) Condicións dos locais:

- Os locais destinados ó aloxamento dos servidores e armarios de comunicación reunirán as condicións de temperatura e humidade axeitadas para este tipo de equipamento, instalando sistemas correctores en caso de ser necesario.
- Disporán de detectores de calor e fume e sistemas de extinción de incendios.
- Contarán con suficiente espacio libre para que se poida realizar unha limpeza diaria completa co fin de reducir no posible a cantidade de po existente.
- Terán exclusivamente esta finalidade e albergarán o material mínimo imprescindible. En particular, estarán libres de papel e outros materiais que poidan dar lugar a incendios e outro tipo de desastres.

e) Mantemento

- Contarase cun mantemento para os equipos servidores e para a Rede de Datos Corporativa.

Plan de continxencia

Elaborarase un Plan de Continxencia para casos de desastres, no que se contemplará desde a habilitación de novos locais ata a recuperación de datos e a posta en marcha de equipos informáticos e de telecomunicacións alternativos co fin de restablecer o funcionamento normal a partir dos datos e aplicacións salvagardados.

Realizaranse probas e simulacións totais ou parciais que permitan garantir o correcto funcionamento do Plan de Continxencia.

5.13. CONTROIS PERIÓDICOS E AUDITORÍAS DE SEGURIDADE

Controis periódicos

Este Regulamento será revisado mensualmente incorporando as posibles modificacións da lexislación en materia de protección de datos, as modificacións no sistema de seguridade do Concello, e a actualización do inventario de ficheiros a través do Rexistro Municipal de Protección de Datos.

Auditaranse os rexistros de accesos, incidencias, soportes, entrada e saída de soportes, permisos de usuarios e os rexistros de operación dos sistemas buscando intentos de acceso indebidos.

O responsable de seguridade elaborará un informe mensual do rexistro de accesos.

Auditorías de seguridade

Cada dous anos realizarase unha auditoría interna ou externa máis detallada do cumprimento do disposto neste Regulamento e no aprobado mediante o Real Decreto 994/1999. O devandito informe, así como as medidas correctoras quedarán a disposición do responsable do ficheiro e da Axencia Española de Protección de datos.

Son obxectivos dos controis periódicos e das auditorías:

- Determinar as deficiencias e debilidades dos controis de seguridade existentes ou en fase de implantación.

- Suxerir as medidas correctivas e preventivas que permitan eliminar as devanditas deficiencias.

Estas revisións incluirán, como mínimo:

- Estudio da completitude e exactitude do Rexistro Municipal de Protección de Datos: se existen ficheiros que non foron incorporados, se o nivel de seguridade do ficheiro é o que se especifica no documento, se foron declarados á Axencia Española de Protección de datos, etc.
- Publicidade e difusión do Regulamento Municipal de Seguridade e dos demais documentos de seguridade entre o persoal con dereitos de acceso a datos de carácter persoal.
- Análise dos procedementos a través dun plan de probas.
- Análise do contido do rexistro de auditoría, cando se trate de ficheiros que conteñan datos de nivel alto, e verificación de que non foi desactivado ou que constan no rexistro de incidencia as desactivacións correspondentes.
- Revisión dos informes elaborados polo Responsable de Seguridade

5.14. CESIÓN DE DATOS E TRATAMENTO DE DATOS POR CONTA DE TERCEIROS.

Consonte ós artigos 11 e 12 da Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal, distínguese entre cesión de datos e acceso a datos por conta de terceiros.

Cesión de datos

Segundo os artigos 21 e 11 da Lei Orgánica 15/1999, do 13 de decembro, de Protección de Datos de Carácter Persoal e a sentencia do Tribunal Constitucional 292/2000 de 30 de novembro, os datos de carácter persoal recollidos ou elaborados por unha Administración Pública no desempeño das súas atribucións, soamente poderán ser comunicados a outras Administracións Públicas para o exercicio das mesmas competencias ou de competencias que versen sobre as mesmas materias, ou cando a comunicación se realice con fins históricos, estatísticos ou científicos. Do mesmo xeito, poderanse comunicar os datos que unha Administración obteña ou elabore con destino a outra.

Só se poderá efectuar a comunicación de datos accesibles ó público a ficheiros de titularidade privada co consentimento do interesado ou cando unha Lei o teña previsto.

Os datos de carácter persoal obxecto do tratamento poderán ser comunicados a un terceiro para o cumprimento de fins directamente relacionados coas funcións lexítimas do cedente e do cesionario, con consentimento previo do interesado ou cando a cesión estea autorizada por unha Lei.

Toda cesión ou comunicación de datos realizarase previa solicitude ó responsable do tratamento, utilizando o documento tipo incluído no Anexo I.11 do presente documento.

Tratamento de datos por conta de terceiros

Ós efectos do establecido no artigo 12 da Lei 15/1999 a Xunta de Goberno Local aprobou o Protocolo Municipal de Seguridade para a Protección de Datos de Carácter Persoal.

Toda prestación dun servicio ó Concello de Santiago de Compostela estará suxeita ó devandito Protocolo, para o que se incluirá a correspondente mención no contrato que a regula.

Aínda que en principio só sería necesaria a súa aplicación nos contratos que para a súa execución requiran o tratamento de datos de carácter persoal, recoméndase a súa utilización incluso cando inicialmente esto non sexa así, posto que o propio Protocolo inclúe o procedemento de creación de ficheiros no caso de chegar a ser necesario.

Convenios de colaboración

Os convenios de colaboración estarán suxeitos ó cumprimento da lexislación en materia de Protección de Datos de Carácter Persoal.

Incluirán unha memoria sobre seguridade e protección de datos de carácter persoal. Esta memoria pasará a formar parte este Regulamento no momento da sinatura, e servirá así mesmo para a actualización do inventario municipal de ficheiros e usuarios, así como para a declaración de ficheiros á Axencia de Protección de Datos de ser necesario.

Esta memoria incluirá información detallada sobre:

- Datos de carácter persoal obxecto de tratamento e nivel de seguridade correspondente.
- Ficheiros con datos de carácter persoal necesarios, indicando qué parte asinante será a responsable do ficheiro en cada caso.
- Especificación detallada do funcionamento da aplicación ou aplicacións informáticas e dos tratamentos previstos, indicando en cada caso qué parte asinante será a encargada.
- Información detallada sobre as medidas de seguridade previstas nas aplicacións informáticas subministradas, así como o compromiso explícito da súa conformidade coa lexislación nesta materia.
- Toda a información que deba ser incluída neste Regulamento, atendendo ó definido na lexislación vixente como contido mínimo do documento de seguridade.

Cada unha das partes asinantes ofrecerá a información necesaria en cada caso, ou ben na propia memoria ou ben posteriormente pero en todo caso antes do inicio do tratamento, para que poidan ser actualizados os correspondentes documentos de seguridade e inventarios de ficheiros e usuarios, así como declarados os devanditos ficheiros á Axencia de Protección de Datos.

Con respecto ó intercambio de información entre as partes e ás medidas de seguridade esixibles, todo convenio estará suxeito a este Regulamento e ó establecido no Protocolo Municipal de Seguridade para a Protección de Datos de Carácter Persoal.

5.15. PROCEDEMENTO DE ACCESO, OPOSICIÓN, RECTIFICACIÓN E CANCELACIÓN.

Os procedementos para exercitar os dereitos de oposición, acceso, así como os de rectificación e cancelación ós ficheiros de datos de carácter persoal, mentres non se dicte o Regulamento que desenvolva a Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal, rexeranse polo establecido na Instrucción 1/1998, de 19 de xaneiro, da Axencia Española de Protección de Datos, relativo ó exercicio de acceso, rectificación e cancelación.

Os formularios de solicitude de información deseñados para recoller datos de carácter persoal deberán incluír un texto que informe ó interesado da utilización prevista e dos dereitos que pode exercitar ó respecto. O Anexo I, no seu apartado 12 inclúe unha cláusula tipo que pode ser utilizada coas correspondentes adaptacións en cada ocasión.

En calquera caso, deberá constar:

- Información expresa e inequívoca da existencia dun ficheiro ou tratamento de datos de carácter persoal.
- Información do carácter obrigatorio ou facultativo da súa resposta a cada pregunta do formulario e as consecuencias de obtención dos datos ou da negativa a subministralos. É

unha práctica aconsellable marcar cun indicador os campos que deben ser cubertos de xeito obrigatorio.
- Posibilidade de exercitar os dereitos de acceso, rectificación, cancelación e oposición.
- Identidade e enderezo do responsable do ficheiro ou, se é o caso, do seu representante.

5.16. DIFUSIÓN DE INFORMACIÓN SOBRE AS MEDIDAS DE SEGURIDADE E PROTECCIÓN DE DATOS.

Publicación de información sobre protección de datos de carácter persoal

Porase a disposición do persoal, a través da Intranet do Concello e dos medios que se considere oportunos, a información que se detalla de seguido:

1. Lexislación en materia de protección de datos:
   - Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal.
   - Real Decreto 1332/1994, de 20 de xuño, polo que se desenvolven algúns preceptos da Lei Orgánica.
   - Real Decreto 994/1999, de 11 de xuño, polo que se aproba o Regulamento de medidas de seguridade dos ficheiros automatizados que conteñan datos de carácter persoal.
   - Directiva 95/46/CE do Parlamento Europeo e do Consello de 24 de outubro de 1995 relativa á protección de datos das persoas físicas no que respecta ó tratamento de datos persoais e á libre circulación destes datos.

2. O Documento Municipal de Seguridade, composto por: Este Regulamento e o Rexistro Municipal de Protección de Datos

3. O Protocolo Municipal de Seguridade para a Protección de Datos de Carácter Persoal.

4. Un resumo da información máis relevante, un documento específico no que se reflictan as obrigas do persoal incluídas neste Regulamento, e unha páxina de Preguntas Máis Frecuentes

5. Impresos e formularios normalizados de solicitude e autorización e outros recursos necesarios para a implantación das medidas previstas neste Regulamento.

6. Información sobre os inventarios, rexistros de entrada/saída e de anotacións de incidencias mencionados neste Regulamento.

7. Utilidades de cifrado, de borrado físico de información nun soporte informático, de etiquetado, etc.

A través de medios como o correo electrónico e a propia Intranet do Concello, informarase de calquera novidade en materia de seguridade.

Plan de formación

Establecerase un Plan de Formación sobre protección de datos de carácter persoal no que se desenvolverán actividades formativas tendo en conta a existencia de distintos perfiles ou roles involucrados.

Procesos selectivos

Os procesos selectivos para a provisión de prazas incluirán nos seus temarios a normativa existente en materia de protección de datos de carácter persoal, e en especial o Protocolo Municipal de Protección de Datos deste Concello e este Regulamento.

6. FUNCIÓNS E OBRIGAS DO PERSOAL

6.1. FUNCIÓNS DO PERSOAL.

En relación cos ficheiros de datos de carácter persoal, as funcións do persoal deste Concello son as seguintes:

Responsable do ficheiro

O responsable do ficheiro, segundo establece o R.D. 994/1999, terá asignadas as seguintes responsabilidades:

a) Autorizar a creación, supresión ou modificación do ficheiro.
b) Autorizar o documento de seguridade aplicable ó ficheiro e verificar a súa adaptación á normativa vixente.
c) Adoptar as medidas necesarias para que o persoal coñeza as normas en materia de seguridade e as consecuencias do seu incumprimento.
d) Manter unha relación de usuarios do sistema cos seus dereitos de acceso.
e) Establecer os criterios para a definición dos dereitos de acceso dos usuarios.
f) Establecer mecanismos para evitar que os usuarios accedan a recursos con dereitos distintos aos autorizados.
g) Autorizar expresamente o tratamento fóra dos locais de ubicación.
h) Autorizar a saída de soportes fóra dos locais.
i) Verificar a definición e ampliación dos procedementos de copia e recuperación.
j) Designar o responsable de seguridade, no seu caso.
k) Adoptar medidas correctoras de deficiencias detectadas en auditorías.
l) Implantar un mecanismo de identificación de usuarios e verificación de que está autorizado.
m) Autorizar por escrito a execución dos procesos de recuperación de datos.

Responsables de seguridade.

Atendendo a criterios de optimización de recursos e facilidade de xestión, será posible delegar certas tarefas nun ou varios responsables de seguridade, o que deberá constar por escrito durante o proceso de creación do ficheiro.

Ademais da coordinación e control das medidas de seguridade, e segundo o establecido no R.D. 994/1999, os responsables de seguridade terán asignadas as seguintes funcións:

a) Xestionar o rexistro de incidencias.
b) Analizar os informes de auditoría bianual, elevando conclusións ó responsable do ficheiro.
c) Realizar un control directo do rexistro de accesos e elaborar un informe mensual.

Responsable Municipal de Protección de Datos

O Responsable Municipal de Protección de Datos terá asignada as seguintes funcións:

a) Xestionar o Documento Municipal de Seguridade, o que inclúe o mantemento do Rexistro Municipal de Protección de Datos e a anexión dos documentos de seguridade creados polos responsables de ficheiro, os prestadores de servicio, etc., segundo o procedemento que se estableza.
b) Xestionar a declaración de ficheiros á Axencia Española de Protección de Datos.
c) Informar as solicitudes de creación, supresión e modificación de ficheiros.
d) Asesorar en materia de protección de datos de carácter persoal e medidas de seguridade.
e) Coordinar os distintos responsables de seguridade, especialmente no caso de actuacións ou establecemento de medidas que excedan o ámbito para o que foron designados como tales.
f) Unificar criterios sobre as medidas de seguridade que deben ser aplicadas e os medios para levalas a cabo tendo en conta aspectos como a facilidade de xestión e a optimización de recursos.
g) Actuar como interlocutor co departamento de Informática para a implantación das medidas de seguridade, cando se trate de ficheiros que utilicen as tecnoloxías de información, e cos departamentos correspondentes no caso contrario.
h) Impulsar o desenvolvemento dun Modelo para a Xestión da Seguridade de Información.
i) As que corresponden ó responsable de seguridade dos ficheiros para os que se lle teña asignada esta función.

Persoal do departamento de Informática.

O departamento de Informática será o encargado de implantar as medidas de seguridade e dar apoio técnico ó Responsable de Protección de Datos.

O persoal do departamento terá asignadas as tarefas de xestión dos ficheiros de datos que non requiran coñecemento do seu contido:

a) Administración dos sistemas informáticos e desenvolvemento de aplicacións de forma que permitan o acceso e mantemento dos datos coas garantías de seguridade esixidas polo Regulamento.
b) Administración das bases de datos.
c) Xestión dos usuarios e os contrasinais correspondentes.
d) Realización das copias de seguridade segundo o plano establecido.
e) Realización de calquera copia de datos non permitida polas aplicacións de xestión ó resto dos usuarios.
f) Eliminación dos soportes obsoletos.
g) Mantemento de rexistros de soportes, entrada/saída de soportes e incidencias.
h) Implantación de mecanismos que aseguren a unicidade, redundancia mínima, coherencia, integridade e seguridade dos datos comúns centralizados compartidos por diferentes dependencias do Concello, para facilitar deste xeito a aplicación de medidas de seguridade.

Unidades responsables da xestión.

Cada unidade será responsable do contido dos ficheiros de datos de carácter persoal que está encargada de xestionar para o desenvolvemento normal das súas funcións.

Sempre que sexa tecnicamente posible, serán as unidades responsables da xestión as encargadas da extracción de información para a redacción de informes, estatísticas, listados, etc. ou para a comunicación de datos a outros departamentos ou a terceiros, utilizando con este fin as aplicacións de xestión correspondentes.

6.2. OBRIGAS DO PERSOAL

É obrigatorio para todo o persoal o cumprimento deste Regulamento no tratamento de datos de carácter persoal e, en especial:

- Respectar o dereito de información na recollida de datos dos afectados polos ficheiros de datos de carácter persoal.
- Respectar en todo momento os dereitos de acceso, rectificación e cancelación dos afectados polos ficheiros de datos de carácter persoal.
- Non crear, suprimir ou modificar ou tratar ficheiros con datos de carácter persoal sen a correspondente autorización.
- Non realizar ou manter copias non autorizadas de datos de carácter persoal.
- Gardar segredo sobre as informacións que coñeza no exercicio das súas funcións, incluso despois de cesar as mesmas. Esta mesma obriga afecta a todo profesional contratado directa ou indirectamente, e manterase unha vez rematada a relación contractual.
- Manter en secreto os contrasinais e demais sistemas de identificación, para o que adoptará as medidas de seguridade necesarias, procedendo de xeito inmediato a cambialos en caso de que se fagan públicos.
- Non utilizar usuarios distintos do propio, incluso para levar a cabo tarefas para as que se conta con autorización.
- Informar inmediatamente ó responsable de seguridade de calquera acceso non autorizado ou anomalía, ameaza, vulnerabilidade ou risco de seguridade observado ou que se coñeza.
- Desconectar os equipos informáticos cando o posto de traballo quede desatendido durante un período de tempo significativo, cancelando previamente as sesións activas e pechando todos os aplicativos de forma axeitada.
- Protexer o equipo cos protectores de pantalla, bloqueadores de teclado, chaves e sistemas similares cos que conte, se o período de tempo no que o posto quedará desatendido é curto.

- Gardar baixo chave os documentos e soportes do usuario que conteñan datos de carácter persoal que non están sendo utilizados.
- Utilización a información do ficheiro de acordo ós fins para os que se creou.
- Manter limpo de programas non facilitados ou autorizados pola sección de Informática o seu posto de traballo.
- Manter as medidas de seguridade axeitadas sempre que se utilicen ficheiros temporais creados a partir dos ficheiros ós cales teña acceso, eliminándoos en canto deixe de ser de utilidade.
- Non está permitida a saída do centro de traballo de soportes que conteñan datos de carácter persoal (aínda que sexan ficheiros temporais) a menos que esta estea rexistrada adecuadamente no rexistro de saída, debidamente autorizado.
- Usar no posible o correo electrónico para o envío interno de ficheiros en lugar de soportes magnéticos, co fin de limitar a súa circulación, posibilidade de perda ou subtracción.

Redactarase un Código Ético que inclúa unha cláusula de confidencialidade e que deberán aceptar e cumprir todas as persoas que poidan intervir en calquera fase do tratamento dos datos de carácter persoal independentemente do cargo que ocupen ou funcións que realicen.

Consecuencias do incumprimento das normas.

De conformidade co establecido no artigo 44 da Lei orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal, as infraccións cualifícanse como leves, graves ou moi graves:

Son infraccións **leves:**

a) Non atender, por motivos formais, a solicitude do interesado de rectificación ou cancelación dos datos persoais obxecto do tratamento cando legalmente proceda.

b) Proceder á recollida de datos de carácter persoal dos propios afectados sen proporcionarlles a información que sinala o artigo 5 da Lei 15/1999.

c) Incumprir o deber de segredo establecido no artigo 10 da Lei 15/1999, salvo que constitúa infracción grave.

Son infraccións **graves:**

a) Proceder á recollida de datos de carácter persoal sen recabar o consentimento expreso das persoas afectadas, nos casos en que este sexa esixible.

b) Tratar os datos de carácter persoal ou usalos posteriormente con conculcación dos principios e garantías establecidos na presente Lei ou con incumprimento dos preceptos de protección que impoñan as disposicións regulamentarias de desenvolvemento, cando non constitúe infracción moi grave.

c) O impedimento ou obstaculización do exercicio dos dereitos de acceso e oposición e a negativa a facilitar a información que sexa solicitada.

d) Manter datos de carácter persoal inexactos ou non efectuar as rectificacións ou cancelacións dos mesmos que legalmente procedan cando resulten afectados dereitos das persoas que a presente Lei ampara.

e) A vulneración do deber de gardar segredo sobre os datos de carácter persoal incorporados a ficheiros que conteñan datos relativos á comisión de infraccións administrativas ou penais, facenda pública, servicios financeiros, prestación de servicios de solvencia patrimonial e crédito, así como aqueloutros ficheiros que conteñan un conxunto de datos de carácter persoal suficientes para obter unha avaliación da personalidade do individuo.

f) Manter os ficheiros, locais, programas ou equipos que conteñan datos de carácter persoal sen as debidas condicións de seguridade que por vía regulamentaria se determinen.

g) A obstrucción ó exercicio da función inspectora.

h) Incumprir o deber de información que se establece nos artigos 5, 28 e 29 da Lei 15/1999, cando os datos fosen recabados de persoa distinta do afectado.

Son infraccións **moi graves:**

a) A recollida de datos en forma enganosa e fraudulenta.

b) A comunicación ou cesión dos datos de carácter persoal, fóra dos casos nos que estean permitidas.

c) Recabar e tratar os datos de carácter persoal ós que se refire o apartado 2 do artigo 7 cando non medie o consentimento expreso do afectado; recabar e tratar os datos referidos no apartado 3 do artigo 7 cando non o dispoña unha lei ou o afectado non consentise expresamente, ou violentar a prohibición contida no apartado 4 do artigo 7 da Lei 15/1999.

d) Non cesar no uso ilexítimo dos tratamentos de datos de carácter persoal cando sexa requirido para isto polo director da Axencia Española de Protección de datos ou polas persoas titulares do dereito de acceso.

e) A transferencia temporal ou definitiva de datos de carácter persoal que fosen obxecto de tratamento ou fosen recollidos para sometelos a dito tratamento, con destino a países que non proporcionen un nivel de protección equiparable sen autorización do director da Axencia Española de Protección de datos.

f) Tratar os datos de carácter persoal de forma ilexítima ou con menosprezo dos principios e garantías que lles sexan de aplicación, cando con isto se impida ou se atente contra o exercicio dos dereitos fundamentais.

g) A vulneración do deber de gardar segredo sobre os datos de carácter persoal a que fan referencia os apartados 2 e 3 do artigo 7 da Lei 15/1999, así como os que fosen recabados para fins policiais sen consentimento das persoas afectadas.

h) Non atender, ou obstaculizar de forma sistemática o exercicio dos dereitos de acceso, rectificación, cancelación ou oposición.

i) Non atender de forma sistemática o deber legal de notificación da inclusión de datos de carácter persoal nun ficheiro.

A vulneración de calquera das normas descritas neste documento implicará o inmediato bloqueo do identificador que cometeu a infracción e a notificación da incidencia ó responsable do ficheiro.

O responsable do ficheiro adoptará as medidas necesarias para que o persoal coñeza as normas de seguridade que afecten ó desenvolvemento das súas funcións, así como as consecuencias nas que puidera incorrer no caso do seu incumprimento.

O procedemento e as sancións a aplicar no caso das infraccións cometidas polo persoal do Concello de Santiago de Compostela será o establecido na lexislación sobre réxime disciplinario das Administracións Públicas.

Comunicaranse á Axencia Española de Protección de Datos as resolucións que resolvan en relación coas medidas e actuacións referidas ós apartados anteriores.

Cando as infraccións sexan cometidas por terceiros que manteñan co Concello relacións contractuais, estarase ó disposto no artigo 46.1 da Lei 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal.

7. ESTRUCTURA DOS FICHEIROS CON DATOS DE CARÁCTER PERSOAL E DESCRICIÓN DOS SISTEMAS DE INFORMACIÓN

O Rexistro Municipal de Protección de Datos incluirá información detallada sobre a estructura dos ficheiros inscritos.

Esta información, que se obterá a partir dos impresos de solicitude de creación dos ficheiros, estará estructurada segundo o estándar establecido pola Axencia Española de Protección de Datos a través dos formularios de inscrición e as aplicacións de axuda que se poden descargar desde o seu sitio web.

Estes formularios e a propia aplicación de axuda estarán dispoñibles a través da Intranet do Concello co fin de facilitar a realización de solicitudes.

8. PROCEDEMENTO DE NOTIFICACIÓN, XESTIÓN E RESPOSTA ANTE INCIDENCIAS

A efectos deste Regulamento, considérase incidencia calquera anomalía que afecte ou puidera afectar á seguridade dos datos.

8.1. PROCEDEMENTO DE NOTIFICACIÓN E RESPOSTA A SEGUIR FRONTE A INCIDENCIAS.

Cada vez que se detecte algunha anomalía (incidencias que afecten á confidencialidade, integridade, dispoñibilidade e autenticidade da información), que poida ser considerada como incidencia, esta notificarase inmediatamente ó responsable de seguridade.

O responsable de seguridade rexistrará e analizará a devandita incidencia e porá en marcha as medidas necesarias para enmendar o problema, se este é de índole técnica.

En caso de tratarse dun intento, errado ou non, de acceso a datos de persoal non autorizado, informarase ó usuario non autorizado (se este é identificado) e, de ser o caso, tomaranse as medidas disciplinarias pertinentes. Cando se detecte un fallo nos mecanismos de protección dos datos, estes serán inmediatamente revisados para incrementar o nivel de protección dos mesmos.

Se fora necesaria unha recuperación de datos, estes restaurararanse das copias de seguridade, previa autorización por escrito do responsable do ficheiro no caso de tratarse de ficheiros de nivel medio, e realizaranse manualmente as actualizacións necesarias para deixar a información no mesmo estado que se atopaba antes da incidencia, sempre que sexa posible. Introducirase no rexistro de incidencias a información completa e detallada da devandita recuperación, como se describe máis adiante.

Existirá persoal que dispoña dunha autorización xenérica limitada unicamente para os casos de urxencia nos que non sexa localizado o responsable do ficheiro, apuntando esta situación como unha incidencia no Rexistro de incidencias.

8.2. REXISTRO DE INCIDENCIAS.

Este rexistro conterá a seguinte información para cada incidencia:

- Referencia única
- Ficheiro afectado
- Equipo no que se atopa
- Tipo de incidencia (acceso, palabras clave, corrupción de ficheiro, borrado accidental de información, etc.)
- Efectos derivados da incidencia
- Data
- Hora
- Quén a notifica
- A quén se notifica
- Proceso de recuperación (si/non) [Procedementos de recuperación de datos aplicados, quén executou o proceso de recuperación, datos restaurados, datos recuperados manualmente]
- Sancións (si/non) [Sanción aplicada, a quén se aplica]

A este rexistro poderán acceder os usuarios autorizados a través da aplicación correspondente publicada na Intranet do Concello.

9. PROCEDEMENTO DE COPIA DE RESPALDO E RECUPERACIÓN DE DATOS

9.1. COPIA DE RESPALDO

Existirá un documento denominado "Plano de copias de seguridade e recuperación", que conterá información detallada sobre o esquema de copias que se ven realizando para cada servidor, o tipo de almacenamento, a codificación de cada soporte, o procedemento de realización da copia, o formato e aplicación utilizada, os sistemas de ficheiro copiados, etc. Este documento estará actualizado e á dispoñibilidade dos responsables da realización das copias e recuperacións, dos responsables dos ficheiros, e dos responsables de seguridade.

En calquera caso, as copias de respaldo de ficheiros realizaranse diariamente en todos os equipos servidores do Concello nos que residan datos, sexan estes de carácter persoal ou non. Estas copias almacenaranse en cartuchos de cinta magnética de diferentes formatos tales como cintas DAT 4mm, cintas DLT, etc.

Manterase como mínimo unha copia diaria dos últimos 30 días, unha copia mensual dos últimos 12 meses, e unha copia anual. Para a realización das copias diarias poderase utilizar unha combinación de copias incrementais e completas, de tal xeito que alomenos se realice unha copia completa cada semana.

Todos os soportes estarán almacenados nos armarios destinados a tal fin nas dependencias de Informática, a excepción dos soportes que permanezan continuamente nas unidades de copia, necesarios para a realización automática das copias de seguridade. Estes soportes atoparanse protexidos fisicamente coas mesmas garantías que os propios datos contidos nos discos duros dos sistemas.

Manterase unha segunda copia semanal nun edificio do Concello distinto daquel no que se atopan os servidores, co fin de que non poidan afectar a todas as cintas as mesmas incidencias. O movemento de soportes realizarase tendo en conta os requisitos establecidos neste mesmo Regulamento.

Utilizaranse dous sistemas de copia de seguridade, que corresponden cos dous sistemas operativos dos servidores existentes:

- Formato 1: Utilidade VERITAS BACKUPEXEC para equipos con sistemas de Microsoft.
- Formato 2: Utilidade "vdump" de True64 UNIX.

O uso de sistemas de copia alternativos deberá ser convenientemente aprobado e documentado.

O Plano de copias de seguridade e recuperación incluirá unha auditoría anual e a definición dun procedemento que permita resolver a eventual obsolescencia dos soportes de almacenamento.

Encargado da realización da copia de respaldo.

Os encargados da realización das copias de respaldo dos servidores son os membros da Unidade de Sistemas da Sección de Informática.

Encargado da verificación do proceso de copia de respaldo.

Realizaraa o responsable de seguridade en representación do responsable do ficheiro.

9.2. RECUPERACIÓN DE DATOS

O documento "Plano de copias de seguridade e recuperación" conterá información detallada sobre o procedemento de localización e recuperación de datos, etc. Este documento estará actualizado e á dispoñibilidade dos responsables da realización das copias e recuperacións, dos Responsables dos ficheiros, e dos Responsables de seguridade.

A recuperación de ficheiros ou bases de datos contendo datos de carácter persoal require a autorización escrita previa do responsable do ficheiro. A devandita recuperación quedará documentada no rexistro de incidencias.

No rexistro de soportes poderase localizar facilmente o soporte onde se atopa a información que se deba restaurar.

Os sistemas de recuperación que se utilizarán, dependendo do sistema operativo do servidor, son os seguintes:

- Formato 1: Utilidade VERITAS BACKUPEXEC de Microsoft.
- Formato 2: Utilidade "vrestore" de True64 UNIX.

O uso de sistemas alternativos deberá ser convenientemente aprobado e documentado.

Á hora de localizar as cintas onde se atopa a información dentro do rexistro de soportes, sempre que se trate dos últimos 30 días, será suficiente con acceder á cinta diaria correspondente. No caso de tratarse de ficheiros de maior antigüidade, as recuperacións terán que realizarse a través de cintas mensuais.

Encargado da realización do proceso de recuperación de datos.

Os encargados da realización das copias de respaldo dos servidores son so membros da Unidade de Sistemas da Sección de Informática.

Encargado da verificación do proceso de recuperación de datos.

Realizaraa o responsable de seguridade en representación do responsable do ficheiro.

10. PROCEDEMENTO DE APROBACIÓN E MODIFICACIÓN DO DOCUMENTO DE SEGURIDADE

O Documento Municipal de Seguridade tratarase como un documento dinámico e requirirá actualizacións periódicas debido ó establecemento de novos mecanismos de seguridade, a modificacións nos sistemas de información, á incorporación de novos ficheiros e usuarios, etc.

Para facer máis áxil a súa actualización, considéranse constituído por dous elementos que poden ser aprobados de xeito independente:

- Este Regulamento, que ten un contido máis estable e xeral.
- O Rexistro Municipal de Protección de Datos, que conterá información sobre ficheiros, sistemas de información, usuarios e permisos de acceso, e que requirirá unha maior frecuencia de actualización.

Aprobación inicial do Documento Municipal de Seguridade

Consistirá na aprobación polo Pleno da Corporación do Regulamento Municipal de Seguridade para a Protección de Datos de Carácter Persoal.

Revisións do documento de seguridade

Corresponderá ó Pleno da Corporación a aprobación das actualizacións do Documento Municipal de Seguridade que afecten ó Regulamento Municipal de Protección de Datos.

Corresponderá á Xunta de Goberno Local a aprobación das actualizacións do Documento Municipal de Seguridade que afecten ó Rexistro Municipal de Protección de Datos.

Adición de documentación ó documento de seguridade

O Responsable Municipal de Protección de Datos manterá, xunto co documento de seguridade, unha copia do Plano de copias de seguridade e outros documentos referenciados neste Regulamento ou que considere oportunos.

Ó Documento Municipal de Seguridade orixinal irase anexando copia daqueloutros documentos de seguridade creados polos responsables de ficheiro e os aportados por terceiros que realicen a prestación dun servicio o Concello.

Neste caso non será necesaria a aprobación do documento na súa totalidade senón que será suficiente a aprobación por parte do órgano competente en cada caso do documento anexado.

Existirá un mecanismo de comprobación do grado de cumprimento de Documento Municipal de Seguridade e un cuestionario que permita medir o nivel de cumprimento xeral e establecer prioridades.

11. ANEXOS

ANEXO I- MODELOS DE DOCUMENTACIÓN E FORMULARIOS.

Os modelos que se presentan neste anexo pretenden servir como base para a redacción de documentos ou o deseño de formularios de recollida de datos, tanto se se presentan en formato papel como en forma de pantallas de introducción de datos para a utilización en aplicacións informáticas.

Estes modelos non se centran no deseño e formato de presentación, senón na estructura e contido dos documentos.

I.1. Modelo de autorización de alta/baixa/modificación de ficheiros.

"_____ (o responsable dos ficheiro), autoriza a _____(alta/baixa/modificación) do ficheiro _____, suxeito á Lei 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal, para o que se achega o formulario do Rexistro de Ficheiros da Axencia de Protección de Datos de Carácter Persoal.

[SÓ NO CASO DE SOLICITUDE DE CREACIÓN DE FICHEIRO:]

Presta a súa conformidade ó Regulamento Municipal de Seguridade para a Protección de Datos de Carácter Persoal elaborado polo Responsable Municipal de Protección de Datos para a súa aplicación ó devandito ficheiro.

En particular, presta a súa conformidade ós procedementos de copias de respaldo establecidos no Regulamento, e fai constar a autorización expresa que se outorga ós responsables técnicos encargados da recuperación das bases de datos, para a realización da devandita recuperación cando o responsable do ficheiro non sexa localizado, se produza unha incidencia e sexa precisa a reconstrucción inmediata para o correcto funcionamento dos sistemas de información que operan sobre a devandita base de datos.

Así mesmo, acorda designar o Responsable Municipal de Protección de Datos como responsable de seguridade do ficheiro, co obxecto de que coordine e controle as medidas de seguridade establecidas no devandito Regulamento.

Data e sinatura do responsable do ficheiro."

I.2. Modelos de alta/baixa/modificación de usuarios.

SOLICITUDE DE ALTA/MODIFICACIÓN DE USUARIO	
NOME COMPLETO :	
DATA ALTA/BAIXA:	**DATA RENOVACIÓN:**

AREA:	**SERVICIO:**	**SECCIÓN:**	**NEGOCIADO:**

INFORMACIÓN A LA QUE PRECISA ACCEDER:			
SERVICIO	**TIPO ACCESO**	**PROPIETARIO**	**AUTORIZA**

SERVICIOS DE INTERNET, táchese o que non proceda.

ACCESO A INTERNET: AUTORIZADO / DESAUTORIZADO
CORREO ELECTRÓNICO: AUTORIZADO / DESAUTORIZADO

DOMINIO : **USUARIO :** **ID. EQUIPO :** **TLFNO. :**
GRUPOS A QUE PERTENCE:
Santiago de Compostela, ... de ..... de ..... **O XEFE DO SERVICIO** **O RESPONSABLE DE SEGURIDADE**

I.3. Modelo de inventario de soportes

INVENTARIO DE SOPORTES	
Clave única:	
Etiqueta lóxica:	
Descrición:	
Equipo:	
Tipo de Copia: (respaldo periódico, respaldo ocasional, traspaso de datos)	
Tipo de Soporte: (Streamer, 8mm, 4mm, diskette, CD, etc.)	
Data de copia:	
Data de eliminación: (caducidade da copia)	

I.4. Modelo de rexistro de entrada de soportes

REXISTRO DE ENTRADA DE SOPORTES	
Identificación do soporte: (se está dispoñible)	
Tipo de soporte:	

(streamer, DAT, CD, diskette, cinta, etc.)		
Número de soportes:		
Recepción:	Data:	
	Hora:	
Emisor:		
Forma de envío:		
Responsable da recepción:		
Información que contén:		

I.5. Modelo de rexistro de saída de soportes

REXISTRO DE SAÍDA DE SOPORTES		
Identificación do soporte: (Clave única do inventario)		
Tipo de soporte: (streamer, DAT, CD, diskette, cinta, trans. por rede etc.)		
Número de soportes:		
Envío:	Data:	
	Hora:	
Destinatario:		
Forma de envío:		
Responsable do envío:		
Información que contén:		

I.6. Modelo de rexistro de accesos

REXISTRO DE ACCESOS		
Identificación do usuario:		
Acceso:	Data:	
	Hora:	
Tipo de acceso:		
Autorizado/denegado:		
Información accedida:		

I.7. Modelo de rexistro de incidencias

REXISTRO DE INCIDENCIAS	
Clave incidencia:	
Ficheiro afectado:	
Equipo no que se atopa:	
Tipo de incidencia: (acceso, palabras clave, corrupción de ficheiro,	

borrado accidental de información, etc.)			
	Data:		
	Hora:		
Notificada por:		Nome:	
		Departamento:	
Notificada a:			
Danos derivados da incidencia:			
Accións propostas:			
Proceso de recuperación:		Procedementos de recuperación:	
		Responsable da recuperación:	
		Datos restaurados:	
		Datos recuperados manualmente:	
Sancións:		Sanción aplicada:	
		Aplicada a:	

I.8. Modelo de solicitude de xeración de soporte informático

SOLICITUDE DE XERACIÓN DE SOPORTE INFORMÁTICO	
Solicitante:	
Departamento:	
Equipo que contén os datos:	
Ficheiros/datos que solicita:	
Data da solicitude:	
Tipo de soporte que solicita:	
Formato da copia:	
Autorizado por:	
Data da autorización:	

A autorización da copia sempre se condicionará ó establecido no ordenamento xurídico no ámbito da seguridade informática, estando obrigada a persoa depositaria da copia a responder en todo momento do cumprimento da Lei 15/1999, de 13 de decembro, de Protección de Datos e do Regulamento de Seguridade en relación cos datos incluídos no soporte xerado.

I.9. Modelo de autorización xenérica de recuperación de datos

"_____ (o responsable dos ficheiros), responsable dos ficheiros con datos de carácter persoal _____, que foron creados mediante as correspondentes disposicións publicadas nos BOE/DOG números _____ con datas _____, fai constar a autorización expresa que se outorga aos responsables técnicos da Sección de Informática, encargados da recuperación das bases de datos, a realizar a devandita recuperación, cando o responsable do ficheiro e os Responsables de seguridade non sexan localizados, se produza unha incidencia deste tipo e sexa precisa a súa reconstrucción inmediata para o correcto funcionamento dos sistemas de información que operan sobre a devandita base de datos.

Data e sinatura do responsable do ficheiro e do responsable de seguridade".

I.10. Modelo de autorización de transporte de información de carácter persoal.

"_____ (o responsable dos ficheiro), responsable do ficheiro _____, e na súa representación o responsable de seguridade do mesmo, autoriza a _____ para poder levar o soporte denominado _____(identificación do inventario de soportes) rexistrado como _____ (identificación no rexistro de E/S de soportes) que contén información relativa a _____, con destino a _____, polos seguintes motivos:

Data e sinatura do responsable do ficheiro."

I.11. Modelo de autorización de cesión.

"_____ (responsable do ficheiro), atendendo ó especificado na Lei orgánica 15/1999 de protección de datos de carácter persoal, que ten por obxecto garantir e protexer, no que concirne ó tratamento de datos de carácter persoal, as liberdades públicas e os dereitos fundamentais das persoas físicas, e especialmente da súa honra e intimidade persoal e familiar, autorizo a ____ (cesión ou comunicación) dos datos de carácter persoal solicitados obrantes no ficheiro _____ (ficheiro), coa finalidade de _____(finalidade).

Data e sinatura do responsable do ficheiro"

I.12. Modelo de cláusula para os formularios de solicitude de información de carácter persoal.

De conformidade co disposto na Lei Orgánica 15/1999, de 13 de decembro, de Protección de Datos de Carácter Persoal, os seus datos serán tratados de xeito confidencial e poderán ser incorporados ós correspondentes ficheiros do CONCELLO DE SANTIAGO DE COMPOSTELA, para a xestión do servicio. En calquera momento poderá exercitar, en relación cos seus datos persoais, os dereitos de acceso, cancelación, rectificación e oposición comunicándoo por escrito a _____ (responsable do ficheiro e dirección de contacto).

4. DAR CONTA DE RESOLUCIÓNS DA ALCALDÍA E DA XUNTA DE GOBERNO LOCAL.

Dáse conta ao pleno das resolucións dictadas polo Sr. Alcalde no período que abrangue dende o 16 de xuño ata o 15 de xullo de 2005.

Dase tamén conta ao pleno dos acordos adoptados pola Xunta de Goberno Local na sesión que tivo lugar o día 30 do mes de maio de 2005, e dos que tiveron lugar os días 6, 13 e 20 do mes de xuño de 2005.