ANEXO II:

REXISTRO DE ACTIVIDADES

REXISTRO DE ACTIVIDADE – PORTELO UNICO E REXISTRO	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade e ALEJANDRA PARDO VAZQUEZ que ocupa el posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Rexistro de entrada de documentación na Xunta, procedemento administrativo.
CATEGORÍAS DE INTERESADOS	Cidadáns e Residentes, Solicitantes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal, Administracións
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Deputación
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres non se solicite a supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE
1.- APLICACIÓNS INFORMÁTICAS
Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.
2.- XESTIÓN DE SOPORTES E DOCUMENTOS
Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.
3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN
O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS
No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE : 1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento 2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións. 3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE
5.- procedemento DE IDENTIFICACIÓN
Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.
6.- procedemento DE AUTENTICACIÓN
O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .
7.- POLÍTICA DE CONTRASINAIS
- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas. - - privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS - O límite de intentos errados está limitado: 3 - procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso. - Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas. - Periodicidade do cambio de contrasinal: ANUALMENTE - Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas
8.- CONTROL DE ACCESOS
Permisos de acceso aos usuarios: -Quen o concede, altera ou anula: o responsable de seguridade . -Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo -Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario. -Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados. -Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III. -O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos. Autorización de accesos: O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de

carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.
-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e libertades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – PADRON DE HABITANTES	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa el posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Rexistro de entrada de documentación na Xunta, procedemento administrativo.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes, Solicitantes.

PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal, Administración
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Sinatura, Data de nacemento, lugar de nacemento, Académicos e profesionais
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Instituto Nacional de Estatística, Órganos da Administración do Estado, de Comunidade Autónoma que necesiten datos do padrón de habitantes para realizar notificacións de ausentes, órganos xudiciais.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite a supresión dos mesmos.
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saida de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á

información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación

do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .

2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.

3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.

Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.

No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.

Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.

No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.

O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e

informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ". Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.
13.- ACTUALIZACIÓN DO DOCUMENTO
Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .
14.- REVISION DO DOCUMENTO
Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado. de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – PERSOAL	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Recursos Humans, XESTIÓN de nóminas.
CATEGORÍAS DE INTERESADOS	Empregados.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal, Administracións Públicas.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Nº seguridade. Social, Sinatura, Características Persoais, Académicos E profesionais, Detalles do emprego, Económicos, financeiros e de seguros, Transaccións de bens e servizos.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Organismos de la Seguridade. Social, Facenda Pública E Administración Tributaria, Órganos de Comunidade Autónoma, en concreto: Xunta de Galicia: Presidencia, traballo E benestar, Órganos de la Administración de

	Estado: INEM.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite a supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte

do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.

- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE

Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .

2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.

3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.

Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.

No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.

Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.

No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.

O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".

Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.

de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente

documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – CURRICULUMS	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa el posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Recursos Humans
CATEGORÍAS DE INTERESADOS	Solicitantes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Sinatura, , Características persoais, Circunstancias sociais, Académicos e profesionais, detalles do emprego, Imaxe
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	-
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite a supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE
1.- APLICACIÓNS INFORMÁTICAS
Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.
2.- XESTIÓN DE SOPORTES E DOCUMENTOS
Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.
3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
  Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:
O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.
-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase

ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – SERVIZOS SOCIAIS	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa el posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Servizos Sociais.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.

PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Nº seguridade. Social, Sinatura, Tarxeta sanitaria, Características persoais, Circunstancias sociais, Académicos e profesionais, detalles do emprego, Económicos, financeiros e de seguros, Saúde, Vida sexual, Datos relativos a infraccións penais ou administrativas. ESPECIALMENTE SENSIBLES: Saúde, Vida Sexual. OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Órganos Xudiciais, Outros Órganos da Comunidade Autónoma: Xunta: Traballo e Benestar, Deputación Provincial.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite a supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente

Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
  Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á

política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .

2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.

3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.

Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.

No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.

Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.

No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal

están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – DESENVOLVEMENTO LOCAL	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Asesoramento sobre a búsqueda de emprego, creación de novas empresas.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Sinatura, Características persoais Académicos E Profesionais, Detalles do emprego.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Entidades privadas que soliciten currículums para cubrir postos vacantes propios.

TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de

acceso.

- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE

Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.

realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – AXENTES DE PROMOCIÓN ECONÓMICA	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	xestionar os datos dos axentes de promoción económica que prestan os servizos no CONCELLO, coa finalidade de ser identificables polos usuarios aos que se dirixen as accións.
CATEGORÍAS DE INTERESADOS	Empregados
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Outros Órganos da Comunidade Autónoma: Concellería de traballo e Benestar.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE
1.- APLICACIÓNS INFORMÁTICAS
Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.
2.- XESTIÓN DE SOPORTES E DOCUMENTOS
Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.
3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
  Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .

2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.

3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.

Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de incidencia e o detalle da mesma. Encargarase

ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – PARTICIPANTES EN ACCIÓNS DE PROMOCIÓN DE EMPREGO	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Recursos Humans.
CATEGORÍAS DE INTERESADOS	Solicitantes, Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.

CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Información Comercial, Características Persoais, Académicos e profesionais, Detalles do Emprego, Imaxe. ESPECIALMENTE SENSIBLES: OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Outros Órganos da Comunidade Autónoma: Concellería de Traballo e Benestar.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .

2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.

3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.

Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.

No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.

Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.

No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.

O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".

Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO
Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .
14.- REVISION DO DOCUMENTO
Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado. de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – FORMACION	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	XESTIÓN de cursos de formación, Educación e cultura.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal, outras persoas físicas, Administración Pública.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: nome e apelidos, DNI, Dirección, Teléfono, Sinatura, Nº seguridade, social, Académicos e profesionais.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Administración do Estado: INEM.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite a supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.
DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE	
1.- APLICACIÓNS INFORMÁTICAS	
Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se	

facilita a relación das mesmas.
2.- XESTIÓN DE SOPORTES E DOCUMENTOS
Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.
3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN
O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.
4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS
No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE : 1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento 2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións. 3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE
5.- procedemento DE IDENTIFICACIÓN
Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.
6.- procedemento DE AUTENTICACIÓN
O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .
7.- POLÍTICA DE CONTRASINAIS
- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas. - privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS - O límite de intentos errados está limitado: 3 - procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso. - Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas. - Periodicidade do cambio de contrasinal: ANUALMENTE - Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas
8.- CONTROL DE ACCESOS
Permisos de acceso aos usuarios: -Quen o concede, altera ou anula: o responsable de seguridade . -Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.
-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.
-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.
-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.
Autorización de accesos:
O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.
-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS
O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan. Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"
11.- REXISTRO DE INCIDENCIAS
As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS. O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia. No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos. Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida. No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.
12.- FUNCIONS DO PERSOAL
As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento. O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ". Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.
13.- ACTUALIZACIÓN DO DOCUMENTO
Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .
14.- REVISION DO DOCUMENTO
Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado. de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – XESTIÓN ECONOMICA	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.

DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Xestión Contable, fiscal e administrativa.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, teléfono, Económicos, financeiros e de seguros, Transaccións de bens e servizos. ESPECIALMENTE SENSIBLES: OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Facenda Pública E Administración Tributaria, Tribunal de contas, Concellería de contas, Órganos de Comunidade Autónoma: Xunta de Galicia, Deputación Provincial, Bancos, caixas de aforro e caixas rurais.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante la prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude minima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un

contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL
As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento. O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ". Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.
13.- ACTUALIZACIÓN DO DOCUMENTO
Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .
14.- REVISION DO DOCUMENTO
Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado. de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – RECADACIÓN	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Cobro de tributos municipais.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Sinatura, Económicos.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Facenda Pública e Administración Tributaria.
TRANSFERENCIAS INTERNACIONAIS	-

PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite a supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de seguridade .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e ininteligible polo Responsable de

seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:
-Quen o concede, altera ou anula: o responsable de seguridade .
-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo
-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.
-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.
-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.
-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.
Autorización de accesos:
O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.
-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de

realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – CONTRATACIÓN	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	XESTIÓN de contratación de obras E/o servizos para o CONCELLO.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes, PROVEDORES.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, dirección, Teléfono, Sinatura, Características persoais, Circunstancias sociais, Académicos e profesionais, Económicos, financeiros e de seguros, Transaccións de bens e servizos.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Tribunal de contas, Órganos da Administración do Estado: Ministerio de Facenda, Outros Órganos de Comunidade Autónoma: Concellería de contas, Entidades Aseguradoras.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE
1.- APLICACIÓNS INFORMÁTICAS
Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.
2.- XESTIÓN DE SOPORTES E DOCUMENTOS
Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN
O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.
4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS
No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE : 1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento. 2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións. 3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE
5.- procedemento DE IDENTIFICACIÓN
Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.
6.- procedemento DE AUTENTICACIÓN
O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .
7.- POLÍTICA DE CONTRASINAIS
- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas. - privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS - O límite de intentos errados está limitado: 3 - procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso. - Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas. - Periodicidade do cambio de contrasinal: ANUALMENTE Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas
8.- CONTROL DE ACCESOS
Permisos de acceso aos usuarios: -Quen o concede, altera ou anula: o responsable de seguridade . -Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo -Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario. -Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados. -Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III. -O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause

baixa algún traballador con acceso a datos.
Autorización de accesos:
O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.
-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – LICENZAS E AUTORIZACIONS	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	El responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Xestión de licenza de apertura, de obras, feiras o actividades culturais, procedemento administrativo
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes

PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, teléfono, Nº seguridade. Social, Sinatura, Circunstancias sociais, Académicos E profesionais, Detalles emprego, Económicos, financeiros e de seguros, transaccións de bens e servizos.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Instituto Nacional de Estatística, Órganos da Administración DO Estado: Ministerio de Fomento, Delegación de Goberno, Órganos de Comunidade Autónoma: Xunta: Concellería de Medio, Territorio e Infraestruturas, Deputación Provincial, Garda Civil, SGAE.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o

rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento. O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade". Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.
13.- ACTUALIZACIÓN DO DOCUMENTO
Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .
14.- REVISION DO DOCUMENTO
Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado. de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – URBANISMO	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	XESTIÓN de actos de planeamento, XESTIÓN E disciplina urbanística
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Sinatura, Circunstancias sociais, Económicos, financeiros e de seguros.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Órganos da Administración de Estado: Ministerio de Fomento, Órganos de Comunidade Autónoma: Xunta: Concellería de Medio, Territorio e Infraestruturas,

	Deputación Provincial.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante la prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte

do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.

- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores e/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente

documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – REXISTRO DE INTERESES MEMBROS DA CORPORACIÓN	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa O posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	XESTIÓN E control de choque de intereses dos membros da corporación.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Sinatura, Características persoais, Circunstancias sociais, Académicos E profesionais, Económicos.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	-
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE
1.- APLICACIÓNS INFORMÁTICAS
Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.
2.- XESTIÓN DE SOPORTES E DOCUMENTOS
Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN
O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.
4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS
No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE : 1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento 2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións. 3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE
5.- procedemento DE IDENTIFICACIÓN
Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.
6.- procedemento DE AUTENTICACIÓN
O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .
7.- POLÍTICA DE CONTRASINAIS
- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas. - privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS - O límite de intentos errados está limitado: 3 - procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso. - Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas. - Periodicidade do cambio de contrasinal: ANUALMENTE - Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas
8.- CONTROL DE ACCESOS
Permisos de acceso aos usuarios: -Quen o concede, altera ou anula: o responsable de seguridade . -Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo -Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario. -Caracteristicas do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados. -Caracteristicas do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III. -O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause

baixa algún traballador con acceso a datos.
Autorización de accesos:
O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.
-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – RESPONSABILIDADE ADMINSITRATIVA	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Resarcir aos particulares das lesións producidas nos seus bens e DEREITOS polo funcionamento do CONCELLO.

CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Sinatura.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Outros Órganos de Comunidade Autónoma: Xunta: Consello Consultivo, Entidades Aseguradoras.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma

que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .

2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.

3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.

Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.

No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.

Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.

No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.

O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".

Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera

medida de seguridade reflectida no mesmo.
13.- ACTUALIZACIÓN DO DOCUMENTO
Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .
14.- REVISION DO DOCUMENTO
Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado. de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – ELECCIONS	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Selección dos membros das mesas electorais e Xestión administrativa das eleccións.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Administracións Públicas.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, dirección, Características persoais, Académicos e profesionais.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Instituto Nacional de Estatística, Órganos xudiciais, Outros Órganos da Administración DO Estado: Ministerio de Interior, outros Órganos de Comunidade Autónoma: Xunta: Presidencia
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto

DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantia de integridade: Cada usuario ten un identificador que se autentica mediante

contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – CULTURA E DEPORTES	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Educación e cultura, organización de eventos e actividades deportivas, de ocio e culturais.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Sinatura, características persoais, Circunstancias sociais, Académicos e profesionais, Académicos E profesionais, Económicos, financeiros E de seguros.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Entidades privadas que colaboran na organización de actividades culturais e/ou deportivas, Deputación Provincial, Órganos de Comunidade Autónoma: Concellerías de la Xunta para solicitar subvencions.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE
1.- APLICACIÓNS INFORMÁTICAS
Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.
2.- XESTIÓN DE SOPORTES E DOCUMENTOS
Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.
3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN
O equipamento informático no que se trata datos de carácter persoal, atópase descrito no

ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.
-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.

No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – BIBLIOTECA	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Educación e Cultura.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	

CATEGORÍAS DE DATOS TRATADOS	Propio interesado ou o seu representante legal.
CESIÓNS PREVISTAS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Características persoais.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	-
SISTEMA DE TRATAMENTO	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	Mixto
RESPONSABLE DE TRATAMENTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados,

cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".

Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.
13.- ACTUALIZACIÓN DO DOCUMENTO
Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .
14.- REVISION DO DOCUMENTO
Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado. de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – MEDIOAMBENTE	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	XESTIÓN de denuncias en materia de medioambente.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Fonteses accesibles ó público, Administracions Públicas.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Circunstancias sociais.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Órganos Xudiciais, Órganos de la Administración DO Estado e de Comunidade Autónoma con competencia en medio ambente para dar traslado das denuncias nesta materia a nivel estatal e autonómico.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto

DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante

contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8. CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – REXISTRO CANINO E ANIMAIS PERIGOSOS	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa el posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	procedemento administrativo, seguridade. Pública e Defensa.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal, Administración Pública.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, Teléfono, Sinatura, Transaccións de bens e servizos, Datos relativos a infracciones penais o administrativas.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Outros Órganos de Comunidade Autónoma: Xunta: Presidencia.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS
No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE : 1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento 2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións. 3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE
5.- procedemento DE IDENTIFICACIÓN
Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.
6.- procedemento DE AUTENTICACIÓN
O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .
7.- POLÍTICA DE CONTRASINAIS
- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas. - privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS - O límite de intentos errados está limitado: 3 - procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso. - Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas. - Periodicidade do cambio de contrasinal: ANUALMENTE - Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas
8.- CONTROL DE ACCESOS
Permisos de acceso aos usuarios: -Quen o concede, altera ou anula: o responsable de seguridade . -Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo -Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario. -Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados. -Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III. -O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos. Autorización de accesos: O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de

carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.
-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles

detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – POLICÍA	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Seguridade. pública e defensa
CATEGORÍAS DE INTERESADOS	Propio interesado ou o seu representante legal, Outras persoas físicas, Administracións públicas
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal, Administracións
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS:

	Nome apelidos, DNI, Teléfono, Dirección, Sinatura, Circunstancias sociais, Económicos, financeiros e de seguros.
	ESPECIALMENTE SENSIBLES: Saúde
	OUTROS DATOS TIPIFICADOS: Datos relativos a infracciones penalS o administrativas
CESIÓNS PREVISTAS	Órganos xudiciais, Órganos da Administración do Estado e de Comunidade Autónoma con competencia en seguridade. ciudadana para dar traslado a las denuncias.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	O esixido por cada normativa en concreto.
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensíbles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude minima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .

2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.

3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.

Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.

No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.

Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.

No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.

O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".

Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO
Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .
14.- REVISION DO DOCUMENTO
Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado. de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – VIDEOVIXILANCIA	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	seguridade
CATEGORÍAS DE INTERESADOS	Propio interesado ou o seu representante legal
PROCEDENCIA DOS DATOS	Propio interesado
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: imaxe
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Forzas e Corpos da Seguridade , Órganos Xudiciais.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Máximo de 30 días
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE
1.- APLICACIÓNS INFORMÁTICAS
Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS
Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.
3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN
O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.
4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS
No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE : 1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento 2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións. 3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE
5.- procedemento DE IDENTIFICACIÓN
Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.
6.- procedemento DE AUTENTICACIÓN
O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .
7.- POLÍTICA DE CONTRASINAIS
- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas. - privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS - O límite de intentos errados está limitado: 3 - procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso. - Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas. - Periodicidade do cambio de contrasinal: ANUALMENTE - Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas
8.- CONTROL DE ACCESOS
Permisos de acceso aos usuarios: -Quen o concede, altera ou anula: o responsable de seguridade . -Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo -Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en

base ás funcións do usuario.
-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.
-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.
-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.
Autorización de accesos:
O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.
-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan

sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – ESCOLA INFANTIL	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.

DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Xestión administrativa de la escola infantil, XESTIÓN de prazas.
CATEGORÍAS DE INTERESADOS	Tutores e menores
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos; DNI;Data Nacemento; Dirección; Teléfono; Sinatura; Datos Académicos E profesionais; Económicos, Financeiros e de Seguros; Datos da unidade familiar; datos de saúde; Imaxe.
	ESPECIALMENTE SENSIBLES: Saúde.
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Entidade Privada encargada da XESTIÓN do espazo infantil de xogo.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles

perdas ou subtraccións.
3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:
-Quen o concede, altera ou anula: o responsable de seguridade .
-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo
-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.
-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.
-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.
-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.
Autorización de accesos:
O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.
-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén

o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .

2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.

3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.

Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.

No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.

Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.

No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL
As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento. O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ". Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.
13.- ACTUALIZACIÓN DO DOCUMENTO
Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .
14.- REVISION DO DOCUMENTO
Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado. de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – PARELLAS DE FEITO E MATRIMONIOS CIVÍS	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Tramitación e rexistro das parellas de feito e matrimonios civís
CATEGORÍAS DE INTERESADOS	Propio interesado ou o seu representante legal
PROCEDENCIA DOS DATOS	Propio interesado
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, Dirección, data de Nacemento, Sinatura
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Órganos xudiciais.

TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	-
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de

acceso.

- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.

realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – OMIC. OFICINA MUNICIPAL DE INFORMACION O CONSUMIDOR	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa el posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Prestar os servizos de información, orientación E asesoramento en materia de consumo.
CATEGORÍAS DE INTERESADOS	Cidadáns e residentes, Solicitantes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, dirección, teléfono, Sinatura, detalle da reclamación.
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Oficina De Consumo Da Xunta.
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite a supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com.

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE
1.- APLICACIÓNS INFORMÁTICAS
Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.
2.- XESTIÓN DE SOPORTES E DOCUMENTOS
Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.
3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:
O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.
-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase

ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – OFICINA MUNICIPAL DE TURISMO	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Prestar os servizos de información a visitantes, organización de actividades lúdicas para a cidadanía do CONCELLO e realización de enquisas para a elaboración de estatísticas.

CATEGORÍAS DE INTERESADOS	cidadanía, residentes e visitantes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, dirección, teléfono, características persoais, circusntancias sociais
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Xunta de Galicia
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	CARIÑO, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma

que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .

2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.

3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.

Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.

No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.

Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.

No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.

O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".

Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera

medida de seguridade reflectida no mesmo.
13.- ACTUALIZACIÓN DO DOCUMENTO
Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .
14.- REVISION DO DOCUMENTO
Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado. de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos. realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – CENTRO DE INFORMACIÓN Á MULLER	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa el posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Prestar servizo de apoio, axuda e asesoramento a mulleres en situación de exclusión, o mulleres víctimas de violencia de xénero.
CATEGORÍAS DE INTERESADOS	cidadanía, residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, características persoais, dirección, teléfono, Sinatura
	ESPECIALMENTE SENSIBLES: saúde
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Garda Civil, Policía Local, Administración de Xustiza
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Mentres no se solicite la supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA);

PROTECCIÓN DE DATOS	concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE

1.- APLICACIÓNS INFORMÁTICAS

Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.

2.- XESTIÓN DE SOPORTES E DOCUMENTOS

Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.

3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN

O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.

4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS

No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento

2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.

3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e

intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:

-Quen o concede, altera ou anula: o responsable de seguridade .

-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo

-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.

-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.

-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.

-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.

Autorización de accesos:

O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.

Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.

-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III

-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.

-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.

Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"

Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:

-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.

-As copias almacénanse DENTRO DAS INSTALACIÓNS

-As copias almacénanse cifradas: NON

-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.

-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.

Copias de recuperación:

-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.

procedementos de recuperación:

1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que

contar coa autorización do responsable de seguridade .

2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.

3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.

Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.

O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.

No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.

Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación indebida.

No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.

O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".

Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.

de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.

realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

REXISTRO DE ACTIVIDADE – OFICINA DE INFORMACIÓN Á XUVENTUDE	
RESPONSABLE DE TRATAMENTO	CONCELLO DE CARIÑO
REPRESENTANTE do responsable de tratamento	JOSE MIGUEL ALONSO PUMAR
DPO/RESPONSABLE DE SEGURIDADE	O responsable de seguridade es ALEJANDRA PARDO VAZQUEZ que ocupa o posto de SECRETARIA.
DIRECCIÓN DE CONTACTO	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA)
FINALIDADES DO TRATAMENTO	Prestar servicio de información e tramite de XESTIÓNs relativas o colectivo xoven do CONCELLO
CATEGORÍAS DE INTERESADOS	cidadanía, residentes.
PROCEDENCIA DOS DATOS	Propio interesado ou o seu representante legal.
CATEGORÍAS DE DATOS TRATADOS	IDENTIFICATIVOS: Nome e apelidos, DNI, características persoais, dirección, teléfono, Sinatura, académicos e profesionais
	ESPECIALMENTE SENSIBLES:
	OUTROS DATOS TIPIFICADOS:
CESIÓNS PREVISTAS	Xunta de Galicia
TRANSFERENCIAS INTERNACIONAIS	-
PRAZO DE CONSERVACIÓN	Durante a prestación do servizo e mentres no se solicite a supresión dos mesmos
SISTEMA DE TRATAMENTO	Mixto
DEPENDENCIA EXERCICIO DEREITOS PROTECCIÓN DE DATOS	AVDA PAZ, 2, 15360 - CARIÑO (A CORUÑA); concello@concellodecarino.com

DESCRICIÓN DE MEDIDAS TÉCNICAS E ORGANIZATIVAS DE SEGURIDADE
1.- APLICACIÓNS INFORMÁTICAS
Respecto das aplicacións informáticas con acceso autorizado, véxase o ANEXO III no que se facilita a relación das mesmas.
2.- XESTIÓN DE SOPORTES E DOCUMENTOS
Os soportes que conteñan datos de carácter persoal deberán permitir identificar o tipo de información que conteñen, ser inventariados. En caso de datos considerados especialmente sensibles segundo o Regulamento UE, serán almacenados nun lugar de acceso restrinxido ao que só terán acceso as persoas con autorización que se relacionan a en o ANEXO III.
3.- SOPORTES AUTOMATIZADOS E SISTEMAS DE INFORMACIÓN
O equipamento informático no que se trata datos de carácter persoal, atópase descrito no ANEXO III.
4.- EXECUCIÓN DO TRATAMENTO FORA DOS LOCAIS
No caso de que os soportes que conteñan datos de carácter persoal saian FORA das instalacións do responsable de tratamento deberán adoptarse as seguintes medidas de SEGURIDADE :

1.- contar coa autorización demostrable do responsable de seguridade ou representante do responsable de tratamento
2.- en caso de soporte manual, a documentación irá protexida nun cartafol, maletín ou calquera outro soporte que poida ir pechado e/ou precintado para protexelo de posibles perdas ou subtraccións.
3.- cando os datos para trasladar sexan especialmente sensibles, será requisito indispensable o rexistro de entrada e saída de documentación dispoñible no ANEXO VII E VIII DO presente Documento de SEGURIDADE

5.- procedemento DE IDENTIFICACIÓN

Todo usuario con acceso a datos deberá estar identificado e contará cun usuario de acceso á información en soporte automatizado.

6.- procedemento DE AUTENTICACIÓN

O acceso de cada usuario identificado, deberá protexerse mediante un contrasinal. De forma que, para acceder a calquera soporte informatizado cada persoa con acceso a datos autorizado, deberá introducir o seu usuario identificativo e o seu contrasinal de SEGURIDADE .

7.- POLÍTICA DE CONTRASINAIS

- procedementos de asignación de contrasinais: os contrasinais son asignadas mediante un procedemento definido polo responsable de seguridade que será o encargado de custodialas.
- privacidade: os contrasinais deberán ter unha lonxitude mínima de 7 caracteres, ALFANUMÉRICOS
- O límite de intentos errados está limitado: 3
- procedementos de distribución de contrasinais: os contrasinais se proporcional por parte do responsable de seguridade de forma persoal ao propio interesado. Unha vez entregada, o usuario deberá destruír o soporte a través do cal se lle informou do seu contrasinal de acceso.
- Almacenamento: gárdanse de forman interna e inintelixible polo Responsable de seguridade, de maneira que permanecen almacenadas de forma protexida, dado que só o Responsable de seguridade, terá acceso ao almacenamento das mesmas.
- Periodicidade do cambio de contrasinal: ANUALMENTE
- Garantía de integridade: Cada usuario ten un identificador que se autentica mediante contrasinal. Os identificadores de usuario E o contrasinal de acceso son de uso persoal e intransferible E non poden ser compartidas

8.- CONTROL DE ACCESOS

Permisos de acceso aos usuarios:
-Quen o concede, altera ou anula: o responsable de seguridade .
-Alcance do acceso: o necesario para desenvolver as funcións propias do posto de traballo
-Criterio de concesión, alteración ou anulación do acceso: polo Responsable de seguridade en base ás funcións do usuario.
-Características do control de acceso aos equipos: cada persoa con acceso a datos terá un usuario e un contrasinal de acceso diferenciados.
-Características do control de acceso: limítase o acceso a usuarios non autorizados. Pódese comprobar o detalle de usuarios autorizados no ANEXO III.
-O detalle de usuarios actualizarase cada vez que se incorpore novo persoal ou ben cause baixa algún traballador con acceso a datos.
Autorización de accesos:
O acceso aos computadores E/ou soportes nos que se tratan e/ou almacenen datos de carácter persoal autorízase en virtude de que se trate dunha persoa que necesite o acceso aos mesmos para o desempeño das súas funcións.
Relación de usuarios actualizada: o responsable de seguridade encargarase de manter actualizada a relación de persoal con acceso autorizado aos ficheiros/rexistro de actividades.

-Suxeitos: a relación dos usuarios que teñen acceso autorizado, así como os seus perfís, atópase detallada no ANEXO III.
-Procesos: as aplicacións con acceso autorizado están identificadas no ANEXO III
-Baixa de usuarios: ao dar de baixa un usuario con acceso autorizado, darase de baixa tamén o seu identificador e contrasinal. Non podendo reutilizar nunca un identificador ou un contrasinal de acceso.
-Alta dun usuario: para conceder o acceso autorizado a un usuario realizarase atendendo á política de contrasinais descrita no apartado anterior, así como a política de control E autorización de accesos descritas neste mesmo.
Nos accesos aos datos especialmente sensibles, rexistrarase por cada acceso a identificación do usuario, a data e hora en que se realizou, o ficheiro accedido, o tipo de acceso E se foi autorizado ou denegado. Para o rexistro de accesos a soportes non automatizados, cumprimentarase a táboa do ANEXO IV: "Rexistro de accesos de nivel alto"
Os datos do rexistro de accesos conservásense durante un período de polo menos dous anos.

9.- COPIAS DE RESPALDO E RECUPERACIÓN DOS DATOS

Copias de respaldo:
-Descrición da copia: a copia de seguridade execútase en SERVIDOR E DISCO DURO.
-As copias almacénanse DENTRO DAS INSTALACIÓNS
-As copias almacénanse cifradas: NON
-Programación de copia: estableceuse un protocolo de realización de copias de seguridade, pautándose a realización de copias de seguridade sempre coa mesma periodicidade.
-Periodicidade: cunha periodicidade SEMANALMENTE fanse copias de seguridade dos ficheiros que conteñen os datos de carácter persoal.
Copias de recuperación:
-Descrición de procedementos: semestralmente, o responsable de tratamento encárgase de verificar a correcta definición e funcionamento e aplicación dos procedementos de realización de copias de respaldo e recuperación dos datos. As probas non se realizan con datos reais.
procedementos de recuperación:
1.- Cumprimentarase unha solicitude (ANEXO VI) por parte do peticionario que terá que contar coa autorización do responsable de seguridade .
2.- Procederase a trasladar a orde de recuperación ao persoal autorizado, enviando copia ao solicitante indicando a aprobación ou denegación.
3.- O responsable de seguridade anotará o feito no Rexistro de Incidencias.

10.- PROCEDEMENTOS DE INCIDENCIAS

O responsable de tratamento recollerá tantas incidencias de seguridade como se produzan sobre os datos de carácter persoal que se tratan.
Infórmase a todo o persoal con acceso a datos do procedemento para seguir mediante a "Circular informativa sobre medidas de seguridade de protección de datos"

11.- REXISTRO DE INCIDENCIAS

As incidencias detállanse no ANEXO IX: REXISTRO DE INCIDENCIAS.
O responsable de seguridade anotará o tipo de Incidencia e o detalle da mesma. Encargarase ademais de contactar coas persoas oportunas para corrixir a incidencia.
No caso de que a incidencia que se produciu afecte a datos especialmente sensibles detallarase ademais, as accións que se levaron a cabo para proceder á recuperación dos mesmos.
Cando sexa probable que a violación da seguridade. dos datos persoais entrañe un alto risco para os dereitos e liberdades das persoas físicas, comunicarase ao interesado sen dilación

indebida.
No caso de que a comunicación supoña un esforzo desproporcionado, a comunicación realizarase por un medio público, de forma que se informe de maneira igualmente efectiva aos interesados.

12.- FUNCIONS DO PERSOAL

As funcións do persoal de CONCELLO DE CARIÑO con acceso aos datos de carácter persoal están descritas no ANEXO III do presente documento.
O responsable de tratamento emitiu un acordo de confidencialidade, así como unha circular na que se establecen as directrices para todo o persoal con acceso a datos da organización, e informouse ao responsable de seguridade das súas funcións mediante o "Nomeamento de responsable de seguridade ".
Ademais, o persoal terá acceso a este documento de seguridade para consultar calquera medida de seguridade reflectida no mesmo.

13.- ACTUALIZACIÓN DO DOCUMENTO

Actualizarase cando sexa necesario, conforme aos cambios que se produzan no sistema de información ou na normativa vixente en materia de medidas de seguridade .

14.- REVISION DO DOCUMENTO

Será revisado se se producen cambios relevantes no sistema de información ou na organización do mesmo, así como na relación de persoal con acceso autorizado.
de forma programada realizarase un punto de control anual, que permitirá unha análise exhaustiva do grao de cumprimento das medidas de seguridade descritas no presente documento de seguridade, así como unha revisión de posibles cambios no protocolo de tratamento de datos.
realizarase unha auditoría cada dous anos para revisar a adecuación das medidas de seguridade establecidas, cumprindo así co establecido no Real Decreto 1720/2007

ANEXO III:

RELACIÓN DE USUARIOS, ENCARGADOS DE TRATAMENTO E APLICACIÓNS CON ACCESO AUTORIZADO. DESCRICIÓN DO SISTEMA INFORMÁTICO