

**CONCELLO DE CARBALLO**

C.I.F.: P1501900C

Praza do Concello S/N

Teléfono 981 70 41 00

[www.carballo.gal](http://www.carballo.gal)

[infocarballo@carballo.gal](mailto:infocarballo@carballo.gal)

15100 CARBALLO - A Coruña



**TEMA 1. A Protección de Datos. A protección de datos da persoa traballadora: Responsable do tratamento. Finalidade, Lexitimación e prazos de conservación. Destinatario dos seus datos. Exercicio de dereitos. Transferencias internacionais. Obrigas que asume a persoa traballadora: Obrigas de protección de datos. Confidencialidade e segredo profesional.**

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



## A Protección de Datos

### 1. Protección de Datos da Persoa Traballadora

De conformidade co Regulamento (UE) 2016/679 (RGPD) e coa Lei Orgánica 3/2018 (LOPDGDD), infórmase a toda persoa traballadora dos seguintes puntos:

#### 1.1. Responsable do Tratamento

Concello de Carballo

NIF: [pendente de completar]

Domicilio: Praza do Concello, s/n. 15100 Carballo (A Coruña)

Contacto do Delegado/a de Protección de Datos: [indicar dirección de contacto]

#### 1.2. Finalidade, Lexitimación e Prazos de Conservación

A finalidade do tratamento é:

a) Exercicio da potestade de dirección e control da actividade laboral ou funcional, xestión de nóminas e recursos humanos, control de desprazamentos, exercicio da potestade disciplinaria, rexistro de xornada, así como outros aspectos relacionados coa prestación do servizo.

A base legal do tratamento dos datos é a execución do contrato laboral ou a vinculación como empregado/a público/a, e conservanse polo tempo establecido no Real Decreto Lexislativo 5/2000, de 4 de agosto, polo que se aproba o texto refundido da Lei sobre Infraccións e Sancións na Orde Social.

Tamén se terá en conta o disposto no Real Decreto Lexislativo 2/2015, de 23 de outubro (Estatuto dos Traballadores) e no Real Decreto Lexislativo 5/2015, de 30 de outubro (Estatuto Básico do Empregado Público).

b) Cumprimento das obrigas en materia de Seguridade Social.

A base legal é o cumprimento dunha obrigación legal imposta polo Real Decreto Lexislativo 8/2015, de 30 de outubro, polo que se aproba o texto refundido da Lei Xeral da Seguridade Social.

c) Xestión da prevención de riscos laborais.

A base legal é o cumprimento dunha obrigación legal imposta pola Lei 31/1995, de 8 de novembro, de Prevención de Riscos Laborais, e demais normativa aplicable. Os datos conservanse polo prazo legal establecido.

d) Xestión contable.

A base legal é o cumprimento dunha obrigación legal segundo o Real Decreto de 22 de agosto de 1885, polo que se publica o Código de Comercio, e conservanse polo tempo indicado nesta norma e na demais lexislación aplicable.

e) Xestión fiscal.

A base legal é o cumprimento dunha obrigación legal establecida na Lei 58/2003, Xeral Tributaria, e conservanse polo prazo que determine a norma.

#### 1.3. Destinatarios dos seus Datos

Procederase á cesión dos datos persoais da persoa traballadora ás seguintes entidades:

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### TEMARIO TICS

a) Administracións Públicas competentes, tales como a Oficina Pública de Emprego, a Tesouraría Xeral da Seguridade Social e a Axencia Tributaria, co fin de dar cumprimento ás obrigas legais establecidas.

b) Entidades bancarias designadas pola persoa traballadora, co obxectivo de realizar os ingresos correspondentes ás retribucións derivadas do seu traballo, conforme o disposto no Real Decreto Legislativo 2/2015, de 23 de outubro (Estatuto dos Traballadores) e no Real Decreto Legislativo 5/2015, de 30 de outubro (Estatuto Básico do Empregado Público).

c) Entidades aseguradoras, en base ao interese lexítimo, para a contratación e xestión dos riscos asegurados que correspondan.

d) En calquera outro caso de cesión ou utilización de datos diferente dos indicados nos apartados anteriores, a persoa traballadora será informada previamente, mediante os canais habituais do Concello de Carballo, de acordo coa normativa vixente.

#### 1.4. Exercicio de Dereitos

A persoa traballadora pode exercer os seus dereitos de acceso, rectificación, supresión, limitación do tratamento, oposición e portabilidade dos datos persoais.

Para iso, deberá enviar unha solicitude por correo electrónico ao Delegado/a de Protección de Datos, quen facilitará o modelo correspondente.

Lémbrese ademais que a persoa traballadora ten dereito a presentar unha reclamación ante a Autoridade de Control competente, cando considere que os seus dereitos foron vulnerados.

En España, a autoridade competente é a Axencia Española de Protección de Datos<sup>1</sup>(AEPD).

#### 1.5. Transferencias Internacionais

Infórmase á persoa traballadora de que non se realizarán transferencias internacionais de datos a terceiros países nin organizacións internacionais.

### 2. Obrigas que asume a Persoa Traballadora

#### 2.1. Obrigas de Protección de Datos

A persoa vinculada ao Responsable do Tratamento deberá cumprir en todo momento as medidas e procedementos establecidos no Regulamento Interno de Protección de Datos e Seguridade da Información do Concello de Carballo.

De acordo co artigo 5.1.f) do Regulamento (UE) 2016/679 (RGPD), a persoa traballadora comprométese expresamente a manter a confidencialidade de toda a información relativa a datos de carácter persoal tratada pola entidade pública, e a non revelala a persoas non autorizadas.

Esta obriga mantense incluso despois da finalización da relación laboral ou profesional.

O incumprimento destas obrigas poderá dar lugar á existencia de responsabilidades administrativas, segundo o establecido no Título VIII do RGPD e na Lei Orgánica 3/2018 (LOPDGDD), así como a outras responsabilidades de distinta natureza.

En concreto, a persoa traballadora comprométese a:

1. Devolver toda a documentación impresa á que teña acceso durante a súa xornada laboral ao rematar o seu uso, non deixando documentos sobre a mesa sen supervisión.

- Se se envían fax ou se fan fotocopias/escáneos de documentos, deberán retirarse de inmediato dos dispositivos correspondentes e gardarse no seu lugar habitual.

---

1. [www.aepd.es](http://www.aepd.es)

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



2. Pechar e bloquear o equipo informático antes de ausentarse, especialmente cando conteña información confidencial en formato electrónico.

3. Manter as mesas de traballo limpas e ordenadas.

- Non deben quedar documentos con datos persoais á vista.
- A documentación en uso debe gardarse baixo chave ou devolverse ao arquivo ao rematar.

4. Evitar que queden documentos impresos ou retidos nas bandexas de saída das impresoras, fax ou escáner.

- A persoa traballadora retirará os documentos conforme se impriman.

5. Non introducir nin extraer soportes con datos persoais (USB, discos externos, etc.) fóra das dependencias do Concello, salvo autorización expresa.

### 2.2. Confidencialidade e Segredo Profesional

A persoa traballadora comprométese expresamente, tanto durante a vixencia do contrato como despois da súa extinción, a non difundir nin revelar a terceiros ningunha información da entidade pública á que teña acceso pola súa actividade laboral.

Tampouco poderá utilizar dita información en beneficio propio nin de terceiras persoas (familiares, amizades, empresas, etc.).

Esta prohibición abrangue calquera tipo de reprodución ou almacenamento da información —en formato físico ou dixital— relativa a:

- cidadáns,
- procedementos e sistemas internos,
- programas informáticos, ou
- calquera outro contido de carácter reservado.

Só se poderá acceder ou reproducir esa información cando sexa estritamente necesario para o desempeño do posto de traballo, e sempre dentro do ámbito da entidade pública.

Todos os documentos, notas e informes elaborados pola persoa traballadora durante a súa relación laboral son propiedade do Concello de Carballo e deberán ser custodiados adecuadamente.

O incumprimento desta cláusula poderá ser considerado causa xustificada de extinción do contrato, sen dereito a indemnización, e poderá dar lugar ademais á reclamación de danos e prexuízos derivados da violación do deber de confidencialidade e segredo profesional.

**CONCELLO DE CARBALLO**  
C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



**TEMA 2. Uso dos Sistemas Informáticos Municipais.** Obxecto, alcance, vixencia, revisión e avaliación, marco de referencia. Utilización do equipamento informático e de comunicacións. Identificación e autenticación. Acceso de terceiros aos edificios municipais. Uso do correo electrónico corporativo. Acceso a internet e outras ferramentas de colaboración. Normativa en materia de uso de redes sociais. Incidentes en materia de seguridade. Compromiso dos usuarios. Monitorización e aplicación desta normativa. Postos de traballo e os seus equipos. Traballo fora das instalacións. Incumprimento da normativa.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



# Uso dos Sistemas Informáticos Municipais

## 1. Obxecto

A continua evolución tecnolóxica que se está a experimentar na administración pública, e máis en concreto no Concello de Carballo, encamiñándonos cara a unha administración totalmente dixital, cunha xestión considerable de volumes de datos, ferramentas específicas e gran variedade de dispositivos, implica a existencia dun sistema informático complexo no que a seguridade debe estar garantida en todo momento.

O persoal usuario debe ser consciente da importancia desta seguridade e dispoñer dun conxunto de normas de obrigado cumprimento respecto do uso dos sistemas informáticos.

Por iso, co fin de garantir a correcta xestión do sistema, o Concello de Carballo acorda aprobar as seguintes normas de utilización do Sistema Informático da Institución, para asegurar o bo uso dos medios técnicos postos á disposición das persoas usuarias.

## 2. Alcance

Esta normativa é de aplicación a todo o ámbito de actuación do Concello de Carballo, e o seu contido trae causa das directrices de carácter máis xeral definidas na Política de Seguridade da Información.

A presente normativa é de aplicación e de obrigado cumprimento para todo o persoal que, de maneira permanente ou eventual, preste os seus servizos no Concello de Carballo, incluíndo o persoal de provedores externos, cando sexan usuarios dos Sistemas de Información do Concello.

No ámbito da presente normativa, enténdese por *usuario* calquera persoa, pertencente ou allea ao Concello de Carballo, así como persoal de organizacións privadas externas, entidades colaboradoras ou outras que manteñan algún tipo de vinculación co Concello de Carballo e que utilicen ou teñan acceso aos seus Sistemas de Información.

## 3. Marco de referencia

O presente procedemento fundaméntase no marco de referencia descrito no documento "Normativa de marco de referencia: lexislación e normativa aplicable", que recolle a normativa legal e técnica en materia de seguridade da información e administración electrónica.

## 4. Vixencia

A presente Normativa de Seguridade da Información do Concello de Carballo foi aprobada polo Comité de Seguridade, establecendo deste xeito as directrices xerais para o uso axeitado dos recursos de tratamento da información que o Concello pon a disposición das persoas usuarias para o exercicio das súas funcións.

Correlativamente, as persoas usuarias asumen as obrigas descritas nesta normativa, comprometéndose a cumprir o disposto nos seguintes epígrafes.

Calquera modificación posterior entrará en vigor inmediatamente despois da súa publicación por parte do Concello de Carballo.

## 5. Revisión e avaliación

A xestión desta normativa corresponde ao Comité de Seguridade da Información, que é competente para:

- Interpretar as dúbidas que poidan xurdir na súa aplicación.
- Proceder á súa revisión cando sexa necesario para actualizar o seu contido ou se cumpran os prazos máximos establecidos para iso.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Verificar a súa efectividade.
- Anualmente (ou cunha periodicidade menor, se existen circunstancias que así o aconsellen), o Comité de Seguridade revisará a presente Normativa, que, no caso de producirse modificacións, será sometida á aprobación do propio Comité de Seguridade.
- A revisión orientarase tanto á identificación de oportunidades de mellora na xestión da seguridade da información, como á adaptación aos cambios producidos no marco legal, na infraestrutura tecnolóxica ou na organización xeral.
- A persoa Responsable de Seguridade será a encargada da custodia e difusión da versión aprobada deste documento.

### 6. Utilización do equipamento informático e de comunicacións

O Concello de Carballo facilita ás persoas usuarias que así o precisen os equipos informáticos e dispositivos de comunicación, tanto fixos como móbiles, necesarios para o desenvolvemento da súa actividade profesional.

Deste xeito, os datos, dispositivos, programas e servizos informáticos que o Concello de Carballo pon a disposición das persoas usuarias deberán empregarse exclusivamente para o exercicio das funcións encomendadas, é dicir, para fins profesionais.

Calquera uso dos recursos con fins distintos aos autorizados está estritamente prohibido.

En termos xerais, o ordenador persoal (PC) constitúe o recurso informático que permite o acceso das persoas usuarias aos Sistemas de Información e servizos informáticos do Concello de Carballo, sendo un elemento esencial na cadea de seguridade destes sistemas. Por esta razón, é necesario adoptar unha serie de precaucións e establecer normas para o seu uso axeitado.

Este apartado refírese especificamente a todos os equipos facilitados polo Concello de Carballo para a súa utilización por parte das persoas usuarias, incluíndo equipos de sobremesa, portátiles e dispositivos móbiles con capacidade de acceso aos Sistemas de Información da organización.

#### 6.1. Normas xerais

- Os ordenadores persoais deberán empregarse unicamente para fins corporativos e como ferramenta de apoio ás competencias profesionais das persoas usuarias autorizadas.
- Unicamente o persoal autorizado poderá distribuír, instalar ou desinstalar software e hardware, ou modificar a configuración de calquera dos equipos, especialmente naqueles aspectos que poidan repercutir na seguridade dos Sistemas de Información do Concello de Carballo.
- Cando sexa preciso instalar dispositivos non fornecidos polo Concello de Carballo, deberá solicitarse autorización previa á Unidade de Informática.
- Está prohibido alterar, sen a debida autorización, calquera dos compoñentes físicos ou lóxicos dos equipos informáticos e dispositivos de comunicación, salvo autorización expresa da Unidade de Informática.
- Agás autorización expresa da Unidade de Informática, as persoas usuarias non disporán de privilexios de administración sobre os equipos.
- As persoas usuarias deberán facilitar ao persoal de soporte técnico o acceso aos seus equipos para tarefas de reparación, instalación ou mantemento.
- Este acceso limitarase exclusivamente ás accións necesarias para o mantemento ou resolución dos problemas detectados no uso dos recursos informáticos e de comunicación, e finalizará unha vez completadas as tarefas correspondentes.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



TEMARIO TICS

Se o persoal de soporte técnico detectase calquera anomalía que indique unha utilización dos recursos contraria á presente norma, poñerá en coñecemento do Responsable de Seguridade, quen adoptará as medidas correctoras oportunas.

- Os ordenadores persoais da organización deberán manter actualizados os parches de seguridade de todos os programas instalados. Deberase prestar especial atención á correcta actualización, configuración e funcionamento dos programas antivirus e cortafuegos (*firewall*).
- As persoas usuarias deberán notificar á Unidade de Informática do Concello de Carballo, coa maior brevidade posible, calquera comportamento anómalo do seu ordenador persoal, especialmente cando existan sospeitas de que se produciu algún incidente de seguridade no mesmo.
- O coñecemento e a non notificación dunha incidencia por parte dunha persoa usuaria serán considerados como unha falta contra a seguridade da información do Concello de Carballo.
- A persoa usuaria debe ser consciente das ameazas provocadas por malware. Moitos virus e troianos requiren a participación activa das persoas usuarias para propagarse, xa sexa a través de CD/DVD, memorias USB, mensaxes de correo electrónico ou da instalación de programas descargados desde Internet.
- É imprescindible, polo tanto, vixiar o uso responsable dos equipos para reducir este risco.
- A persoa usuaria será responsable de toda a información extraída fóra da organización mediante dispositivos como memorias USB, CD, DVD, etc., que lle foran asignados. É obrigatorio facer un uso responsable destes dispositivos, especialmente cando conteñan información sensible, confidencial ou protexida.
- O cese de actividade de calquera persoa usuaria deberá ser comunicado de forma inmediata á Unidade de Informática, co fin de que lle sexan retirados os recursos informáticos que lle foran asignados.
- De igual modo, cando os medios informáticos ou de comunicación proporcionados polo Concello de Carballo estean asociados ao desempeño dun determinado posto ou función, a persoa que os teña asignados deberá devolvelos inmediatamente á unidade responsable no momento en que finalice a súa vinculación con dito posto ou función.

### 6.2. Usos especificamente prohibidos

Están terminantemente prohibidos os seguintes comportamentos:

- A utilización de calquera tipo de software daniño (*malware*).
- O uso de programas que, pola súa natureza, realicen un consumo abusivo da rede.
- A conexión á rede informática corporativa de calquera equipo ou dispositivo non facilitado polo Concello de Carballo, sen a autorización previa da Unidade de Informática.
- A utilización de conexións ou medios inalámbricos baseados en tecnoloxías WiFi, Bluetooth ou infravermellos que non estean debidamente autorizados polo Concello de Carballo.
- O uso de dispositivos USB, teléfonos móbiles ou outros elementos como mecanismo alternativo de conexión a Internet, salvo autorización expresa e previa solicitude á Unidade de Informática.
- A instalación e/ou utilización de programas ou contidos que vulneren a lexislación vixente en materia de propiedade intelectual.
- Este comportamento estará suxeito ás previsións disciplinarias, administrativas, civís ou penais recollidas nas leis.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Intentar distorsionar ou falsear os rexistros LOG do sistema.
- Intentar descifrar contrasinais, sistemas ou algoritmos de cifrado, así como calquera outro elemento de seguridade que interveña nos procesos telemáticos do Concello de Carballo.
- Obstaculizar voluntariamente o acceso doutras persoas usuarias á rede, mediante o consumo masivo de recursos informáticos ou telemáticos, así como realizar accións que poidan danar, interromper ou xerar erros nos devanditos sistemas.
- A utilización de plataformas externas para compartir información, como por exemplo Dropbox, WeTransfer, Mega, ou calquera outra de natureza similar.

### 6.3. Normas específicas para equipos portátiles e móbiles

- Os equipos portátiles e móbiles serán asignados pola Unidade de Informática, por petición da persoa Responsable da Área correspondente.
- Existirá un inventario actualizado dos equipos portátiles e móbiles, do cal será responsable a Unidade de Informática, encargada da súa xestión e mantemento.
- Este tipo de dispositivos permanecerán baixo a custodia da persoa usuaria que os empregue, quen deberá adoptar as medidas necesarias para evitar danos, substraicións ou accesos non autorizados.
- En caso de substraición ou perda destes equipos, deberá comunicarse inmediatamente o feito á Unidade de Informática, para a adopción das medidas correspondentes e a baixa no inventario.
- Os equipos portátiles e móbiles deberán empregarse unicamente para fins institucionais, especialmente cando se utilicen fóra das instalacións do Concello de Carballo.
- As persoas usuarias destes equipos serán responsables de que non sexan empregados por terceiras persoas alleas ao Concello de Carballo ou non autorizadas para iso.
- As persoas usuarias de equipos portátiles deberán realizar conexións periódicas á rede corporativa, segundo as instrucións proporcionadas polo Concello de Carballo, co fin de permitir a actualización das aplicacións, do sistema operativo, das sinaturas antivirus e demais medidas de seguridade.
- Cando a tipoloxía da información tratada así o requira, os ordenadores portátiles afectados deberán contar co disco duro cifrado, dispoñer de software que garanta un arranque seguro, así como mecanismos de auditoría capaces de crear un rexistro por cada ficheiro extraído do sistema, por calquera medio (rede, dispositivos extraíbles, impresoras, etc.).
- As persoas usuarias non disporán de privilexios de administración sobre os equipos portátiles, estando prohibido realizar modificacións de hardware ou software nos mesmos.
- Corresponderalle á Unidade de Informática levar a cabo calquera cambio ou actualización técnica necesaria.

### 6.4. Uso de memorias USB

- Con carácter xeral, o uso de memorias USB no Concello de Carballo non está autorizado.
- En caso de ser necesario, a autorización deberá ser concedida pola persoa Responsable da Área correspondente.
- En todo caso, as memorias USB deberán ser fornecidas polo propio Concello.
- Por razóns de seguridade, os portos USB dos postos de usuario permanecerán deshabilitados.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### TEMARIO TICS

- No caso de que sexa necesaria a súa habilitación, esta deberá xustificarse debidamente pola persoa usuaria e requirirá autorización previa tanto da Responsable da Área como da Responsable do Sistema.
- No caso de que se autorice o uso do porto USB dun posto de traballo, as memorias USB utilizadas serán as proporcionadas polo Concello de Carballo, e deberán cumprir coas normas de seguridade da organización.
- Lémbrese que as memorias USB están destinadas exclusivamente a un uso profesional, como ferramenta para o transporte temporal de ficheiros, e non como medio de almacenamento permanente.
- O Concello de Carballo poderá poñer á disposición das persoas usuarias unidades de almacenamento en rede, asociadas ás aplicacións, servizos e sistemas municipais, que poderán empregarse con esta finalidade.
- A perda ou subtracción dunha memoria USB, indicando o seu contido, deberá ser comunicada inmediatamente á Unidade de Informática.

#### 6.5. Gravación de CD e DVD

- Con carácter xeral, o uso de equipos gravadores de CD e DVD no Concello de Carballo non está autorizado.
- En caso necesario, a autorización deberá ser emitida pola persoa Responsable da Área correspondente.

#### 6.6. Impresoras en rede e fotocopiadoras

- Con carácter xeral, deberán empregarse as impresoras en rede e as fotocopiadoras corporativas.
- A súa instalación deberá contar coa autorización previa da persoa responsable da unidade solicitante.
- En ningún caso as persoas usuarias poderán facer uso de impresoras, fotocopiadoras ou equipos de fax non proporcionados polo Concello de Carballo e, por tanto, non inventariados oficialmente.
- Cando se imprima documentación, esta deberá permanecer o menor tempo posible nas bandexas de saída das impresoras, co obxecto de evitar que terceiras persoas poidan acceder a ela.
- Deberase recordar recoller os orixinais da fotocopiadora unha vez finalizado o proceso de copia.
- Se se atopase documentación sensible, confidencial ou protexida abandonada nunha fotocopiadora ou impresora, a persoa usuaria deberá tentar localizar á súa propietaria para que a recolla de inmediato.
- No caso de descoñecer a identidade da propietaria ou non poder localizala, deberá comunicarse o achado inmediatamente ao Responsable de Seguridade.

#### 6.7. Dixitalización de documentos

- Con carácter xeral, cando se dixitalicen documentos, a persoa usuaria deberá ser especialmente coidadosa na selección do directorio compartido no que deban almacenarse as imaxes obtidas, especialmente se conteñen información sensible, confidencial ou protexida.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### TEMARIO TICS

- Deberase recordar recoller os orixinais do escáner unha vez finalizado o proceso de dixitalización.
- Se se atopase documentación sensible ou confidencial abandonada nun escáner, a persoa usuaria deberá tentar localizar á súa propietaria para que a recolla inmediatamente.
- No caso de descoñecer a identidade da propietaria ou non poder localizala, deberá poñelo de inmediato en coñecemento da persoa Responsable de Seguridade.

#### 6.8. Telefonía móbil

- Debe evitarse perder de vista o dispositivo e, en caso de perda ou roubo, deberase informar o antes posible para proceder ao seu bloqueo inmediato.
- Os dispositivos deberán ter activado o bloqueo por PIN e, sempre que o permitan, habilitarase a opción de bloqueo automático do terminal tras un tempo de inactividade, así como a solicitude dunha contrasinal para o seu desbloqueo.
- Non se permite a modificación do hardware ou do software do dispositivo móbil sen a autorización previa da Unidade de Informática.
- Sempre que sexa posible, non se almacenará información sensible nos dispositivos móbiles, asegurándose de limpar periodicamente os ficheiros temporais.
- Poderanse empregar programas de cifrado co fin de protexer a información sensible contida no dispositivo.
- Só se realizarán conexións de dispositivos móbiles a redes sen fíos (WiFi) que ofrezan garantías de confianza e seguridade.
- O Bluetooth deberá permanecer desactivado cando non se utilice, configurado como oculto e con contrasinal.
- Non se permitirá a conexión con dispositivos Bluetooth de orixe descoñecido, e deberá evitarse o emparellamento en lugares públicos.
- A persoa usuaria será responsable de realizar as copias de seguridade da información almacenada no dispositivo móbil.

#### 6.9. Coidado e protección da documentación impresa

- A documentación impresa que conteña datos sensibles, confidenciais ou protexidos deberá ser especialmente resgardada, de maneira que só teña acceso a ela o persoal autorizado. Esta documentación deberá recollese rapidamente das impresoras e fotocopiadoras e ser custodiada en armarios pechados con chave.
- Cando conclúa a vida útil dos documentos impresos que conteñan información sensible, confidencial ou protexida, deberán ser eliminados nas máquinas destructoras do Concello de Carballo, de forma que a información non poida ser recuperada nin reconstruída.
- Se, unha vez impresa, fose necesario almacenar dita documentación, a persoa usuaria deberá asegurarse de protexer adecuadamente e baixo chave aquelas copias que conteñan información sensible, confidencial, protexida ou crítica para o seu traballo.

#### 6.10. Pizarras

- Antes de abandonar as salas ou permitir o acceso de persoas alleas, deberán limparse axeitadamente as pizarras das salas de reunións ou despachos, coidando que non permaneza ningún tipo de información sensible nin datos que poidan ser reutilizados por terceiras persoas.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



TEMARIO TICS

### 7. Identificación e autenticación

- As persoas usuarias disporán dun código de usuario e dunha contrasinal para acceder aos Sistemas de Información do Concello de Carballo, sendo responsables da súa custodia e de toda actividade realizada mediante o seu acceso autorizado.
- O código de usuario é único e intransferible para cada persoa na organización, e é independente do ordenador ou terminal dende o que se realice o acceso.
- As persoas usuarias non deberán revelar nin entregar, baixo ningún concepto, as súas credenciais de acceso nin a tarxeta criptográfica a outra persoa, nin mantelas por escrito á vista ou ao alcance de terceiros.
- As persoas usuarias non poderán utilizar o acceso autorizado doutra persoa, aínda que dispoñan da súa autorización.
- Se unha persoa usuaria sospeita que as súas credenciais están sendo utilizadas por outra, deberá cambiar inmediatamente a contrasinal e comunicar o incidente de seguridade á Unidade de Informática.
- As persoas usuarias deberán empregar contrasinais seguras, de acordo coa política de calidade de contrasinais establecida polo Concello de Carballo.
- As contrasinais non deberán estar compostas unicamente por palabras de dicionario nin por termos previsibles ou asociados á persoa usuaria, como nomes de familiares, enderezos, matrículas de vehículos, números de teléfono, nomes comerciais, organizacións, identificadores de usuario, DNI, etc.
- Se, en algún momento, unha persoa usuaria recibise unha chamada telefónica solicitándolle o seu nome de usuario e contrasinal, non deberá facilitar en ningún caso eses datos e deberá comunicar inmediatamente este feito á Unidade de Informática.

### 8. Acceso de terceiras persoas aos edificios

As terceiras persoas alleas ao Concello de Carballo que, de maneira eventual, permanezan nos seus edificios, instalacións ou dependencias deberán observar as seguintes normas:

- O persoal alleo ao Concello de Carballo que deba acceder temporalmente aos Sistemas de Información da entidade deberá facelo sempre baixo a supervisión dun membro acreditado do Concello de Carballo (persoa responsable).
- Calquera incidente que se produza antes ou durante o acceso ás instalacións do Concello de Carballo deberá poñerse en coñecemento da persoa responsable correspondente.
- Para os accesos de terceiras persoas aos sistemas de información do Concello de Carballo, e sempre que sexa posible, crearánselles usuarios temporais, que serán eliminados inmediatamente despois de concluído o seu traballo.
- Se, de maneira excepcional, fose necesario empregar identificadores de usuarios xa existentes, unha vez finalizadas as tarefas realizarase o cambio inmediato das contrasinais dos usuarios utilizados.
- Estas persoas deberán cumprir rigorosamente a presente Normativa de uso, así como o resto da normativa de seguridade do Concello de Carballo, na parte que lles sexa aplicable.
- Para acceder aos edificios, instalacións ou dependencias do Concello de Carballo deberán dispoñer da correspondente documentación de identificación persoal admitida en dereito (*DNI, pasaporte, etc.*), e figurar na relación nominal previamente proporcionada pola empresa á que pertencen.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- A primeira vez que accedan fisicamente deberán identificarse e solicitar a presenza da persoa responsable do Concello de Carballo, que actuará como enlace durante a súa estancia.
- Unha vez no interior dos edificios, dependencias ou instalacións do Concello de Carballo, as terceiras persoas só terán autorización para permanecer no posto de traballo asignado e nas zonas de uso común.
- Así mesmo, deberán solicitar autorización da persoa responsable cando necesiten desprazarse entre distintos departamentos do Concello de Carballo.
- As terceiras persoas deberán atender en todo momento ás instrucións do persoal de seguridade dos edificios, instalacións ou dependencias ás que teñan acceso.

### 9. Uso do correo electrónico corporativo

O correo electrónico corporativo é unha ferramenta de mensaxería electrónica centralizada posta a disposición das persoas usuarias do Concello de Carballo para o envío e recepción de mensaxes mediante o uso de contas de correo corporativas.

Trátase dun recurso compartido por todo o persoal da organización, polo que un uso indebido do mesmo repercute directamente na calidade do servizo ofrecido ao conxunto de usuarios.

Por este motivo, establécense as seguintes normas de uso:

#### 9.1. Normas xerais

- Todas as persoas usuarias que o precisen para o desenvolvemento da súa actividade profesional disporán dunha conta de correo electrónico corporativo, destinada ao envío e recepción de mensaxes internos e externos á organización.
- Unicamente poderán empregarse as ferramentas e programas de correo electrónico subministrados, instalados e configurados polo Concello de Carballo.
- O correo electrónico corporativo deberá utilizarse exclusivamente para o desempeño das funcións profesionais encomendadas, evitando o uso privado ou persoal do mesmo.
- Deberase notificar á Unidade de Informática calquera tipo de anomalía detectada, así como a recepción dun volume elevado de correos non desexados (spam), co fin de que se poidan configurar adecuadamente as medidas de seguridade oportunas.
- Deberase prestar especial atención aos ficheiros adxuntos recibidos por correo electrónico.
- Non se deberán abrir nin executar ficheiros procedentes de fontes non fiables, xa que poderían conter virus ou código malicioso.
- En caso de dúbida sobre a súa fiabilidade, deberase notificar esta circunstancia á Unidade de Informática.
- Está terminantemente prohibido suplantar a identidade doutra persoa usuaria de Internet, correo electrónico ou calquera outra ferramenta colaborativa.
- Para fins de verificación e monitorización, os datos de conexión e tráfico conservaranse nun rexistro durante o tempo establecido pola normativa vixente en cada caso.
- En ningún suposto esta retención de datos afectará ao secreto das comunicacións.
- Recoméndase utilizar a opción "CCO" (Copia Oculta) do correo electrónico para protexer a privacidade no caso de mensaxes con múltiples destinatarios.
- Se se envía (de forma autorizada) información contida nun ficheiro adxunto que inclúa datos sensíbles, confidenciais ou protexidos, este deberá ir cifrado.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Así mesmo, se procede, deberá protexerse tamén o corpo da mensaxe.
- A clave necesaria para o descifrado do ficheiro comunicáraselle ao destinatario mediante un acto e medio de comunicación distintos.

### 9.2. Usos especialmente prohibidos

As seguintes actuacións están expresa e especialmente prohibidas:

- O envío de correos electrónicos con contido inadecuado, ilegal, ofensivo, difamatorio, inapropiado ou discriminatorio por razón de sexo, raza, idade ou discapacidade; así como aqueles que conteñan programas informáticos sen licenza, que vulneren dereitos de propiedade intelectual, que difundan alertas falsas de virus ou propaguen virus reais ou código malicioso, ou calquera outro tipo de contido que poida prexudicar ás persoas usuarias, á identidade e imaxe corporativa ou aos propios sistemas de información da organización.
- O acceso a un buzón de correo electrónico distinto do propio, así como o envío de correos empregando contas de usuario alleas.
- A difusión da conta de correo corporativa do usuario en listas de distribución, foros, servizos de novas, etc., que non estean directamente relacionados coa súa actividade profesional.
- Responder mensaxes das que se teña sospeita sobre a súa autenticidade, fiabilidade ou contido, así como aquelas que conteñan publicidade non desexada.
- A utilización do correo corporativo como medio de intercambio de ficheiros de gran tamaño, sen autorización expresa, así como o envío de información sensible, confidencial ou protexida por medios non seguros.

### 10. Acceso a Internet e outras ferramentas de colaboración

O acceso corporativo a Internet é un recurso centralizado que o Concello de Carballo pon a disposición das persoas usuarias como ferramenta necesaria para o acceso a contidos e recursos en liña, servindo de apoio ao desempeño da súa actividade profesional.

O Concello de Carballo velará polo bo uso do acceso a Internet, tanto desde o punto de vista da eficiencia e produtividade do persoal, como dos riscos de seguridade asociados ao seu uso.

#### 10.1. Normas xerais

- As conexións que se realicen a Internet deberán responder exclusivamente a fins profesionais, tendo sempre en conta que se están a empregar recursos informáticos corporativos limitados.
- O acceso a Internet para fins persoais deberá restringirse ao mínimo imprescindible e, de ser absolutamente necesario, só poderá facerse durante un tempo razoable, que non interfira no rendemento profesional nin na eficiencia dos recursos informáticos corporativos.
- Só se poderá acceder a Internet mediante o navegador subministrado e configurado polo Concello de Carballo nos postos de usuario.
- Non se poderá alterar a configuración do navegador nin empregar un navegador alternativo sen a debida autorización da Unidade de Informática.
- Deberase notificar á Unidade de Informática do Concello de Carballo calquera anomalía detectada no uso do acceso a Internet, así como sospeitas de posibles problemas ou incidentes de seguridade relacionados con dito acceso.

#### 10.2. Usos especificamente prohibidos

Quedan prohibidas as seguintes actuacións:

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- A descarga de arquivos de gran tamaño, especialmente durante horarios coincidentes coa atención ao público, salvo autorización expresa.
- A descarga de programas informáticos ou ficheiros con contido daniño, que poidan supoñer unha ameaza para a seguridade da organización.
- O acceso a recursos ou páxinas web, así como a descarga de programas ou contidos que vulneren a lexislación en materia de propiedade intelectual.
- O uso de aplicacións ou ferramentas (especialmente programas de intercambio de información tipo P2P) para a descarga masiva de arquivos, programas ou outros contidos (música, películas, etc.).

### 11. Normativa en materia de uso das redes sociais

Os seguintes epígrafes recollen o conxunto de medidas e boas prácticas que deben terse en conta cando se utilicen ou se pretendan utilizar as redes sociais como ferramenta de comunicación e difusión institucional das funcións competenciais do Concello de Carballo.

#### 11.1. Autorización previa

Con carácter xeral, e agás as excepcións que poidan ser expresamente autorizadas no Concello de Carballo, ningunha persoa que preste servizos na entidade poderá darse de alta en ningunha rede social en nome ou representación do Concello, salvo autorización expresa da Secretaría Xeral, coa coñecemento do Responsable de Seguridade.

Polo tanto, salvo no suposto sinalado, a presenza dun empregado público do Concello de Carballo nas redes sociais será sempre a título persoal.

#### 11.2. Normas de comportamento

Unha vez autorizada a alta nunha rede social en representación do Concello de Carballo, o empregado público usuario da rede social deberá observar as seguintes normas de comportamento:

- Lembrar en todo momento que as redes sociais constitúen un foro público. Polo tanto, ao engadir calquera dato, comentario ou información, a persoa usuaria asume que este poderá ser visto polo resto de usuarios da rede, polo Concello de Carballo e, en xeral, por calquera persoa.
- Se a persoa usuaria está a empregar o perfil da rede social en representación do Concello de Carballo, convén mostrar abertamente esa representación, agás que existan circunstancias excepcionais que non o aconsellen, como por exemplo unha ameaza potencial á seguridade persoal.
- En todo caso, non deberán proporcionarse detalles persoais, como enderezos ou números de teléfono particulares.
- A persoa usuaria deberá tratar con respecto ao resto de usuarios, empregando unha linguaxe adecuada e correcta, e actuando sempre como se estivese en presenza das demais persoas.
- Agás autorización expresa, non se poderá publicar material publicitario nin comunicacional do Concello de Carballo, nin empregar o perfil da rede social con fins lucrativos ou comerciais, nin para comparar as funcións, competencias ou actuacións do Concello con outras entidades.
- Os contidos publicados nas redes sociais poden estar suxeitos a dereitos de propiedade intelectual, polo que a publicación de calquera contido require asegurarse de que está libre de restricións ou cargas.

A contribución da persoa usuaria na rede social deberá conter datos reais, concretos e unha argumentación coherente.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



TEMARIO TICS

Permítense as citas ou a reprodución de pequenos fragmentos de textos, libros ou obras de terceiros, sempre que se indique a fonte e o nome do autor.

Se a persoa usuaria realiza unha achega propia (texto, fotografías, gráficos, vídeos ou audios), debe saber que autoriza ao Concello de Carballo a reproducila en calquera medio físico ou virtual, indicando o nome do empregado público como autor, todo iso sen prexuízo de que outros usuarios tamén poidan gardalos ou reproducilos.

- O logotipo do Concello de Carballo e, en xeral, calquera outro logotipo ou distintivo gráfico do Concello ou doutra entidade do sector público constitúen marcas rexistradas.
- Así mesmo, os contidos publicados no portal ou sede electrónica do Concello de Carballo son titularidade da entidade, polo que o Concello resérvase todos os dereitos de propiedade intelectual e industrial asociados a eles.
- A persoa usuaria deberá comprometerse a respectalos e a non utilízaos sen a debida autorización, calquera que sexa o medio empregado.
- A descarga de contidos, a súa copia ou impresión requirirá autorización da persoa superior xerárquica do empregado (xefe/a de área, servizo ou departamento).
- En ningún caso deberá empregarse a rede social para o intercambio de credenciais ou contrasinais, de ningún sistema e para calquera finalidade.
- A información contida no perfil dunha rede social non deberá considerarse nunca como información oficial en relación coas funcións e competencias do Concello de Carballo, nos termos reservados ás funcións da sede electrónica municipal, segundo o disposto no artigo 38 da Lei 40/2015.

O Concello de Carballo velará en todo momento polo bo uso do perfil institucional e, por iso, como administrador, resérvase o dereito de eliminar, sen dereito a réplica, calquera achega que:

- Considere ilegal, irrespectuosa, ameazante, infundada, calumniosa, inapropiada, ética ou socialmente discriminatoria, ou laboralmente reprochable, ou que, dalgún modo, poida ocasionar danos ou prexuízos materiais ou morais ao Concello de Carballo, ao seu persoal, colaboradores ou terceiros.
- Incorpore datos de terceiros sen a súa autorización.
- Conteña recomendacións relativas ás funcións e competencias do Concello de Carballo, ou material publicitario ou comunicacional, sexa de carácter persoal ou en beneficio de terceiros, tanto persoas físicas como xurídicas.
- Sexa redundante.
- Non estea relacionada coa finalidade perseguida polo Concello de Carballo ao darse de alta na rede social correspondente.

### 11.3. Uso dos medios sociais con fins exclusivamente persoais

En ocasións, o uso persoal ou profesional dunha rede social pode chegar a confundirse. Por tanto, débese ser consciente das responsabilidades derivadas de mesturar a vida persoal e laboral nestes medios.

As persoas que traballan para o Concello de Carballo deben empregar o seu bo xuízo e asumir a responsabilidade persoal e profesional dos contidos que publiquen a través dos medios sociais.

É habitual que se admita o uso dunha conta persoal para comentar asuntos non relacionados co traballo, aínda que non debería permitirse, con carácter xeral, que o uso de tales contas se realice

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



en horario laboral nin, por motivos de seguridade, empregando os medios electrónicos do Concello de Carballo.

En calquera caso, o uso das plataformas de redes sociais nunca deberá interferir coas funcións principais do posto de traballo, salvo naqueles casos en que as tarefas asignadas inclúan expresamente o uso destas ferramentas sociais.

Débase lembrar que o uso dunha conta privada non exime do cumprimento dos códigos de boa conduta, tanto os xeralmente aceptados como os especificamente recollidos na Política de Seguridade da Información do Concello de Carballo.

Por todo iso, non deberán publicarse opinións persoais a través de contas oficiais, nin promover contas persoais mediante as contas institucionais.

Non debe comunicarse nin comentarse en redes sociais información que non deba ser de dominio público, aínda que se pretenda excluír unha soa persoa.

As redes sociais poden actuar como amplificadores e comprometer ás persoas usuarias.

Aquelas persoas con responsabilidades de goberno, en virtude da súa posición, deberán considerar se os comentarios persoais que publiquen, mesmo en espazos claramente privados, poden ser mal interpretados como declaracións oficiais realizadas polo Concello de Carballo.

### 11.4. Medidas de seguridade da información

En primeiro lugar, é preciso identificar claramente as canles oficiais do Concello de Carballo que poidan existir e, na medida do posible, diferenciar as canles auténticas, así como impulsar a vixilancia e o peche das canles falsas.

### 11.5. Medidas de seguridade tecnolóxica

As contas en redes sociais do Concello de Carballo crearánse a partir de correos electrónicos corporativos, delegándose a súa xestión nas unidades organizativas designadas para cada unha delas.

O Responsable de Seguridade do Concello de Carballo estenderá as súas competencias aos perfís das redes sociais que poidan crearse.

A custodia das contrasinais dos perfís das redes sociais ou dos seus administradores, cando así se requira, estará centralizada e será responsabilidade da unidade organizativa correspondente.

Calquera instalación de aplicacións de terceiros que requira permisos sobre contas das redes sociais deberá ser autorizada previamente polo Responsable de Seguridade do Concello de Carballo, co fin de verificar que a aplicación non poña en risco nin os datos nin a seguridade da conta.

A modificación de calquera das opcións de privacidade ou a publicación de comentarios deberá ser autorizada previamente polo Concello de Carballo, contando coa opinión do Responsable de Seguridade.

Como norma xeral, as contrasinais das plataformas de xestión deberán ser robustas. Sempre que sexa posible, recoméndase manter as contas a través dunha ferramenta de xestión que permita asignar permisos diferenciados de publicación e cuxo acceso non se realice mediante a contrasinal directa da rede social correspondente.

A persoa responsable de cada conta definirá quen son as persoas encargadas da súa xestión, velando polo cumprimento da confidencialidade das contrasinais de acceso.

Sempre que sexa posible, o acceso ás contas realizarase dende sistemas corporativos.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



TEMARIO TICS

No caso de necesitar publicar contidos dende un dispositivo móbil, farase a través dunha aplicación diferente á de uso persoal.

### 12. Incidentes de seguridade

Cando unha persoa usuaria detecte calquera anomalía ou incidencia de seguridade que poida comprometer o bo uso e funcionamento dos Sistemas de Información do Concello de Carballo ou a súa imaxe institucional, deberá informar inmediatamente á Unidade de Informática, que rexistrará o incidente debidamente e o trasladará, se procede, ás instancias correspondentes.

### 13. Compromiso das persoas usuarias

É responsabilidade directa da persoa usuaria:

- Custodiar as credenciais que lle sexan proporcionadas e seguir todas as recomendacións de seguridade establecidas polo Concello de Carballo, co fin de garantir que non poidan ser utilizadas por terceiras persoas.
- Deberá pechar a súa sesión ao rematar o traballo ou bloquear o equipo cando o deixe desatendido.
- No caso de que o seu equipo conteña información sensible, confidencial ou protexida, esta deberá cumprir todos os requisitos legais aplicables e as medidas de protección establecidas pola normativa do Concello de Carballo ao respecto.
- Ademais do anterior, non se poderá acceder aos recursos informáticos e telemáticos do Concello de Carballo para desenvolver actividades que teñan como finalidade ou consecuencia algunha das seguintes accións:
  - O uso intensivo de recursos de proceso, memoria, almacenamento ou comunicacións con fins non profesionais.
  - A degradación dos servizos.
  - A destrución ou modificación non autorizada da información, de maneira premeditada.
  - A violación da intimidade, do segredo das comunicacións ou do dereito á protección dos datos persoais.
  - O deterioro intencionado do traballo doutras persoas.
  - O uso dos sistemas de información para fins alleos aos do Concello de Carballo, salvo as excepcións contempladas na presente normativa.
  - Danar intencionadamente os recursos informáticos do Concello de Carballo ou doutras institucións.
  - Incurrir en calquera outra actividade ilícita, sexa do tipo que fora

### 14. Monitorización e aplicación desta normativa

O Concello de Carballo, por motivos legais, de seguridade e de calidade do servizo, e cumprindo en todo momento cos requisitos establecidos pola lexislación vixente, realizará as seguintes accións:

- a) Revisará periodicamente o estado dos equipos, o software instalado, os dispositivos e as redes de comunicación baixo a súa responsabilidade.
- b) Monitorizará os accesos á información contida nos seus sistemas.
- c) Auditará a seguridade das credenciais e aplicacións utilizadas.
- d) Monitorizará os servizos de Internet, correo electrónico e outras ferramentas de colaboración.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### TEMARIO TICS

O Concello de Carballo levará a cabo esta actividade de monitorización sen empregar sistemas nin programas que poidan atentar contra os dereitos constitucionais das persoas usuarias, tales como o dereito á intimidade persoal e ao secreto das comunicacións, mantendo en todo momento a privacidade da información tratada.

Só por requirimento legal ou investigación dun uso ilexítimo ou ilegal, poderá accederse a dita información, salvagardando en todo momento os dereitos fundamentais das persoas usuarias.

Os sistemas nos que se detecte un uso inadecuado ou nos que non se cumpran os requisitos mínimos de seguridade poderán ser bloqueados ou suspendidos temporalmente.

O servizo restablecerase cando desaparezan as causas da súa inseguridade ou degradación.

O Responsable de Seguridade, coa colaboración das restantes unidades do Concello de Carballo, velará polo cumprimento da presente Normativa Xeral e informará ao Comité de Seguridade sobre os incumprimentos ou deficiencias observadas, co obxectivo de que se adopten as medidas oportunas.

O sistema que proporciona o servizo de correo electrónico poderá, de forma automatizada, rexeitar, bloquear ou eliminar parte do contido das mensaxes enviadas ou recibidas nas que se detecte algún problema de seguridade ou incumprimento da presente Normativa.

Poderase inserir contido adicional nas mensaxes enviadas co obxecto de advertir aos destinatarios sobre os requisitos legais e de seguridade que deben cumprir en relación con ditos correos.

O sistema que proporciona o servizo de navegación por Internet poderá contar con filtros de acceso que bloqueen o acceso a páxinas web con contidos inadecuados, programas lúdicos de descarga masiva ou sitios potencialmente inseguros que conteñan virus ou código daniño.

Así mesmo, o sistema poderá rexistrar e gardar traza das páxinas ás que se acceda, así como do tempo de conexión, volume e tamaño dos arquivos descargados.

O sistema permitirá establecer controis que posibiliten detectar e notificar usos prolongados ou indebidos do servizo.

### 15. Postos de traballo despexados e pantallas limpas

Os postos de traballo do persoal deberán situarse preferentemente en lugares que non queden expostos ao acceso de persoas externas.

Esta norma non será de aplicación aos equipos destinados ao uso público.

Os postos situados en zonas de atención ou tránsito de público deberán colocarse de forma que as pantallas non poidan ser visualizadas por persoas alleas.

Cando unha persoa usuaria deixe de atender o seu ordenador durante un tempo determinado, deberá bloquear a sesión de usuario ou activar o protector de pantalla, co fin de evitar o uso indebido das súas credenciais e a posible suplantación da súa identidade.

Este mecanismo de bloqueo deberá estar protexido mediante un método de autenticación de usuario, como unha contrasinal, e deberá salvagardar calquera información, documento, soporte informático ou dispositivo de almacenamento extraíble que poida conter información sensible ou protexida, fronte a posibles revelacións ou roubos.

Por razóns de seguridade, o PC bloquearase automaticamente tras un período de inactividade.

En ningún caso deberán manterse sobre as mesas documentos con información relevante que poidan ser lidos por outras persoas.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



A información sensible ou confidencial, tanto en formato papel como en soportes electrónicos, deberá gardarse nunha caixa forte, armario ou outro moble de seguridade cando non se precise, especialmente cando a oficina estea baleira.

### 16. Traballo fóra das instalacións

O obxectivo da presente norma é regular o traballo do persoal do Concello de Carballo cando desenvolva a súa actividade profesional fóra dos edificios, dependencias ou instalacións municipais.

O traballo fóra das instalacións comprende tanto o teletraballo habitual e permanente do persoal desprazado, como o traballo ocasional, empregando, en ambos os casos, dispositivos de computación e comunicación (normalmente ordenador portátil, tableta, teléfono móbil, etc.).

Este modo de traballo inclúe tamén as conexións remotas realizadas dende congresos, sesións de formación, aloxamentos, ou mesmo chamadas telefónicas profesionais realizadas ou atendidas en espazos públicos.

O traballo fóra das instalacións do Concello de Carballo implica o risco de traballar en lugares desprotexidos, é dicir, sen as barreiras de seguridade físicas e lóxicas implementadas nas dependencias municipais.

Fóra deste perímetro de seguridade, aumentan as vulnerabilidades e a probabilidade de materialización das ameazas, o que fai necesario adoptar medidas de seguridade adicionais.

A continuación inclúese un conxunto de normas de obrigado cumprimento, cuxo obxectivo é reducir o risco ao traballar fóra das instalacións do Concello de Carballo.

#### 16.1. Uso persoal e profesional

Os dispositivos móbiles de computación e comunicación asignados ás persoas usuarias do Concello de Carballo son de uso exclusivo e estritamente profesional.

Non poderán prestarse a terceiros, salvo autorización expresa da Unidade de Informática, que deberá definir expresamente as condicións de uso en cada caso.

#### 16.2. Conexións a redes sen fíos públicas

Está prohibido conectarse a redes WiFi públicas ou gratuítas, xa que os principais riscos asociados son o roubo de datos persoais, a infección do dispositivo, o secuestro de sesión e o roubo dos datos transmitidos.

Deberase empregar unha VPN (Virtual Private Network ou Rede Privada Virtual) para garantir a seguridade das comunicacións.

#### 16.3. Saída de documentación e dispositivos

A saída fóra das dependencias do Concello de Carballo de documentación, equipos e dispositivos informáticos ou de comunicación require autorización previa da Unidade de Informática.

Así mesmo, será necesaria a autorización correspondente para empregar equipos persoais da persoa usuaria no tratamento de información da organización ou no acceso a recursos ou sistemas de información do Concello de Carballo.

#### 16.4. Copias de seguridade

Deberase realizar copia de seguridade da información contida nos dispositivos móbiles.

De igual modo, deberán adoptarse medidas adecuadas para a protección destas copias, garantindo a súa integridade e confidencialidade.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 16.5. Transmisión de información e acceso remoto

A transmisión de información e o acceso remoto realizaranse exclusivamente a través dos canles establecidos, seguindo os procedementos e requisitos definidos para tal fin e adoptando as seguintes precaucións:

- En caso de empregar contrasinais na autenticación, estas deberán ser robustas.
- Pechar sempre a sesión ao rematar o traballo.
- Cifrar a información sensible, confidencial ou protexida que se vaia transmitir por correo electrónico ou calquera outro canle que non garanta unha confidencialidade adecuada.

### 16.6. Vixilancia permanente

A documentación e os dispositivos móbiles deberán permanecer baixo vixilancia e control directo para evitar perdas ou furtos que poidan comprometer a información almacenada ou accesible desde eles.

Durante desprazamentos en avión, este tipo de equipamento non debe facturarse e deberá viaxar sempre coa persoa usuaria.

### 16.7. Prevención do acceso non autorizado

O traballo en lugares públicos deberá realizarse coa máxima cautela e precaución, evitando que persoas non autorizadas poidan ver ou escoitar información interna da organización.

### 16.8. Acceso remoto (vía web)

En relación co acceso remoto a través da web, deberán adoptarse as seguintes cautelas:

- Os navegadores empregados para o acceso web deberán estar permanentemente actualizados á súa última versión, especialmente no que respecta aos parches de seguridade, e deberán atoparse correctamente configurados.
- Unha vez finalizada a sesión web, é obrigatoria a desconexión co servidor mediante un proceso que elimine calquera posibilidade de reutilización da sesión pechada.
- Desactivar a función de lembrar contrasinais no navegador.
- Activar a opción de borrado automático ao peche do navegador da información sensible rexistrada polo mesmo: historial de navegación, descargas, formularios, caché, cookies, contrasinais, sesións autenticadas, etc.
- Agás autorización expresa, está prohibida a instalación de complementos (*addons*) no navegador.

A documentación e os equipos que saian das instalacións do Concello de Carballo deberán transportarse de maneira segura, evitando facilitar información sobre o seu contido e empregando, de ser o caso, maletíns de seguridade que impidan o acceso non autorizado.

É obrigatorio o uso de peches de seguridade e/ou cables de ancoraxe para os dispositivos de computación que deban permanecer desatendidos fóra das instalacións do Concello de Carballo.

Os equipos deberán manterse conforme ás especificacións técnicas de uso, almacenamento e transporte proporcionadas polo fabricante.

En particular, deberá evitarse o seu uso en condicións inadecuadas de temperatura ou humidade, ou en contornos desaconsellables (mesas con alimentos ou líquidos, espazos sucios, etc.).

Realizarase unha revisión periódica dos equipos para verificar a ausencia de software daniño.

**CONCELLO DE CARBALLO**

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña

**TEMARIO TICS**

Durante o desenvolvemento da actividade profesional fóra das instalacións do Concello de Carballo, deberán seguirse as normas, procedementos e recomendacións internas vixentes.

**17. Incumprimento da normativa**

Todas as persoas usuarias do Concello de Carballo están obrigadas a cumprir o establecido na presente normativa.

No suposto de que unha persoa usuaria non cumpra algún dos preceptos recollidos nesta Normativa, sen prexuízo das accións disciplinares ou administrativas que poidan corresponder e, de ser o caso, das responsabilidades legais pertinentes, poderá acordarse a suspensión temporal ou definitiva do uso dos recursos informáticos asignados a esa persoa usuaria.

**CONCELLO DE CARBALLO**

C.I.F.: P1501900C

Praza do Concello S/N

Teléfono 981 70 41 00

[www.carballo.gal](http://www.carballo.gal)

[infocarballo@carballo.gal](mailto:infocarballo@carballo.gal)

15100 CARBALLO - A Coruña



**TEMA 3.** Postos de traballo e uso dos Sistemas Informáticos Municipais. Certificado dixital da FNMT. Contraseñas. Actuacións fronte aos ciberataques. Arquivos compartidos de maneira segura. Metadatos. Guía para usuarios: Comprobacións básicas antes de contactar co Soporte Técnico. Uso seguro da Wi-Fi. Protección de datos persoais na rede. O Transporte seguro de información dixital. Actuacións fronte ao phishing e a enxeñería social no correo electrónico. Reporte de incidentes de seguridade da información. A Intelixencia Artificial (IA) nos cibertataques. Seguridade nas videoconferencias. A suplantación de identidade nos ciberataques. Copias de seguridade. Limpeza do escritorio. Uso de software libre ou de código aberto. Uso seguro de medios e dispositivos electrónicos. Ransomware. Navegación web. Arquivos comprimidos. Lexislación sobre seguridade da información e protección de datos. Doble factor de autenticación.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



## Postos de traballo e uso dos Sistemas Informáticos Municipais

### > Certificado dixital da FNMT

#### ✓ Instrucións para instalar un certificado dixital en Windows 11

##### ✚ 1. Requisitos previos

Antes de comezar:

- Ten o ficheiro do certificado en formato .p12 ou .pfx (a copia que descargaches ou exportaches).
- Coñece o contrasinal que lle puxeches ao crear a copia de seguridade.
- Usa unha conta de Windows con permisos de administrador.

##### ■ 2. Iniciar o asistente de instalación

1. Busca o ficheiro do certificado no teu ordenador (ex.: certificado.p12).
  2. Fai dobre clic sobre el.
- Isto abrirá o Asistente de importación de certificados de Windows.

##### ■ 3. Seleccionar o almacén do certificado

1. O asistente preguntará onde queres instalar o certificado.
2. Escolle a opción:  
"Usuario actual" (recomendado para certificados persoais).
3. Preme en "Seguiente".

##### ■ 4. Introducir o contrasinal do certificado

1. Aparecerá unha ventá pedíndoche o contrasinal.
2. Introduce o contrasinal que lle asignaches cando gardaches o certificado.
3. Marca as seguintes opcións (se aparecen):
  - "Habilitar protección de clave privada"
  - "Marcar esta clave como exportable" (permite crear novas copias de seguridade)
4. Preme "Seguiente".

##### ■ 5. Elixir o almacén correcto

1. Selecciona:  
"Colocar todos os certificados no seguinte almacén"
2. Preme en "Examinar...".
3. Escolle:  
"Personal" (tamén chamado Personal / *Certificates* ou Persoal).
4. Acepta e logo fai clic en "Seguiente".

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 6. Finalizar a instalación

1. Preme "Rematar".
2. Debería aparecer unha mensaxe indicando:  
"A importación se completou correctamente".  
Se aparece este aviso, o certificado xa está instalado.

### 7. Verificar que o certificado está instalado en Windows 11

Para comprobar que todo está correcto:

1. Preme Tecla Windows → escribe "certificados".
2. Abre:  
"Xestionar certificados de usuario".
3. Vai a:  
Certificados → Persoal → Certificados.
4. Debes ver o teu certificado listado coa túa información.

### 8. Proba de funcionamento

Para asegurar que funciona:

1. Entra nun servizo que use certificado dixital:
  - Sede electrónica da Axencia Tributaria
  - Seguridade Social
  - Sede electrónica da Xunta de Galicia
2. O navegador debería pedirche seleccionar o certificado.

Se o recoñece, a instalación está correcta.

### Recomendacións de seguridade

- Garda o ficheiro .p12/.pfx nunha localización segura.
- Non compartas o contrasinal con ninguén.
- Borra o ficheiro do certificado se non é necesario telo no PC.
- Mantén Windows e o navegador actualizados.

#### > Contrasinais

#### Política de Contrasinais e Boas Prácticas de Seguridade

##### 1. Obxectivo

Esta política establece as normas para a creación, xestión e uso de contrasinais, así como recomendacións de seguridade destinadas a protexer os sistemas informáticos, a información sensible e os datos persoais da organización.

##### 2. Ámbito de aplicación

Documento electrónico asinado dixitalmente cuxa integridade garántese mediante cotexo na Sede Electrónica deste Organismo co Código de Verificación Dixital (CVD) especificado á marxe.  
(artigo 42.b da Lei 40/2015, de 1 de outubro, de Réxime Xurídico do Sector Público)

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



A política aplícase a:

- Todo o persoal da organización.
- Provedores e colaboradores con acceso aos sistemas.
- Contas, dispositivos e servizos internos ou externos que procesen información corporativa.

### 3. Política de contrasinais

#### 3.1. Requisitos mínimos dos contrasinais

Todos os contrasinais deben cumprir:

- Lonxitude mínima: 12 caracteres.
- Complexidade: debe incluír 3 dos 4 tipos seguintes:
  - Letras maiúsculas
  - Letras minúsculas
  - Números
  - Caracteres especiais (!, %, &, \_, ?, etc.)
- Non conter información persoal (nome, apelidos, data de nacemento, usuario, etc.).
- Non usar palabras comúns ("contrasinal", "123456", "empresa", etc.).

#### 3.2. Ciclo de vida do contrasinal

- Renovación obrigatoria cada 180 días (ou antes se hai sospeita de compromiso).
- Prohibido reutilizar calquera dos últimos 5 contrasinais empregados.
- Cambio inmediato se se detecta acceso non autorizado ou comportamento sospeitoso.

#### 3.3. Protección dos contrasinais

- Non escribir nin gardar contrasinais en papel ou en documentos non cifrados.
- Non compartir contrasinais con ningún compañeiro ou supervisor.
- No caso de usar xestores de contrasinais, deben estar aprobados e configurados pola organización.
- Activar autenticación en dous pasos (2FA) sempre que sexa posible.

### 4. Boas prácticas de seguridade

#### 4.1. Uso responsable dos dispositivos

- Bloquear a sesión ao afastarse do posto de traballo.
- Manter os equipos actualizados con parches de seguridade e antivirus.
- Non instalar software sen autorización.
- Usar só dispositivos corporativos para acceder a información sensible.

#### 4.2. Navegación segura

- Evitar facer clic en ligazóns sospeitosas ou abrir anexos non solicitados.
- Verificar que as páxinas web empreguen HTTPS antes de introducir credenciais.
- Non conectarse a redes Wi-Fi públicas para acceder a información corporativa sen VPN.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 4.3. Xestión de datos e información

- Manter a información sensible cifrada.
- Realizar copias de seguridade periódicas.
- Cumprir coas normativas vixentes (RGPD, LOPDGDD, políticas internas).

### 4.4. Resposta ante incidentes

- Notificar inmediatamente ao equipo técnico calquera incidente:
  - Accesos sospeitosos
  - Emails de phishing
  - Perda ou roubo de dispositivos
  - Malware ou erros anómalos
- Non intentar resolver incidentes graves sen supervisión.

## 5. Formación e concienciación

A organización comprométese a:

- Ofrecer formación periódica sobre ciberseguridade.
- Actualizar as políticas cando sexa necesario.
- Comunicar boas prácticas e avisos sobre novas ameazas.

## 6. Cumprimento

O incumprimento desta política poderá derivar en restrición de acceso aos sistemas e, se procede, en medidas disciplinarias segundo o regulamento interno da organización.

---

### Como cambiar a contrasinal en Windows 11 cunha conta de Active Directory

---

#### Método 1: Desde o propio Windows (Ctrl+Alt+Supr)

Este é o método máis directo e funciona sempre que o PC está unido ao dominio.

1. Preme simultaneamente Ctrl + Alt + Supr.
2. Escolle a opción "Cambiar un contrasinal".
3. Introduce:
  - Contrasinal actual
  - Nova contrasinal
  - Confirmación da nova contrasinal
4. Preme Aceptar.

Se a nova contrasinal cumpre as políticas do dominio (lonxitude, complexidade...), actualízase ao momento.

#### Método 2: Desde Configuración de Windows 11

1. Preme Windows + I para abrir Configuración.
2. Vai a Contas.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



3. Entra en Opcións de inicio de sesión.
4. Selecciona Contraseñal → Cambiar.
5. Introduce o contraseñal actual e establece un novo.

⚠ Este método funciona só se a túa conta do dominio está correctamente sincronizada co controlador de dominio.

### ✓ Método 3: Conexión remota (VPN)

Se estás fóra da oficina e necesitas cambiar a contraseñal:

1. Conéctate á VPN corporativa.
2. Unha vez conectada a VPN, usa o método Ctrl + Alt + Supr → Cambiar contraseñal.
3. Reinicia sesión para asegurarte de que a caché do dominio se actualiza.

👉 Isto garante que a nova contraseñal queda almacenada no equipo local e evita erros ao iniciar sesión sen VPN.

### ⚠ Problemas frecuentes e solucións

- Erro: "O dominio non está dispoñible"
  - O PC non pode comunicarse co controlador de dominio.
  - ➔ Solución: conectar cable/wi-fi corporativo ou VPN e repetir o cambio.
- Non me deixa usar a nova contraseñal
  - Pode incumplir a política de contraseñais (historial, complexidade, lonxitude...).
  - ➔ Proba con unha frase de contraseñal máis longa (12-16 caracteres).
- O PC está desconectado do dominio dende hai tempo
  - ➔ É posible que necesite reconectar fisicamente á rede da empresa ou que o administrador resete a conta.

### ✓ Consello

Se queres evitar problemas posteriores coa sincronización local da contraseñal, pecha sesión e volve iniciar sesión no PC despois do cambio.

### > Actuacións fronte aos ciberataques

#### 🚨 QUE FACER SE CREES QUE ESTÁS SENDO VÍTIMA DUN CIBERATAQUE

##### ✓ 1. Mantén a calma e non apagues o dispositivo

Moitas veces apagar o equipo pode eliminar rastros útiles para a investigación ou permitir que o malware actúe ao iniciar de novo.

##### 🔒 2. Desconecta o dispositivo de Internet

Isto evita que o atacante siga accedendo.

- Desconecta o cable de rede.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Desactiva o Wi-Fi ou pon o dispositivo en "modo avión".
- Se é un móbil, tamén desactiva os datos móbiles.

### ● 3. Non continúes usando contas nin aplicacións

Evita iniciar sesión en:

- Correo electrónico
- Redes sociais
- Bancos
- Servizos corporativos

Isto pode evitar o roubo de credenciais adicionais.

### 🔒 4. Toma nota dos síntomas

Moi útil para investigadores ou técnicos:

- Ventás estrañas
- Movementos do rato ou teclado sen tocar nada
- Programas que non recoñeces
- Contraseñas que xa non funcionan
- Mensaxes de ransomware
- Actividade sospeitosa en contas (correos enviados, inicios de sesión, etc.)

### 👤 5. Contacta canto antes co servizo técnico ou responsable de seguridade

Se é nunha empresa ou institución, avisa ao departamento de IT ou ao DPO / SOC.

Se é persoal, busca axuda dun profesional de confianza.

### 🔑 6. Cambia as contraseñas DESDE OUTRO DISPOSITIVO SEGURO

Nunca o fagas no equipo comprometido.

Recomendacións:

- Empeza polo correo electrónico (é a porta de entrada a todo o demais).
- Segue coa banca en liña, redes sociais, servizos gobernamentais, etc.
- Activa a autenticación en dous pasos (2FA) se aínda non a tes.

### 🦠 7. Realiza unha análise antivirus / antimalware completa

Podes usar:

- Windows Defender (moi eficaz)
- Malwarebytes
- Ferramentas de análise recomendadas polo servizo técnico

Ideal: Escaneo completo e escaneo offline.

### ⚠️ 8. Se hai risco para datos persoais ou económicos

Dependendo da gravidade, deberías:

- 🏦 Contactar co banco

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Bloquear tarxetas
- Revisar movementos
- Activar alertas de operacións

🔵 Se se comprometeron datos persoais importantes

Pódese chegar a notificar a:

- Axencia Española de Protección de Datos (AEPD)
- INCIBE (Instituto Nacional de Ciberseguridade)

### 📄 9. Documenta todo o sucedido

Podería ser necesario para:

- Investigacións internas
- Denuncias
- Procesos de recuperación

### 👮 10. En caso grave, presenta denuncia

Se ocorre roubo, chantaxe ou fraude:

- Garda probas (capturas, correos, mensaxes)
- Acude ás Forzas e Corpos de Seguridade  
(Policía Nacional / Garda Civil → unidades especializadas en delitos telemáticos)

## ★ RESUMO RÁPIDO

1. Desconecta internet
2. Non uses o dispositivo
3. Avisa a soporte técnico
4. Cambia contrasinais noutro equipo
5. Analiza o PC con antivirus
6. Contacta co banco se hai risco económico
7. Denuncia se é necesario

### > Arquivos compartidos de maneira segura

#### COMO COMPARTIR UN ARQUIVO EN ONEDRIVE (OFFICE 365)

##### ✅ 1. Compartir desde o navegador (onedrive.com)

##### PASO 1: Acceder a OneDrive

1. Vai a <https://onedrive.com> ou entra desde o portal de Office.com.
2. Inicia sesión coa túa conta de Microsoft 365.

##### PASO 2: Seleccionar o arquivo

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



1. Na túa listaxe de arquivos, busca o arquivo ou cartafol que queiras compartir.
2. Preme co botón dereito ou selecciona o arquivo e escolle Compartir.

### PASO 3: Elixir o tipo de acceso

Aparecerá unha xanela con varias opcións:

- “Calquera persoa con ligazón pode ver ou editar”  
→ Permite compartir con xente fóra da organización.
- “Persoas da túa organización”  
→ Só usuarios internos.
- “Persoas específicas”  
→ Ideal se queres controlar exactamente quen accede.

Podes configurar:

- Ver ou Editar
- Establecer data de caducidade
- Establecer contrasinal (se a túa organización o permite)

Preme Aplicar.

### PASO 4: Enviar a ligazón

- Introduce o correo das persoas coa que queres compartir ou
- Preme “Copiar ligazón” para pegala nun correo, Teams, WhatsApp, etc.

## 2. Compartir un arquivo desde o Explorador de Windows (app de escritorio OneDrive)

### PASO 1: Abrir o cartafol de OneDrive

1. No Explorador de arquivos, vai ao cartafol OneDrive.

### PASO 2: Botón dereito → Compartir

1. Preme co botón dereito sobre o arquivo ou cartafol.
2. Escolle “Compartir” ou “Compartir con OneDrive”.

### PASO 3: Configurar permisos

1. Aparece a mesma ventá de configuración de permisos.
2. Escolle quen pode acceder (ver/editar).
3. Envía o enlace ou cópiao.

## 3. Compartir directamente desde Word, Excel ou PowerPoint (Office 365)

### PASO 1: Abrir o documento

1. Abre o arquivo en Word/Excel/PowerPoint versión Microsoft 365.

### PASO 2: Gardar en OneDrive

Se non está en OneDrive, gárdao:

Arquivo → Gardar como → OneDrive.

### PASO 3: Premer en “Compartir”

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



1. Na esquina superior dereita, preme Compartir.
2. Engade:
  - Correos das persoas
  - Permisos (ver ou editar)
3. Preme Enviar.

### 🔒 CONSELLOS DE SEGURIDADE AO COMPARTIR

- Usa "persoas específicas" para documentos sensibles.
- Revoga permisos cando xa non sexan necesarios:
  - Botón dereito → Administrar acceso.
- Evita dar permisos de edición se non son necesarios.
- Activa a caducidade da ligazón en enlaces públicos.

### ★ RESUMO RÁPIDO

Para compartir un arquivo en OneDrive:

1. Selecciona o arquivo → Compartir
2. Escolle quen pode acceder
3. Define permisos
4. Envía a ligazón ou copia o enlace

### > Metadatos

### 🔍 COMO VER E ELIMINAR METADATOS EN LIBREOFFICE

#### ✅ 1. Ver os metadatos dun documento

1. Abre o documento en LibreOffice Writer / Calc / Impress.
2. Vai ao menú Ficheiro.
3. Preme en Propiedades....
4. Verás varias lapelas con información:
  - Xeral → nome do ficheiro, tamaño, datas.
  - Descrición → título, tema, palabras clave.
  - Estatísticas → número de páxinas, palabras, caracteres.
  - Propiedades personalizadas → datos engadidos polo usuario.
  - Seguridade → permisos.

👉 Aquí podes consultar toda a información que LibreOffice garda como metadatos.

#### ✂ 2. Eliminar metadatos automaticamente (método rápido)

LibreOffice ten unha función para eliminar metadatos e datos persoais nun só clic.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



1. Vai a Ficheiro.
2. Selecciona Gardar como....
3. Na xanela de gardado, pulsa o botón "Ferramentas" (na parte inferior).
4. Escolle "Limpar información persoal".
5. Garda o documento cun nome novo (recomendado).

Isto elimina:

- Autor do documento
- Datas de creación/modificación
- Historial interno
- Propiedades personalizadas

### 3. Eliminar metadatos manualmente (máis control)

Se queres revisar antes de eliminar:

1. Vai a Ficheiro → Propiedades.
2. Na lapela Xeral:
  - Desmarca "Aplicar datas automaticamente" (se aparece).
  - Podes limpar autor, título, tema, etc.
3. Na lapela Descrición:
  - Elimina campos como Título, Asunto, Palabras clave.
4. Na lapela Propiedades personalizadas:
  - Selecciona propiedades → Eliminar.
5. Preme Aceptar e garda o documento.

### 4. Eliminar rexistro de cambios e comentarios (tamén considerados metadatos)

- Eliminar comentarios
  - Ferramentas → Comentarios → Eliminar todos os comentarios (ou botón dereito nun comentario → "Eliminar todos os comentarios").
- Aceptar/rexeitar cambios
  - Editar → Seguir cambios → Aceptar ou rexeitar.

### 5. Exportar como PDF sen metadatos

Se vas compartir o documento en PDF:

1. Vai a Ficheiro → Exportar como → Exportar como PDF.
2. Na lapela Xeral, desmarca:
  - "Incluir metadatos do documento".
3. Exporta o PDF.

## ★ RESUMO RÁPIDO

Ver metadatos: Ficheiro → Propiedades

Eliminar datos persoais: Ficheiro → Gardar como → Ferramentas → Limpar información persoal

Eliminar comentarios e cambios: menú Ferramentas / Editar

PDF sen metadatos: Exportar como PDF → desmarcar "incluir metadatos"

## > Guía para usuarios: Comprobacións básicas antes de contactar co Soporte Técnico

Esta guía axúdache a resolver problemas comúns e a recoller información útil para o equipo de soporte.

Seguir estes pasos adoita solucionar a maioría das incidencias sinxelas.

### ✓ 1. Verifica o máis básico

#### 🔌 1.1. O dispositivo está acendido?

- Asegúrate de que o ordenador, móbil ou impresora están acesos.
- Comproba os cables de alimentación e o enchufe.

#### 🔄 1.2. Reinicia o dispositivo

- Moitos erros corrixen ao reiniciar o equipo.
- Garda o traballo antes de facelo.

#### 🌐 2. Conexión á rede e Internet

##### 📶 2.1. Comproba que estás conectado ao Wi-Fi ou cable

- O icono da rede debe aparecer conectado.
- Se usas cable, comproba que está firmemente conectado en ambos extremos.

##### 🔄 2.2. Proba a desconectarte e conectarte de novo

- Desactiva o Wi-Fi e reactívalo.
- Se tes cable, desconéctao e volve conectalo.

##### 💻 2.3. Comproba noutra páxina ou dispositivo

- Se Internet non funciona:
  - Proba a abrir outra web.
  - Se outros dispositivos tampouco se conectan, pode ser un problema xeral.

### 🔑 3. Contraseñas e acceso a contas

#### 🔑 3.1. Asegúrate de que a contrasinal é correcta

- Compróbaa escribindoa nun bloc de notas para ver se hai erros.
- Lembra que as contraseñas distinguen maiúsculas/minúsculas.

#### 🔄 3.2. Se non lembrás a contrasinal, proba a restaurala

- Usa a opción "Esquecín a miña contrasinal" se está dispoñible.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 4. Programas e aplicacións

#### 4.1. Pecha e abre de novo a aplicación

- Moitos bloqueos arránxanse reiniciando só o programa.

#### 4.2. Comproba actualizacións

- Moitos erros prodúcense por versións antigas.

#### 4.3. Borrar caché / ficheiros temporais

- Navegadores e apps solucionan moitos erros así.

### 5. Impresoras

#### 5.1. Hai papel e tinta?

- Comproba bandeixa, atascos e niveis de tinta/toner.

#### 5.2. A impresora está conectada á rede?

- Se é Wi-Fi, comproba que aparece conectada.
- Se é USB, comproba que o cable está ben.

#### 5.3. Reinicia a impresora

- Apaga, agarda 10 segundos e acende outra vez.

### 6. Comprobacións para equipos de traballo / empresa

#### 6.1. Se usas VPN

- Comproba que a VPN está conectada se precisas acceder a recursos internos.

#### 6.2. Conta bloqueada

- Despois de varios intentos errados podes bloquear a conta.
- Proba a esperar 10 minutos e volver tentar.

### 7. Recolle información antes de chamar a soporte

Para axilizar a resolución, é útil ter:

- Descrición clara do problema
- Mensaxes de erro (ideal: captura de pantalla)
- Que estabas facendo cando ocorreu
- Se o problema afecta só a ti ou a máis persoas
- Pasos que xa probaches

### 8. Cando contactar co soporte técnico

Contacta co soporte se:

- O problema persiste despois das comprobacións básicas
- Non podes iniciar sesión, nin sequera reparando a contrasinal
- Un dispositivo non responde ou non acende
- Ves avisos sospeitosos, posibles virus ou comportamento anómalo
- Tes risco de perda de datos

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### ★ RESUMO RÁPIDO

1. Reinicia o equipo
2. Comproba cables / Wi-Fi
3. Revisa contrasinal e acceso
4. Pecha e abre programas
5. Verifica impresora
6. Se nada funciona → chama a soporte

### > Uso seguro da Wi-Fi

#### Guía para usar unha Wi-Fi de forma segura

Usar redes Wi-Fi é cómodo, pero tamén pode supoñer riscos se non se toman certas precaucións. Seguindo estes pasos garantirás máis seguridade nos teus dispositivos e datos.

#### 1. Conéctate só a redes de confianza

- Usa preferiblemente a Wi-Fi da túa casa, empresa ou institución.
- Evita redes públicas ou descoñecidas (cafetaría, aeroportos, centros comerciais).
- Se é imprescindible usar unha pública, non introduces datos sensibles (contrasinais, banca online, compras).

#### 2. Comproba que a rede está protexida con contrasinal

- A maioría das redes seguras usan cifrado WPA2 ou WPA3.
- Non te conectes a redes abertas (sen contrasinal).
- Se a túa rede doméstica non ten contrasinal, configúraa inmediatamente.

#### 3. Emprega unha contrasinal forte para a túa Wi-Fi

- Mínimo 12 caracteres.
- Mestura letras maiúsculas/minúsculas, números e símbolos.
- Non uses o nome, datas de nacemento ou "12345678".
- Cambia a contrasinal se cres que foi compartida con demasiada xente.

#### 4. Desactiva a conexión automática a redes abertas

Moitos dispositivos conéctanse automaticamente ao primeiro Wi-Fi dispoñible.

- En Windows, macOS, Android e iPhone podes desmarcar "Conectar automaticamente".
- Isto evita conectar por erro a redes perigosas.

#### 5. Usa unha VPN en redes públicas

Se necesitas usar unha Wi-Fi pública:

- Activa unha VPN (Rede Privada Virtual).
- A VPN cifra o tráfico e dificulta que alguén intercepte os teus datos.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 6. Comproba sempre o candado do navegador

Ao entrar nunha web, asegúrate de que a dirección comeza por https:// e aparece o candado. Isto indica que a conexión está cifrada.

### 7. Mantén o dispositivo actualizado

- Actualiza o sistema operativo e as aplicacións.
- Moitas actualizacións solucionan fallos de seguridade.

### 8. Activa o cortalumes (Firewall)

- En Windows e macOS vén activado por defecto.
- Non o desactives salvo indicación técnica.

### 9. Evita compartir arquivos ou carpetas na rede pública

- Desactiva a opción "Compartir arquivos" cando uses redes alleas.
- En Windows: Configuración → Rede → Rede pública → desactivar compartición.

### 10. Desactiva o Wi-Fi cando non o uses

- Aforra batería.
- Impide que o dispositivo busque automaticamente redes inseguras.

### 11. Coida coas redes falsas (Wi-Fi spoofing)

- Os atacantes poden crear redes cun nome similar ao dunha rede lexítima (por ex. "Café\_Free\_WiFi").
- Conéctate só se estás seguro de que é a rede oficial.

### 12. Revisa os dispositivos conectados á túa rede doméstica

Moitos routers permiten ver que dispositivos están conectados:

- Se aparece un dispositivo descoñecido → cambia a contrasinal da Wi-Fi.
- Actualiza o firmware do router.

### 13. Se sospeitas dun ataque

- Desconecta o dispositivo da Wi-Fi.
- Cambia contrasinais sensibles (email, banca, redes sociais).
- Avisalle ao responsable de TI se estás nunha empresa.

---

## ★ RESUMO RÁPIDO

---

1. Conéctate só a redes seguras
2. Usa contrasinais fortes e WPA2/WPA3
3. Evita redes abertas
4. Usa VPN en Wi-Fi públicas
5. Candado HTTPS sempre
6. Actualiza o dispositivo
7. Cortalumes activado

## > Protección de datos persoais na rede

### **Guía para protexer os teus datos persoais en Internet**

A privacidade en liña é esencial para evitar roubos de identidade, fraudes e accesos non autorizados. Seguindo estes pasos, manterás a túa información moito máis segura.

#### **1. Usa contrasinais fortes e únicas**

- Mínimo 12-14 caracteres.
- Mestura letras, números e símbolos.
- Evita datos persoais (data de nacemento, nomes, etc.).
- Non reutilices a mesma contrasinal en varias contas.
- Usa un xestor de contrasinais para gardalas de forma segura.

#### **2. Activa sempre a verificación en dous pasos (2FA)**

Engade unha capa extra de protección:

- Código por SMS ou aplicación (Authy, Google Authenticator...).
- Chaves de seguridade (YubiKey) en contas sensibles.

#### **3. Coida a información que compartes nas redes sociais**

- Evita publicar datos como dirección, número de teléfono, documentos, horarios ou información persoal sensible.
- Revisa a configuración de privacidade das túas redes.
- Non aceptes solicitudes de amizade de descoñecidos.

#### **4. Desconfía de correos, mensaxes ou chamadas sospeitosas**

Antes de abrir ligazóns ou descargar arquivos:

- Comproba o remitente.
- Busca faltas de ortografía ou mensaxes alarmistas.
- Non fagas clic en ligazóns dubidosas: poderían ser phishing.
- Nunca compartas contrasinais ou códigos de seguridade.

#### **5. Navega só en sitios seguros (HTTPS)**

- Verifica que aparece o candado na barra do navegador.
- Evita introducir datos en webs sen HTTPS.

#### **6. Configura adecuadamente a privacidade dos teus dispositivos e apps**

- Revisar permisos das aplicacións (cámara, micrófono, localización).
- Desactiva a localización cando non a precisas.
- Elimina apps que non uses.

#### **7. Mantén sempre actualizado o teu dispositivo**

Actualiza:

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Sistema operativo (Windows, macOS, Android, iOS...)
- Navegadores
- Aplicacións

As actualizacións solucionan moitas vulnerabilidades.

### 8. Usa antivirus e cortalumes

- Mantén o antivirus activo e actualizado.
- Non desactives o cortalumes do sistema operativo.
- Realiza análises periódicas.

### 9. Coida das túas contas de correo electrónico

- É unha das claves de acceso ao resto de contas.
- Usa 2FA obrigatoriamente.
- Evita usar o mesmo correo para contas persoais e profesionais.
- Comproba accesos recentes se sospeitas algo.

### 10. Cautela co uso de Wi-Fi públicas

- Evita introducir contrasinais, datos bancarios ou información persoal en redes públicas.
- Usa unha VPN se necesitas conectarte a servizos sensibles.

### 11. Fai copias de seguridade regularmente

- Copias en nube cifrada (OneDrive, Google Drive, iCloud).
- Copias locais en discos externos.
- Ter unha copia axuda en caso de ransomware ou perda de datos.

### 12. Elimina información persoal cando xa non a precisas

- Borra contas antigas.
- Elimina arquivos sensibles de dispositivos que xa non uses.
- Restablece de fábrica calquera equipo antes de vendelo ou reciclalo.

### 13. Vixía actividades sospeitosas nas túas contas

- Inicios de sesión desde sitios descoñecidos.
- Cambios non autorizados.
- Correos de recuperación inesperados.

Actúa rápido: cambia contrasinais e habilita 2FA.

### RESUMO RÁPIDO

1. Contrasinais fortes e 2FA
2. Ollo co que publicas
3. Coidado con correos e ligazóns
4. Navega só en HTTPS

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



5. Actualizacións e antivirus
6. Nada de datos sensibles en Wi-Fi públicas
7. Copias de seguridade

### > O Transporte seguro de información dixital

#### Guía para o transporte seguro de información dixital

O transporte de información dixital (en USB, nube, correo, dispositivos móbiles, etc.) supón riscos de perda, roubo ou acceso non autorizado. Estas boas prácticas axudan a protexer datos persoais, documentos sensibles e información corporativa.

##### 1. Cifra sempre os datos antes de transportalos

- Usa cifrado forte (AES-256 ou equivalente).
- Para USB ou discos externos, utiliza ferramentas como:
  - BitLocker (Windows)
  - FileVault (macOS)
  - Veracrypt (multiplataforma)
- A información cifrada segue protexida aínda que se perda o dispositivo.

##### 2. Emprega dispositivos de almacenamento seguros

- Prefire USB con cifrado hardware (token criptográficos, pendrives seguros).
- Evita USB promocionais ou de procedencia descoñecida.
- Non uses o mesmo USB para traballo e persoal.

##### 3. Usa contrasinais fortes e 2FA

- Protexe accesos á nube, portátiles e dispositivos móbiles con:
  - Contrasinais robustas
  - Autenticación en dous factores (2FA)
- Nunca transportes datos sensibles en dispositivos sen contrasinal.

##### 4. Transporte en nube só con seguridade reforzada

Se usas OneDrive, Google Drive, Dropbox ou similares:

- Activa 2FA obrigatoriamente.
- Comparte ficheiros con ligazóns protexidas, non públicas.
- Limita o acceso por usuarios e tempo.
- Evita sincronizar automaticamente datos moi sensibles.

##### 5. Ao enviar información por correo electrónico

- Cifra o arquivo antes de envialo.
- Non poñas a contrasinal no mesmo correo: envíaa por outro medio.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Verifica o destinatario antes de premer "Enviar".

### 6. Transporte en dispositivos móbiles

- Activa PIN, contrasinal, Face ID, Touch ID ou patrón seguro.
- Cifra o dispositivo (a maioría xa o fan por defecto).
- Evita levar información crítica en móbiles persoais.
- Ten activado "Buscar o meu dispositivo" en caso de perda.

### 7. Evita o transporte innecesario

- Non te leves datos sensibles se non é imprescindible.
- Usa acceso remoto seguro en vez de transportar datos (VPN corporativa).

### 8. Coidado coas redes Wi-Fi públicas

- Non subas nin descargues datos confidenciais en redes abertas.
- Usa VPN se necesitas traballar fóra da oficina.
- Desactiva Wi-Fi automática.

### 9. Boas prácticas ao desprazarse

- Non perdas de vista os dispositivos en ningún momento.
- Usa mochilas resistentes con compartimento acolchado.
- En transporte público, lévao sempre contigo, non no maletreiro.

### 10. Custodia da documentación física asociada

Se transportas documentos impresos relacionados:

- Gardaos nun maletín pechado.
- Non mestures documentos persoais e profesionais.
- Destrúe copias que xa non precises (tritadora).

### 11. Elimina datos de dispositivos temporais

Se usas un dispositivo que non é teu ou é compartido:

- Non gardes contrasinais no navegador.
- Elimina os arquivos cando acabes.
- Pecha sesión en todas as contas.

### 12. Fai copias de seguridade antes de transportar datos

- Guarda unha copia cifrada nun lugar seguro.
- Evitarás perda de información se o dispositivo desaparece.

### 13. Que facer en caso de perda ou roubo

1. Notificar inmediatamente ao responsable de TI ou seguridade.
2. Cambiar contrasinais relacionadas.
3. Bloquear remotamente o dispositivo, se é posible.
4. Informar segundo proceda (por exemplo, RGPD en contornas corporativas).

## ★ RESUMO RÁPIDO

- Cifra sempre os datos
- Usa USB e dispositivos seguros
- 2FA obrigatoria
- Non uses Wi-Fi pública para información sensible
- Revisa destinatarios antes de enviar
- Custodia física estrita
- Copias de seguridade sempre

## > Actuacións fronte ao phishing e a enxeñería social no correo electrónico

### 🔍 Guía para previr o phishing en correos electrónicos

O phishing é un dos ataques máis comúns: os cibercriminosos fanse pasar por empresas ou persoas coñecidas para roubar información persoal, contrasinais ou datos bancarios. Seguindo estas recomendacións, reducirás ao mínimo o risco.

#### 🔍 1. Desconfía dos correos inesperados

Se recibes un correo que non estabas agardando, especialmente se pide accións urxentes ou datos, toma precaución.

Pregúntate:

- Coñezo este remitente?
- Esperaba este correo?
- Ten sentido o que pide?

#### 👁️ 2. Revisa atentamente o remitente

Os atacantes imitan direccións oficiais cambiando só algunhas letras.

Exemplos perigosos:

- seguridade@micros0ft-support.com
- banco@cliente-servizo.info

⚠️ Se ves erros, dominios raros ou nomes estraños, non abras enlaces nin descargues arquivos.

#### 🔍 3. Busca erros de escritura ou un ton pouco profesional

Moitos correos de phishing conteñen:

- Faltas de ortografía
- Traducións incorrectas ou estrañas
- Logos de baixa calidade
- Un ton alarmante ou demasiado amable

#### 🔍 4. Desconfía das mensaxes que crean urxencia

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



O phishing adoita usar presión psicolóxica:

- “A túa conta será bloqueada en 24 horas”
- “Paga agora para evitar sancións”
- “Actualiza a contrasinal inmediatamente”

As organizacións serias non adoitan actuar así.

### 5. Non fagas clic en ligazóns sospeitosas

- Pasa o rato por enriba do enlace (sen facer clic) para ver a URL real.
- Se a ligazón non coincide coa páxina oficial → non abras.
- Sempre é máis seguro entrar manualmente na web desde o navegador.

### 6. Non abras arquivos anexos dubidosos

Especialmente perigosos:

- .zip, .exe, .html, .docm, .jar
- Arquivos con nomes do tipo “Factura\_urxente.zip”

Se non esperabas o anexo, non o abras nunca.

### 7. Nunca envías contrasinais, códigos ou datos persoais por correo

Ningún banco, empresa nin servizo oficial pide contrasinais por email.

Regra de ouro:

Se piden información persoal por correo, é unha estafa.

### 8. Activa a autenticación en dous pasos (2FA)

Aínda que caias nun engano, isto impide que o atacante acceda á túa conta.

### 9. Usa filtros antispam e ferramentas de seguridade

- Mantén o correo, navegador e antivirus actualizados.
- Moitos sistemas xa detectan phishing automaticamente.

### 10. Verifica sempre mediante outro canal

Se un correo parece do teu banco, empresa ou dun compañeiro:

- Chama por teléfono
- Pregunta por chat corporativo
- Busca o contacto na web oficial

Nunca uses o número ou enlace incluído no propio correo sospeitoso.

### 11. Se sospeitas, non interactúes

- Non contestes
- Non descargues
- Non fagas clic
- Se é posible, marque o correo como phishing ou spam

### 12. Que facer se xa fixeches clic

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



1. Desconecta o dispositivo de Internet.
2. Cambia as contrasinais das contas afectadas.
3. Activa 2FA se non o tiñas.
4. Analiza o equipo con antivirus.
5. Informa ao soporte técnico (se é no ámbito laboral).

### ★ RESUMO RÁPIDO

- Revisa o remitente
- Non fagas clic en ligazóns sospeitosas
- Non abras anexos non solicitados
- Nunca compartas contrasinais
- Desconfía da urxencia
- Verifica sempre por outro medio

### 📘 Guía técnica de enxeñería social (enfoque defensivo)

Identificación, análise e prevención de ataques baseados no factor humano

#### ✳ 1. Que é a enxeñería social?

É o conxunto de técnicas que aproveitan erros humanos, confianza ou falta de información para manipular ás persoas e obter acceso non autorizado a sistemas, datos ou recursos.

Un ataque de enxeñería social pode:

- Enganar a un usuario para revelar información.
- Manipular comportamentos.
- Saltarse medidas técnicas de seguridade explotando o factor humano.

#### 📖 2. Principios psicolóxicos empregados polos atacantes

Estes principios axudan a recoñecer patróns de manipulación sen describir como executalos:

##### ✓ Autoridade

O atacante finxe ser un superior, un técnico ou unha organización oficial.

##### ✓ Urgencia

Presión temporal para que a vítima actúe rápido e sen pensar.

##### ✓ Escaseza

"Última oportunidade", "acceso limitado", etc.

##### ✓ Reciprocidade

O atacante ofrece algo para obter algo a cambio.

##### ✓ Confianza e familiaridade

Simula relacións persoais ou profesionais.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### ✓ Medo e ameaza

Advertencias de sancións, bloqueos ou problemas graves.

### 🔧 3. Principais vectores de ataque

#### 3.1. Phishing (correo electrónico)

Imitación de empresas, bancos ou servizos para roubar contrasinais ou datos.

Sinais de alerta:

- Remitentes sospeitosos.
- Ligazóns que non coinciden coa web oficial.
- Faltas de ortografía ou ton alarmista.
- Solicitude de información sensible.

#### 3.2. Smishing e vishing (SMS e chamadas)

Mensaxes ou chamadas que piden códigos, datos bancarios ou que instan a realizar accións inmediatas.

Como previlo:

- Non fornecer datos por teléfono.
- Verificar sempre a identidade do interlocutor por outra vía.

#### 3.3. Pretexting

O atacante crea un escenario falso para obter confianza (ex: "son técnico de TI").

Como detectalo:

- Solicitudes inesperadas.
- Datos incoherentes.
- Falta de identificación verificable.

#### 3.4. Baiting (cebo)

Entrega de dispositivos físicos manipulados (USB, CD), descargas tentadoras ou ofertas enganosas.

Prevención:

- Non inserir USB descoñecidos.
- Descargar software só de fontes oficiais.

#### 3.5. Tailgating / Piggybacking (intrusión física)

Acceso a instalacións seguindo a un empregado que abre a porta.

Medidas defensivas:

- Pechar portas con control de acceso.
- Non permitir que persoas non autorizadas entren sen identificación.

### 🔧 4. Métodos de análise e detección

- Monitorización do comportamento
  - Tentativas de acceso non habituais.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Solicitudes de información fora de procedemento.
- Revisión de comunicacións sospeitosas
  - Correo antispam avanzado.
  - Filtros de reputación de dominios.
  - Alertas sobre anexos perigosos.
- Formación continua
  - Simulacións éticas de phishing (sen dano).
  - Talleres de concienciación.
  - Avaliación periódica de riscos humanos.

### 5. Medidas técnicas de prevención

- Control de acceso robusto
  - 2FA / MFA obrigatoria.
  - Segregación de privilexios.
- Políticas de contrasinais
  - Longas, únicas e almacenadas nun xestor de contrasinais.
- Cifrado de datos
  - Cifrado en tránsito e en repouso.
  - Cifrado de dispositivos portátiles e USB.
- Actualizacións
  - Parches regulares de software.
  - Navegadores e antivirus actualizados.

### 6. Medidas organizativas

- Políticas claras
  - Normas sobre uso de correo, acceso físico e remoto.
  - Procedementos para verificar identidade de provedores e compañeiros.
- Cultura de seguridade
  - O persoal debe sentirse cómodo dicindo “non” a solicitudes sospeitosas.
  - Fomentar a denuncia de comportamentos estraños.
- Canles de reporte
  - Correo dedicado a incidentes.
  - Ferramentas de reporte rápido en apps corporativas.

### 7. Resposta ante incidentes de enxeñería social

1. Non interactuar máis co atacante.
2. Cambiar inmediatamente contrasinais implicadas.
3. Informar ao equipo de seguridade ou TI.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



4. Illar o dispositivo se se fixo clic nun enlace malicioso.
5. Análise forense (segundo proceda).
6. Notificación legal se hai datos afectados (ex: RGPD).

### ★ RESUMO TÉCNICO

- A enxeñería social explota persoas, non sistemas.
- O recoñecemento de sinais psicolóxicas é clave.
- Os vectores máis comúns: phishing, smishing, chamadas, pretexting e intrusión física.
- A prevención require formación, procedementos, tecnoloxía e cultura de seguridade.
- A resposta rápida reduce impacto e perdas.

### > Reporte de incidentes de seguridade da información

#### 📌 Guía para reportar incidentes de seguridade da información

Un incidente de seguridade é calquera evento que poida comprometer datos, sistemas, servizos ou usuarios. Reportar axiña permite reducir danos, evitar propagación e cumprir coas obrigas legais (ex: RGPD).

#### 📌 1. Que é un incidente de seguridade?

Considérase incidente, entre outros:

- Phishing ou intentos de estafa
- Contraseñas comprometidas
- Malware, virus ou ransomware
- Acceso non autorizado a contas ou equipos
- Perda/roubo de dispositivos (portátiles, móbiles, USB...)
- Envío accidental de información sensible a destinatarios erróneos
- Fallos de servizos críticos (correo, VPN, sistemas corporativos)
- Descubrir dispositivos ou software estraño ou non autorizado

#### 📌 2. Que facer se detectas un incidente? (pasos iniciais)

1. Manter a calma e evitar accións que empeoren a situación.
2. Non apagar o equipo
  - Agás instrucións do departamento de TI (importante para investigación).
3. Desconectar de Internet (se hai malware ou comportamento sospeitoso)
  - Apagar Wi-Fi / retirar cable de rede.
4. Non borrar arquivos nin modificar probas
  - Isto dificulta a análise.
5. Non interactuar con correos ou ligazóns sospeitosas

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Nin responder nin abrir anexos.

### 3. Como reportar correctamente un incidente

#### 3.1. Canles oficiais de notificación

Segundo a organización, pode ser:

- Correo: [seguridade@empresa.com](mailto:seguridade@empresa.com)
- Sistema interno de tickets
- Teléfono de urxencias de TI
- Responsable de seguridade / DPD
- Aplicación corporativa de reporte

(Se queres, pode crear un modelo de procedemento adaptado á túa empresa.)

#### 3.2. Información que debes incluír no reporte

- Datos básicos
  - Nome e contacto do usuario afectado.
  - Departamento/servizo.
- Descrición breve do incidente
  - Que aconteceu?
  - Cando o detectaches?
  - Como o descubriches?
- Elementos implicados
  - Equipo ou dispositivo (PC, móbil, USB...).
  - Contas ou servizos afectados (correo, ERP, OneDrive, VPN...).
- Accións que xa realizaches
  - Desconectar Internet, cambiar contrasinal, informar a un superior...
- Evidencias dispoñibles
  - Capturas de pantalla.
  - Correos sospeitosos sen abrir.
  - Mensaxes de erro.

(Non manipules as evidencias, só descríbeas ou achégaas sen alterar.)

### 4. Cando reportar?

Sempre canto antes, incluso se non estás seguro de que é un incidente real.

Reporta inmediatamente se:

- Fixeches clic nun enlace sospeitoso.
- Deches datos por erro.
- Tes un comportamento estraño no ordenador.
- Estás vendo actividade non recoñecida na túa conta.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Perdes un dispositivo con información corporativa.
- Ocorre un ataque de phishing masivo.

### 5. Que fará o equipo de seguridade?

1. Confirmará o incidente (análise inicial).
2. Conterá a ameaza (illamento, bloqueo de contas, etc.).
3. Eliminará o risco (limpeza, restauración, parcheado).
4. Analizará o impacto (usuarios afectados, datos implicados).
5. Notificará se é necesario segundo RGPD / lexislación.
6. Reforzará medidas preventivas para evitar repeticións.

### 6. Boas prácticas adicionais

- Formación continua en phishing, contrasinais e seguridade.
- Usar 2FA en todos os servizos posibles.
- Non instalar software non autorizado.
- Non conectar USB descoñecidos.
- Actualizar equipos e apps regularmente.

## ★ RESUMO RÁPIDO

1. Detectas algo raro → non ignores.
2. Non apagues nin borres nada.
3. Desconecta Internet se ves actividade perigosa.
4. Recopila información básica.
5. Reporta inmediatamente polo canal oficial.

## > A Intelixencia Artificial (IA) nos cibertataques

### ☉ Intelixencia Artificial nos Ciberataques: Guía Completa

A IA converteuse nunha ferramenta poderosa para mellorar a eficiencia e automatización, pero tamén está sendo utilizada polos ciberdelincuentes para aumentar a complexidade, velocidade e impacto dos ciberataques.

É importante coñecer como a IA pode ser usada de forma maliciosa para poder previr e defenderse.

#### 🔥 1. Como utilizan a IA os ciberdelincuentes?

##### 1.1. Phishing hiperpersoalizado

A IA analiza datos públicos (redes sociais, webs corporativas, filtracións) e xera correos ou mensaxes:

- altamente personalizados
- con linguaxe natural moi convincente

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- adaptados ao estilo da vítima

Isto aumenta drasticamente a taxa de éxito.

### 1.2. Xeración automática de contidos maliciosos

A IA pode crear:

- Correos de spear phishing perfectos
- Páxinas de phishing realistas
- Documentos con macro-malware
- Chatbots falsos que interactúan coa vítima

Todo isto a gran escala e case sen erros gramaticais.

### 1.3. Ataques de forza bruta intelixentes

A IA aprende patróns de contrasinais e é capaz de:

- Predicir contrasinais máis probables
- Reducir o tempo de descifrado
- Optimizar ataques de "password spraying"

### 1.4. Evasión de sistemas de detección

Os ciberdelincuentes usan IA para:

- Modificar malware automaticamente ata que non sexa detectado
- Saltar filtros de antispam
- Cambiar comportamentos para evitar EDR/XDR

É un xogo do gato e rato, pero automatizado.

### 1.5. Ataques de deepfake

A IA pode crear:

- Voces falsas de directivos
- Vídeos manipulados
- Chamadas automáticas convincentes

Isto permite fraudes como o CEO fraud, onde un directivo falso ordena transferencias ou acceso a información.

### 1.6. Exploración automatizada de vulnerabilidades

Co uso de IA é posible:

- Identificar servizos expostos
- Buscar vulnerabilidades coñecidas
- Crear exploits adaptados
- Escanear internet de forma masiva

Todo cunha velocidade moi superior á humana.

## 2. Tipos de ataques con IA máis comúns

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Phishing e spear-phishing automatizado
- Ataques de ransomware máis rápidos e eficientes
- Ataques contra dispositivos IoT
- Ataques autónomos que toman decisións
- DDoS adaptativo e autooptimizado
- Suplantación de identidade mediante deepfake

### 3. Como defenderse dos ciberataques con IA?

#### 3.1. Emprender tamén IA para defensa

A mellor defensa é empregar IA na ciberseguridade, como en:

- Sistemas EDR/XDR con detección comportamental
- Análise de comportamento de usuario (UEBA)
- Filtros antiphishing intelixentes
- Firewall con modelado de tráfico

#### 3.2. Formación continua en novas ameazas

As persoas son o obxectivo principal. Necesitan saber recoñecer:

- deepfakes
- correos intelixentes de phishing
- mensaxes demasiado personalizadas
- usos sospeitosos de chatbots

#### 3.3. Políticas robustas

- MFA obrigatorio
- Contraseñais fortes + xestores
- Acceso baseado en privilexios mínimos
- Parches e actualizacións regulares

#### 3.4. Seguridade por capas

A defensa debe incluír:

- Antivirus/EDR
- Firewall
- Seguridade en correo
- Seguridade cloud
- Monitorización continua

#### 3.5. Xestión de identidades e accesos (IAM)

A IA é moi eficaz explotando malas prácticas: compartir contraseñais, contas similares, permisos excesivos.

A disciplina IAM minimiza o impacto.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 🗣️ 4. IA defensiva vs IA ofensiva: o equilibrio actual

A carreira entre atacantes e defensores con IA está en pleno crecemento.

Os ciberdelinquentes gañan velocidade e automatización, pero os equipos de seguridade dispoñen tamén de ferramentas capaces de:

- detectar comportamentos anómalos
- bloquear patróns sospeitosos
- responder a incidentes de forma automatizada

A clave está na actualización constante e na adopción de tecnoloxías modernas.

### 📌 5. Resumo

A IA nos ciberataques permite:

- ataques máis rápidos
- máis difíciles de detectar
- máis personalizados
- máis baratos de executar

Pero tamén permite mellores defensas se se implementan correctamente.

### > Seguridade nas videoconferencias

#### 🔒 Guía de Seguridade en Videoconferencias

As ferramentas de videoconferencia son fundamentais no traballo e formación, pero tamén introducen riscos: accesos non autorizados, filtración de datos, suplantación de identidade ou gravacións non autorizadas.

Seguir boas prácticas reduce estes riscos e garante reunións seguras.

#### 📌 1. Antes da videoconferencia

##### 1.1. Usa só plataformas oficiais ou aprobadas

Evita ferramentas descoñecidas ou non autorizadas pola túa organización.

Asegúrate de ter a versión máis recente.

##### 1.2. Configura unha contrasinal ou chave de acceso

A reunión debe ter:

- Contrasinal
- Sala de espera (lobby)
- Control de acceso do anfitrión

Isto evita intrusións (zoombombing).

##### 1.3. Actualiza a aplicación

Moitos ataques explotan versións antigas.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



Activa as actualizacións automáticas.

### 1.4. Revisa permisos da cámara e micrófono

Só permite acceso ás apps necesarias.

### 1.5. Comproba a configuración de privacidade

Desactiva por defecto:

- compartición automática de pantalla
- acceso de invitados sen control
- inicio automático da cámara

## 2. Durante a videoconferencia

### 2.1. Controla quen entra

Acepta só participantes recoñecidos.

Se a plataforma o permite, bloquea a reunión unha vez comecen todos.

### 2.2. Activa a autenticación

Prioriza:

- acceso mediante conta corporativa
- autenticación multifactor (MFA)
- invitacións personalizadas

### 2.3. Desactiva o micrófono e cámara de participantes por defecto

Evita interrupcións e uso inadecuado.

### 2.4. Restrinxe o uso de chat, ficheiros ou pantallas compartidas

Só para persoas que realmente o necesiten.

### 2.5. Coida a información que se mostra

Evita amosar:

- documentos sensibiles
- pantallas con datos persoais
- notas privadas visibles detrás de ti

### 2.6. Evita conexións en Wi-Fi públicas

Se é imprescindible: usa VPN.

## 3. Gravacións da reunión

### 3.1. Grava só se é necesario

E sempre informando os participantes, por motivos legais (protección de datos).

### 3.2. Garda as gravacións de forma segura

- nube corporativa (OneDrive/SharePoint)
- acceso limitado
- cifrado e control de permisos

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 3.3. Evita envialas por correo ou reenviarlle a terceiros

Usa ligazóns con vencemento ou permisos específicos.

## 4. Seguridade dos dispositivos

### 4.1. Ten o equipo actualizado

Sistema operativo, navegador e cliente de videoconferencia.

### 4.2. Antivirus e firewall activados

Especialmente en equipos persoais.

### 4.3. Cambia fondo, se estás nun lugar privado

Evitas que aparezan datos persoais ou información sensible detrás de ti.

## 5. Sinais de alerta durante a reunión

Presta atención a:

- participantes descoñecidos
- solicitudes de compartir pantalla sospeitosas
- mensaxes no chat pedindo códigos, contrasinais ou documentos
- comportamento non habitual
- intentos de expulsar ao anfitrión

Ante calquera dúbida: pecha a reunión e volve abríla con novos axustes de seguridade.

## 6. Despois da reunión

### 6.1. Revise as gravacións e documentos compartidos

Elimina os que non necesites.

### 6.2. Revise os permisos

Retira acceso a participantes externos ou convidados temporais.

### 6.3. Pecha sesión na plataforma se non se usa

Especialmente en computadores compartidos.

## 7. Recomendacións adicionais para administradores

- Configurar políticas corporativas de seguridade
- Desactivar funcións de risco por defecto (chat externo, transferencias...)
- Activar rexistros de auditoría
- Implementar acceso mediante SSO/MFA
- Analizar alertas de contas comprometidas
- Formar aos usuarios en riscos e boas prácticas

---

## Resumo rápido

---

1. Usa plataforma oficial e actualizada.
2. Pon contrasinal e sala de espera.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



3. Controla acceso e permisos.
4. Non compartas información sensible.
5. Grava só se é imprescindible.
6. Revisa permisos ao rematar.

### > A suplantación de identidade nos ciberataques

#### Guía sobre os ataques de Suplantación de Identidade (Identity Spoofing / Impersonation)

A suplantación de identidade é unha das técnicas máis utilizadas polos ciberdelinquentes para enganar persoas ou sistemas, co obxectivo de obter información, acceder a contas, roubar cartos ou comprometer dispositivos.

#### 1. Que é a suplantación de identidade?

É un ataque no que o agresor finge ser outra persoa ou entidade para gañar confianza e conseguir que a vítima realice unha acción:

- abrir unha ligazón
- descargar un ficheiro
- dar información confidencial
- aprobar un pago
- instalar software

Pode facerse por correo, SMS, chamadas, redes sociais, videoconferencias ou webs falsas.

#### 2. Tipos máis comúns de suplantación de identidade

##### 2.1. Phishing tradicional

Correos que simulan ser dunha empresa ou servizo:

- bancos
- correos oficiais
- redes sociais
- provedores de servizos

Piden que introduzas datos nunha páxina falsa.

##### 2.2. Spear phishing

Moito máis dirixido.

O atacante investiga á vítima e envía un correo personalizado co seu nome, cargo, clientes, etc.

##### 2.3. CEO fraud / Business Email Compromise (BEC)

O ciberdelincente suplanta a un directivo e solicita:

- transferencias urxentes
- envío de datos sensibles
- compra de tarxetas regalo

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



Moi frecuente en empresas.

### 2.4. Smishing (SMS)

Mensaxes que finxen ser dun banco, seguridade social ou empresas de reparto.

### 2.5. Vishing (chamadas telefónicas)

Manipulación por voz.

O atacante pode usar IA para imitar voces de directivos ou familiares.

### 2.6. Suplantación en redes sociais

Perfís falsos que solicitan información, diñeiro ou enlaces fraudulentos.

### 2.7. Suplantación técnica

- falsificación de correo (spoofing)
- manipulación de IP ou DNS
- páxinas web falsas idénticas ás reais

## 🔔 3. Sinais de alerta dunha posible suplantación

No correo electrónico:

- remitente sospeitoso ou semellante ao real (+ ou - unha letra)
- ligazóns acurtadas ou que non coinciden coa web real
- erros gramaticais
- ton urxente ou ameazante
- peticións de datos persoais

En SMS ou WhatsApp:

- mensaxes inesperadas cun enlace
- solicitudes de códigos 2FA
- supostos problemas con pagos ou entregas

En chamadas telefónicas:

- petición de datos confidenciais
- presión para actuar rápido
- uso de tecnoloxía para simular números oficiais (caller ID spoofing)

En redes sociais:

- perfís recién creados
- fotos roubadas
- solicitudes de cartos ou datos
- mensaxes con ligazóns raras

## 🔒 4. Como protexerse da suplantación de identidade

### 4.1. Verificar sempre a identidade

- Comprobar o correo do remitente

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Confirmar por outra vía (teléfono, chat corporativo)
- Non confiar en números que aparecen como “oficiais”

### 4.2. Non facer clic en ligazóns sospeitosas

Accede sempre manualmente á páxina escribindo o enderezo no navegador.

### 4.3. Usar Autenticación Multifactor (MFA)

Incluso se rouban o contrasinal, sen o 2FA non poden acceder.

### 4.4. Configurar contrasinais fortes

E NON reutilices a mesma nas túas contas.

### 4.5. Actualiza sistemas e aplicacións

Moitos ataques explotan fallos xa corrixidos.

### 4.6. Formación continua

O factor humano é a liña de defensa máis importante.

Recoñecer sinais sospeitosos é clave.

### 4.7. Non compartas información sensible

Ningunha empresa lexítima pedirá:

- contrasinais
- códigos 2FA
- datos bancarios por correo ou SMS

## 5. Que facer se sospeitas que estás sendo vítima?

1. Non interactúes (non respondas, non fagas clic).
2. Captura pantallas se é necesario para reporte.
3. Cambia inmediatamente o contrasinal da conta afectada.
4. Activa ou revisa o 2FA.
5. Desconecta o dispositivo da rede se hai comportamento estraño.
6. Contacta co departamento de TI ou soporte de seguridade.
7. Denuncia se procede (policía, INCIBE).

## 6. Medidas para empresas e organizacións

- Implementación de filtros antiphishing avanzados
- Solucións de protección de correo con análise de ameazas
- Políticas claras de validación de pagos e solicitudes sensibles
- Bloqueo de dominios fraudulentos
- Campañas regulares de concienciación
- Auditorías periódicas de seguridade
- Sistemas de detección de comportamento anómalo

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### ■ Resumo rápido

- ➡ A suplantación de identidade baséase na confianza.
- ➡ Os ciberdelincuentes buscan que actúes con rapidez e sen pensar.
- ➡ Verificar a identidade e manter boas prácticas de seguridade evita a maioría de ataques.

### > Copias de seguridade

#### 📘 Guía de Copias de Seguridade (Backups)

As copias de seguridade son unha das medidas máis importantes para protexer a información fronte a perdas, fallos técnicos, erros humanos, malware (incluído ransomware) ou roubos.

Dispoñer dun bo sistema de backup evita interrupcións graves e garante a continuidade do traballo.

#### 🔴 1. Que é unha copia de seguridade?

É unha copia dos teus datos feita nun lugar diferente ao orixinal, coa finalidade de recuperalos en caso de perda, borrado accidental ou ataque informático.

#### 🔴 2. Por que son tan importantes?

Porque protexen fronte a:

- Fallos de hardware
- Ransomware ou malware
- Erros humanos
- Roubo ou perda de dispositivos
- Incendios, inundacións ou danos físicos
- Corrupción de arquivos

Unha copia de seguridade só é útil se pode restaurarse cando se precisa.

#### 🔴 3. Principios básicos dunha boa estratexia de backup

##### 3.1. Regra 3-2-1 (recomendada a nivel internacional)

- 3 copias dos datos
- 2 almacenadas en soportes distintos
- 1 fóra da túa localización (cloud, dispositivo externo, backup remoto)

Esta combinación ofrece protección fronte a calquera escenario.

##### 3.2. Copias automáticas

As copias manuais esquecen e fallan.

Sempre que sexa posible, configura backups automáticos segundo unha programación fixa.

##### 3.3. Comprobar a integridade das copias

Non basta con ter copias:

Hai que verificar periodicamente que se poden restaurar.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 3.4. Cifrado

A información nos backups debe estar cifrada, especialmente se contén datos persoais ou profesionais.

## 4. Tipos de copias de seguridade

### 4.1. Backup completo

Copia todo o contido.

- Recuperación rápida
  - Gran tamaño

### 4.2. Backup incremental

Só copia o que cambiou desde a última copia incremental.

- Ocupa menos
  - Recuperación máis lenta

### 4.3. Backup diferencial

Copia todos os cambios desde o último backup completo.

- Punto intermedio entre completo e incremental
  - Tamaños maiores que o incremental

### 4.4. Backup continuo (CBT)

Ideal en empresas; monitorea cambios en tempo real.

## 5. Onde gardar as copias de seguridade?

### 5.1. Nube

(OneDrive, Google Drive, iCloud, Dropbox, servizos corporativos)

- cómodo e automático
- acceso dende calquera lugar
- seguro se se usa MFA e cifrado

### 5.2. Discos externos

- baratos
- non conectalos sempre ao PC (para evitar ransomware)

### 5.3. NAS (servidores domésticos ou empresariais)

- ideais para varias máquinas
- permiten automatizar tarefas
- deben estar protexidos e actualizados

### 5.4. Backup fóra das instalacións

Crucial para empresas (BaaS, centros remotos, cintas).

## 6. Boas prácticas ao facer backups

### 6.1. Usa contrasinais fortes e MFA

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



Especialmente para servizos baseados na nube.

### 6.2. Aílla copias críticas de ransomware

Un disco conectado permanentemente pode infectarse.

Usa:

- copias desconectadas
- snapshots inmutables
- almacenamento só-lectura

### 6.3. Documenta o que se copia

Que datos inclúese, con que frecuencia e onde se gardan.

### 6.4. Non dependas só dun servizo

Diversifica: local + nube.

### 6.5. Garda versións

Se un arquivo se corrompe, unha única copia non resolve nada.

Activa a opción de "versións anteriores".

## 7. Plan de recuperación ante desastres (DRP)

Un bo sistema de backup debe incluír:

- como restaurar os datos
- quen é o responsable
- tempos máximos aceptables de recuperación
- orden de prioridade
- probas periódicas de restauración

Nunha empresa, isto é esencial para continuidade de negocio.

## 8. Que facer se perdes datos?

1. Non seguir usando o dispositivo.
2. Non reinstalar nin borrar nada.
3. Comprobar dispoñibilidade das copias.
4. Restaurar a versión máis recente íntegra.
5. Revisar por que ocorreu para evitar repeticións.

---

## Resumo rápido

---

- 3 copias
- 2 soportes diferentes
- 1 fóra da localización
- Copias automáticas e cifradas
- Probar a restauración periodicamente

## > Limpeza do escritorio

### ✂ Guía para Manter un Escritorio Limpo e Seguro

Un escritorio limpo mellora a produtividade, reduce erros, evita perdas de información e reforza a seguridade dos datos. Manter a zona de traballo ordenada tamén axuda a cumprir políticas de protección da información (Clean Desk Policy).

#### ✦ 1. Beneficios dun escritorio limpo

- Menos distraccións → mellor concentración
- Menor risco de perda ou fuga de documentos
- Prevención de accesos non autorizados
- Facilitade para atopar o que necesitas
- Boa imaxe profesional
- Menos risco de danos físicos (derrames, caídas, desorde nos cables)

#### 📁 2. Principios básicos para manter o escritorio limpo

##### 2.1. Só debe haber o necesario

Deixa no escritorio unicamente:

- ordenador
- teclado e rato
- libreta ou bloco
- material mínimo imprescindible

O resto gárdao en caixóns ou armarios.

##### 2.2. Nada de papel visible con información sensible

Evita deixar á vista:

- documentos con datos persoais
- contrasinais
- informes internos
- listados de clientes ou estudantes

Destrúe o que non se use (tritadora) ou gárdao en lugar seguro.

##### 2.3. Cables organizados

Usa:

- bridas de velcro
- clips organizadores
- pasacables

Evita enredos e caídas, e facilita limpeza.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 2.4. Mantén comida e bebida afastadas

Evita derrames sobre equipos e documentos.

### 3. Seguridade: política de "escritorio limpo"

Especialmente importante en oficinas e administracións públicas.

#### 3.1. Pechado de sesión obrigatorio

Cando te ausentes:

- bloquea o equipo (Win + L)
- pecha sesión se marchas máis tempo

#### 3.2. Documentación gardada e segura

Usa:

- caixóns con chave
- armarios de seguridade
- bandeixas personalizadas

Nunca deixes documentos sensíbles á vista.

#### 3.3. Nada de contrasinais en post-its

Usa un xestor de contrasinais (1Password, KeePass, Bitwarden...).

### 4. Organización física do escritorio

#### 4.1. Unha revisión diaria (2 minutos)

Ao final da xornada:

- tira o lixo
- garda documentos
- recoloca materiais
- limpa a superficie

#### 4.2. Cestas ou bandeixas de entrada/saída

Separar o pendente do completado axuda a evitar caos.

#### 4.3. Limpeza semanal máis profunda

- monitor
- teclado
- rato
- superficie completa
- cables

### 5. "Escritorio limpo" tamén no ordenador

O escritorio do PC tamén debe estar ordenado.

#### 5.1. Evita cheo de iconos

Garda arquivos en:

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Documentos
- Nube corporativa (OneDrive, SharePoint...)
- Cartafóles organizados

### 5.2. Nomea os arquivos de forma clara

Evita "novo.docx", "copia(5).xlsx"...

Use:

Proxecto\_Informe\_2025\_v1.docx

### 5.3. Borrado regular do que non se necesita

Un escritorio cargado ralentiza e dificulta o traballo.

## 6. Recomendacións para empresas e centros

- Crear unha política formal de escritorio limpo
- Revisar periodicamente o cumprimento
- Formar ao persoal en seguridade da información
- Instalar contedores de destrución de documentación
- Facilitar armarios e caixóns con chave
- Habilitar zonas libres de papel para áreas sensibles

---

## Resumo rápido

---

1. Deixa só o necesario no escritorio.
2. Nada de documentos sensibles á vista.
3. Bloquea o PC sempre que te ausentes.
4. Organiza cables e materiais.
5. Mantén tamén o escritorio do PC ordenado.
6. Fai unha revisión diaria e limpo semanal.

---

## > Uso de software libre ou de código aberto

---

### Guía sobre o Uso de Software Libre

O software libre é aquel que respecta a liberdade dos usuarios e dálles control sobre o programa, permitindo usalo, estudalo, modificalo e redistribuílo. É unha alternativa sólida, segura e ética ao software privativo.

#### 1. Que é o software libre?

Segundo a Free Software Foundation, un software é libre se garante estas catro liberdades:

1. Liberdade de usar o programa con calquera propósito.
2. Liberdade de estudar como funciona e modificalo.
3. Liberdade de distribuír copias.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 4. Liberdade de mellorar o programa e compartir melloras.

O software libre pode ser gratuíto ou non, pero sempre é aberto e auditable.

#### ★ 2. Vantaxes do software libre

##### 2.1. Seguridade e transparencia

O código é aberto → calquera pode auditalo.

Menos portas traseiras, mellor detección de vulnerabilidades.

##### 2.2. Aforro económico

Moito software libre é gratuíto, reducindo custos en:

- licenzas
- actualizacións
- escalabilidade

##### 2.3. Independencia de provedores

Evita quedar “atrapado” cunha marca ou empresa concreta (vendor lock-in).

##### 2.4. Personalización total

O código pode adaptarse ás necesidades da organización.

##### 2.5. Colaboración e comunidade

Miles de voluntarios e organizacións melloran o software continuamente.

##### 2.6. Cumprimento legal e ético

Especialmente relevante en administracións públicas, educación e entidades sen ánimo de lucro.

#### 📁 3. Exemplos de software libre popular

- Sistema operativo:
  - GNU/Linux (Ubuntu, Debian, Fedora, Mint...)
- Navegadores:
  - Firefox, Chromium
- Ofimática:
  - LibreOffice, OnlyOffice
- Edición de imaxe e vídeo:
  - GIMP, Inkscape, Krita
  - Blender, Kdenlive
- Desenvolvemento:
  - VS Code – OSS, Atom, Eclipse
  - Linguaxes: Python, PHP, Ruby, Go...
- Servizos de infraestrutura:
  - Apache, Nginx
  - PostgreSQL, MariaDB

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Proxmox, pfSense
- Comunicación:
  - Thunderbird
  - Jitsi (videoconferencia)

### 4. Software libre e seguridade

O software libre adoita ser máis seguro porque:

- permite auditorías externas
- as actualizacións son rápidas
- non depende dunha única empresa
- o código é verificable
- a comunidade detecta erros antes

Pero tamén require:

- configuración adecuada
- mantemento e actualizacións regulares
- elección de proxectos activos e con soporte

### 5. Boas prácticas no uso do software libre

#### 5.1. Escoller proxectos con comunidade activa

Actualizacións recentes, documentación e soporte.

#### 5.2. Verificar a orixe das descargas

Sempre dende:

- páxina oficial
- repositorios oficiais
- fontes confiables

#### 5.3. Manter o software actualizado

Actualizacións = máis seguridade.

#### 5.4. Revisar licenzas

Licenzas típicas:

- GPL
- LGPL
- MIT
- Apache

Son abertas, pero algunhas teñen requisitos de redistribución.

#### 5.5. Usar repositorios corporativos en empresas

Para controlar versións e dependencias.

### 6. Adopción de software libre en organizacións

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 6.1. Avaliación inicial

- necesidades reais
- compatibilidade
- formación necesaria
- soporte técnico

### 6.2. Migración progresiva

Comezar con ferramentas compatibles:

- LibreOffice
- Firefox
- Thunderbird

E despois sistemas máis avanzados se é viable (servidores Linux).

### 6.3. Formación do persoal

A clave para o éxito é ensinar a usar as ferramentas.

### 6.4. Soporte profesional

Moitas empresas ofrecen soporte comercial para software libre.

#### ■ Resumo rápido

- O software libre é seguro, transparente e económico.
- Permite modificar, estudar e compartir o código.
- É ideal para educación, administración pública e empresas que buscan independencia.
- Require manterse actualizado e escoller proxectos activos.

#### > Uso seguro de medios e dispositivos electrónicos

##### Guía para o Uso Seguro de Medios Electrónicos

Os medios electrónicos inclúen calquera soporte ou dispositivo que permita almacenar, transmitir ou procesar información, como:

- Ordenadores, portátiles
- Móviles, tablets
- Discos duros, USB, SSD
- Tarxetas SD
- Correos electrónicos
- Servizos na nube
- Plataformas de mensaxería
- Redes e conexións de internet

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### TEMARIO TICS

Para reducir riscos e manter a seguridade da información, é fundamental seguir boas prácticas como as que se describen a continuación.

#### 1. Seguridade en dispositivos físicos

##### 1.1. Protexe o acceso ao dispositivo

- Usa contrasinais seguras ou frase de paso longa.
- Activa autenticación biométrica cando sexa posible.
- Configura o bloqueo automático tras uns minutos de inactividade.

##### 1.2. Mantén o dispositivo actualizado

- Instala actualizacións do sistema operativo e das aplicacións.
- Activa a actualización automática.

##### 1.3. Cifra o dispositivo

Isto protexe a información mesmo se o dispositivo é roubado ou perdido.

- Windows: BitLocker
- macOS: FileVault
- Linux: LUKS
- Móviles: cifrado nativo do sistema

##### 1.4. Controla o acceso aos portos USB

- Non utilices dispositivos USB descoñecidos.
- Desactiva portos USB se non precisas usalos (opción corporativa).

#### 2. Boas prácticas no uso de memorias externas (USB, discos duros)

##### 2.1. Compra dispositivos de calidade e marcas coñecidas

- Evitas fallos e malware preinstalado.

##### 2.2. Escanea sempre os dispositivos

- Usa antivirus para analizar calquera soporte externo antes de abrir ficheiros.

##### 2.3. Cifra o contido sensible

- Usa ferramentas como VeraCrypt, BitLocker-To-Go ou LUKS.

##### 2.4. Evita almacenar datos críticos en memorias sen control

- Especialmente información persoal, contrasinais, documentos corporativos.

##### 2.5. En caso de perda ou roubo

- Comunica o incidente ao soporte ou responsable de seguridade.
- Bloquea as contas asociadas (se era un móbil ou portátil).

#### 3. Uso seguro de correo electrónico e mensaxería

##### 3.1. Verifica sempre o remitente

- O phishing é a principal vía de ataque.

##### 3.2. Non abras ligazóns sospeitosas

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



Desconfía de:

- URIs abreviadas
- mensaxes inesperadas
- peticións urxentes

### 3.3. Non envíes información sensible por correo sen cifrar

Utiliza:

- anexos cifrados (ZIP con contrasinal forte, 7z, VeraCrypt)
- servizos corporativos seguros

### 3.4. Evita mensaxería persoal para traballo

Ex.: WhatsApp persoal, Telegram sen control, etc.

## 4. Seguridade en conexións e redes

### 4.1. Evita redes Wi-Fi públicas para tarefas sensibles

Se non hai alternativa, usa:

- VPN corporativa
- Navegación cifrada (HTTPS)

### 4.2. Configura adecuadamente a túa rede doméstica

- Cambia o contrasinal do router
- Actualiza o firmware
- Usa WPA3 ou WPA2 como mínimo

### 4.3. Desactiva Bluetooth, NFC e Wi-Fi cando non os uses

- Reduce riscos de ataques automáticos.

## 5. Uso seguro de servizos na nube

### 5.1. Usa plataformas oficiais e verificadas (OneDrive, Google Drive...)

Desconfía de webs descoñecidas.

### 5.2. Non subas datos sensibles sen cifrado previo

O cifrado extremo-a-extremo ofrece maior seguridade.

### 5.3. Controla os permisos de compartición

Revisa:

- quen pode ver
- quen pode editar
- durante canto tempo

### 5.4. Elimina ligazóns compartidas que xa non necesitas.

## 6. Xestión segura de contrasinais

### 6.1. Usa un xestor de contrasinais

KeePass, Bitwarden, 1Password...

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 6.2. Activa a autenticación en dous pasos (2FA)

Mellor con aplicacións tipo Authenticator.

### 6.3. Non reutilices contrasinais

Cada conta debe ter unha diferente.

### 7. Uso seguro en videoconferencias e plataformas online

- Actualiza o software de videoconferencias.
- Usa salas protexidas con contrasinal.
- Non compartas pantalla sen revisar antes que se vai ver.
- Pecha sesións e salas ao rematar.

### 8. Que facer ante un incidente?

Se cres que un dispositivo ou medio electrónico foi comprometido:

1. Desconéctao da rede.
2. Non continúes usando o dispositivo.
3. Informa inmediatamente ao servizo de soporte ou ao responsable de seguridade.
4. Se hai datos persoais afectados, é posible que teña que notificarse á autoridade correspondente (AEGD/autoridade autonómica).

### Resumo rápido

- Mantén todo actualizado
- Usa contrasinais fortes + 2FA
- Cifra dispositivos e arquivos sensibles
- Coidado co que conectas (USB, redes Wi-Fi)
- Usa correo e nube de maneira segura
- Reacciona rápido ante incidentes

### > Ransomware

#### Guía para a Detección e Protección ante Ransomware

O ransomware é un tipo de malware que cifra os datos dun dispositivo ou rede e esixe un rescate para recuperalos. É unha das ameazas máis graves para persoas e empresas.

Esta guía explica como detectalo, como protexerte e que facer se fas fronte a un ataque.

#### 1. ¿Como funciona o ransomware?

O ataque adoita seguir estas fases:

- 1. Infección
  - A través dun correo malicioso, descarga fraudulenta, vulnerabilidade ou USB contaminado.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- 2. Execución silenciosa
  - O malware instálase sen avisar.
- 3. Cifrado de ficheiros
  - Bloquea documentos, imaxes, bases de datos...
- 4. Eliminación de copias locais (se é posible)
  - Moitas variantes tentan borrar copias de seguridade conectadas.
- 5. Pantalla de rescate
  - Aparece unha mensaxe pedindo diñeiro a cambio da clave de descifrado.

### 2. Sinais temperás de infección (detección)

- Indicios no sistema
  - Forte ralentización sen motivo.
  - Procesos descoñecidos usando moito CPU.
  - Actividade de disco inusual ou continua.
  - Mensaxes de erro sobre ficheiros inaccesibles.
- Cambios en ficheiros
  - Arquivos que non se poden abrir.
  - Extensións modificadas (.lock, .crypted, .enc...).
- Comportamentos sospeitosos
  - Ventás que aparecen e desaparecen.
  - Tentativas de desactivar antivirus.
  - Alertas do EDR/antivirus sobre cifrado masivo.
- Actividade na rede
  - Conexións estrañas a servidores externos.
  - Incremento de tráfico cifrado inesperado.

### 3. Medidas de protección antes dun ataque

#### 3.1. Copias de seguridade (o máis importante)

- Fai copias periódicas, íntegras e probadas.
- Segue a regra 3-2-1:
  - 3 copias en total
  - 2 en medios diferentes
  - 1 fóra da rede (offline ou na nube segura)
- Impide que os usuarios teñan permisos de borrar copias.

#### 3.2. Protección perimetral e antivirus

- Antivirus/EDR sempre actualizado.
- Firewall activado e configurado.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Bloqueo de macros de Office por defecto.
- Filtrado de correo e URLs sospeitosas.

### 3.3. Boas prácticas de usuario

- Non abrir correos nin anexos de remitentes descoñecidos.
- Non descargar software ou cracks de webs non fiables.
- Non conectar USB descoñecidos.
- Sospeitar de mensaxes urxentes ou estrañas.

### 3.4. Actualizacións e parches

- Sistema operativo actualizado.
- Navegadores e plugins ao día.
- Parcheo regular de aplicacións corporativas.
- Moito ransomware entra por vulnerabilidades coñecidas.

### 3.5. Principio de mínimos privilexios

- Os usuarios non deben ter permisos de administrador.
- Control de acceso a cartafóles críticos.
- Segmentar a rede para limitar o impacto.

## 4. Que facer se sospeitas dun ataque?

### 4.1. Aillamento inmediato

- Desconecta o dispositivo da rede (Wi-Fi e cable).
- Non apagues o equipo se estás nunha empresa (pode ser necesario analizar memoria).
- Se es usuario doméstico, si podes apagalo para evitar máis cifrado.

### 4.2. Informa ao equipo de soporte ou seguridade

- Non intentes restaurar o sistema pola túa conta.
- Non elimines ficheiros nin programas recentes.

### 4.3. Non pagues o rescate

- Non garante a recuperación dos datos.
- Financia o delito.
- En moitos países desaconséllase legalmente.

### 4.4. Usa ferramentas de descifrado se existen

Algunhas variantes están documentadas e teñen ferramentas de recuperación legais e gratuítas (por exemplo, NoMoreRansom).

## 5. Recuperación tras un ataque

- Restaurar copias de seguridade fiables
  - Nunca dende copias conectadas no momento do ataque.
- Reinstalar sistemas infectados

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Reinstalación limpa e segura.
- Cambiar todas as contrasinais
  - O atacante puido capturalas.
- Auditar a infraestrutura
  - Para evitar reinfeccións.
- Informar ás autoridades se houbo datos persoais
  - Obrigatorio en moitos casos (RGPD/GDPR).

## 6. Resumo rápido

Para detectar ransomware:

- Lentitud, arquivos cifrados, procesos sospeitosos, alertas de antivirus.

Para protexerte:

- Copias de seguridade 3-2-1
- Actualizacións e antivirus
- Precaución con correos e descargas
- Mínimos privilexios

Se xa estás infectado:

- Ailla o equipo
- Notifica a seguridade
- Non pagues rescates
- Restaura dende copias seguras

## > Navegación web

### Guía de Seguridade na Navegación Web

A maior parte das ameazas actuais entran a través da web: páxinas comprometidas, descargas perigosas, scripts maliciosos, anuncios infectados ou formularios falsos. Navegar con seguridade é clave para protexer os teus datos, os teus dispositivos e a túa privacidade.

#### 1. Usa sempre conexións seguras (HTTPS)

- Comproba que a páxina comeza por https:// e mostra un cadeado no navegador.
- Evita introducir contrasinais ou datos persoais en páxinas sen HTTPS.
- Se o navegador mostra un aviso de “conexión non segura”, non continúes.

#### 2. Mantén actualizado o navegador

- Actualiza Chrome, Firefox, Edge ou Safari regularmente.
- Activa as actualizacións automáticas.
- Moitas vulnerabilidades explótanse a través de versións antigas.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### 3. Coidado coas ligazóns sospeitosas

- Non fagas clic en ligazóns que che cheguen por correo, SMS ou mensaxería sen estar seguro da súa lexitimidade.
- Pasa o cursor sobre a ligazón para ver o destino real antes de abrir.
- Desconfía sempre de mensaxes con urxencia artificial ("a túa conta será bloqueada").

### 4. Descargas seguras

- Descarga só de:
  - páxinas oficiais
  - repositorios fiables
  - tendas de aplicacións coñecidas
- Evita programas "crackeados", extensións non verificadas ou software dubidoso.
- Usa antivirus ou EDR para analizar arquivos descargados.

### 5. Controla as extensións do navegador

- Instala só extensións necesarias.
- Revisa os permisos que solicitan (acceso a todas as webs, lectura de datos...).
- Elimina extensións que non uses ou que non teñan boa reputación.

### 6. Non introduces datos persoais en webs non verificadas

- Verifica sempre que o sitio é auténtico: URL, certificado, grafismo, dominio.
- Evita entregar:
  - DNI/pasaporte
  - datos bancarios
  - contrasinais
  - información profesional sensible
- Se unha web pide máis datos dos necesarios, desconfía.

### 7. Usa ferramentas de protección

- Antivirus ou EDR actualizado
  - Bloquea páxinas maliciosas e descargas perigosas.
- Bloqueador de anuncios
  - Moitos ataques entran por publicidade infectada (malvertising).
- Navegadores con protección antiphishing
  - Chrome, Edge e Firefox teñen listas actualizadas de sitios perigosos.
- DNS seguro
  - Emprega DNS filtrado (como Cloudflare Family ou OpenDNS) para bloquear dominios maliciosos.

### 8. Protexe a túa privacidade mentres navegas

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Borrar regularmente cookies e historial.
- Usar modo incógnito para sesións puntuais (non é seguridade total, pero axuda).
- Desactivar ou limitar a localización.
- Evitar acceder a contas persoais en dispositivos alleos.

### 9. Navegación segura en redes públicas

- Non introduzas contrasinais nin datos sensibles.
- Usa VPN sempre que poidas.
- Desconecta Wi-Fi/Bluetooth cando non os uses.
- Evita descargar ficheiros en redes abertas.

### 10. Recoñece sinais dunha páxina fraudulenta

- Erros ortográficos ou deseño pobre.
- Logotipos ou estilos que non coinciden coa entidade real.
- Dominio parecido pero non idéntico (ex.: "micros0ft.com").
- Solicitude de información persoal que normalmente non se pide.
- Ventás emerxentes insistentes.

### 11. Que facer se algo parece sospeitoso?

- Pecha a xanela ou pestana sen facer clic en nada.
- Non descargues nin aceptes ningún ficheiro.
- Escanea o equipo cun antivirus.
- Cambia contrasinais se sospeitas que unha web falsa puido capturalas.
- Se é un equipo corporativo, informa a soporte ou seguridade.

### Resumo rápido

- Navega sempre con HTTPS.
- Mantén navegador e sistema actualizados.
- Coidado con ligazóns e descargas sospeitosas.
- Usa ferramentas de protección (antivirus, bloqueadores, DNS seguro).
- Non introduzas datos persoais en webs non fiables.
- Evita redes Wi-Fi públicas para tarefas sensibles.
- Se algo parece raro, detén e revisa.

### > Arquivos comprimidos

#### Como comprimir un ficheiro ou carpeta

##### 1. En Windows (ZIP estándar)

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



Windows permite comprimir sen instalar nada.

Comprimir unha carpeta ou ficheiro:

1. Localiza o ficheiro ou carpeta.
2. Fai clic dereito enriba.
3. Selecciona "Enviar a".
4. Escolle "Carpeta comprimida (zip)".
5. Crearase un arquivo ZIP no mesmo lugar co mesmo nome.

Descomprimir:

- Fai dobre clic no ZIP e logo en "Extraer todo".

### 2. Comprimir cun contrasinal (arquivo cifrado)

Moi útil para enviar documentos sensibles.

En Windows con 7-Zip:

1. Clic dereito → 7-Zip → Add to archive...
2. En "Encryption" escribe o contrasinal.
3. Marca "Encrypt file names" para máis seguridade.
4. Preme OK.

### Formatos máis comúns

- ZIP: o estándar, compatible con todo.
- 7Z: mellor compresión, pero require 7-Zip.
- RAR: moi usado, pero require WinRAR.
- TAR.GZ: común en Linux.

## > Lexislación sobre seguridade da información e protección de datos

### Principais normas en España — protección de datos e seguridade da información

| Norma / Regulación                     | Obxecto / O que regula                                                                                                                                                                                                                                                                                   | Ámbito principal                                                        |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Reglamento (UE) 2016/679 (RGPD / GDPR) | Regulación europea xeral sobre protección de datos persoais. Establece principios, dereitos das persoas (acceso, rectificación, supresión, portabilidade, etc.), obrigacións para quen trata datos, criterios de seguridade, notificación de brechas, consentimento, transferencias internacionais, etc. | Todos os Estados da UE; en España trasposto mediante normativa nacional |

**CONCELLO DE CARBALLO**

C.I.F.: P1501900C

Praza do Concello S/N

Teléfono 981 70 41 00

www.carballo.gal

infocarballo@carballo.gal

15100 CARBALLO - A Coruña

**TEMARIO TICS**

| Norma / Regulación                                                                                                                          | Obxecto / O que regula                                                                                                                                                                                                                                                                                      | Ámbito principal                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Ley Orgánica 3/2018, de Protección de Datos Personales e garantía de los Derechos Digitales (LOPDGDD)                                       | Adapta o RGPD ao ordenamento español e regula tamén dereitos dixitais específicos en España. Recolla regras sobre tratamento e protección de datos, dereitos dos interesados, obrigas de seguridade, consentimento, menores, dereito ao "olvido", transparencia, e define sancións.                         | Toda España, empresas, administracións, organizacións, profesionais... que traten datos persoais                         |
| Ley Orgánica 7/2021, de protección de datos persoais tratados para fins de prevención, investigación e enjuiciamiento de infraccións penais | Regula o tratamento de datos persoais relacionados con condenas, delitos e execución penal — un subgrupo especial de datos especialmente protexido.                                                                                                                                                         | Organismos de xustiza, policía, administracións públicas, procesos penais                                                |
| Real Decreto-ley 12/2018, de seguridade das redes e sistemas de información                                                                 | Transpoñía á lexislación española a directiva europea NIS (seguridade das redes e sistemas). Obriga a operadores de servizos esenciais e provedores de servizos dixitais a aplicar medidas de seguridade, notificar incidentes, garantir resiliencia.                                                       | Infraestruturas críticas, servizos esenciais, telecomunicacións, empresas de servizos dixitais, administracións públicas |
| Real Decreto 43/2021, de 26 de xaneiro — desenvolvemento do Real Decreto-ley 12/2018                                                        | Regulación detallada das obrigas de seguridade, notificacións de incidentes, requisitos técnicos e organizativos para redes e sistemas de información de entidades suxeitas á norma NIS.                                                                                                                    | Mesmos suxeitos que o anterior — infraestruturas críticas, servizos esenciais e provedores dixitais                      |
| Real Decreto 311/2022 — Esquema Nacional de Seguridade (ENS)                                                                                | Establece principios básicos e requisitos mínimos de seguridade que deben cumprir administracións públicas e, en moitos casos, organizacións que colaboran con elas. Regula confidencialidade, integridade, dispoñibilidade, trazabilidade, protección da información que se xestiona en entornos públicos. | Administración pública, entidades que prestan servizos públicos, organismos, empresas contratistas etc.                  |

**✓ Que implica para cidadáns, empresas ou entidades**

- Se tratas datos de persoas (nome, DNI/NIE, contacto, saúde, datos sensibles...), debes cumprir co RGPD + LOPDGDD. Isto significa garantir consentimento, transparencia, dereitos de usuarios, seguridade, notificación se hai brecha de seguridade...
- As empresas ou organizacións con servizos críticos ou de infraestrutura deben aplicar os requirimentos do Real Decreto-ley 12/2018 / Real Decreto 43/2021: medidas de seguridade, xestión de riscos, resiliencia, notificacións ante incidentes.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



### TEMARIO TICS

- No caso da administración pública (ou empresas que colaboran con ela), deben cumprir o ENS (Real Decreto 311/2022) para garantir confidencialidade, integridade e dispoñibilidade da información e dos servizos.
- Para datos de criminalidade, condenas ou infraccións penais, aplícase a Lei Orgánica 7/2021, que impón restricións especiais e maior protección.

#### ✦ Aspectos claves da normativa de protección de datos

- Dereito ao acceso, rectificación, supresión, oposición, portabilidade dos datos.
- Obrigación de obter consentimento claro e informado para tratar datos persoais — e fronte a menores, regras especialmente estritas.
- Obrigación de aplicar medidas de seguridade técnica e organizativa adaptadas ao risco (conforme RGPD / LOPDGDD + normas de seguridade como ENS)
- En caso de brecha de seguridade ou incidente que comprometa datos persoais → obriga a notificar á autoridade competente (na maior parte dos casos, a Agencia Española de Protección de Datos — AEPD) nun prazo determinado.

#### 🔍 Normativas de seguridade da información e ciberseguridade

Co aumento das ameazas dixitais, non só se regula a protección de datos persoais, senón tamén a seguridade de redes e sistemas:

- A directiva NIS (e a súa transposición estatal co Real Decreto-ley 12/2018 + Real Decreto 43/2021) obriga a entidades que xestionan servizos esenciais a implantar medidas de seguridade, avaliar riscos e notificar incidentes.
- O Esquema Nacional de Seguridade (ENS) define requisitos mínimos para organismos públicos, reforzando a protección da información en administracións e en calquera organización que traballe con datos públicos.

Isto supón que as normas de ciberseguridade e protección de datos van de man, especialmente para administracións e empresas que xestionan información de terceiros ou crítica.

#### 📌 Como usar este marco legal no día a día

1. Identificar se tratas datos persoais ou datos sensibles — aplicar RGPD + LOPDGDD.
2. Garantir dereitos aos interesados: información, consentimento, acceso, supresión, portabilidade...
3. Implantar medidas de seguridade: cifrado, control de acceso, copias, políticas internas.
4. Para organizacións/institucións: avaliar se están suxeitas a NIS ou ENS; se é así, elaborar plans de seguridade e risco.
5. Diseñar procedementos para brechas: detección, resposta, notificación.
6. Formar ao persoal: concienciación, boas prácticas, políticas de protección de datos.

#### > Doble factor de autenticación

##### 🔑 Guía sobre sistemas de dobre factor de autenticación (2FA)

#### 1. Que é o 2FA?

O dobre factor de autenticación é un método de seguridade que require dous pasos diferentes para verificar a identidade dun usuario.

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



En vez de iniciar sesión só cunha contrasinal, engádese un segundo factor adicional que dificulta o acceso non autorizado.

### 2. Tipos de factores de autenticación

O 2FA baséase normalmente en tres categorías de factores:

1. Algo que sabes
  - Contrasinal
  - PIN
  - Preguntas de seguridade
2. Algo que tes
  - Código dun token físico
  - Código dun authenticator (Google Authenticator, Microsoft Authenticator...)
  - SMS ao móbil
  - Tarxeta intelixente (SmartCard)
  - USB de seguridade (YubiKey, SoloKey...)
3. Algo que es
  - Biometría: pegada dixital, recoñecemento facial, iris, voz...

Un sistema 2FA sempre combina dous destes factores.

Por exemplo: contrasinal (algo que sabes) + código no móbil (algo que tes).

### 3. Métodos de 2FA máis comúns

- Aplicacións de autenticación
  - Google Authenticator
  - Microsoft Authenticator
  - Authy
  - FreeOTP

Vantaxes: moi seguras, non dependen de cobertura móbil.

Desvantaxes: se perdes o móbil é importante ter códigos de recuperación.

- SMS ou chamada telefónica
  - Envíase un código dun só uso (OTP) ao móbil.

Vantaxes: fácil e sen instalar apps.

Desvantaxes: menos seguro (posible SIM swapping ou interceptación).

- Correos de verificación
  - Envíase un código ou ligazón ao correo electrónico.

Vantaxes: moi sinxelo.

Desvantaxes: menos seguro, depende da seguridade do propio correo.

- Chaves de seguridade (hardware)

## CONCELLO DE CARBALLO

C.I.F.: P1501900C  
Praza do Concello S/N  
Teléfono 981 70 41 00  
www.carballo.gal  
infocarballo@carballo.gal  
15100 CARBALLO - A Coruña



- Dispositivos físicos USB/NFC como YubiKey, SoloKey ou FidoKey.

Vantaxes: o método máis seguro actualmente.

Desvantaxes: teñen un custo e poden perderse.

### — Biometría

- FaceID, pegada dixital, recoñecemento de iris...

Vantaxes: cómodo e rápido.

Desvantaxes: non sempre válido como único factor, depende do dispositivo.

## 4. Por que deberías usar 2FA?

### Beneficios principais

- Protexe contas incluso se rouban a contrasinal.
- Evita accesos non autorizados por filtracións de bases de datos.
- Impide ataques de forza bruta ou probas automáticas de contrasinais.
- Reduce riscos de phishing (especialmente con hardware keys).
- É esixido por moitos estándares de seguridade (ENS, ISO 27001...).

## 5. En que contas é imprescindible activalo

É recomendable activalo en todas as contas, pero especialmente nestas:

- Correo electrónico (Gmail, Outlook...)
- Servizos corporativos
- Redes sociais (Facebook, Instagram, X/Twitter, TikTok)
- Servizos bancarios
- OneDrive, Google Drive, Dropbox
- Github / Gitlab
- Amazon / compras online
- Administración electrónica (Chave365, etc.)

## 6. Boas prácticas para usar 2FA

- Garda códigos de recuperación nun lugar seguro e físico.
- Se cambias ou perdes o móbil, actualiza o 2FA antes.
- Prefire aplicacións de autenticación antes que SMS.
- Para máxima seguridade, usa chaves físicas FIDO2.
- Non compartas códigos coa ninguén; son persoais e dun só uso.
- Activa tamén notificacións de login para detectar accesos sospeitosos.

## 7. Riscos a ter en conta

- Phishing sofisticado pode intentar capturar códigos (sobre todo SMS).
- Ataques de SIM swapping poden redirixir SMS.
- Perder o teléfono sen ter códigos de emerxencia pode bloquear o acceso.

**CONCELLO DE CARBALLO**

C.I.F.: P1501900C

Praza do Concello S/N

Teléfono 981 70 41 00

[www.carballo.gal](http://www.carballo.gal)[infocarballo@carballo.gal](mailto:infocarballo@carballo.gal)

15100 CARBALLO - A Coruña

**TEMARIO TICS****8. Conclusión**

O 2FA é unha das medidas de seguridade máis sinxelas, baratas e efectivas que existen. Engade unha capa adicional de protección que dificulta enormemente os ataques, e debería estar sempre activado en contas importantes.

En Carballo, documento asinado dixitalmente na data indicada á marxe

Luis Miguel Castro García

Xefe do servizo de Informática e Novas Tecnoloxías