

MARCO NORMATIVO DE SEGURIDADE

NOR_001 NORMATIVA DE USO DE MEDIOS ELECTRÓNICOS



CONCELLO DE RIANXO

CONTROL DE SINATURAS

ELABORADO POR:

RESPONSABLE DO SISTEMA

20/01/2026

APROBADO POR:

RESPONSABLE DO GOBERNO - ALCALDE

20/01/2026

CONTROL DE VERSIÓNS

- | | | |
|-----|------------|----------------------------------|
| 1.0 | 20.01.2026 | Responsable do Sistema |
| | | Versión inicial do documento |
| 1.1 | 03.03.2026 | Responsable do Sistema |
| | | Revisión do control de sinaturas |

NORMATIVA DE USO DE MEDIOS ELECTRÓNICOS

1. OBXECTIVO

Esta normativa foi aprobada pola Alcaldía do Concello de Rianxo e entrará en vigor ao día seguinte da súa aprobación até que sexa substituída por unha nova modificación ou unha nova normativa.

2. REVISIÓN E ACTUALIZACIÓN

O contido desta normativa revisarse cunha periodicidade anual. As modificacións que se puideren producir deberán ser aprobadas polo mesmo órgano. Tras cada modificación, a nova normativa deberá ser informada e difundida entre as persoas afectadas por ela.

3. OBXECTO

Este documento establece a normativa de uso seguro de los medios electrónicos no Concello de Rianxo (de aquí en diante, a Organización), dentro do ámbito sinalado no Esquema Nacional de Seguridade (ENS).

Os sistemas de información son elementos básicos para o desenvolvemento da actividade da Organización. Estes medios póñense ao dispor das persoas usuarias como instrumentos de traballo para o desempeño da súa actividade profesional, motivo polo cal estes recursos débense utilizar de maneira responsable, mediante o seguimento de normas e boas prácticas que salvagarden a seguridade da información, os sistemas de información e os recursos tecnolóxicos proporcionados pola entidade.

4. ALCANCE

Mediante esta normativa, a Organización establece a regulación do Uso dos Medios Electrónicos do seu sistema de información, incluído o acceso remoto aos mesmos, a través do establecemento de medidas de **cumprimento obrigatorio para todo o persoal**, quedando suxeitos á mesma, así como aos principios morais e éticos na utilización dos recursos postos ao seu dispor.

O persoal de terceiros (empresas provedoras, convenios, etc.) con acceso ao sistema queda asemade suxeito á mesma normativa, na medida na que lle sexa de aplicación, así como aos principios morais e éticos na utilización dos recursos postos ao dispor destas persoas usuarias para o desempeño das súas actividades na Organización.

En diante, utilizarase “as persoas usuarias” ou “o persoal” para referirse tanto ao persoal propio coma ao de terceiros.

5. CANLE DE SOLICITUDES E NOTIFICACIÓNS

As solicitudes de autorización e as notificacións reflectidas nesta normativa dirixiranse con carácter xeral á persoa co rol asignado de Responsable de Seguridade a **seguridade@concelloderianxo.gal**

Cando cumpra a comunicación dun incidente de seguridade segundo a normativa aprobada, segundo o establecido a nivel de procedemento, ou como primeira resposta a un posible incidente de seguridade, ademais de á persoa Responsable de Seguridade, as persoas usuarias da organización deberán contactar sen demora coa Deputación da Coruña a través do Centro de Atención ao Usuario (CAU) en horario laboral ou por teléfono no caso de producirse o incidente fóra dese horario.

6. INCIDENTES DE SEGURIDADE

Cando unha persoa usuaria detecte calquera anomalía (mal funcionamento, aplicacións que non arrincan ou que se pechan de maneira inesperada, perda de documentos, de memorias USB, etc.) ou incidente de seguridade (virus, suplantación de identidade, perdas de clave, etc.) que poida comprometer o bo uso e funcionamento dos Sistemas de Información da Organización ou poida danar á súa imaxe, deberá informar inmediatamente á canle especificada no punto anterior.

7. NORMATIVA DE USO DOS MEDIOS ELECTRÓNICOS

7.1 NORMAS DE UTILIZACIÓN DO EQUIPAMENTO INFORMÁTICO E DE COMUNICACIÓNS

Estas normas aplícanse de forma específica **a todos os dispositivos facilitados e configurados pola Organización**, incluíndo equipos de sobremesa, portátiles e dispositivos móbiles con capacidades de acceso aos Sistemas de Información.

A Organización proporcionará ao persoal o equipamento debidamente configurado con acceso aos servizos e aplicacións que sexan necesarios para o desempeño das súas funcións.

O persoal aplicará as normas xerais para todo o equipamento, e para os equipos portátiles e dispositivos móbiles aplicará as normas específicas para este tipo de equipamento.

7.1.1 NORMAS XERAIS

- Os equipos deberán de utilizarse unicamente para fins institucionais profesionais e como ferramenta para o desempeño das tarefas encomendadas. Cada equipo estará asignado a unha única persoa. Esta persoa é responsable do seu correcto uso.
- No caso de que un equipo deba ser compartido entre varias persoas, cada unha delas disporá dun perfil protexido para o seu uso exclusivo, ou mecanismo similar.
- Agás autorización expresa, non se dispoñerán de privilexios de administrador sobre os equipos.
- Unicamente o persoal autorizado poderá distribuír, instalar ou desinstalar software e hardware, ou modificar a configuración de calquera dos equipos.
- Cando sexa necesario instalar equipos que non fosen provistos pola Organización, será necesario solicitar unha autorización previa.
- As persoas usuarias deberán notificar, o máis axiña posible, calquera comportamento anómalo dos seus equipos (lentitude, non arrinca, non funciona correctamente, etc.), especialmente cando existan sospeitas de que se produciu algún incidente de seguridade no mesmo. Do mesmo xeito deberase comunicar a ausencia de cables ou accesorios ou calquera outra evidencia de deterioración ou manipulación do equipo.
- Con carácter xeral, non está permitido o uso de dispositivos propios para o acceso ou almacenamento de información, agás autorización expresa.

7.1.2 NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTILES E DISPOSITIVOS MÓBILES

Para os portátiles e móbiles, ademais das normas xerais, serán de aplicación aa seguintes:

- Estes dispositivos estarán, en todo momento baixo a custodia da persoa usuaria que os utilice, que será a responsable de adoptar as medidas necesarias para evitar danos ou subtracción, así como do acceso a eles por parte de persoas non autorizadas.
- A subtracción ou perda destes equipos hase de notificar inmediatamente para a adopción das medidas que correspondan.
- Cando estes equipamentos se deban utilizar para conectarse remotamente a través de redes que non estean baixo o control da organización ou que non fosen autorizadas, deberase solicitar unha autorización, que se fará extensible tamén aos servizos aos que se accede.
- Cando se modifiquen as circunstancias profesionais (finalización dunha tarefa, cesamento no cargo, etc.) que orixinaron a entrega dun recurso informático portable, a persoa usuaria devolverao, co obxecto de proceder ao borrado seguro da información almacenada e restaurar o equipo ao seu estado orixinal para que poida ser asignado a

unha nova persoa.

7.2 NORMAS PARA O ALMACENAMENTO DE INFORMACIÓN E COPIAS DE SEGURIDADE

Para garantir a dispoñibilidade da información fronte a un incidente de seguridade, de forma periódica realízanse **copias de seguridade das unidades de rede compartidas**.

Por este motivo, as persoas usuarias deberán almacenar nestas unidades os datos xerados no desempeño das súas competencias profesionais. Toda a información que non sexa gardada nestas unidades non se considerará información relevante para a Organización, polo que poderá ser destruída en calquera momento no caso de ser necesaria unha intervención no equipamento ou calquera outra circunstancia que obrigue a facelo.

Nos casos de equipamentos que non estean conectados ás unidades compartidas de rede, estableceranse outras formas de garantir a copia de seguridade da información relevante.

Non está permitido o almacenamento de información privada nin de terceiros alleos nestes recursos da Organización.

A información almacenada nas copias de seguridade poderá ser recuperada no caso de que se produza algún incidente de seguridade. Para recuperar esta información débese xerar unha solicitude de restauración.

7.3 NORMAS DE USO PARA SOPORTES DE ALMACENAMENTO EXTRAÍBLES

Como norma xeral, o uso de soportes ou medios de almacenamento extraíbles (memorias USB, discos ríxidos, etc.) non está autorizado. Para a súa utilización deberase de contar coa debida autorización xustificada.

No caso de que á persoa usuaria se lle autorice o uso deste tipo de soportes de traballo, as normas a ter en conta son as seguintes:

- Como norma xeral, utilizaranse os soportes extraíbles proporcionados pola Organización, que estarán destinados a un uso exclusivamente profesional, como ferramenta de **transporte puntual** de ficheiros, e non como ferramenta de almacenamento.
- Polo tanto, non se poderán almacenar nestes medios datos persoais.
- O uso de medios de almacenamento extraíbles particulares, non está autorizado, agás autorización específica.
- Os dispositivos extraíbles **deberán estar cifrados e protexidos por un contrasinal** por medio dun sistema de cifrado de código aberto, seguindo as instrucións da persoa responsable do Sistema.

Estes dispositivos deberán de almacenarse en lugares seguros, co obxecto de previr roubos ou o acceso de terceiras persoas non autorizadas. A perda ou subtracción destes dispositivos, con indicación do seu contido, deberá poñerse en coñecemento de forma inmediata.

O transporte destes soportes fóra das instalacións da Organización deberá ser realizado exclusivamente por persoal autorizado, autorización que contemplará igualmente a propia información que sala. Nese caso deberase de enviar unha solicitude para que se lle asesore sobre as medidas de seguridade que será necesario adoptar (por exemplo, cifrado da información).

7.3.1 NORMAS PARA O BORRADO E ELIMINACIÓN DE SOPORTES INFORMÁTICOS

Os medios de almacenamento que, por obsolescencia ou degradación, perdan a súa utilidade, e especialmente aqueles que conteñan datos de carácter persoal, deberán ser eliminados de forma segura para evitar accesos á devandita información. Neste sentido, a persoa usuaria deberá ter en conta as seguintes indicacións:

- Asegurarse que o contido do soporte pode ser eliminado.
- Solicitar ás persoa responsable do Sistema a eliminación segura da información.

A reutilización de medios de almacenamento para outros fins diferentes dos que orixinaron o seu uso require dun borrado seguro previo do medio.

7.4 NORMAS RESPECTO Á XESTIÓN DE DOCUMENTOS

7.4.1 IMPRESORAS EN REDE, FOTOCOPIADORAS E ESCÁNERES

Con carácter xeral, deberán utilizarse as impresoras de rede e as fotocopiadoras corporativas. Excepcionalmente, poderán instalarse impresoras locais, xestionadas por un posto de traballo de usuario. Neste caso, a instalación irá precedida da autorización pertinente.

En ningún caso se poderá facer uso de impresoras e fotocopiadoras que non fosen proporcionadas pola Organización.

Con relación aos sistemas de copia, impresión e documentación impresa, o persoal debe seguir as seguintes directrices:

- Os documentos, con carácter xeral, xeraranse en formato electrónico. Deberanse dixitalizar todos aqueles que non sexan susceptibles de ser xerados de forma electrónica.
- Cando se impriman documentos en sistemas de impresión ou copia comúns, contarase cun servizo de impresión segura, autenticándose o usuario a través dun PIN para evitar

que terceiras persoas poidan acceder aos documentos.

- Tras a realización de copias de documentos e escaneados, débense retirar os orixinais.
- No caso de atoparse documentación allea nun sistema de copia ou impresión, a persoa usuaria tentará localizar á persoa propietaria para que proceda á súa recollida inmediata. No caso de descoñecer á persoa propietaria ou non estar localizable, poñerá inmediatamente en coñecemento das persoas responsables.
- Evitárase na maior medida posible a impresión de documentos en papel, a menos que sexa absolutamente necesario, coa fin de minimizar os riscos de seguridade e tamén coa fin de evitar un uso excesivo dos recursos, e mellorar o impacto ambiental.

7.4.2 COIDADO E PROTECCIÓN DA DOCUMENTACIÓN IMPRESA

A documentación debe ser protexida, de forma que só teña acceso a ela o persoal autorizado.

Para estes efectos, as persoas usuarias terán en conta as seguintes medidas:

- Os postos de traballo permanecerán despexados, sen máis material enriba da mesa que o requirido para a actividade que se está a realizar en cada momento.
- Mentres a documentación non estea sendo utilizada, deberase gardar en sistemas de almacenamento (armarios ou archivadores) preferentemente baixo chave. Non poderán ser exhibidos en taboleiros ou similares.
- Unha vez que un documento deixe de ser necesario, débese eliminar utilizando os medios postos ao dispor por parte da entidade (destrutora de documentos), de forma que non sexa recuperable a información que puidesen conter.
- Antes de abandonar as salas de reunións ou permitir que alguén alleo acceda ás mesmas, limparanse adecuadamente os encerados e recolleranse todos os documentos, coidando de que non quede ningún tipo de información sensible ou interna accesible a persoas non autorizadas.

7.4.3 ACCESO A DOCUMENTOS COMPARTIDOS E TRABALLO COLABORATIVO

As solucións autorizadas para compartir documentos e traballar neles de forma colaborativa son:

- O xestor de expedientes corporativo (TEDeC)
- As ferramentas específicas corporativas (Sivalwin, Ginpix, GRM, Intercops...)
- Xestores de expedientes externos (SUISS, Plataforma de Contratación...)
- As unidades de rede compartidas (discos de rede)

- O correo electrónico corporativo (GMail corporativo)
- Outras ferramentas relacionadas cos servizos asociados ao correo corporativo (Google Workspace corporativo: calendarios, mensaxería, videoconferencia...)
- Calquera outra autorizada previamente polo Responsable do Sistema

Non está permitido o almacenamento ou compartición de información de forma remota ou na nube en sistemas ou servizos que non sexan os previstos pola Organización para esa fin. O anexo 10.2 recolle as solucións preferentes e non permitidas para o seu uso no Concello de Rianxo.

Se fose estritamente necesario, de forma excepcional, para enviar ou compartir arquivos de gran tamaño, tanto de forma interna como externa, poderase empregar a plataforma *Almacén* do Estado: <https://ssweb.seap.minhap.es/almacen/>

Os permisos asignados aos cartafoles e documentos que se almacenan nestas plataformas serán revisados para asegurar que só teñen permisos as persoas adecuadas e os documentos non sexan accesibles de forma pública.

Non se pode almacenar información da Organización no almacenamento local dos equipos, agás para traballo temporal ou outros documentos de apoio que non sexan documentos oficiais.

Como garantía adicional para a documentación sensible, dispoñeráse dunha ferramenta que permita que a información corporativa se poida compartir protexida e baixo control e monitorizando os accesos aos documentos, que permita establecer permisos de acceso e reportar os accesos bloqueados aos documentos.

Estableceranse as seguintes medidas de protección dos documentos:

- A documentación unicamente será accesible polas persoas autorizadas, de forma que as persoas usuarias da plataforma colaborativa ou de compartición unicamente accederán aos cartafoles ou documentos autorizados, xa sexa para consulta, descarga, modificación ou supresión, así como para incorporar novos documentos.
- Estableceranse permisos a nivel de usuario ou grupos de usuarios.
- Debe dispoñerse da máxima trazabilidade posible de acceso aos documentos.

7.5 POSTO DE TRABALLO DESPEXADO

Os postos de traballo deben permanecer despexados, sen máis material encima da mesa que o requirido para a actividade que se está realizando en cada momento.

7.6 BLOQUEO DO POSTO DE TRABALLO DESPEXADO

Cando a persoa usuaria deixe de atender o seu equipo durante un certo tempo, procederá a bloquear a sesión para evitar o acceso por parte de persoas non autorizadas (suplantación de identidade). Asemade, o equipo bloquearase automaticamente tras 2 minutos de inactividade.

7.7 ACCESO AOS SISTEMAS DE INFORMACIÓN E AOS DATOS TRATADOS

Para acceder aos sistemas e recursos informáticos é necesario ter asignada previamente unha conta de usuario.

O alta dos usuarios será solicitada e autorizada de acordo coas políticas da organización.

A autorización do acceso establecerá o perfil necesario co que se configuren as funcionalidades e privilexios dispoñibles nas aplicacións segundo as competencias de cada persoa, adoptando unha política de asignación de privilexios mínimos necesarios para a realización das funcións encomendadas.

Os Usuarios dispoñerán de credenciais persoais de acceso (código de usuario e contrasinal, certificado electrónico, etc.) para o acceso aos sistemas de información da Organización empregando a rede segura, protexida cos servizos de seguridade destinados para ese efecto, sendo responsables da súa custodia e de toda actividade relacionada co uso do seu acceso autorizado, respecto dos que deberá de observar as seguintes medidas:

- O código de usuario é único para cada persoa, intransferible e independente do PC ou terminal desde o que se realiza o acceso.
- Os usuarios non deben revelar ou entregar, baixo ningún concepto, as súas credenciais de acceso a outra persoa, nin mantelas por escrito á vista ou ao alcance de terceiros.
- De igual modo, non deben utilizar ningún acceso doutra persoa, aínda que dispoñan da autorización da súa titular.
- Se unha persoa ten sospeitas de que as súas credenciais están a ser utilizadas por outra persoa, debe comunicalo inmediatamente.
- As persoas usuarias deben utilizar contrasinais seguros e fortes, de acordo coa política establecida na Organización; non deben estar compostas unicamente por palabras do dicionario ou outras facilmente previsibles ou asociables á persoa usuaria (nomes de familiares, enderezos, matrículas, teléfonos, nomes de produtos comerciais ou organizacións, identificadores de usuario, de grupo ou do sistema, DNI, etc.)
- Os sistemas que así o permitan, forzarán o cambio do contrasinal polo menos unha vez cada seis meses, con previo aviso. Se o sistema non o permite, é responsabilidade de cada persoa usuaria facer efectivo o cambio de contrasinal coa mesma

periodicidade.

7.8 ACCESO A CONTAS DE USUARIO DURANTE AUSENCIAS OU BAIXAS

Non está permitido o uso de contas de usuario doutras persoas.

Cando por ausencias temporais se deban levar a cabo tarefas operativas ás que só ten acceso esa persoa, asignaranse os privilexios necesarios ás contas do persoal que a substitúa nas devanditas tarefas. Unha vez a persoa ausente se reincorpore ao seu posto, a súa persoa responsable deberá repor os privilexios outorgados á persoa substituta.

Esta casuística incide na norma xa indicada de que toda a información e a documentación relativas ao traballo na Organización deben figurar nas plataformas e recursos proporcionados, e por norma xeral non de forma exclusiva no almacenamento local dos equipos.

Se por circunstancias excepcionais fose necesario acceder á información local dun equipo, será o Comité de Seguridade quen decida este suposto.

7.9 CONFIDENCIALIDADE, PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL E DEBER DE SEGREDO

A información contida no Sistema de Información da Organización é responsabilidade da propia entidade, polo que as persoas usuarias deben absterse de comunicar, divulgar, distribuír ou poñer en coñecemento ou ao alcance de terceiros (externos ou internos non autorizados) esta información, salvo autorización expresa da propia Organización. Ademais, deberá de ter en conta as seguintes premisas:

- Todas as persoas usuarias que por razón da súa actividade profesional tivesen acceso a información xestionada pola Organización (documentos, metodoloxías, claves, análises, programas, etc.) deberán manter sobre ela, por tempo indefinido, unha absoluta reserva.
- As persoas usuarias só poderán acceder coas debidas autorizacións a aquela información necesaria para o desempeño dos seus labores. En todo caso, non deberán acceder a información sen as debidas autorizacións.
- Toda a información contida nos sistemas de información da Organización ou que circule polas súas redes de comunicacións debe ser utilizada unicamente para o cumprimento das funcións que teñen encomendadas as persoas usuarias.
- Os dereitos de acceso das persoas usuarias á información e aos sistemas de información que a tratan deberán sempre outorgarse en base aos principios de “mínimo privilexio”, “necesidade de coñecer e responsabilidade de compartir” e “capacidade de autorizar”.
- A información que comprenda datos de carácter persoal quedará afectada tamén pola normativa vixente en materia de Protección de Datos persoais, e polo tanto á obriga de

gardar segredo sobre os mesmos, deber que se manterá de maneira indefinida, mesmo máis aló da relación laboral ou profesional coa Organización.

7.10 LIMPEZA DE METADATOS E DATOS OCULTOS DOS DOCUMENTOS ELECTRÓNICOS

Os metadatos son elementos de información estruturada que describe, explica, localiza e fai máis doada a recuperación, utilización ou xestión dun recurso de información, que non forman parte do contido visible dun documento.

A información ou datos ocultos son aqueles datos existentes no contido dos documentos electrónicos que non son visibles coa configuración estándar ou configuración por defecto dos programas utilizados para a súa creación e tratamento, sendo necesario aplicar algunha opción específica dentro da configuración destes programas para a súa visualización: texto oculto, filas ou columnas ocultas, comentarios, etc.

As imaxes e fotografías, e os documentos ofimáticos (textos, follas de cálculo...) son documentos informáticos que integrados nas súas propiedades unha serie de datos ocultos e metadatos, como poden ser o nome da persoa que creou o documento, o programa co que se xerou, a data de creación, a de modificación, rutas locais de disco, e mesmo o lugar ou as coordenadas xeográficas desde onde se tomou a imaxe. Isto pode prexudicar á confidencialidade da información e á boa imaxe da entidade, pero tamén pode dar lugar a vulnerabilidades debidas a fallos coñecidos en versións específicas dos programas que se utilizaron para elaborar os documentos.

Todo arquivo que vaia ser difundido internamente, remitido electronicamente a un terceiro ou publicado na internet (páxina web, sede electrónica, etc.) deberá ser revisado para determinar os metadatos asociados ao mesmo e proceder á eliminación dos que proceda.

A Organización instruirá a todo o persoal sobre a forma de eliminar os metadatos nos documentos, ou evitar que se inclúan.

7.11 USO DO CORREO ELECTRÓNICO CORPORATIVO

O correo electrónico corporativo é unha ferramenta de mensaxería electrónica centralizada, posta ao dispor das persoas usuarias do sistema de información da Organización para o envío e recepción de correos electrónicos mediante o uso de contas de correo corporativas. Ao tratarse dun recurso compartido, un uso indebido do mesmo repercute de maneira directa no servizo ofrecido a todas as persoas.

O correo electrónico deberase empregar en base ao "sentido común" e tendo en conta a responsabilidade e funcións desempeñadas, tratando en calquera caso de non poñer en compromiso nin os sistemas nin a imaxe da Organización.

A Organización queda facultada para filtrar o contido do correo electrónico da conta de correo proporcionada para o desenvolvemento das súas funcións laborais, ao obxecto de previr virus ou no caso de que existan razóns fundamentadas nunha firme sospeita por parte da Organización sobre a existencia de actividades delituosas ou dolosas do persoal.

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 nos que se detecte algún problema de seguridade ou de incumprimento desta Normativa.

Recoméndase inserir contido adicional nas mensaxes enviadas co obxecto de advertir ás persoas receptoras dos requisitos legais e de seguridade que deberán cumprir en relación cos correos recibidos.

As características singulares deste medio de comunicación (universalidade, baixo custo, anonimato, etc.) propiciaron a aparición de ameazas que utilizan o correo electrónico para propagarse ou que aproveitan as súas vulnerabilidades. Por este motivo establécense as seguintes directrices co obxectivo de reducir o risco no uso do correo electrónico:

- Utilizar o correo electrónico exclusivamente para propósitos profesionais.
- Non ceder o uso da conta de correo a terceiras persoas, agás usando os mecanismos propios do sistema de correo que permiten que outras persoas o xestionen.
- Informar de correos sospeitosos de seren virus, *phishing*, *scam* e outros tipos de *malware* (programas malignos), e non redirixilos, para evitar a súa posible propagación.
- Non contestar as mensaxes de *spam*
- Asegurar a identidade do remitente antes de abrir unha mensaxe
- Non executar ningún programa recibido por correo electrónico. Non está permitida a execución de ningún programa ou aplicativo que non estea instalado no equipo pola Organización.

Respecto ao uso do correo electrónico, queda terminantemente prohibido:

- Falsificar, ocultar, suprimir ou substituír a identidade do emisor en calquera correo electrónico.
- Ler ou acceder a correos electrónicos alleos.
- Enviar correos electrónicos que conteñan no corpo ou nos adxuntos información con datos de categorías especiais de datos ou datos especialmente sensibles, isto é, saúde, ideoloxía, relixión, crenzas, orixe racial, étnico, etc. ou aqueles considerados como de especial protección pola organización, agás que se conte coa autorización pertinente e aplicáronse as medidas de seguridade oportunas (cifrado ou similares).

Dado que a conta de correo proporcionada pola entidade non poderá ser usada para

comunicacións persoais, senón unicamente para fins relacionados co exercicio das funcións e actividades propias do posto de traballo, a persoa empregada non debe supoñer que exista privacidade sobre o contido das comunicacións contidas na súa conta corporativa.

En caso de extinción da relación entre a persoa empregada e a Organización, o contido da caixa de correos asociada á conta corporativa quedará en poder da entidade, e a persoa empregada non está autorizada a obter unha copia dos contidos, tendo en conta que a propiedade da información aí contida é propiedade da Organización.

Non está permitido o uso de contas de correo non corporativas nos equipos da Organización, como poden ser contas persoais.

7.12 ACCESO A INTERNET E OUTRAS FERRAMENTAS DE COLABORACIÓN

O acceso corporativo á Internet é un recurso centralizado que a Organización pon ao dispor das persoas usuarias, como ferramenta necesaria para o acceso a contidos e recursos da internet e como apoio ao desempeño da súa actividade profesional. A Organización velará polo bo uso do acceso á Internet, tanto desde o punto de vista da eficiencia e da produtividade do persoal, como desde os riscos de seguridade asociados ao seu uso. As normas de uso son as seguintes:

- As conexións que se realicen á Internet deben obedecer a fins profesionais.
- Só se poderá acceder á Internet mediante os navegadores fornecidos e configurados nos postos de usuario. Non poderá alterarse a súa configuración, nin utilizar un navegador alternativo, sen contar coa debida autorización.
- O sistema que proporciona o servizo de navegación poderá contar con filtros de acceso que bloqueen o acceso a determinadas páxinas web con contidos non relacionados co traballo da Organización, programas lúdicos de descarga masiva ou páxinas potencialmente inseguras ou que conteñan virus ou código daniño.
- Deberá notificarse calquera anomalía detectada no uso do acceso a Internet, así como a sospeita de posibles problemas ou incidentes de seguridade relacionados con estes accesos: redirección a outras páxinas diferentes ás que se queren visitar, avisos de sitio non seguro en páxinas habitualmente utilizadas, etc.

Considéranse usos prohibidos, que implican un risco de seguridade, as seguintes actuacións:

- A descarga de ningún programa informático. De ser necesaria a instalación dunha ferramenta concreta, deberase solicitar á Organización, que considerará a necesidade e procederá a executala con todas as garantías de seguridade.
- O acceso, a descarga e o almacenamento en calquera soporte de páxinas con contidos ilegais, danos, inadecuados ou que atenten contra a moral e os bos costumes e, en

xeral, de todo tipo de contidos que incumpran as normas éticas e de cortesía da Organización.

- O acceso a recursos e páxinas web, ou a descarga de programas ou contidos que vulneren a lexislación en materia de Propiedade Intelectual.
- A utilización de aplicacións ou ferramentas (especialmente, o uso de programas de intercambio de información, P2P) para a descarga masiva de arquivos, programas ou outro tipo de contidos que non estean expresamente autorizados.
- O uso de *plug-ins* ou engadidos aos navegadores web para conseguir calquera dos obxectivos dos puntos anteriores.

7.14 PREFERENCIA DO USO DE SOFTWARE LIBRE E DE ESTÁNDARES ABERTOS

O Concello de Rianxo utilizará, de forma preferente, sistemas operativos e programas de software libre, evitando dentro do posible aplicacións privativas, aínda que estas sexan de uso gratuito.

Sistemas operativos:

Os sistemas operativos instalados nos equipamentos da Organización serán variantes libres de GNU/Linux, e non se deberán conectar ás redes das diferentes sedes do concello equipos informáticos con outros sistemas operativos.

De ser necesario conectar equipos con algún outro sistema operativo, precisarase unha autorización previa da persoa Responsable de Seguridade.

Por norma xeral, a conexión dalgún dispositivo con sistemas non libres farase mediante medios sen fíos (nunca por cable) en redes illadas do direccionamento da rede, de forma que se evite o acceso aos equipos corporativos, servidores, impresoras, etc.

O anterior aplícase moi especialmente aos equipos portátiles e móbiles, que deberán, ademais, teren instaladas versións non obsoletas dos seus sistemas e contar con software de protección de *malware*.

Software:

Os equipos do Concello de Rianxo só terán instalado, por norma xeral, aplicativos de software libre. Só en situacións moi específicas poderíase optar por solucións non libres, e sempre baixo a autorización da persoa responsable do Sistema.

Asemade, débese evitar o uso de aplicativos substitutivos en liña ou calquera outra solución de terceiros destinada a uso persoal ou coa que o Concello de Rianxo non teña un contrato ou acordo de uso.

Isto inclúe aplicativos de Intelixencia Artificial que non sexan software libre (entendido no eido

máis amplo da acepción: uso libre para calquera propósito e acceso ao código), e en todo caso nunca se utilizarán sobre documentos que conteñan datos persoais ou confidenciais da Organización.

Formatos:

De forma análoga, os formatos dos ficheiros deberán ser, na medida do posible, estándares abertos, e seren editados e manipulados con software libre.

Os ficheiros adquiridos desde fontes externas ao concello deberán transformarse, o antes posible, en ficheiros en formatos libres.

8. MONITORAXE E APLICACIÓN DESTA NORMATIVA

A Organización, por motivos legais, de seguridade e de calidade do servizo, e cumprindo en todo momento os requisitos que para o efecto establece a lexislación vixente:

- Revisará periodicamente o estado dos equipos, o software instalado, os dispositivos e redes de comunicacións da súa responsabilidade.
- Monitorizará os accesos á información contida nos seus sistemas.
- Auditará a seguridade das credenciais e aplicacións.
- Monitorizará os servizos da internet, correo electrónico e outras ferramentas de colaboración.

Esta supervisión realizarase en todo caso con plenas garantías do dereito á honra, á intimidade persoal e familiar e á propia imaxe dos afectados, e de acordo coa normativa sobre protección de datos persoais, de función pública e laboral, e demais disposicións que resulten de aplicación, rexistraranse as actividades das persoas usuarias, retendo a información necesaria para monitorizar, analizar, investigar e documentar actividades indebidas ou non autorizadas, permitindo identificar en cada momento á persoa que actúa.

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 a causa da súa inseguridade ou degradación desapareza.

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 nos que se detecte algún problema de seguridade ou de incumprimento da presente Normativa. Poderase inserir contido adicional nas mensaxes enviadas con obxecto de advertir ás persoas receptoras dos requisitos legais e de seguridade que deberán cumprir en relación cos devanditos correos.

O sistema que proporciona o servizo de navegación poderá contar con filtros de acceso que bloqueen o acceso a páxinas web con contidos inadecuados, programas lúdicos de descarga

masiva ou páxinas potencialmente inseguras ou que conteñan virus ou código daniño. Igualmente, o sistema poderá rexistrar e deixar traza das páxinas ás que se accedeu, así como do tempo de acceso, volume e tamaño dos arquivos descargados. O sistema permitirá o establecemento de controis que posibiliten detectar e notificar sobre usos prolongados e indebidos do servizo.

9. INCUMPRIMENTO DA NORMATIVA

As persoas usuarias dos sistemas de información da Organización están obrigadas a cumprir o prescrito nesta Normativa de Uso de Medios Electrónicos.

No caso de que unha persoa usuaria non observe algún dos preceptos sinalados nesta Normativa, sen prexuízo das accións disciplinarias e administrativas que procedan e, no seu caso, as responsabilidades legais correspondentes, poderase acordar a suspensión temporal ou definitiva do uso dos recursos informáticos que teña asignados, previa instrución do procedemento legal que corresponda.

No caso de persoal de terceiros, o incumprimento desta normativa podería derivar na imposición de penalidades e mesmo á resolución do contrato, seguindo o procedemento establecido para o efecto na normativa sobre contratación administrativa.

10. ANEXOS

10.1 MODELO DE ACEPTACIÓN E COMPROMISO DE CUMPRIMENTO

Todos os usuarios dos recursos informáticos ou sistemas de información da Organización deberán ter acceso permanente, durante o tempo de desempeño das súas funcións, a esta Normativa de Uso Interno de Medios Electrónicos.

Para a súa aceptación, xunto coa normativa trasladarase a seguinte confirmación de recepción a todas as persoas usuarias, que deberá ser asinada por cada unha delas.

ACEPTACIÓN

Mediante esta declaración, a persoa que a asina, como usuaria de recursos informáticos e sistemas de información da Concello de Rianxo, **declara ler e comprender a Normativa de uso de medios electrónicos do Concello de Rianxo** e aceptar os termos e condicións de uso establecidos nela, e estar de acordo en cumprilos, atender as modificacións do documento que lle fosen debidamente comunicadas, e comprometéndose, baixo a súa responsabilidade, ao seu cumprimento.

Organización:	Concello de Rianxo
Nome e Apelidos:	
Documento de identidade:	
Núm. Rexistro de Persoal:	
Data:	
Sinatura:	RECIBÍN:

10.2 PRIORIDADE DE USO DE APLICACIÓNS DE SOFTWARE LIBRE

Co obxectivo de garantir a seguridade, a eficiencia e a coherencia tecnolóxica da organización, establécese a seguinte relación de aplicacións de referencia baseadas en software libre, que deberán ser utilizadas preferentemente para as tarefas informáticas habituais no Concello de Rianxo.

O uso doutras aplicacións que non se recollan nesta relación deberá estar previamente autorizado polos responsables do Sistema

- Navegación web: Mozilla Firefox. Só se empregará Chromium ou, en última instancia, Google Chrome, en casos xustificados por incompatibilidades graves con determinadas páxinas web institucionais
- Edición de documentos de texto: LibreOffice Writer
- Follas de cálculo: LibreOffice Calc
- Modificación de documentos PDF: LibreOffice Draw, Inkscape, GIMP
- Manipulación de documento PDF: LibreOffice Draw, PDFMod, PDFArranger, PDFPoster, PDFTK, BookletImposer
- Sinatura electrónica: AutoFirma, Okular
- Edición fotográfica: GIMP
- Gráficos vectoriais: Inkscape, LibreOffice Draw
- Maquetación e publicación: Scribus, LibreOffice Draw, Inkscape
- Edición de son e vídeo: Audacity, Kdenlive, Shotcut, Natron, Blender

10.3 USO DE APLICACIÓNS EN LIÑA E FERRAMENTAS EXTERNAS

O uso de ferramentas ou servizos en liña estará restrinxido ás plataformas que dispoñan dunha política de uso compatible co uso institucional por parte dunha administración pública. Non se autoriza o uso de ferramentas cunha licenza limitada ao ámbito persoal ou particular.

Poderanse empregar exclusivamente aquelas solucións postas a disposición da organización polo Concello de Rianxo ou por outras administracións públicas.

- **Intelixencia artificial:** non se permite o uso de ferramentas como ChatGPT, DeepSeek, Gemini ou Grok, que non son abertas nin libres. Utilizar no seu lugar Mistral (mistral.ai) ou outras que permitan usos comerciais. En todo caso, non se deben proporcionar datos ou enviar documentos que conteñan datos persoais, sensibles ou confidenciais a ningunha plataforma externa de IA.
- **Sorteos:** non se permite o uso de webs externas para sorteos. No seu lugar, débese usar a aplicación pública e de código aberto do Concello de Rianxo dispoñible en <https://concelloderianxo.gal/sorteos>
- **Aplicacións de almacenamento na nube:** non está permitido almacenar documentos da organización en sistemas externos como Dropbox, Google Drive ou OneDrive. Só se permite gardar documentos nas plataformas oficiais en liña (TEDeC) e nas unidades NAS de almacenamento compartido que teñan uso remoto habilitado, segundo as instrucións dos responsables do sistema.
- **Compartillado de ficheiros grandes:** non está permitido compartir ficheiros con sistemas externos de terceiros, como WeTransfer, Velaquí, Mega ou similares. As únicas formas de envío de documentos grandes permitidas son o partillado mediante TEdEC, os NAS de almacenamento compartido e o Almacén da Administración do Estado <https://ssweb.seap.minhap.es/almacen/>
- **Mensaxería instantánea:** as aplicacións de mensaxería particulares como WhatsApp, Telegram ou similares non se deben utilizar nunca para o envío de información persoal, confidencial ou, en xeral, información da Organización, fóra de mensaxes persoais das persoas traballadoras que non teñan que ver con asuntos laborais. Permítese a mensaxería interna das contas de correo corporativas (Google Chat).
- **Videoconferencia:** a aplicación de videoconferencia de referencia que debemos usar é a que proporciona o correo corporativo (Google Meet). As reunións iniciadas polo persoas da Organización serán creadas nesta plataforma. Porén, para videoconferencias iniciadas por persoas externas, permítese o uso das plataformas escollidas por aquelas, preferentemente vía navegador web e non con aplicacións nativas que haxa que instalar nos equipos.

- **Aplicacións de edición ou creación de documentos e imaxes en liña:** non se permite o uso de aplicacións que impliquen ter que enviar un arquivo pola rede a servidores externos, como Canva, iLovePDF, Photopea e similares. No seu lugar, utilizaranse as aplicacións libres nativas: Inkscape, GIMP, Scribus, LibreOffice Draw, Okular, PDFSam, PDFArranger...
- **Descargas de música, imaxes ou vídeo:** non se permite o uso de imaxes, vídeos ou ficheiros de son que non teñan unha licenza de uso libre, Creative Commons ou outra que sexa compatible co seu uso polas administracións públicas, e polo tanto non se permite o uso de ferramentas que graven, descarguen e/ou transformen este tipo de contidos cando non están dispoñibles de forma directa para a súa descarga.

10.4 PROCEDEMENTO DE LIMPEZA DE METADATOS

Este procedemento describe os procesos a seguir para realizar a limpeza dos metadatos dos documentos, coa fin de evitar a distribución non desexada de datos persoais ou de datos técnicos acerca das características técnicas do equipo informático, do software utilizado ou das versións, do sistema operativo ou dos datos de usuario. Esta limpeza debe realizarse sempre antes de proceder al intercambio de documento con terceiras persoas, ou ao publicar documentos nas contornas web.

FERRAMENTA DE LIMPEZA DE METADATOS

Os equipos informáticos do Concello de Rianxo incorporan o programa libre **mat2**, que se pode atopar nos menús de aplicacións baixo o nome **Limpador de metadatos**.

Sempre que se desexen eliminar os metadatos dun arquivo, pódese premer enriba del co botón secundario para despregar o menú contextual, e seleccionar **Abrir con → Limpador de metadatos**. Este programa permitirá ver os metadatos gardados xunto co arquivo e eliminalos de forma doada premendo no botón **Limpar**, que sobreescribirá o arquivo pero cos metadatos eliminados.

Fóra desta solución, convén tamén coñecer os medios de eliminación de metadatos propios dos aplicativos de uso habitual de Concello de Rianxo. Este anexo describe a xestión dos metadatos nalgunhas ferramentas informáticas, mais é conveniente facelo para calquera outro aplicativo utilizado parta a modificación de documentos.

LIMPEZA DE METADATOS EN DOCUMENTOS DE LIBREOFFICE

A acción recomendada no caso do LibreOffice, tanto para os documentos de texto como para as follas de cálculo, máis tamén para as presentacións e os debuxos, é configuralo para evitar que nunca se garden os metadatos coa información persoal.

Para iso, os pasos habituais, aínda que poden variar lixeiramente dunha versión a outra, son os seguintes:

1. Menú Ferramentas → Opcións
2. Escoller LibreOffice → Seguranza
3. Premer no botón de Opcións na sección de **Opcións de seguranza e advertencias**
4. Desmarcar a cela de **Retirar información persoal ao gardar**

Con todo, o formato recomendado para a publicación de documentos é o PDF.

METADATOS EN DOCUMENTOS DE OTRAS SUITES OFIMÁTICAS

Posto que no Concello de Rianxo non se permite o uso de outras suites ofimáticas fóra do LibreOffice, no caso de precisar da edición dun documento noutros formato editable, recoméndase abrilo co LibreOffice e aplicar a eliminación de metadatos.

OUTROS APLICATIVOS

Ademais dos documentos de texto, no Concello de Rianxo úsanse outros aplicativos para xerar imaxes e carteis en diversos formatos, habitualmente JPG, PNG e PDF. Cómpre tomar as medidas necesarias para evitar que estes documentos conteñan información persoal ou do sistema.

1. GIMP: á hora de exportar, a calquera formato, comprobar que a cela de gardar metadatos estea desactivada (por defecto, esta cela está desactivada).
2. INKSCAPE: Comprobar que nas propiedades do documento (Ficheiro → Propiedades), na pestana de metadatos estean todos os campos baleiros (por defecto, estano). Isto evitará que os arquivos exportados a JPG, PNG ou PDF (formatos habituais) conteñan información persoal.
3. Calquera outro aplicativo de edición: débese consultar na axuda do aplicativo ou coa persoa responsable do sistema a forma específica de eliminación de metadatos dos arquivos producidos que se vaia facer públicos.