NORMATIVA DE USO DE MEDIOS ELECTRÓNICOS DO CONCELLO DE VIMIANZO

1. OBXECTIVO....2

2. REVISIÓN E/OU ACTUALIZACIÓN....2

3. OBXECTO....2

4. ALCANCE....2

5. CANLE DE SOLICITUDES E/OU NOTIFICACIÓNS....2

6. INCIDENTES DE SEGURIDADE....3

7. NORMATIVA DE USO DOS MEDIOS ELECTRÓNICOS....3

7.1 NORMAS DE UTILIZACIÓN DO EQUIPAMENTO INFORMÁTICO E DE COMUNICACIÓNS....3

7.1.1 NORMAS XERAIS....3

7.1.2 NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTIIS E DISPOSITIVOS MÓBILES....4

7.2 NORMAS PARA O ALMACENAMENTO DE INFORMACIÓN E COPIAS DE SEGURIDADE....4

7.3 NORMAS DE USO PARA SOPORTES DE ALMACENAMENTO EXTRAÍBLES....4

7.3.1 NORMAS PARA O BORRADO E ELIMINACIÓN DE SOPORTES INFORMÁTICOS....5

7.4 NORMAS RESPECTO Á XESTIÓN DE DOCUMENTOS....5

7.4.1 IMPRESORAS EN REDE, FOTOCOPIADORAS/ESCÁNERES....5

7.4.2 COIDADO E PROTECCIÓN DA DOCUMENTACIÓN IMPRESA....6

7.4.3 ACCESO A DOCUMENTOS COMPARTIDOS E TRABALLO COLABORATIVO....6

7.5 POSTO DE TRABALLO DESPEXADO....7

7.6 BLOQUEO DE POSTO DE TRABALLO DESPEXADO....7

7.7 ACCESO AOS SISTEMAS DE INFORMACIÓN E AOS DATOS TRATADOS....7

7.8 ACCESO A UNHA CONTA DUN USUARIO NA SÚA AUSENCIA OU BAIXA....8

7.9 CONFIDENCIALIDADE, PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL E DEBER DE SEGREDO....8

7.10 LIMPEZA DE METADATOS E DATOS OCULTOS DOS DOCUMENTOS ELECTRÓNICOS....8

7.11 USO DO CORREO ELECTRÓNICO CORPORATIVO....9

7.12 ACCESO A INTERNET E OUTRAS FERRAMENTAS DE COLABORACIÓN....10

8. MONITORAXE E APLICACIÓN DESTA NORMATIVA....11

9. INCUMPRIMENTO DA NORMATIVA....12

10. ANEXOS....13

10.1 MODELO DE ACEPTACIÓN E COMPROMISO DE CUMPRIMENTO....13

10.2 PROCEDEMENTO DE LIMPEZA DE METADATOS....15

*Praza *do *Concello, nº 6
15129 – Vimianzo (A Coruña)
Tel. 981716001
Fax 981716650
correo@vimianzo.gal
www.vimianzo.gal

1. OBXECTIVO

A presente normativa, foi aprobada por Resolución de Alcaldía e entrará en vigor ao día seguinte da súa aprobación, ata que sexa substituída por unha modificación ou unha nova normativa.

2. REVISIÓN E/Ou ACTUALIZACIÓN

Con periodicidade anual revisarase o seu contido e en caso de ser necesario procederase á súa modificación, que deberán ser aprobadas polos órganos anteriormente indicados, debendo ser difundidas entre as persoas afectadas polas mesmas.

3. OBXECTO

O obxecto do presente documento é establecer a normativa de uso seguro dos medios electrónicos no Concello de Vimianzo en diante, a Organización, dentro do alcance sinalado no Esquema Nacional de Seguridade.

Os sistemas de información son elementos básicos para o desenvolvemento da actividade da Organización. Estes medios póñense ao disposición das persoas usuarias como instrumentos de traballo para o desempeño da súa actividade profesional. Motivo polo cal se deben utilizar estes recursos 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 a presente 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 a disposición.

O persoal de terceiros (empresas provedoras, convenios, etc.) con acceso ao sistema quedan tamén suxeitos á mesma, na medida que lle sexan 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 “o Usuario” para referirse ao persoal propio ou de terceiros.

5. CANLE DE SOLICITUDES E/Ou NOTIFICACIÓNS

As solicitudes de autorización e as notificacións reflectidas nesta normativa dirixiranse con carácter xeral ao correo seguridade@vimianzo.gal

Cando proceda segundo a normativa aprobada, estea establecido a nivel de procedemento, ou como primeira resposta a un posible incidente de seguridade, ademais a comunicación do incidente ao Responsable de Seguridade descrita no parágrafo anterior, 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 do teléfono 981 415 000 en caso de producirse o incidente fóra do devandito horario.

6. INCIDENTES DE SEGURIDADE

Cando un Usuario 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 a canle especificado no punto anterior.

7. NORMATIVA DE USO DOS MEDIOS ELECTRÓNICOS

7.1 NORMAS DE UTILIZACIÓN DO EQUIPAMENTO INFORMÁTICO E DE COMUNICACIÓNS

Estas normas concirnen especificamente 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.

Respecto aos cales aplicará as normas xerais e para os equipos portatis 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.
- Salvo 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 deberá de solicitarse 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 deberá de comunicar a ausencia de cables e/ou accesorios ou calquera outra evidencia de deterioración do mesmo.

- Con carácter xeral, non está permitido o uso de dispositivos propios, "BYOD (Bring Your Own Device)", para o acceso ou almacenamento de información salvo autorización expresa.

7.1.2 Normas específicas para equipos portátiis e dispositivos móbiles

Para os portátiles e móbiles ademais das normas xerais, serán de aplicación a 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 destes equipos hase de notificar inmediatamente para a adopción das medidas que correspondan.
- Débese solicitar autorización cando se usen para conectarse remotamente a través de redes que non estean baixo o control da organización ou que non fosen autorizadas, autorización que se fará extensible tamén aos servizos aos que se accede.
- Cando se modifiquen as circunstancias profesionais (termo dunha tarefa, cesamento no cargo, etc.) que orixinaron a entrega dun recurso informático móbil, a persoa usuaria devolverao, ao 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 de unidades de rede compartidas (NAS) e dos Servidores Virtualizados.

Por este motivo, os usuarios deberán almacenar nestas os datos xerados no desempeño das súas competencias profesionais. A este respecto, infórmase que non se realizan copias de seguridade da información que non se atopen nas unidades indicadas.

Non está permitido o almacenamento de información privada nin de terceiros alleos nos recursos indicados.

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, na Organización 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.

No caso de que á persoa usuaria autoríceselle o uso deste tipo de soportes de traballo, as normas para observar son as seguintes:

- Como norma xeral, utilizaranse os soportes extraíbles proporcionados pola Organización. Estando destinados a un uso exclusivamente profesional, como ferramenta de transporte puntual de ficheiros, non como ferramenta de almacenamento.
- O uso de medios de almacenamento extraíbles particulares, non está autorizado, salvo que se dispoña da debida autorización.

- O seu uso non está autorizado para o almacenamento de datos persoais, salvo que se dispoña da debida autorización.

Este tipo de dispositivos deberá de almacenarse en lugares seguros, ao obxecto de previr roubos ou o acceso de terceiros non autorizados. 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 á propia información que salgue. Nese caso deberase de enviar unha solicitude para que se lle asesore sobre as medidas de seguridade que será necesario implementar (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.
- Calquera petición de eliminación de soporte informático deberá ser solicitada.

Para a reutilización de medios de almacenamento, para outros fins diferentes dos que orixinaron o seu uso deberá solicitarse un borrado seguro de mesmo.

7.4 NORMAS RESPECTO Á XESTIÓN DE DOCUMENTOS

7.4.1 Impresoras en rede, fotocopiadoras/escáneres

Con carácter xeral, deberán utilizarse as impresoras en 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 poderase facer uso de impresoras, fotocopiadoras que non fosen proporcionados pola Organización. Con relación aos sistemas de copia e impresión e documentación impresa, os usuarios debe seguir as seguintes directrices:

- Os documentos, con carácter xeral, xeraranse en formato electrónico, podendo dixitalizar aqueles que non sexan susceptibles de ser xerados no citado formato.
- Cando se impriman documentos, en sistemas de impresión ou copia comúns, contarase cun servizo de impresión segura, autenticándose o usuario a través de PIN para evitar que terceiras persoas poidan acceder á mesma.
- Na realización de copias de documentos e/ou escaneo, non debe esquecerse retirar os orixinais.
- En caso de atoparse documentación nun sistema de copia ou impresión, o Usuario tentará localizar á persoa propietaria para que proceda á súa recollida inmediata. En caso de descoñecer á persoa propietaria ou non estar localizable, poñerao inmediatamente en coñecemento.
- Para evitar un uso excesivo dos recursos, mellorando o impacto medioambiental na xeración de documentos en papel, e por motivos de seguridade, antes de imprimir documentos, o Usuario debe asegurarse de que é absolutamente necesario facelo.

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 ese efecto a persoa usuaria terá en conta as seguintes medidas:

- Os postos de traballo permanecerán despexados, sen máis material encima da mesa que o requirido para a actividade que se está realizando en cada momento.
- Cando non vaia ser utilizada deberase gardar en sistemas de almacenamento (armarios ou arquivadores) preferentemente baixo chave. Non poderán ser publicados en taboleiros ou similares.
- Cando os documentos non sexan necesarios, deberán ser eliminados utilizando para iso os medios postos a disposición 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 as lousas 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

A solución autorizada para compartir documentos é empregar carpetas compartidas no NAS, así como o uso das ferramentas disponibles na plataforma de Google Drive para o dito fin[1].

Revisaranse os permisos asignados aos cartafoles e documentos que se almacenan nestas plataformas, asegurando que só teñen permisos as persoas adecuadas e os documentos non sexan accesibles de forma pública. Prohíbese o almacenamento de información da Organización no almacenamento local dos equipos.

Como garantía adicional para a documentación sensible, dispoñerase dunha ferramenta que permita que a información corporativa póidase compartir protexida e baixo control en todo momento permitindo saber quen accedeu a un documento, establecer permisos de acceso e en caso necesario monitorar accesos bloqueados aos documentos.[2]

Estableceranse as seguintes medidas de protección dos documentos:

- A documentación unicamente será accesible polas persoas autorizadas, que a sensu contrario significa que os usuarios da plataforma colaborativa ou de compartición unicamente accederán aos cartafoles ou documentos autorizados, xa sexa para consulta, descarga, modificación, supresión, así como para incorporar novos documentos.
- Estableceranse permisos a nivel de usuario ou grupo de usuarios.
- Debe dispoñerse de trazabilidade respecto aos documentos.

[1] As solucións de compartición de documentos poden estar proporcionadas desde a Nube (SaaaS), como por exemplo Microsoft OneDrive, Google Drive, etc., ou implementadas en modo local (on-premise).

[2] Existen solucións para controlar os documentos compartidos unha vez saen da organización como é Carla e así evitar fugas de información e accesos non autorizados.

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 DE POSTO DE TRABALLO DESPEXADO

Cando a persoa usuaria deixe de atender o seu equipo durante un certo tempo, procederá ao bloqueo da sesión de usuario para evitar o acceso por parte de persoas non autorizadas (suplantación de identidade). Por razóns de seguridade, o equipo bloquearase automaticamente tras o período de inactividade establecido nos procedementos da organización.

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. A alta dos usuarios será solicitada e autorizada consonte as 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 un 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 de os 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 autorizado doutra persoa, aínda que dispoñan da autorización do seu 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, consonte a política establecida na Organización, non deben estar compostas unicamente por palabras do dicionario ou outras facilmente predicibles ou asociables á persoa usuaria (nomes da súa familia, direccións, matrículas de coche, 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 ao ano, aviso previo cos suficientes días de antelación. Nos que non sexa posible será responsabilidade dos usuarios proceder ao seu cambio na devandita periodicidade.

7.8 ACCESO A UNHA CONTA DUN USUARIO NA SÚA AUSENCIA OU BAIXA

Non está permitido o uso de contas de usuario doutros titulares.

Cando por ausencias temporais (vacacións, baixa por enfermidade, permisos, etc.) débanse levar a cabo tarefas operativas ás que só ten acceso esa conta, asignaranse os privilexios necesarios (previa solicitude e autorización) á conta do persoal que os substitúa nas devanditas tarefas. Unha

vez o ausentado reincorpórese ao seu posto, o seu responsable deberá solicitar a eliminación dos privilexios outorgados ao substituto.

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 devandita 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 Institución. Ademais, deberá de ter en conta as seguintes premisas:

- Todas os usuarios, que por razón da súa actividade profesional tivese acceso a información xestionada pola Organización (documentos, metodoloxías, claves, análises, programas, etc.) deberán manter sobre ela, por tempo indefinido, unha absoluta reserva.
- Os usuarios só poderán acceder coas debidas autorizacións a aquela información necesaria para o desempeño dos seus labores. En todo caso, non deberá acceder a información sen as debidas autorizacións.
- Toda 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 ten encomendadas o usuario.
- Os dereitos de acceso dos usuarios 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, estando obrigado a 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

Defínese **metadato** como información estruturada que describe, explica, localiza e ademais fai máis fácil recuperar, utilizar ou xestionar un recurso de información. Os metadatos son comunmente chamados “datos sobre os datos” ou “información sobre a información”.

Defínese información ou **datos ocultos** como 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. Un exemplo de datos ocultos é o texto oculto, filas ou columnas ocultas, comentarios ou información do documento, etc.

Cando facemos unha fotografía ou creamos documentos con aplicacións de Microsoft Office (Word, Excel, PowerPoint, etc.), estes arquivos levan integrados nas súas propiedades unha serie de datos ocultos e/ou 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, etc. Isto pode prexudicar á confidencialidade da información e á boa imaxe da entidade.

Todos os arquivos electrónicos (documentos ofimáticos, follas de cálculo, imaxes, etc…) poden ter integrados nas súas propiedades unha serie de datos ocultos e/ou 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, etc.

Os metadatos contidos nos arquivos poden chegar a afectar tanto á seguridade da información como á imaxe da Organización. Por iso, 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, procedendo á súa modificación ou supresión, se procede, seguindo o procedemento establecido no anexo "Procedemento de Limpeza de Metadatos".

7.11 USO DO CORREO ELECTRÓNICO CORPORATIVO

O correo electrónico corporativo é unha ferramenta de mensaxería electrónica centralizada, posta a disposición dos usuarios 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 da presente normativa.

Poderase inserir contido adicional nas mensaxes enviadas con obxecto de advertir aos receptores dos requisitos legais e de seguridade que deberán cumprir en relación cos devanditos correos.

As características peculiares 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[3].
- Non se debe ceder o uso da conta de correo a terceiras persoas[4].
- Informar de correos con virus, phishing, malware (programa maligno), etc. sen reenviarlos, para evitar a súa posible propagación.
- Non responder a mensaxes de Spam.[5]

[3] Gran parte das mensaxes de correo electrónico non desexados, que chegan ás organizacións teñen a súa orixe nun uso non profesional das contas de correo.

[4] Isto provocaría unha suplantación de identidade e o acceso a información. É conveniente controlar a difusión das contas de correo, facilitando a dirección profesional só nos casos necesarios e a condición de que o fin último sexa o cumprimento das funcións municipais (p.e., cando nos subscribimos a un foro).

[5] A maior parte dos xeradores de mensaxes de spam (correo electrónico masivo non solicitado) envíase a direccións de correo electrónico aleatoriamente xeradas, esperando que as respostas obtidas confirmen a existencia de direccións de contas reais. Ademais diso, en ocasións teñen o aspecto de mensaxes lexítimas e, mesmo, poden conter información relativa á Corporación. En calquera caso, nunca deben de responderse.

- Asegurar a identidade do remitente antes de abrir unha mensaxe[6].
- Non executar arquivos adxuntos sospeitosos. Non deben executarse os arquivos adxuntos recibidos sen analizalos previamente coa ferramenta corporativa contra código malicioso.[7]

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, sen autorización previa.
- Enviar correos electrónicos que conteñan no corpo ou na 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, salvo 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 o empregado e o Concello de Vimianzo o contido da caixa de correos asociada á conta corporativa quedará en poder da entidade, non estando o empregado autorizado a obter unha copia do mesmo, tendo en conta que a propiedade da información aí contida é propiedade da organización.

7.12 ACCESO A INTERNET E OUTRAS FERRAMENTAS DE COLABORACIÓN

O acceso corporativo a Internet é un recurso centralizado que a Organización pon a disposición dos usuarios, 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 a Internet, tanto desde o punto de vista da eficiencia e produtividade do persoal, como desde os riscos de seguridade asociados ao seu uso. As normas de uso son as seguintes:

- Como norma xeral, as conexións que se realicen a Internet deben obedecer a fins profesionais.
- Só se poderá acceder a 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 páxinas web con contidos inadecuados, programas lúdicos de descarga masiva ou páxinas potencialmente inseguras ou que conteñan virus ou código daniño.

[6] Moito ciberataques orixínanse cando o atacante se fai pasar por unha persoa ou entidade coñecida (amigo, compañeiro, etc.) da persoa atacada. A orixe destas accións é diverso: acceso non autorizado á conta, suplantación visual da identidade, introdución de código malicioso que utiliza a conta remitente para propagarse, etc. En caso de recibir un correo sospeitoso, e dependendo do seu verosimilitud, cabe: ignoralo, non abrilo e poñer o feito en coñecemento do remitente, independentemente de comunicar a incidencia de seguridade correspondente. Igualmente, o envío de información, "confidencial" a pedimento dun correo do que non se pode asegurar a identidade do remitente, debe rexeitarse. É importante ter en conta que resulta moi sinxelo enviar un correo cun remitente falso. Nunca se debe confiar en que a persoa coa que nos comunicamos vía email sexa quen di ser, salvo naqueles casos que se utilicen mecanismos de sinatura electrónica dos correos (non só dos ficheiros adxuntos).

[7] Isto é especialmente importante cando se reciben adxuntos non solicitados ou o correo é sospeitoso. Gran parte do código malicioso adoita inserirse en ficheiros adxuntos, xa sexa en forma de executables (.exe, por exemplo) ou en forma de macros de aplicacións (Word, Excel, etc.).

- Deberá notificarse calquera anomalía (redirección a páxinas solicitadas, aviso de sitio non seguro, en páxinas habitualmente utilizadas, etc.) detectada no uso do acceso a Internet, así como a sospeita de posibles problemas ou incidentes de seguridade relacionados co devandito acceso.

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

- A descarga de programas informáticos sen a autorización previa ou ficheiros con contido daniño que supoñan unha fonte de riscos para a organización. En todo caso debe asegurarse que o sitio web visitado é confiable.
- O acceso, a descarga e/ou o almacenamento en calquera soporte, de páxinas con contidos ilegais, daniños, 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 contido (música, películas, etc.) que non estea expresamente autorizados.

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.
- Monitorará os accesos á información contida nos seus sistemas.
- Auditará a seguridade das credenciais e aplicacións.
- Monitorará 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 consonte a normativa sobre protección de datos persoais, de función pública ou laboral, e demais disposicións que resulten de aplicación, rexistraranse as actividades dos usuarios, retendo a información necesaria para monitorar, 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 aos receptores 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

Os usuarios do sistema de información da Organización están obrigadas a cumprir o prescrito na presente Normativa de Uso de Medios Electrónicos".

No caso de que unha persoa usuaria non observe algunha dos preceptos sinalados na presente 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 normativa do procedemento legal que corresponda.

No caso de persoal de terceiros, o incumprimento desta normativa podería derivar na imposición de penalidades podendo chegar 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 e/ou sistemas de información da Organización deberán ter acceso permanente, durante o tempo de desempeño das súas funcións, á presente Normativa de Uso de Interno de Medios Electrónicos.

Para a súa aceptación xunto coa normativa trasladarase o seguinte "acuse de recibo", que deberá ser asinado, a todos os usuarios.

Mediante o enchemento da seguinte declaración, a persoa abaixo asinante, empregado/a da Concello de Vimianzo, como usuario/a de recursos informáticos e sistemas de información da Organización, declara ler e comprender a *Normativa de Usos e medios electrónicos da organización* e aceptar os termos e condicións de uso establecidos no mesmo, estando de acordo en cumprilos, atender as modificacións do documento que lle fosen debidamente comunicadas, comprometéndose, baixo a súa responsabilidade, ao seu cumprimento.

Organización:	
CIF:	
Traballador/a (Nome e Apelidos):	
DNI número:	
Asinado:	

E para que conste, asina esta declaración en Vimianzo.

A persoa traballadora: <<Nome e Apelidos>>

*Praza *do *Concello, nº 6
15129 – Vimianzo (A Coruña)
Tel. 981716001
Fax 981716650
correo@vimianzo.gal
www.vimianzo.gal

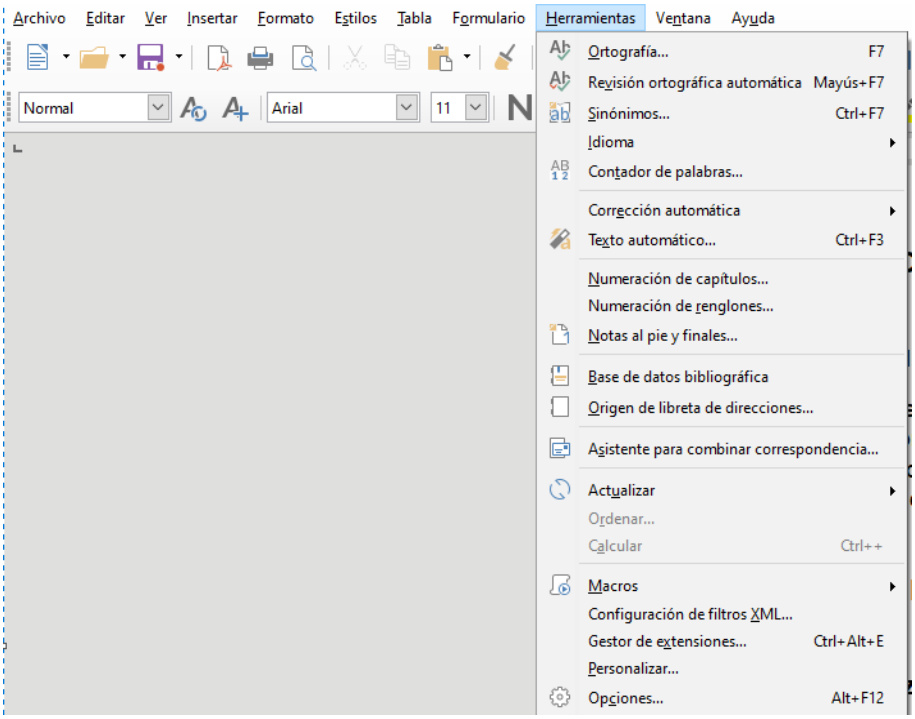
10.2 PROCEDEMENTO DE LIMPEZA DE METADATOS

O obxectivo deste procedemento é describir o proceso para seguir para realizar a limpeza dos metadatos non desexados dos documentos, a realizar antes de proceder ao intercambio de documento con terceiros, ou ao subir contidos aos contornas web.

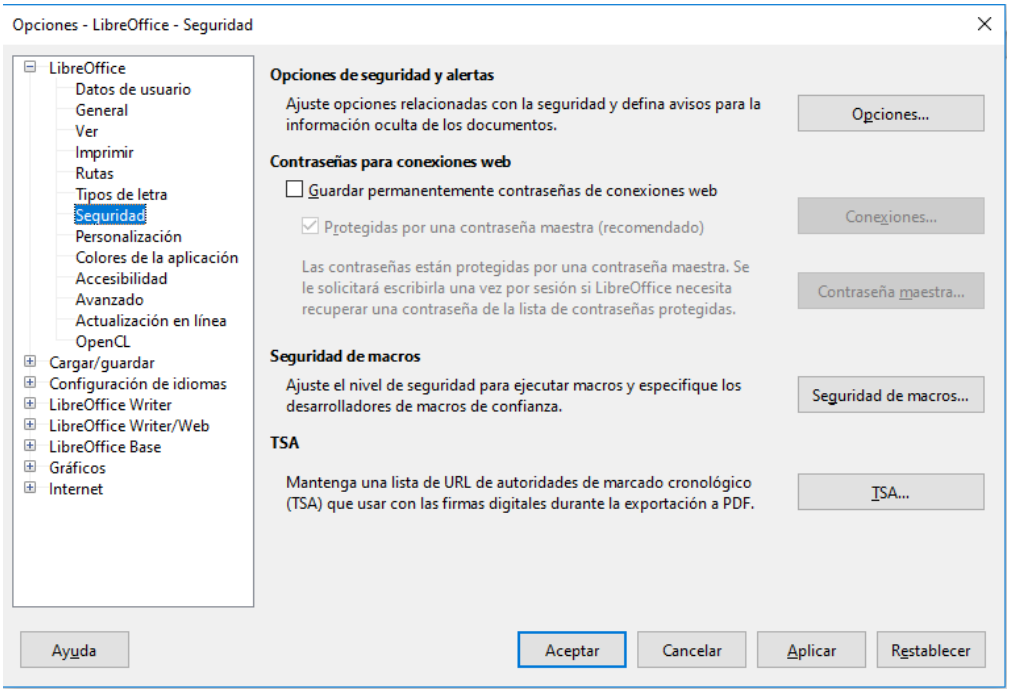
METADATOS EN DOCUMENTOS DE LIBREOFFICE – Evitar que se garden os metadatos no documento

A continuación, establécense as normativas para levar a cabo para evitar que se garden os metadatos en LibreOffice Versión: 6.2.5.2.

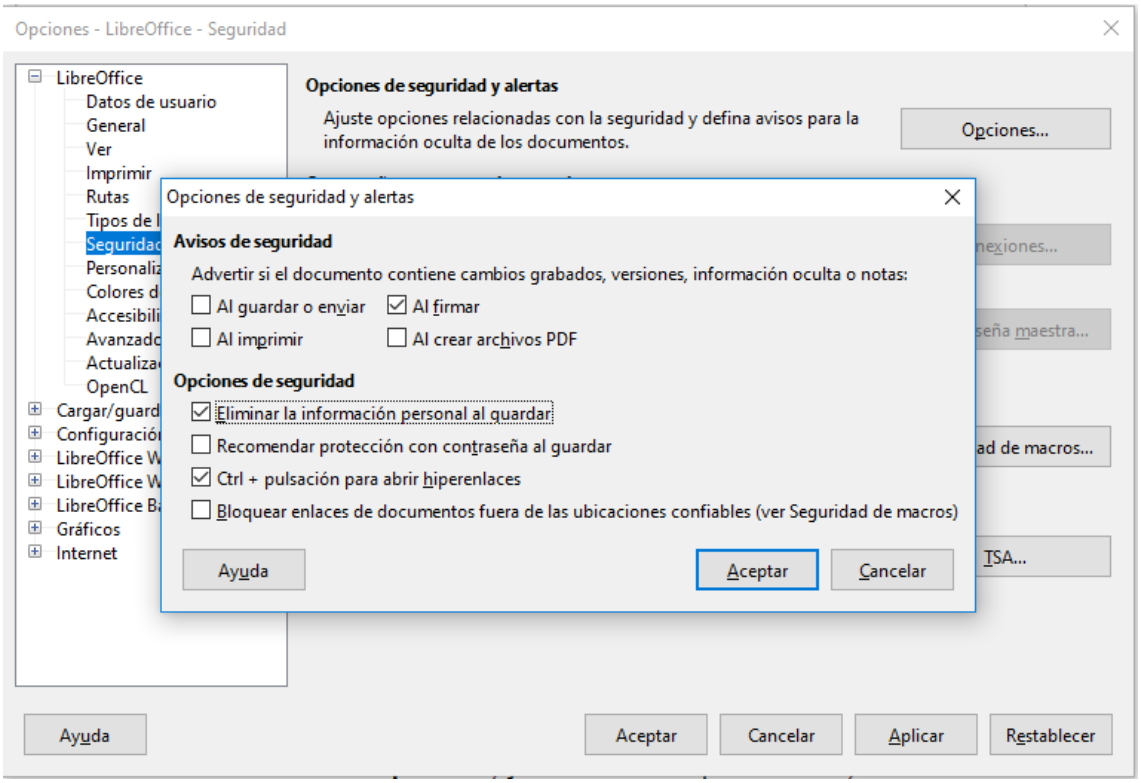
1. Abre LibreOffice e ir Ferramentas → Opcións



2. Na xanela que se abrirá, no menú da esquerda, **fai click en LibreOffice e despois feixe click en Seguridade**



3. Fai click no botón Opcións, e na xanela que se abrirá, selecciona a casa Eliminar a información persoal ao gardar.

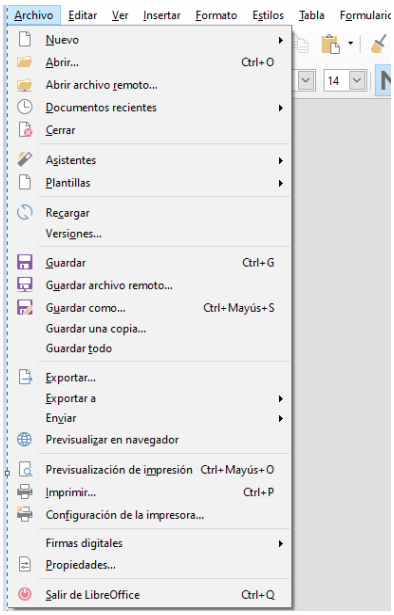


4. Fai click en Aceptar.

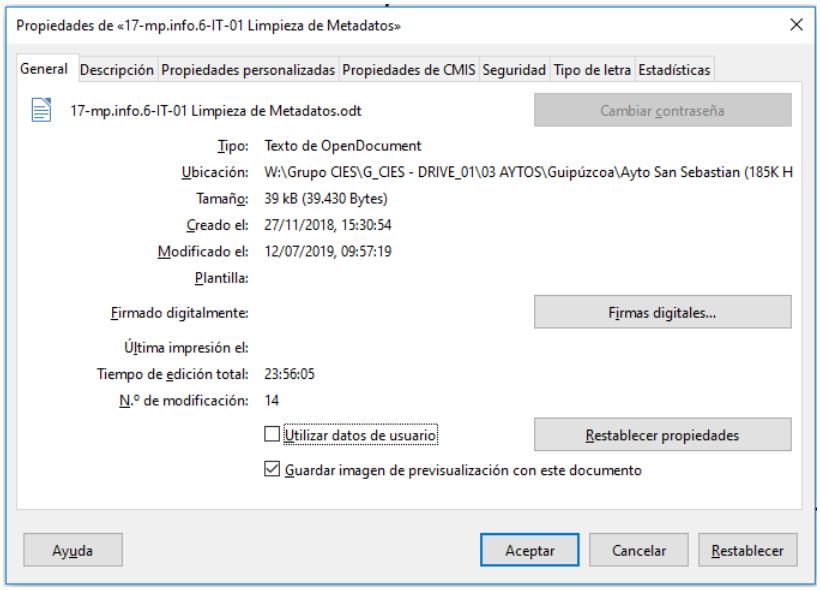
Despois disto, os documentos de LibreOffice gardaranse sen a túa información persoal.

METADATOS EN DOCUMENTOS DE LIBREOFFICE – Eliminar os metadatos nun documento xa creado

1. Ve a Arquivo>Propiedades



2. Na pestana **Xeral,** fai click no botón **Restablecer propiedades** e desmarca a casa **Utilizar datos do usuario**.



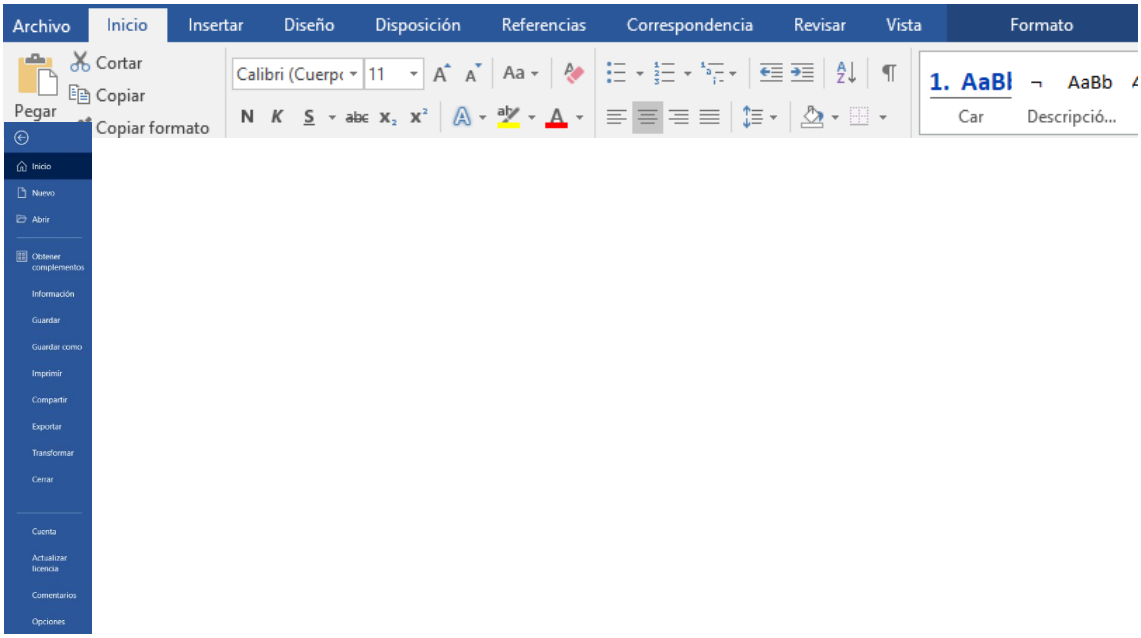
3. Fai click en Aceptar**.**

METADATOS EN DOCUMENTOS DE MICROSOFT OFFICE – Evitar que se garden os metadatos no documento

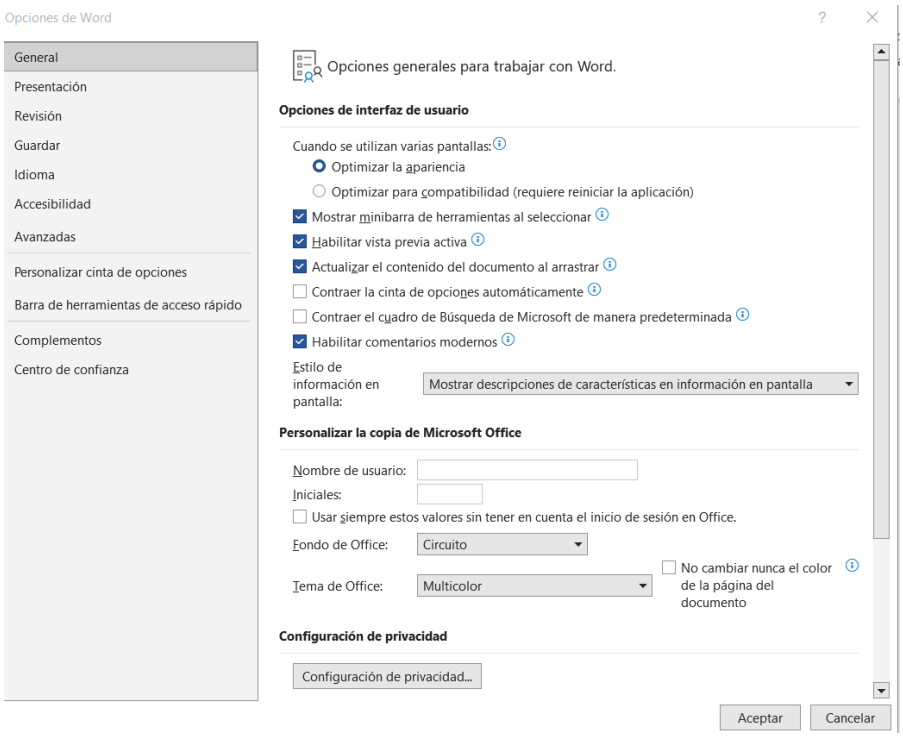
A continuación, establécense as normativas para levar a cabo para evitar que se garden os metadatos en Microsoft Office versión Microsoft 365

- Especificar a información persoal que aparece en todos os documentos de Office.

1. Abrir Microsoft Office e facer clic en Arquivo e en Opcións

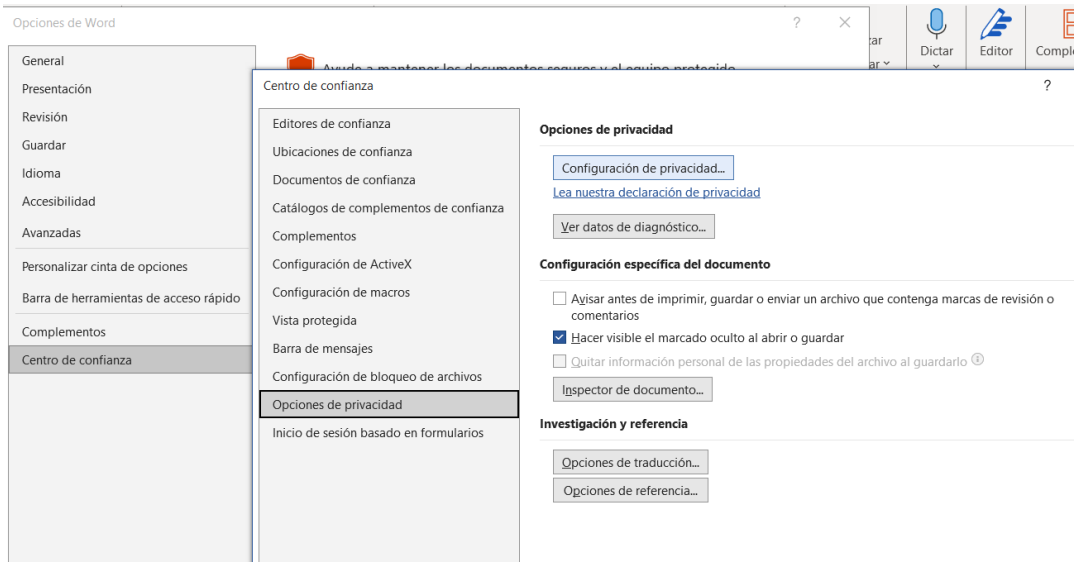


2. En xeral, no apartado Personalizar a copia de Microsoft Office, borraremos o noso nome e iniciais e remplazaremos por un espazo en branco en ambos os casos.



- <u>Non gardar a información persoal nun documento de Office</u>

1. Co arquivo aberto, facer clic en Arquivo e a continuación facer clic en Opcións. Abrirase a xanela de Opcións da aplicación, seleccionar Centro de Confianza e pulsar en Configuración do Centro de Confianza. Ábrese a xanela de Centro de Confianza.
2. Seleccionar Opcións de privacidade e no cadro destinado a Configuración específica do documento aparecerá a opción “Quitar Información persoal das propiedades do arquivo ao gardalo”. Esta opción só poderá seleccionarse cando previamente se eliminase toda a información persoal do documento e fai que cada vez que o documento se garde, elimínese a información persoal.



- 3.2.2 Inspección e borrado de metadatos e información oculta

Usar o Inspector de documento para buscar e quitar os datos ocultos e a información persoal dos documentos de Word.

1. Abra o documento de Word no que desexe buscar datos ocultos ou información persoal.
2. Faga clic na pestana Arquivo, logo en Gardar como e a continuación escriba un nome no cadro Nome de arquivo para gardar unha copia do documento orixinal.
3. Na copia do documento orixinal, faga clic na pestana Arquivo e a continuación faga clic en Información.
4. Faga clic en Comprobar se hai problemas e logo faga clic en Inspeccionar documento.
5. No cadro de diálogo Inspector de documento, active as casas para elixir os tipos de contido oculto que desexe que se inspeccionen.
6. Faga clic en Inspeccionar.
7. Revise os resultados da inspección no cadro de diálogo Inspector de documento.
8. Faga clic na opción Quitar todo situada onda os resultados da inspección dos tipos de contido oculto que desexe quitar do documento.

IMPORTANTE: Recoméndase usar o Inspector de documento nunha copia do documento orixinal, posto que non sempre se poden restaurar os datos que quita este inspector.

A alcaldesa

Mónica Rodríguez Ordóñez

(Documento asinado dixitalmente)

*Praza *do *Concello, nº 6
15129 – Vimianzo (A Coruña)

Tel. 981716001
Fax 981716650

correo@vimianzo.gal
www.vimianzo.gal