ADMINISTRACIÓN LOCAL

MUNICIPAL

VIMIANZO

Normativa de uso de medios electrónicos do Concello de Vimianzo

ANUNCIO

Por Resolución de Alcaldía número 850/2024 de data do 10/07/2024, aprobouse a *Normativa de Uso de Medios Electrónicos do Concello de Vimianzo* e, por medio da Dilixencia de Corrección de Erros, asinada o 26/08/2024, correxíuse un erro material detectado no contido desta, quedando a dita normativa co seguinte contido:

"NORMATIVA DO USO DOS MEDIOS TECNOLÓXICOS NO CONCELLO DE VIMIANZO

1 OBXECTIVO

2 REVISIÓN E/OU ACTUALIZACIÓN

3 OBXECTO

4 ALCANCE

5 CANAL DE SOLICITUDES OU NOTIFICACIÓNS

6 INCIDENTES DE SEGURIDADE

7 NORMATIVA DO USO DOS MEDIOS ELECTRÓNICOS

7.1 NORMAS DE UTILIZACIÓN DO EQUIPAMENTO INFORMÁTICO E DE COMUNICACIÓNS

7.2 NORMAS XERAIS

7.3 NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTILES E DISPOSITIVOS MÓBILES

7.4 NORMAS PARA O ALMACENAMENTO DE INFORMACIÓN E COPIAS DE SEGURIDADE

7.5 NORMAS DE USO PARA SOPORTES DE ALMACENAMENTO EXTRAÍBLES

7.5.1 Normas para o borrado e eliminación de soportes informáticos

7.6 NORMAS RESPECTO Á XESTIÓN DE DOCUMENTOS

7.6.1 Impresoras en rede, fotocopiadoras/escáneres

7.6.2 Coidado e protección da documentación impresa

8 POSTO DE TRABALLO DESPEXADO.

9 ACCESO ÓS SISTEMAS DE INFORMACIÓN E AOS DATOS TRATADOS.

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

11 CONFIDENCIALIDADE, PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL E DEBER DE SECRETO

12 LIMPEZA DE METADATOS E DATOS OCULTOS DOS DOCUMENTOS ELECTRÓNICOS

13 USO DO CORREO ELECTRÓNICO CORPORATIVO

14 ACCESO A INTERNET E OUTRAS FERRAMENTAS DE COLABORACIÓN.

15 MONITORIZACIÓN E APLICACIÓN DESTA NORMATIVA

16 INCUMPRIMENTO DA NORMATIVA.

ANEXOS

1 ANEXO I. MODELO DE ACEPTACIÓN E COMPROMISO DE CUMPRIMENTO.

2 ANEXO 2. PROCEDEMENTO DE LIMPIEZA DE METADATOS

Número de anuncio 2024/6030

1. OBXECTIVO

A presente Normativa, foi aprobada pola 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 deste 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 dispor 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 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 a disposición.

O persoal de terceiros (empresas provedoras, convenios, etc.) con acceso ao sistema quedan tamén suxeitos a esta normativa, 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. CANAL DE SOLICITUDES E/OU NOTIFICACIÓNS

As solicitudes de autorización e as notificacións reflectidas nesta normativa dirixiranse a seguridade@vimianzo.gal

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.

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 portátiles e dispositivos móbiles aplicará as normas específicas para este tipo de equipamento.

7.2. 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.

Número de anuncio 2024/6030

- As persoas usuarias deberán notificar, o máis axiña posible, calquera comportamento anómalo dos seus equipos (vai lento, 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.

7.3. NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTILES 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 notificarase 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.

7.4. 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 tódolos datos dos servidores. Están 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 dirixirase unha solicitude de restauración.

7.5. 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 duros, etc.) non está autorizado. Para a súa utilización deberase de contar coa debida autorización.

No caso de que se lle autorice á persoa usuaria o uso deste tipo de soportes 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.
- 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 sae. Nese caso deberase de enviar unha solicitude para que se lle asesore sobre as medidas de seguridade que será necesario implementar.

7.5.1.Normas para el borrado y 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.

Número de anuncio 2024/6030

7.6. NORMAS RESPECTO Á XESTIÓN DE DOCUMENTOS

7.6.1. 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, estes deberán permanecer o menor tempo posible nas bandexas de saída das impresoras, 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 ambiental 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.

7.6.2.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 a 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.

8. 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.

9. 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 con 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, 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 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.

Número de anuncio 2024/6030

- As persoas usuarias deben utilizar contrasinais seguros, #de acordo con 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 cada tres meses, aviso previo/previo aviso cos suficientes días de antelación. Nos que non sexa posible será responsabilidade dos usuarios proceder ao seu cambio na devandita periodicidade.

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

Cando sexa necesario acceder ao cartafol persoal ou conta de correo corporativa dun Usuario, este acceso deberase realizar contando coa autorización expresa da persoa titular das mesma e só poderá ser realizado polo Responsable do mesmo ou pola persoa en que esta delegue.

No caso de que non resulte posible solicitar esta autorización (falecemento, enfermidade, imposibilidade de localización, etc.), o acceso poderá ser realizado a condición de que estea autorizado de forma expresa polo polo Responsable do mesmo ou pola persoa en que esta delegue.

En ambos os casos, deberase motivar a necesidade de acceso e ser comunicada ao Responsable do Usuario, que procederá á elaborando unha acta no que se recollan todas as accións levadas a cabo.

11. CONFIDENCIALIDADE, PROTECCIÓN DE DATOS DE CARÁCTER PERSOAL E DEBER DE SECRETO

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) dita 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 houbesen tido 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 secreto sobre os mesmos, deber que se manterá de maneira indefinida, mesmo máis aló da relación laboral ou profesional coa Organización.

12. 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.) e/ou fotografías, 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.

Número de anuncio 2024/6030

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 a 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".

13. USO DO CORREO ELECTRÓNICO CORPORATIVO

O correo electrónico corporativo é unha ferramenta de mensaxería electrónica centralizada, posta ao dispor 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 @teniendo en cuenta 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 de o a 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.
- Non se debe ceder o uso da conta de correo a terceiras persoas.
- Informar de correos con virus, phishing, malware (programa maligno), etc. sen reenvialos, para evitar a súa posible propagación.
- Non responder a mensaxes de Spam.
- Asegurar a identidade do remitente antes de abrir unha mensaxe.
- Non executar arquivos adxuntos sospeitosos. Non deben executarse os arquivos adxuntos recibidos sen analizalos previamente coa ferramenta corporativa contra código malicioso.
- 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).

14. ACCESO A INTERNET E OUTRAS FERRAMENTAS DE COLABORACIÓN

O acceso corporativo a Internet é un recurso centralizado que a Organización pon ao dispor 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.
- 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.

Número de anuncio 2024/6030

- 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.

15. MONITORIZACIÓN 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 con 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 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 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.

16. 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 instrución 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.

Número de anuncio 2024/6030

ANEXOS

1. ANEXO I. 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 a enchemento da seguinte declaración, o abaixo asinante, [persoal da Organización / empregado da empresa _____], como usuario 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 a las modificaciones del documento que lle foran debidamente comunicadas, comprometéndose, baixo a súa responsabilidade, ao seu cumprimento.

En _____, a ____ de _____ de 20__

Organización:	
Traballador (Nome e Apelidos):	
DNI número:	
Asinado:	

Por: <<Nome e apelidos>>
DNI número: _____

Número de anuncio 2024/6030

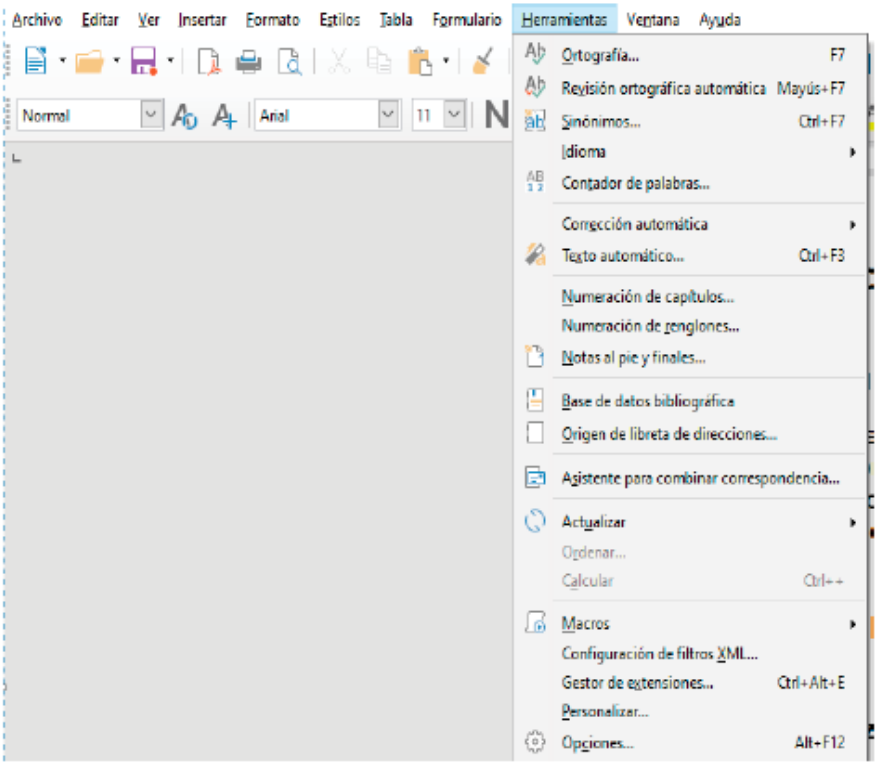
2. ANEXO 2. PROCEDEMENTO DE LIMPEZA DE METADATOS

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.

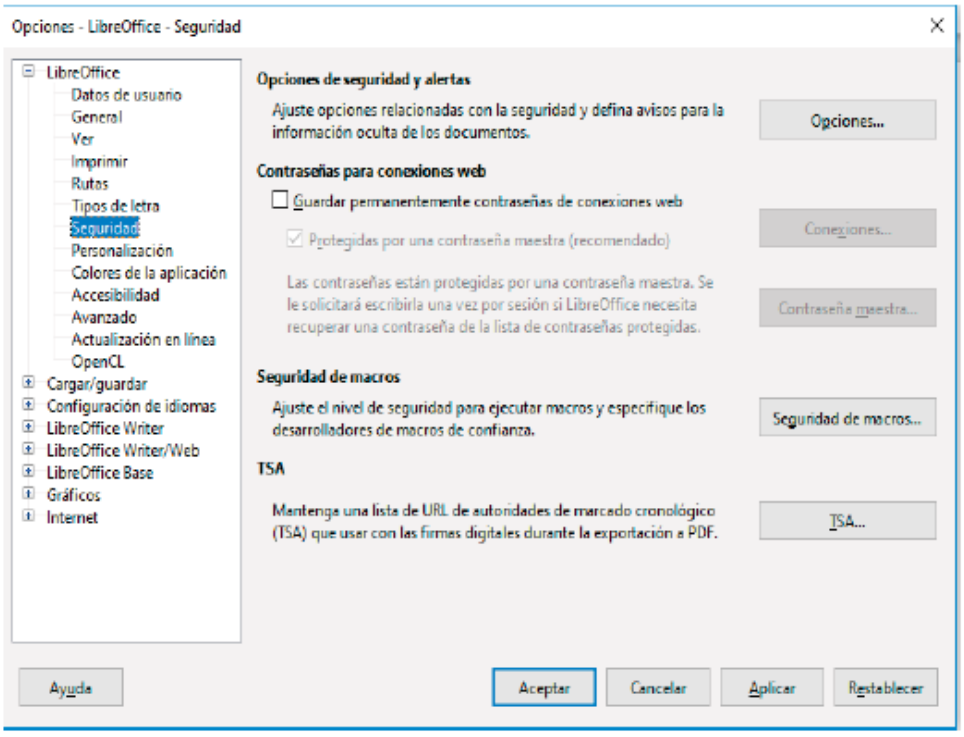
METADATOS EN DOCUMENTOS DE LIBREOFFICE - Evitar que se garden os metadatos no documento

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

1. Abre LibreOffice e ir a Ferramentas __ Opcións

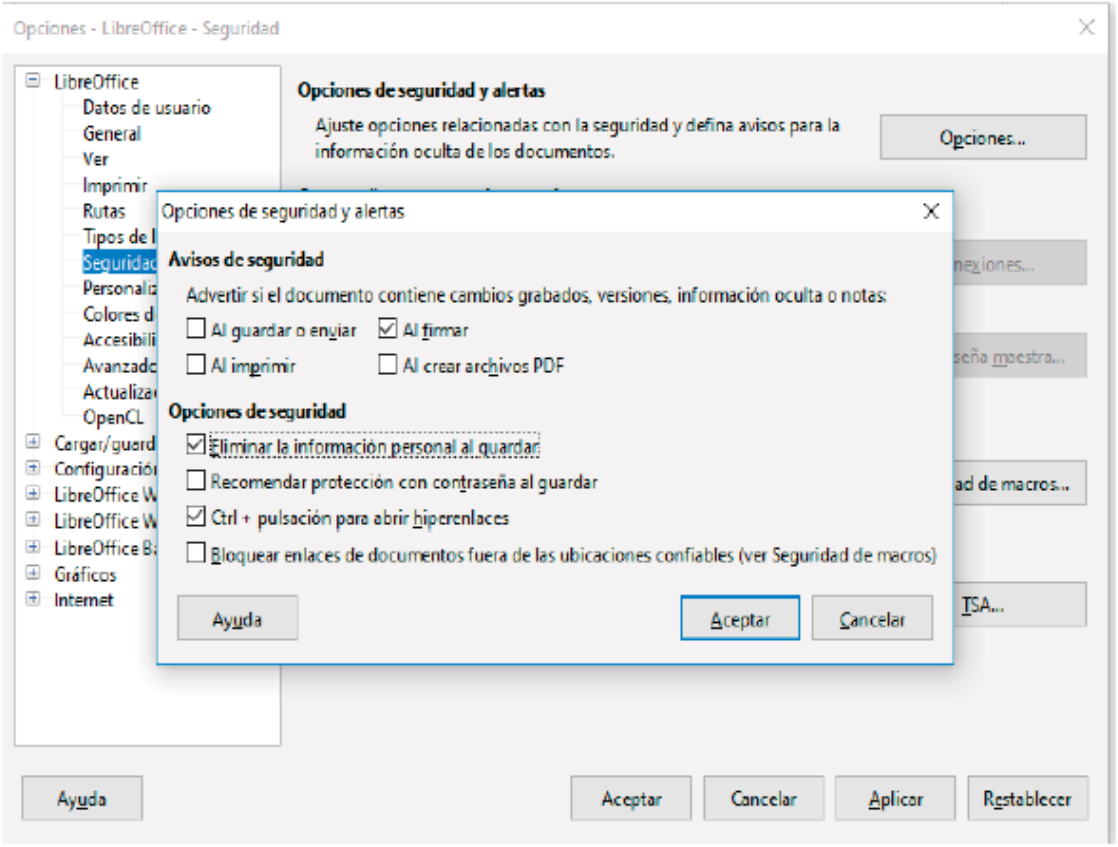


2. Na xanela que se abrirá, no menú da esquerda, hai que facer click en LibreOffice e despois click en Seguridade



Número de anuncio 2024/6030

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

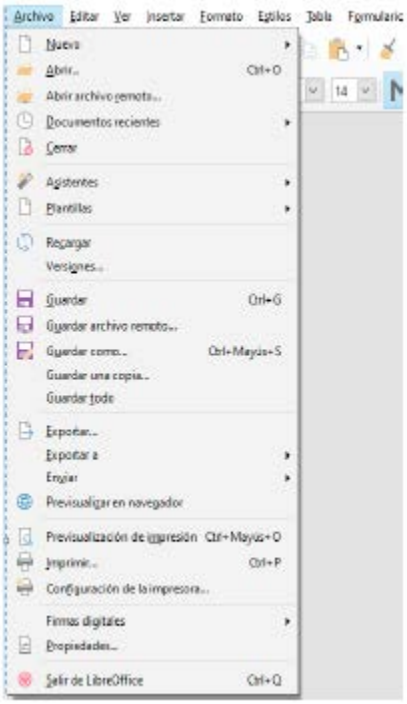


4. Facer click en Aceptar

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

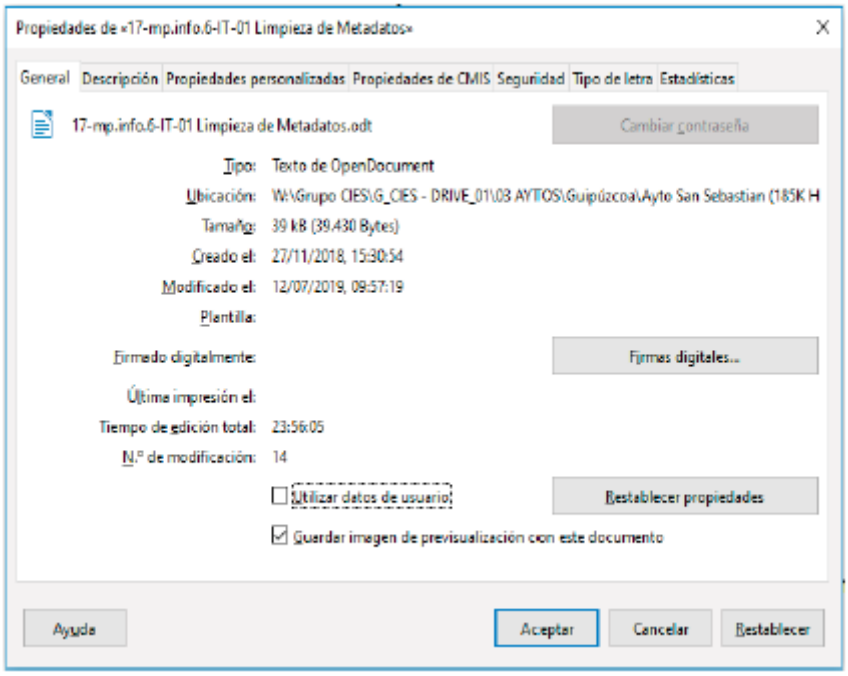
METADATOS EN DOCUMENTOS DE LIBREOFFICE - Eliminar os metadatos nun documento xa creado

1. Vai a Ficheiro>Propiedades



Número de anuncio 2024/6030

2. Na pestaña Xeral, fai click no botón Restablecer propiedades e desmarca a casilla 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 instrucións para levar a cabo para evitar que se garden os metadatos en Microsoft Office versión Microsoft Office Profesional Plus 2016

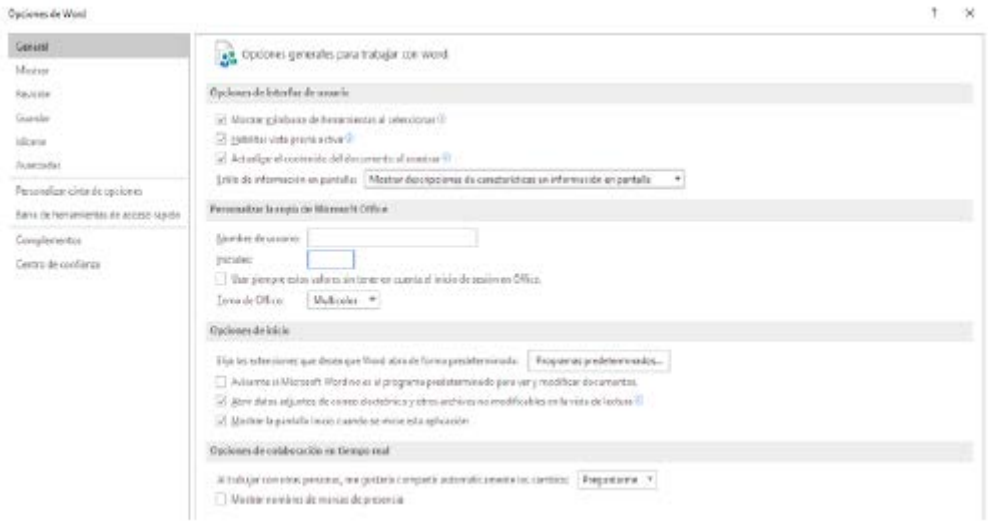
- Especificar a información persoal que aparece en todos os documentos de Office.

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

Abrir Microsoft Office e facer clic en Ficheiro e en Opcións

Número de anuncio 2024/6030

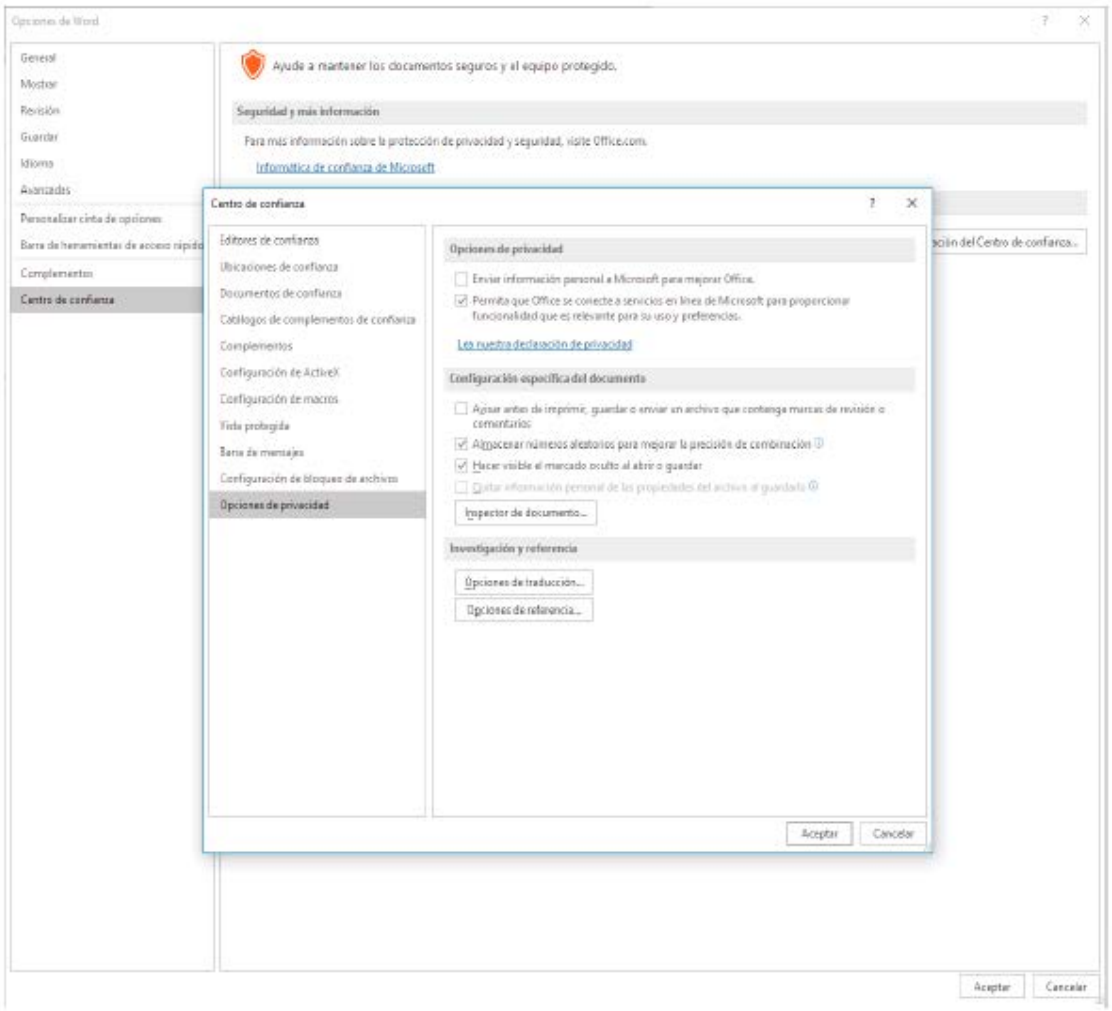
En xeral, no apartado Personalizar a copia de Microsoft Office, borraremos o noso nome e iniciais e remplazaremos por un espazo en branco en ambos os casos.



Non gardar a información persoal nun documento de Office

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.

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 eliminouse toda a información persoal do documento e fai que cada vez que o documento gárdese, elimínese a información persoal.



Número de anuncio 2024/6030

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.

Abra o documento de Word no que desexe buscar datos ocultos ou información persoal.

Faga clic na pestana Arquivo, logo en Gardar como e a continuación escriba un nome no cadro Nomee de arquivo para gardar unha copia do documento orixinal.

Na copia do documento orixinal, faga clic na pestana Arquivo e a continuación faga clic en Información.

Faga clic en Comprobar se hai problemas e logo faga clic en Inspeccionar documento.

No cadro de diálogo Inspector de documento, active as casas para elixir os tipos de contido oculto que desexe que se inspeccionen.

Faga clic en Inspeccionar.

Revise os resultados da inspección no cadro de diálogo Inspector de documento.

Faga clic na opción Quitar todo situada xunto aos 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, debido a que non sempre se poden restaurar os datos que quita este inspector."

Vimianzo, 26 de agosto de 2024

A alcaldesa

Mónica Rodríguez Ordóñez

2024/6030