Guía de Seguridad de las TIC
CCN-STIC 890

Anexo VI. Normativa de Uso de Medios Electrónicos

Enero 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

Fecha de Edición: March de 2024

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. OBJETIVO

La presente Normativa, ha sido aprobada por el Pleno de la Corporación de Negreira y entrará en vigor al día siguiente de su aprobación, hasta que sea reemplazada por una modificación o una nueva Normativa.

2. REVISIÓN Y/O ACTUALIZACIÓN

Con periodicidad anual se revisará su contenido y en caso de ser necesario se procederá a su modificación, que deberán ser aprobadas por los órganos anteriormente indicados, debiendo ser difundidas entre las personas afectadas por las mismas.

3. OBJETO

El objeto del presente documento es establecer la normativa de uso seguro de los medios electrónicos en el Ayuntamiento de Negreira, en adelante, la Organización, dentro del alcance señalado en el Esquema Nacional de Seguridad.

Los sistemas de información son elementos básicos para el desarrollo de la actividad de la Organización. Estos medios se ponen a disposición de las personas usuarias como instrumentos de trabajo para el desempeño de su actividad profesional. Motivo por el cual se deben utilizar estos recursos de manera responsable, mediante el seguimiento de normas, y buenas prácticas que salvaguarden la seguridad de la información, los sistemas de información y los recursos tecnológicos proporcionados por la entidad.

4. ALCANCE

Mediante la presente Normativa, la Organización establece la regulación del Uso de los Medios Electrónicos de su sistema de información (incluido el acceso remoto a los mismos), a través del establecimiento de medidas de cumplimiento obligatorio para todo el personal, quedando sujetos a la misma, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición.

El personal de terceros (empresas proveedoras, convenios, etc.) con acceso al sistema quedan también sujetos a la misma, en la medida que le sean de aplicación, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición de estas personas usuarias para el desempeño de sus actividades en la Organización.

En adelante, se utilizará “el Usuario” para referirse al personal propio o de terceros.

5. CANAL DE SOLICITUDES Y/O NOTIFICACIONES

Las solicitudes de autorización y las notificaciones reflejadas en esta normativa se dirigirán a concello@concellodenegreira.es .

6. INCIDENTES DE SEGURIDAD

Cuando un Usuario detecte cualquier anomalía (mal funcionamiento, aplicaciones que no arrancan o que se cierran de manera inesperada, pérdida de documentos, de memorias USB, etc.) o incidente de seguridad (virus, suplantación de identidad, pérdidas de clave, etc.) que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la Organización o pueda dañar a su imagen, deberá informar inmediatamente.

7. NORMATIVA DE USO DE LOS MEDIOS ELECTRÓNICOS

7.1 NORMAS DE UTILIZACIÓN DEL EQUIPAMIENTO INFORMÁTICO Y DE COMUNICACIONES

Estas normas conciernen específicamente a todos los dispositivos facilitados y configurados por la Organización, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información.

La Organización proporcionará al personal, el equipamiento debidamente configurado con acceso a los servicios y aplicaciones que sean necesarios para el desempeño de sus funciones.

Respecto a los cuales aplicará las normas generales y para los equipos portátiles y dispositivos móviles aplicará las normas específicas para este tipo de equipamiento.

7.1.1 8.1.1 Normas Generales

- Los equipos deberán de utilizarse únicamente para fines institucionales profesionales y como herramienta para el desempeño de las tareas encomendadas. Cada equipo estará asignado a una única persona. Esta persona es responsable de su correcto uso.
- Salvo autorización expresa no se dispondrán de privilegios de administrador sobre los equipos.
- Únicamente el personal autorizado podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos.
- Cuando sea necesario instalar equipos que no hayan sido provistos por la Organización deberá de solicitarse autorización previa.
- Las personas usuarias deberán notificar, a la mayor brevedad posible, cualquier comportamiento anómalo de sus equipos (va lento, no arranca, no funciona correctamente, etc.), especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo. Del mismo modo deberá de comunicar la ausencia de cables y/o accesorios o cualquier otra evidencia de deterioro del mismo.

- Con carácter general, no está permitido el uso de dispositivos propios, "BYOD (Bring Your Own Device)", para el acceso o almacenamiento de información salvo autorización expresa.

7.1.2 8.1.2 Normas específicas para equipos portátiles y dispositivos móviles

Para los portátiles y móviles además de las normas generales, serán de aplicación la siguientes:

- Estos dispositivos estarán, en todo momento bajo la custodia de la persona usuaria que los utilice, que será la responsable de adoptar las medidas necesarias para evitar daños o sustracción, así como del acceso a ellos por parte de personas no autorizadas.
- La sustracción de estos equipos se ha de notificar inmediatamente para la adopción de las medidas que correspondan.
- Se debe solicitar autorización cuando se usen para conectarse remotamente a través de redes que no estén bajo el control de la organización o que no hayan sido autorizadas, autorización que se hará extensible también a los servicios a los que se accede.
- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, la persona usuaria lo devolverá, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a una nueva persona.

7.2 NORMAS PARA EL ALMACENAMIENTO DE INFORMACIÓN Y COPIAS DE SEGURIDAD

Para garantizar la disponibilidad de la información frente a un incidente de seguridad, de forma periódica se realizan copias de seguridad de [INDICAR: unidades de red compartidas, unidad local, carpeta “Mis Documentos” de los equipos de usuario, etc.]

Por este motivo, los Usuarios deberán almacenar en estas los datos generados en el desempeño de sus competencias profesionales. A este respecto, se informa que no se realizan copias de seguridad de la información que no se encuentren en las unidades indicadas.

No está permitido el almacenamiento de información privada ni de terceros ajenos en los recursos indicados.

La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente de seguridad. Para recuperar esta información se habrá de dirigir una solicitud de restauración.

7.3 NORMAS DE USO PARA SOPORTES DE ALMACENAMIENTO EXTRAÍBLES

Como norma general, en la Organización el uso de soportes o medios de almacenamiento extraíbles (memorias USB, discos duros, etc.) no está autorizado. Para su utilización se deberá de contar con la debida autorización.

En el caso de que a la persona usuaria se le autorice el uso de este tipo de soportes trabajo, las normas a observar las siguientes:

- Como norma general, se utilizarán los soportes extraíbles proporcionados por la Organización. Estando destinados a un uso exclusivamente profesional, como herramienta de transporte puntual de ficheros, no como herramienta de almacenamiento.
- El uso de medios de almacenamiento extraíbles particulares, no está autorizado, salvo que se disponga de la debida autorización.
- Su uso no está autorizado para el almacenamiento de datos personales, salvo que se disponga de la debida autorización.

Este tipo de dispositivos deberá de almacenarse en lugares seguros, al objeto de prevenir robos o el acceso de terceros no autorizados. La pérdida o sustracción de estos dispositivos, con indicación de su contenido, deberá ponerse en conocimiento, de forma inmediata.

El transporte de estos soportes fuera de las instalaciones de la Organización deberá ser realizado exclusivamente por personal autorizado, autorización que contemplará igualmente a la propia información que sale. En cuyo caso se deberá de enviar una solicitud para que se le asesore sobre las medidas de seguridad que será necesario implementar.

7.3.1 8.3.1 Normas para el borrado y eliminación de soportes informáticos

Los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan datos de carácter personal, deberán ser eliminados de forma segura para evitar accesos a dicha información. En este sentido, la persona usuaria deberá tener en cuenta las siguientes indicaciones:

- Asegurarse que el contenido del soporte puede ser eliminado.
- Cualquier petición de eliminación de soporte informático deberá ser solicitada.

Para la reutilización de medios de almacenamiento, para otros fines diferentes de los que originaron su uso deberá solicitarse un borrado seguro de mismo.

8.4 NORMAS RESPECTO A LA GESTIÓN DE DOCUMENTOS

7.3.2 8.4.1 Impresoras en red, fotocopiadoras/escáneres

Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente.

En ningún caso se podrá hacer uso de impresoras, fotocopiadoras que no hayan sido proporcionados por la Organización. Con relación a los sistemas de copia e impresión y documentación impresa, los Usuarios debe seguir las siguientes directrices:

- Los documentos, con carácter general, se generarán en formato electrónico, pudiendo digitalizar aquellos que no sean susceptibles de ser generados en el citado formato.
- Cuando se impriman documentos, en sistemas de impresión o copia comunes, éstos deberán permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.
- En la realización de copias de documentos y/o escaneo, no debe olvidarse retirar los originales.
- En caso de encontrase documentación en un sistema de copia o impresión, el Usuario intentará localizar a la persona propietaria para que proceda a su recogida inmediata. En caso de desconocer a la persona propietaria o no estar localizable, lo pondrá inmediatamente en conocimiento.
- Para evitar un uso excesivo de los recursos, mejorando el impacto medioambiental en la generación de documentos en papel, y por motivos de seguridad, antes de imprimir documentos, el Usuario debe asegurarse de que es absolutamente necesario hacerlo.

8.4.2 Cuidado y protección de la documentación impresa

La documentación debe ser protegida, de forma que sólo tenga acceso a ella el personal autorizado, a tal efecto la persona usuaria tendrá en cuenta las siguientes medidas:

- Los puestos de trabajo permanecerán despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.
- Cuando no vaya a ser utilizada se deberá guardar en sistemas de almacenamiento (armarios o archivadores) preferentemente bajo llave. No podrán ser publicados en tablones o similares.
- Cuando los documentos no sean necesarios, deberán ser eliminados utilizando para ello los medios puestos a disposición por parte de la entidad

(destructora de documentos) de forma que no sea recuperable la información que pudieran contener.

- Antes de abandonar las salas de reuniones o permitir que alguien ajeno acceda a las mismas, se limpiarán adecuadamente las pizarras y se recogerán todos los documentos, cuidando de que no quede ningún tipo de información "sensible" o "interna" accesible a personas no autorizadas.

8.5 PUESTO DE TRABAJO DESPEJADO

Los puestos de trabajo deben permanecer despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.

8.6 ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS TRATADOS

Para acceder a los sistemas y recursos informáticos es necesario tener asignada previamente una cuenta de usuario. El alta de los usuarios será solicitada y autorizada de acuerdo con las políticas de la organización. La autorización del acceso establecerá el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada persona, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

Los Usuarios dispondrán de credenciales personales de acceso (código de usuario y una contraseña, certificado electrónico, etc.) para el acceso a los sistemas de información de la Organización **empleando la red segura, protegida con los servicios de seguridad destinados a tal efecto**, siendo responsables de su custodia y de toda actividad relacionada con el uso de su acceso autorizado, respecto de los que deberá de observar las siguientes medidas:

- El código de usuario es único para cada persona, intransferible e independiente del PC o terminal desde el que se realiza el acceso.
- Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros. De igual modo, no deben utilizar ningún acceso autorizado de otra persona, aunque dispongan de la autorización de su titular.
- Si una persona tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe comunicarlo inmediatamente.
- Las personas usuarias deben utilizar contraseñas seguras, de acuerdo con la política establecida en la Organización, no deben estar compuestas únicamente por palabras del diccionario u otras fácilmente predecibles o asociables a la persona usuaria (nombres de su familia, direcciones, matrículas de coche, teléfonos, nombres de productos comerciales u organizaciones, identificadores de usuario, de grupo o del sistema, DNI, etc.).

- Los sistemas que así lo permitan, forzarán el cambio de la contraseña al menos una vez al año, previo aviso con los suficientes días de antelación. En los que no sea posible será responsabilidad de los Usuarios proceder a su cambio en dicha periodicidad.

8.7 ACCESO A UNA CUENTA DE UN USUARIO EN SU AUSENCIA O BAJA

Cuando sea necesario acceder a la carpeta personal o cuenta de correo corporativa de un Usuario, este acceso se deberá realizar contando con la autorización expresa de la persona titular de las misma y solo podrá ser realizado por el Responsable del mismo o por la persona en que esta delegue.

En caso de que no resulte posible recabar esta autorización (fallecimiento, enfermedad, imposibilidad de localización, etc.), el acceso podrá ser realizado siempre y cuando esté autorizado de forma expresa por el por el Responsable del mismo o por la persona en que esta delegue.

En ambos casos, se deberá motivar la necesidad de acceso y ser comunicada al Responsable del Usuario, que procederá a la elaborando un acta en el que se recojan todas las acciones llevadas a cabo.

8.9 CONFIDENCIALIDAD, PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DEBER DE SECRETO

La información contenida en el Sistema de Información de la Organización es responsabilidad de dicha entidad, por lo que las personas usuarias deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa de la propia Institución. Además, deberá de tener en cuenta las siguientes premisas:

- Todas los Usuarios, que por razón de su actividad profesional hubiera tenido acceso a información gestionada por la Organización (documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva.
- Los Usuarios solo podrán acceder con las debidas autorizaciones a aquella información necesaria para el desempeño de sus labores. En todo caso, no deberá acceder a información sin las debidas autorizaciones.
- Toda información contenida en los sistemas de información de la Organización o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones que tiene encomendadas el Usuario.
- Los derechos de acceso de los Usuarios a la información y a los sistemas de información que la tratan deberán siempre otorgarse en base a los principios de “mínimo privilegio”, “necesidad de conocer y responsabilidad de compartir” y “capacidad de autorizar”.

- La información que comprenda datos de carácter personal quedará afectada también por la normativa vigente en materia de Protección de Datos personales, estando obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la Organización.

8.10 LIMPIEZA DE METADATOS Y DATOS OCULTOS DE LOS DOCUMENTOS ELECTRÓNICOS

Se define **metadato** como información estructurada que describe, explica, localiza y además hace más fácil recuperar, utilizar o gestionar un recurso de información. Los metadatos son comúnmente llamados "datos sobre los datos" o "información sobre la información".

Se define información o **datos ocultos** como aquellos datos existentes en el contenido de los documentos electrónicos, que no son visibles con la configuración estándar o configuración por defecto de los programas utilizados para su creación y tratamiento, siendo necesario aplicar alguna opción específica dentro de la configuración de estos programas, para su visualización. Un ejemplo de datos ocultos es el texto oculto, filas o columnas ocultas, comentarios o información del documento, etc.

Cuando hacemos una fotografía o creamos documentos con aplicaciones de Microsoft Office (Word, Excel, PowerPoint, etc.), estos archivos llevan integrados en sus propiedades una serie de datos ocultos y/o metadatos, como pueden ser el nombre de la persona que ha creado el documento, el programa con el que se ha generado, la fecha de creación, la de modificación, etc. Esto puede perjudicar a la confidencialidad de la información y a la buena imagen de la entidad.

Todos los archivos electrónicos (documentos ofimáticos, hojas de cálculo, imágenes, etc…) pueden tener integrados en sus propiedades una serie de datos ocultos y/o metadatos, como pueden ser el nombre de la persona que ha creado el documento, el programa con el que se ha generado, la fecha de creación, la de modificación, etc.

Los metadatos contenidos en los archivos pueden llegar a afectar tanto a la seguridad de la información como a la imagen de la Organización. Por ello, todo archivo que vaya a ser difundido internamente, remitido electrónicamente a un tercero o publicado en Internet (página web, sede electrónica, etc…), deberá ser revisado para determinar los metadatos asociados al mismo, procediendo a su modificación o supresión, si procede, siguiendo el procedimiento establecido en el anexo "Procedimiento de Limpieza de Metadatos".

8.10 USO DEL CORREO ELECTRÓNICO CORPORATIVO

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los Usuarios del sistema de información de la Organización para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas. Al tratarse de un recurso compartido, un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todas las personas.

El correo electrónico se deberá emplear en base al "sentido común" y teniendo en cuenta la responsabilidad y funciones desempeñadas, tratando en cualquier caso de no poner en compromiso ni los sistemas ni la imagen de la Organización.

La Organización queda facultada para filtrar el contenido del correo electrónico de la cuenta de correo proporcionada para el desarrollo de sus funciones laborales, al objeto de prevenir virus o en el supuesto de que existan razones fundamentadas en una firme sospecha por del a Organización sobre la existencia de actividades delictivas o dolosas del personal.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa.

Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades. Por este motivo se establecen las siguientes directrices con el objetivo de reducir el riesgo en el uso del correo electrónico:

- Utilizar el correo electrónico exclusivamente para propósitos profesionales[1].
- No se debe ceder el uso de la cuenta de correo a terceras personas[2].
- Informar de correos con virus, phishing, malware (programa maligno), etc. sin reenviarlos, para evitar su posible propagación.
- No responder a mensajes de Spam.[3]

1 Gran parte de los mensajes de correo electrónico no deseados, que llegan a las organizaciones tienen su origen en un uso no profesional de las cuentas de correo.

2 Esto provocaría una suplantación de identidad y el acceso a información. Es conveniente controlar la difusión de las cuentas de correo, facilitando la dirección profesional sólo en los casos necesarios y siempre y cuando el fin último sea el cumplimiento de las funciones municipales (p.e., cuando nos subscribimos a un foro).

3 La mayor parte de los generadores de mensajes de spam (correo electrónico masivo no solicitado) se envía a direcciones de correo electrónico aleatoriamente generadas, esperando que las respuestas obtenidas confirmen la existencia de direcciones de cuentas reales. Además de ello, en ocasiones tienen el aspecto de mensajes legítimos e, incluso, pueden contener información relativa a la Corporación. En cualquier caso, nunca deben de responderse.

- Asegurar la identidad del remitente antes de abrir un mensaje[4].
- No ejecutar archivos adjuntos sospechosos. No deben ejecutarse los archivos adjuntos recibidos sin analizarlos previamente con la herramienta corporativa contra código malicioso.[5]

Respecto al uso del correo electrónico, **queda terminantemente prohibido**:

- Falsificar, ocultar, suprimir o sustituir la identidad del emisor en cualquier correo electrónico.
- Leer o acceder a correos electrónicos ajenos, sin autorización previa.
- Enviar correos electrónicos que contengan en el cuerpo o en los adjuntos información con datos de categorías especiales de datos o datos especialmente sensibles (esto es, salud, ideología, religión, creencias, origen racial, étnico, etc. o aquellos considerados como de especial protección por la organización, salvo que se cuente con la autorización pertinente y se hayan aplicado las medidas de seguridad oportunas (cifrado o similares).

8.11 ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN

El acceso corporativo a Internet es un recurso centralizado que la Organización pone a disposición de los Usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional. La Organización velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso. Las normas de uso son las siguientes:

- Como norma general, las conexiones que se realicen a Internet deben obedecer a fines profesionales.
- Sólo se podrá acceder a Internet mediante los navegadores suministrados y configurados en los puestos de usuario. No podrá alterarse su configuración, ni utilizar un navegador alternativo, sin contar con la debida autorización.
- El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino.

4 Muchos ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida (amigo, compañero, etc.) de la persona atacada. El origen de estas acciones es diverso: acceso no autorizado a la cuenta, suplantación visual de la identidad, introducción de código malicioso que utiliza la cuenta remitente para propagarse, etc. En caso de recibir un correo sospechoso, y dependiendo de su verosimilitud, cabe: ignorarlo, no abrirlo y poner el hecho en conocimiento del remitente, independientemente de comunicar la incidencia de seguridad correspondiente. Igualmente, el envío de información, "confidencial" a petición de un correo del que no se puede asegurar la identidad del remitente, debe rechazarse. Es importante tener en cuenta que resulta muy sencillo enviar un correo con un remitente falso. Nunca se debe confiar en que la persona con la que nos comunicamos vía email sea quien dice ser, salvo en aquellos casos que se utilicen mecanismos de firma electrónica de los correos (no sólo de los ficheros adjuntos).

5 Esto es especialmente importante cuando se reciben adjuntos no solicitados o el correo es sospechoso. Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.).

- Deberá notificarse cualquier anomalía (redirección a páginas solicitadas, aviso de sitio no seguro, en páginas habitualmente utilizadas, etc.) detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

Se consideran **usos prohibidos,** que implican un riesgo de seguridad**,** las siguientes actuaciones:

- La descarga de programas informáticos sin la autorización previa o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio Web visitado es confiable.
- El acceso, la descarga y/o el almacenamiento en cualquier soporte, de páginas con contenidos ilegales, dañinos, inadecuados o que atenten contra la moral y las buenas costumbres y, en general, de todo tipo de contenidos que incumplan las normas éticas y de cortesía de la Organización.
- El acceso a recursos y páginas web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.
- La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizados.

8. MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

La Organización por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

- Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
- Monitorizará los accesos a la información contenida en sus sistemas.
- Auditará la seguridad de las credenciales y aplicaciones.
- Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

Esta supervisión se realizará en todo caso con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los Usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos

temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar sobre usos prolongados e indebidos del servicio.

9. INCUMPLIMIENTO DE LA NORMATIVA

Los Usuarios del sistema de información de la Organización están obligadas a cumplir lo prescrito en la presente Normativa de Uso de Medios Electrónicos".

En el supuesto de que una persona usuaria no observe alguna de los preceptos señalados en la presente Normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos que tenga asignados, previa instrucción del procedimiento legal que corresponda.

En el caso de personal de terceros, el incumplimiento de esta normativa podría derivar en la imposición de penalidades pudiendo llegar incluso a la resolución del contrato, siguiendo el procedimiento establecido al efecto en la normativa sobre contratación administrativa.

10. ANEXOS

11.1 MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

Todos los usuarios de los recursos informáticos y/o sistemas de información de la Organización deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa de Uso de Interno de Medios Electrónicos.

Para su aceptación junto con la normativa se trasladará el siguiente "acuse de recibo", que deberá ser firmado, a todos los usuarios.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [*personal de la Organización / empleado de la empresa* _____ *],* como usuario de recursos informáticos y sistemas de información de la Organización, declara haber leído y comprendido la Normativa de Usos y medios electrónicos de la organización y aceptar los términos y condiciones de uso establecidos en el mismo, estando de acuerdo en cumplirlos, atender a las modificaciones del documento que le hayan sido debidamente comunicadas, comprometiéndose, bajo su responsabilidad, a su cumplimiento.

En _____, a ____ de _____ de 20__

Organización:	
Trabajador (Nombre y Apellidos):	
DNI número:	
Número de Registro de Personal:	
Firmado:	

Por: <<Nombre y Apellidos>>
DNI número: _____
Número de Registro de Personal: _____

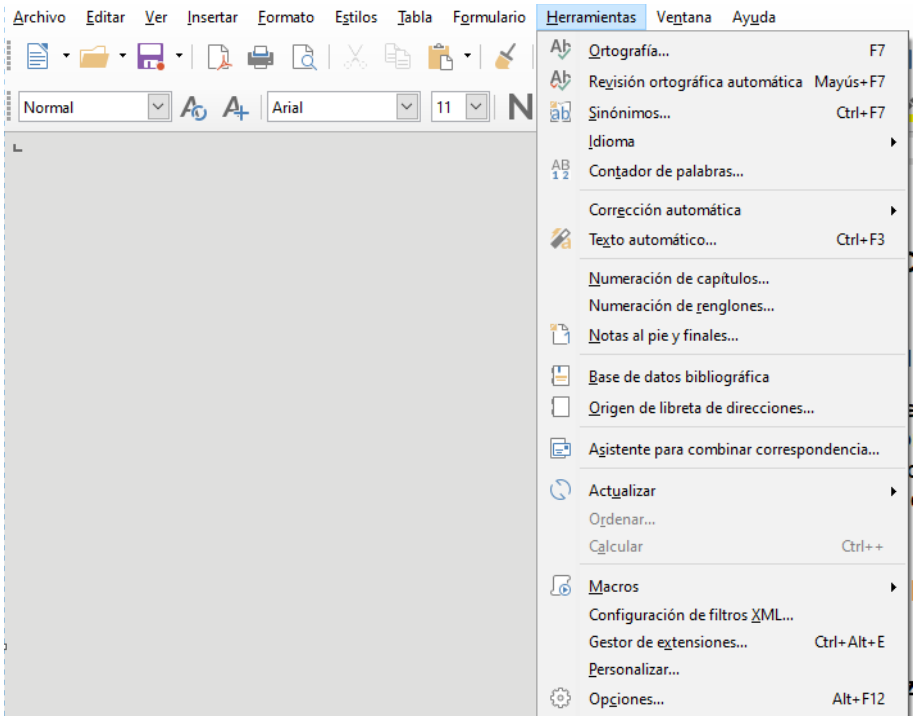
11.2 PROCEDIMIENTO DE LIMPIEZA DE METADATOS

El objetivo de este procedimiento es describir el proceso a seguir para realizar la limpieza de los metadatos no deseados de los documentos, a realizar antes de proceder al intercambio de documento con terceros, o al subir contenidos a los entornos web.

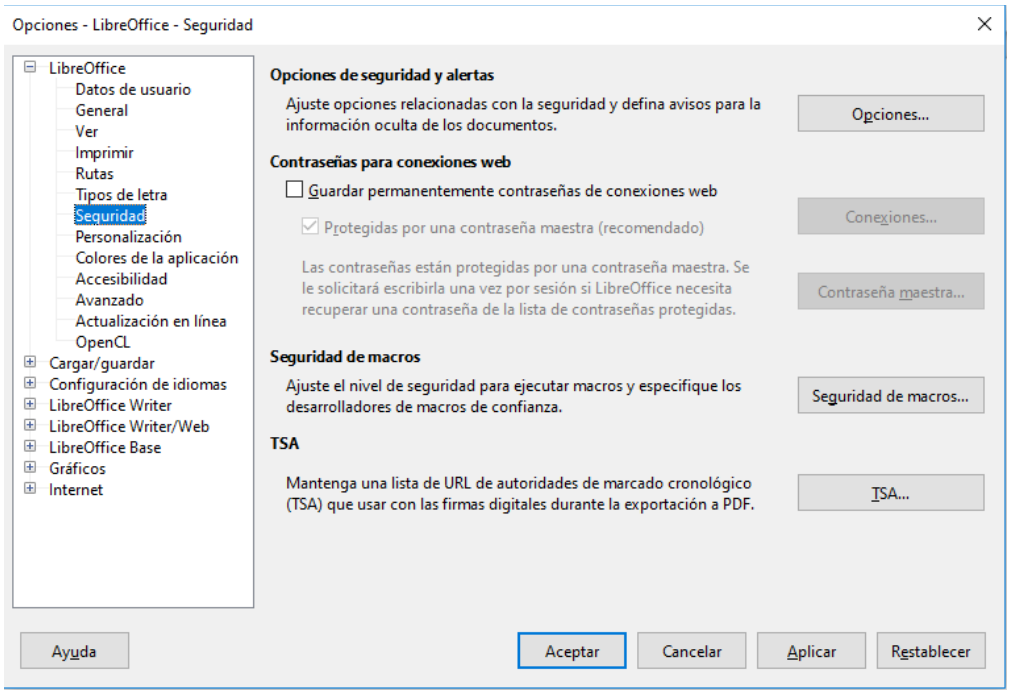
METADATOS EN DOCUMENTOS DE LIBREOFFICE – Evitar que se guarden los metadatos en el documento

A continuación, se establecen las instrucciones a llevar a cabo para evitar que se guarden los metadatos en LibreOffice Versión: 6.2.5.2.

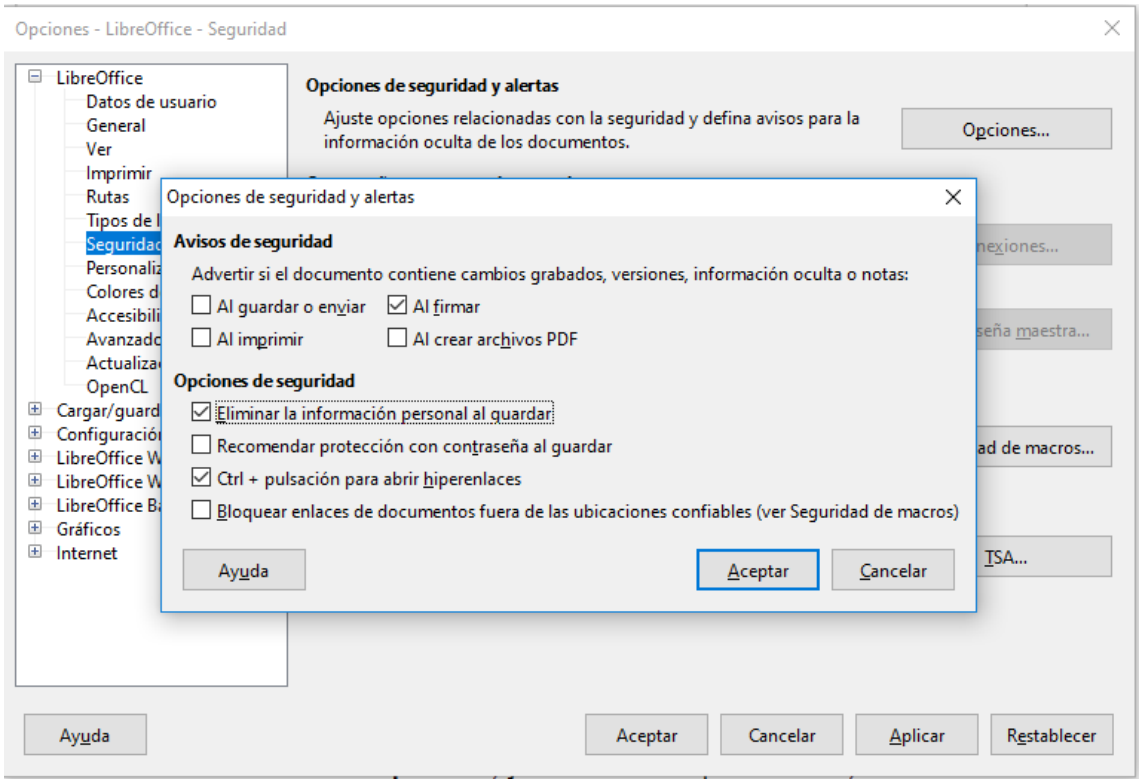
1. Abre LibreOffice e ir Herramientas → Opciones



2. En la ventana que se abrirá, en el menú de la izquierda, **haz click en LibreOffice y después haz click en Seguridad**



3. Haz click en el botón Opciones, y en la ventana que se abrirá, selecciona la casilla Eliminar la información personal al guardar.

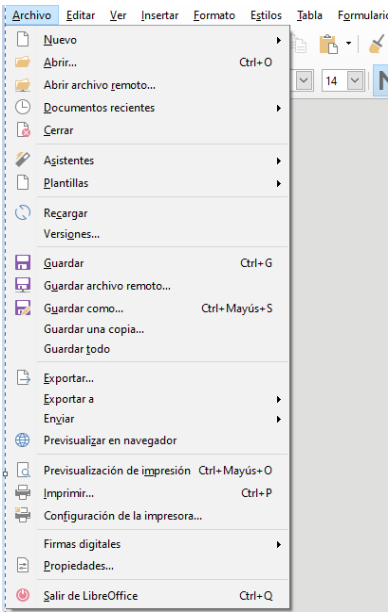


4. Haz click en ***Aceptar***

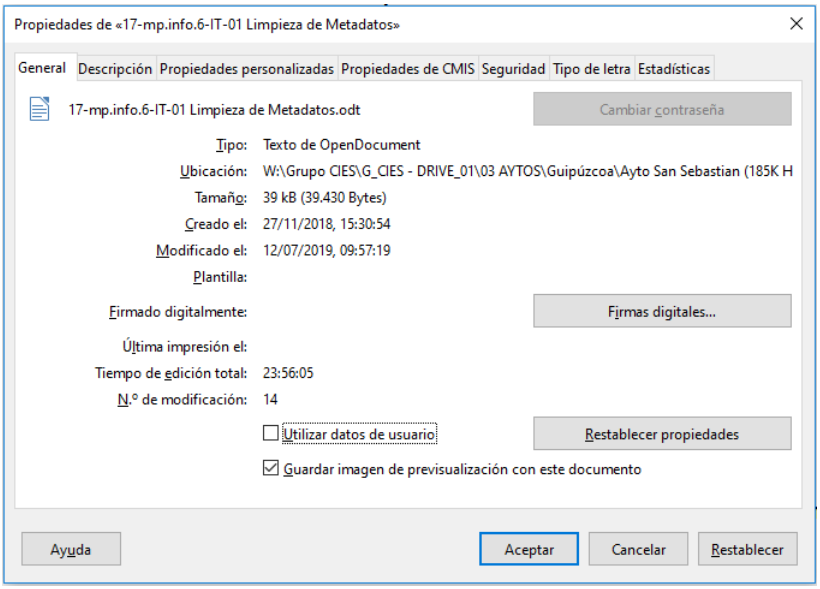
Después de esto, los documentos de LibreOffice se guardaran sin tu información personal.

METADATOS EN DOCUMENTOS DE LIBREOFFICE – Eliminar los metadatos en un documento ya creado

1. Ve a Archivo>Propiedades



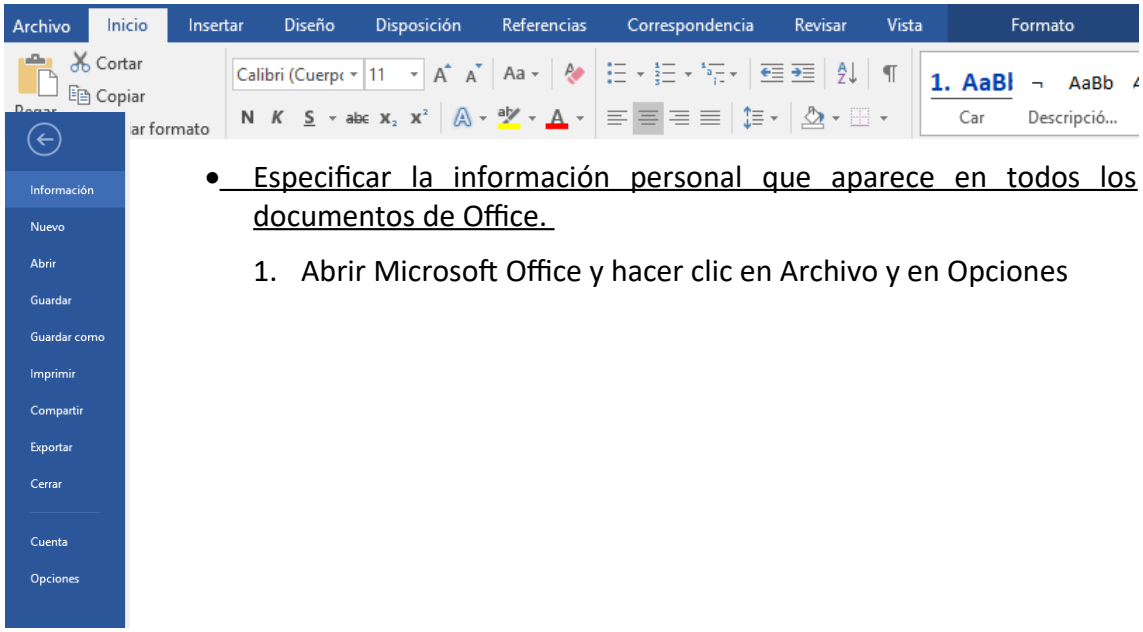
2. En la pestaña **General,** haz click en el botón **Restablecer propiedades** y desmarca la casilla **Utilizar datos del usuario**.



3. Haz click en **Aceptar**.

METADATOS EN DOCUMENTOS DE MICROSOFT OFFICE – Evitar que se guarden los metadatos en el documento

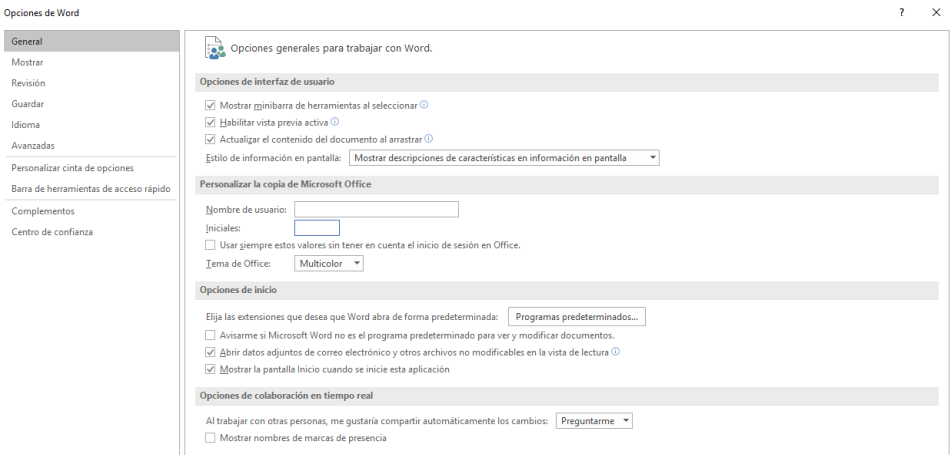
A continuación, se establecen las instrucciones a llevar a cabo para evitar que se guarden los metadatos en Microsoft Office versión Microsoft Office Profesional Plus 2016



- Especificar la información personal que aparece en todos los documentos de Office.

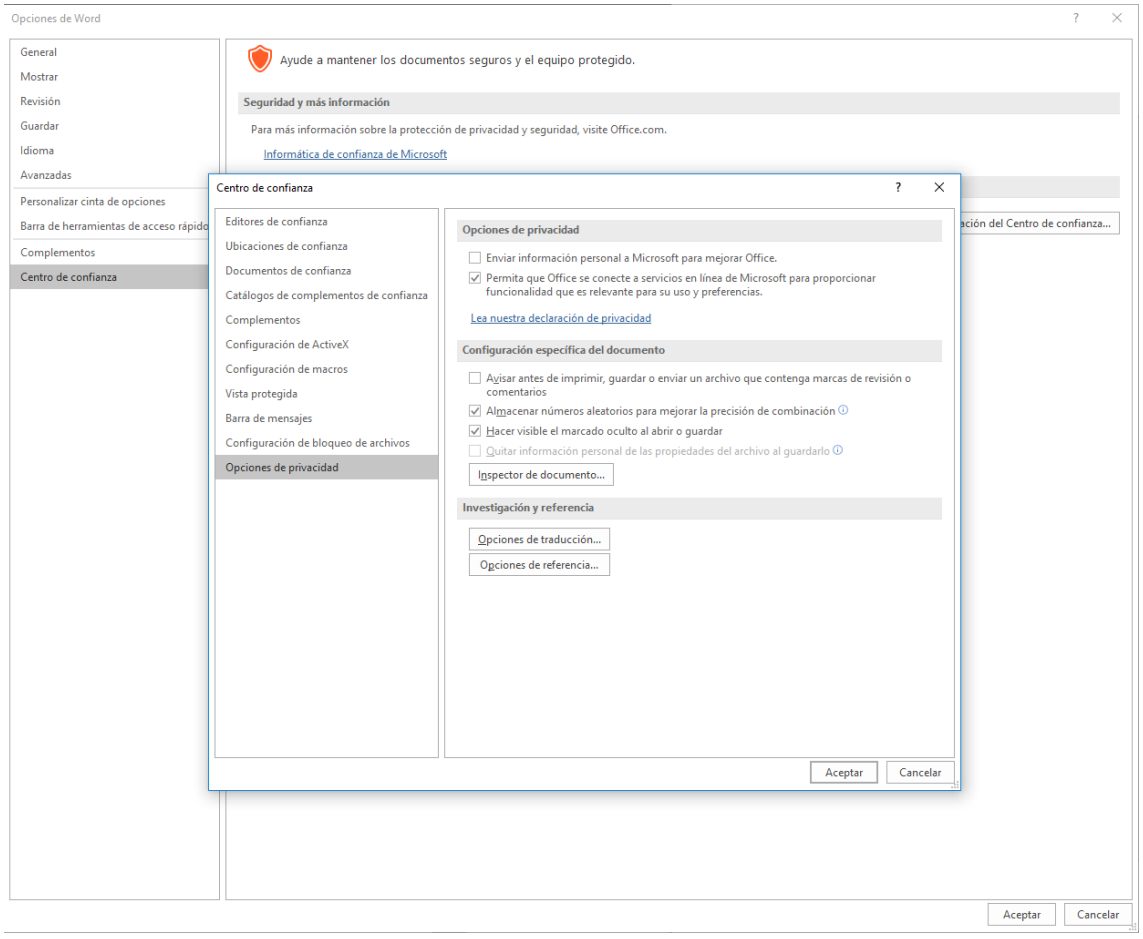
1. Abrir Microsoft Office y hacer clic en Archivo y en Opciones

2. En General, en el apartado Personalizar la copia de Microsoft Office, borraremos nuestro nombre e iniciales y remplazaremos por un espacio en blanco en ambos casos.



- No guardar la información personal en un documento de Office

1. Con el archivo abierto, hacer clic en Archivo y a continuación hacer clic en Opciones. Se abrirá la ventana de Opciones de la aplicación, seleccionar Centro de Confianza y pulsar en Configuración del Centro de Confianza. Se abre la ventana de Centro de Confianza.
2. Seleccionar Opciones de privacidad y en el cuadro destinado a Configuración específica del documento aparecerá la opción "Quitar Información personal de las propiedades del archivo al guardarlo". Esta opción sólo podrá seleccionarse cuando previamente se haya eliminado toda la información personal del documento y hace que cada vez que el documento se guarde, se elimine la información personal.



- 3.2.2Inspección y borrado de metadatos e información oculta

Usar el Inspector de documento para buscar y quitar los datos ocultos y la información personal de los documentos de Word.

1. Abra el documento de Word en el que desee buscar datos ocultos o información personal.

2. Haga clic en la pestaña Archivo, luego en Guardar como y a continuación escriba un nombre en el cuadro Nombre de archivo para guardar una copia del documento original.
3. En la copia del documento original, haga clic en la pestaña Archivo y a continuación haga clic en Información.
4. Haga clic en Comprobar si hay problemas y luego haga clic en Inspeccionar documento.
5. En el cuadro de diálogo Inspector de documento, active las casillas para elegir los tipos de contenido oculto que desee que se inspeccionen.
6. Haga clic en Inspeccionar.
7. Revise los resultados de la inspección en el cuadro de diálogo Inspector de documento.
8. Haga clic en la opción Quitar todo situada junto a los resultados de la inspección de los tipos de contenido oculto que desee quitar del documento.

IMPORTANTE: Se recomienda usar el Inspector de documento en una copia del documento original, puesto que no siempre se pueden restaurar los datos que quita este inspector.

PUBLICACIONES DE DEFENSA
GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL