|  |  |
| --- | --- |
|  | **PROTECCION DE DATOS PERSONALES**  **………**  **MEDIDAS DE SEGURIDAD**  **ENCRIPTAR/CODIFICAR**  **DOCUMENTOS** |
| Servicio de Organización e Información  Enero de 2021 | |

# INDICE

1.- Introducción.

2.- Conceptos sobre Cifrado o Encriptado de información:

3.- Obligación de cifrar la información:

4.- Alcance de este documento:

5.- Herramientas de la RPC para protección por cifrado o encriptado:

6.- Protección de documentos con la suite de Microsoft:

7.- Protección de documentos con la suite OpenOffice o LibreOffice:

8.- Protección de documentos con la aplicación de compresión 7-zip.

9.- Protección de documentos PDF con contraseña.

10.- Protección de cualquier documento con la aplicación dipalCryp.

11.- Protección de cualquier documento con la aplicación en la nube de la RPC dipalBOX.

12.- Protección de cualquier documento con la aplicación en la nube de la RPC proDatos - Valija.

Anexo- Instalación de la aplicación dipalCryp.

# 1.- Introducción:

El uso de cifrado o encriptado es un elemento básico de seguridad en la política de información de una entidad y, en particular, es una de las garantías adicionales que se pueden emplear para reducir el riesgo en el tratamiento de datos de carácter personal.

En el [**RGPD**](http://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807) se encuentran referencias expresas al cifrado en el considerando 83, donde se establece que **el cifrado es una de las medidas posibles** que pueden emplear tanto responsables como encargados del tratamiento **para mitigar el riesgo**.

En el artículo 6 “Licitud del Tratamiento” en el apartado 4, se establece, en su letra e), el cifrado como una de las garantías adecuadas para determinar la compatibilidad de un tratamiento para un fin distinto para el que se recogieron los datos.

En el artículo 32 Seguridad del tratamiento, en su apartado 1, letra a), incluye el cifrado como una de las posibles medidas de seguridad a adoptar tanto por responsables como por encargados:

Finalmente, en el artículo 34 “Comunicación de una violación de la seguridad de los datos personales al interesado”, en el apartado 3 letra a), se establece el cifrado como una de las medidas que, en el caso que se haya producido un acceso no autorizado, eximen de la obligación de comunicación de la brecha de seguridad a los sujetos de los datos comprometidos:

En la [LOPDGDD](https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673), que complementa el RGPD, no se encuentran nuevas referencias al cifrado.

En abril de 2018, el entonces Grupo del Artículo 29, ahora Comité Europeo de Protección de Datos, publicó una [Declaración sobre el cifrado y su impacto en la protección de los individuos con respecto a la protección de sus datos personales en la Unión Europea](https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia). En el texto se considera el cifrado como un elemento capital para garantizar la privacidad de las comunicaciones y defiende la necesidad de implementar sistemas de cifrado robustos, eficientes y estandarizados para la protección de la privacidad de los ciudadanos europeos.

La Declaración establece el cifrado como un elemento necesario e irremplazable para garantizar la privacidad de la comunicación en Internet y que dicha protección ha de implementarse de extremo a extremo, es decir, directamente entre los usuarios finales sin elementos intermedios que tengan acceso a la información.

Para terminar, el [Dictamen 05/2014 sobre técnicas de anonimización del Grupo del Artículo 29](https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia) establece los límites del cifrado con relación a los datos de carácter personal:

*“Las técnicas de seudonimización más utilizadas son las siguientes:*

*- Cifrado con clave secreta:*

*Ni el cifrado ni la codificación con clave sirven en sí mismos para que un interesado no pueda ser identificado, ya que aún se puede acceder a los datos originales o deducirlos, al menos si están en manos del responsable del tratamiento…*

*Es engañoso fiarse exclusivamente de la solidez del mecanismo de cifrado como medida del grado de anonimización de un conjunto de datos,…”*

# En definitiva, el uso de cifrado es una de las garantías que se pueden incorporar en un tratamiento para gestionar el riesgo, en particular cuando la comunicación se realice a través de Internet, cuando los datos personales se van a utilizar para un fin distinto de aquél para el que se recogieron, como técnica apropiada de seudonimización o cuando se ha producido una brecha de seguridad. Además, las aplicaciones de cifrado no pueden ver reducida su fortaleza por consideraciones de seguridad a cualquier nivel.

# Sin embargo, hay que tener presente que la utilización de cifrado no elimina la naturaleza de dato de carácter personal, por lo que la información cifrada no es información anonimizada.

# 2.- Conceptos sobre Cifrado o Encriptado de información:

## 2.1- ¿Qué es cifrar o codificar?

# En el mundo de la informática, el cifrado o encriptado es la conversión de datos de un formato legible a un formato codificado, que solo se pueden leer o procesar después de haberlos descifrado.

# El cifrado es el elemento fundamental de la seguridad de datos y es la forma más simple e importante de impedir que alguien robe o lea la información de un sistema informático con fines malintencionados.

# Utilizado tanto por usuarios individuales como por grandes corporaciones, el cifrado se usa ampliamente en Internet para garantizar la inviolabilidad de la información personal enviada entre navegadores y servidores.

# Esa información podría incluir todo, desde datos de pagos hasta información personal. Las empresas de todos los tamaños suelen utilizar el [cifrado para proteger los datos confidenciales](https://www.kaspersky.com/blog/encryption-kes10/15123/) en sus servidores y bases de datos.

# Más allá de la ventaja obvia de proteger la información privada contra robos o amenazas, el cifrado también ofrece un medio para demostrar tanto la autenticidad como el origen de la información. Se puede utilizar para verificar el origen de un mensaje y confirmar que no ha sufrido modificaciones durante la transmisión.

# Lo esencial del cifrado es el concepto de algoritmos de cifrado y “claves”. Cuando se envía información, esta se cifra mediante un algoritmo y solo se puede descodificar con la clave apropiada. Una clave puede almacenarse en el sistema de recepción, o bien, transmitirse junto con los datos cifrados.

## 2.2- Métodos para cifrar o codificar.

# Se utilizan una serie de métodos para codificar y descodificar la información, y dichos métodos evolucionan a medida que el software informático y los métodos de intercepción y robo de información cambian. Estos métodos incluyen lo siguiente:

# **Cifrado de clave simétrica**: también conocido como algoritmo de clave secreta, es un singular método de descodificación de mensajes que debe ser provisto al receptor antes de que el mensaje se pueda descodificar. La clave que se usa en la codificación es la misma que se utiliza en la descodificación, lo que resulta más conveniente para los usuarios individuales y los sistemas cerrados. De lo contrario, se le tiene que enviar la clave al receptor, lo que aumenta el riesgo de alteraciones en caso de que terceros, como un hacker, la intercepten. La ventaja es que este método es mucho más ágil que el método asimétrico.

# **Criptografía asimétrica**: este método utiliza dos claves diferentes (pública y privada), que están vinculadas entre sí matemáticamente. Las claves son solo números extensos vinculados entre sí, pero no son idénticos, de ahí el término asimétrico. La clave pública se puede compartir con cualquier persona, mientras que la clave privada debe mantenerse en secreto. Ambas se pueden usar para cifrar un mensaje, y la clave opuesta a la que se emplee para cifrarlo se utiliza luego para descodificarlo.

## 2.3- Tipos de cifrado o codificado.

# Existen múltiples tipos de algoritmos para Cifrar o codificar, entre los más utilizados podemos destacar:

# Triple DES

# El algoritmo de cifrado de datos triple o Triple-DES utiliza cifrado simétrico. Es una versión avanzada del cifrado de bloque DES, que solía tener una clave de 56 bits. Sin embargo, y como su nombre lo indica, TDES encripta los datos utilizando una clave de 56 bits tres veces, lo que la convierte en una clave de 168 bits.

# Aunque está desapareciendo, muchas organizaciones financieras y comerciales todavía usan este tipo de cifrado para proteger sus datos.

# AES

# El Estándar de cifrado avanzado (AES) también es cifrado simétrico basado en el algoritmo Rijndael. Utiliza el cifrado de bloque y cifra un bloque de tamaño fijo a la vez. Funciona en 128 bits o 192 bits, pero puede extenderse hasta la longitud de la clave de 256 bits.

# Es considerado como uno de los mejores algoritmos de cifrado porque fue desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU. También es uno de los tipos de cifrados seguros, ya que funciona en una sola clave privada.

# RSA

# El cifrado Rivest – Shamir – Adleman (RSA) es un cifrado asimétrico que funciona en dos claves: una clave pública para el cifrado y una clave privada para el descifrado. Considerado como el mejor algoritmo de cifrado, funciona en 1024 bits y puede extenderse hasta una longitud de clave de 2048 bits. Esto significa que cuanto mayor es el tamaño de la clave, más lento se vuelve el proceso de cifrado.

# También se considera un estándar de cifrado para los datos compartidos en Internet porque es el algoritmo de cifrado más seguro hasta ahora. En comparación con otros tipos de cifrado, RSA le da a los piratas informáticos un momento bastante difícil debido a la longitud de las claves con las que trabaja.

## 2.4- Ámbito del cifrado o encriptado.

# El cifrado de los datos personales los podemos enmarcar en los siguientes ámbitos:

# Medios de almacenamiento:

# Aquí **cifraremos todo el dispositivo** de almacenamiento de la información (disco duro, pendrive, etc..), por lo tanto, sin conocer la clave de descifrado no podremos acceder a ninguna información contenida en él.

# Carpetas:

# En este caso solo protegemos parte de la información almacenada, ya sea en la nube o en el disco duro, toda la que este en la carpeta seleccionada.

# Solo serán**ilegibles las carpetas que elijamos** para el cifrado, el resto se podrá acceder normalmente.

# Documentos o ficheros:

# En este caso solo protegemos Documentos o Ficheros seleccionados ya sea en la nube o en el disco duro. Solo serán elegibles los documentos que estén cifrados o encriptado, al resto se podrá acceder normalmente.

# 3.- Obligación de cifrar la información:

La nueva normativa indica que se debe analizar el riesgo al que estarán sometidos los datos que se vayan a tratar, de manera que se puedan implementar las medidas de seguridad adecuadas, según el estado de la técnica.

Como vamos a observar, en la [nueva normativa](https://protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/) se abre el abanico para que sea obligatoria la implementación de determinados tipos de cifrado a todo tipo de dato o tratamiento, sin distinción, en función del riesgo que exista para estos y para sus titulares.

No obstante, encontraremos diferentes normas que obligan al cifrado de ciertas actividades como:

* hospitales
* clínicas psicológicas
* despachos de abogados
* administraciones publicas

## 3.1.- Normativas:

### LOPD:

Las empresas que deben cifrar datos, según la Ley Orgánica de Protección de Datos ([LOPDGDD](https://protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/)) son aquellas que deben implantar medidas de nivel alto por razón de los datos que tratan o el tratamiento que realizan con ellos.

Es decir, se deben cifrar:

* las que traten [datos sensibles o especialmente protegidos.](https://protecciondatos-lopd.com/empresas/datos-especialmente-protegidos-sensibles/)
* las que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
* si tratan datos derivados de actos de violencia de género.

Se exige que también se cifre:

* cuando se transmita a través de redes públicas o inalámbricas los datos a los que nos hemos referido en el anterior párrafo
* los dispositivos portátiles cuando se encuentren fuera de las instalaciones y contengan este tipo de datos

### RGPD:

En la[nueva normativa europea](https://protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/) ya no se obliga solo a determinados datos a ser cifrados.

Por supuesto que los [datos sensibles](https://protecciondatos-lopd.com/empresas/datos-especialmente-protegidos-sensibles/) deben ser cifrados, pero no solo estos, si no que debemos cifrarlos en función del riesgo que entrañe para el afectado el descubrimiento de los datos personales por otra persona o empresa no autorizada.

* Cifrado Obligatorio

Por lo tanto, si nos atenemos a lo que nos dice el RGPD será obligatorio cifrar los datos de carácter personal en los siguientes casos:

##### Cuando nos lo imponga el Estado

# En nuestro país esta imposición la encontramos en la obligación que tenemos por la LOPD de cifrar los datos de nivel alto como:

* origen étnico o racial
* opiniones políticas
* convicciones religiosas o filosóficas
* afiliación sindical
* datos de salud y vidas sexual

##### Si estamos adheridos a un Código de conducta

# Si nuestra entidad esta adherida a un Código Tipo que regula las medidas de seguridad en nuestro sector de actividad, y este Código exige el cifrado, deberemos hacerlo si no queremos ser sancionados

##### La Evaluación de Impacto en la Protección de Datos nos lo ha recomendado

# Determinadas empresas, por el tipo de tratamiento que realizan, deben cifrar los datos personales que gestionan, según las conclusiones de la [evaluación de impacto](https://protecciondatos-lopd.com/empresas/evaluacion-impacto/) que hayan realizado por imperativo legal.

# Estas empresas son, entre otras, las que tratan [datos biométricos](https://protecciondatos-lopd.com/empresas/datos-biometricos-rgpd/) o las que observan sistemáticamente y a gran escala zonas de acceso público.

##### Tenemos que suprimir o reducir un riesgo

# Debe aplicarse la medida de cifrado si su implantación mitiga un riesgo cierto.

* Cifrado voluntario

Como hemos comentado, cifrado es una de las medidas más adecuadas para mitigar los riesgos inherentes al tratamiento de datos de carácter personal de manera que se pueda mantener la seguridad.

Por lo que, aunque por el tipo de datos y los riesgos que detectemos no estemos obligados a cifrar los datos, nuestra recomendación es que lo hagamos siempre que:

* no sea **demasiado gravoso**
* queramos ser **proactivos** para la seguridad
* deseemos ser un ejemplo de privacidad para otras empresas del sector
* ¿Por qué cifrar es conveniente?

Aquellas empresas que hayan implementado un sistema de cifrado y sufran una brecha de seguridad que afecte a los datos personales que gestiona, están exentos de [notificar la brecha de seguridad a los afectados](https://protecciondatos-lopd.com/empresas/notificar-brechas-seguridad/), ya que al estar protegida la información no hay peligro para los derechos de los usuarios.

En cambio, aquellas empresas que no cifren están compelidas a informar a los usuarios sobre los ataques que sufran si las consecuencias incluyen la afección de sus datos personales.

### LPBC:

La Ley de Prevención de Blanqueo de Capitales, exige a sus sujetos obligados (es decir, las empresas que la tiene que cumplir) que cuando creen el fichero relativo al tratamiento de datos personales conforme a esta ley se apliquen las medidas de nivel alto (de la LOPD) y por tanto los datos deben de cifrarse.

Art 32 LPBC*“serán de aplicación a estos ficheros las medidas de seguridad de nivel alto, que exigen el cifrado de datos”.*

### LGT:

No **existe una obligación clara** para el cifrado de datos personales en la **Ley General de Telecomunicaciones**.

No obstante, se ha incluido en este listado debido a que todas las compañías del sector cifran los datos de sus clientes para evitar tener que informarles sobre las brechas de seguridad que sufren en caso de que los atacantes hayan tenido acceso a los archivos encriptados.

### CDAE:

El **Código Deontológico de la Abogacía Española**, en su [artículo 4](https://www.abogacia.es/wp-content/uploads/2012/06/codigo_deontologico1.pdf), **“obliga”** a no defraudar la confianza de los clientes e instaura el secreto profesional como eje de la actividad jurídica.

El carácter de secreto y confidencial de la información exige su cifrado con el objetivo de convertirla en inteligible e inaccesible a terceros.

Por lo tanto, se entiende que deben aplicar medidas de nivel alto, para el tratamiento de datos personales de los clientes, de ahí la obligación de cifrar la información.

### LAP:

En relación a los datos tratados por profesionales de la salud, la Ley de Autonomía del Paciente, todos los datos personales deben ser cifrados ya que:

* en su [artículo 7.1](https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188#a7) promulga que “Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley”
* al tratarse de datos de salud se le deben de aplicar medidas de nivel alto

### Administraciones Publicas:

En el sector público será obligatorio el cifrado de datos en determinadas actividades para asegurar:

* el acceso
* integridad
* disponibilidad
* autenticidad
* confidencialidad
* trazabilidad
* conservación de los datos

En los servicios utilizados mediante medios electrónicos que gestionen en el ejercicio de sus competencias.

La normativa que lo exige es aquella que regula al Esquema Nacional de Seguridad, el [RDL 3/2010 de 8 de enero](https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330).

# 4.- Alcance de este documento:

El presente documento pretende dar una serie de instrucciones básicas a los usuarios de la Red Provincial de Comunicaciones (RPC), para la protección de Documentos utilizando el cifrado o encriptado que ofrecen distintas herramientas que se utilizan en la RPC. Y así poder enviar por Email los documentos previamente protegidos por estas herramientas.

Lo que se pretende es acercar al usuario de la RPC a las técnicas de cifrado o encriptado, para ello en principio solo vamos a utilizar las técnicas de Cifrado Simétrico que como hemos dicho anteriormente es el que utiliza una única Clave tanto para el Cifrado como para el Descifrado.

Y el ámbito lo vamos a limitar a la codificación de Documentos, dejando la codificación de soportes (disco, Pendrive, etc..), y carpetas para otro documento más avanzado.

Cuando la normativa española exige cifrado, otorga a las empresas dos posibilidades: un sistema de cifrado o cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros. Únicamente son válidos los sistemas de cifrado que garantizan que la información no se entienda ni pueda manipularse por terceros.

Se consultó a la Agencia Española de Protección de Datos si los sistemas de cifrado de ciertas herramientas, como las de compresión de archivos (ZIP) y los sistemas de claves de los PDF, eran suficientes para cumplir la normativa. El Gabinete Jurídico de la AEPD, en su Informe 0494/2009, respondió: no son suficientes.

# 5.- Herramientas de la RPC para protección por cifrado o encriptado:

Existen muchas herramientas en el mercado para el cifrado o encriptación de documentos, pero solo nos vamos a centrar en este documento en las que se utilizan en la RPC, y realizaremos una breve descripción de su uso para cifrado y descifrado de documentos.

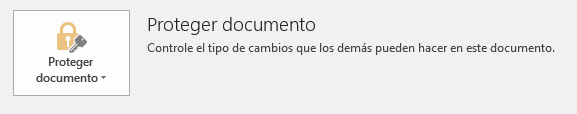
Las aplicaciones y utilidades de las que realizaremos una breve descripción son:

* Aplicaciones de escritorio con protección por contraseña:
  + Microsoft (Word, Excel, PowerPoint, etc.)
  + OpenOffice y StarOficce (Writer, Calc, Impres, etc..)
  + LibreOffice (Writer, Clac, Impress, etc..)
  + Adobe Acrobat
  + 7-zip
* Aplicaciones de escritorio para Encriptado y Desencriptado.
  + dipalCryp (aplicación de desarrollo propio)
* Aplicaciones en la Nube de la RPC.
  + dipalBOX
  + proDatos-Valija (aplicación de desarrollo propio)

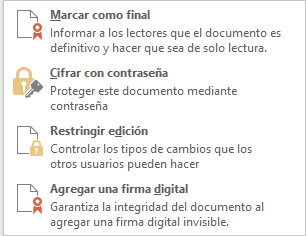
El uso de las aplicaciones de escritorio con protección por contraseña, son herramientas con una baja seguridad ya que existen múltiples herramientas para poder averiguar las contraseñas de protección de los documentos, pero se aprueba su utilización para la protección de documentos de nivel de seguridad bajo. Para documentos de seguridad Media o Alta se deben utilizar los otros sistemas enumerados, u otros que se aprueben.

# 6.- Protección de documentos con la suite de Microsoft:

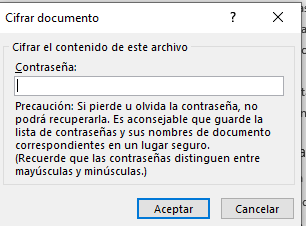
Para codificar cualquier documento en la Suite de Microsoft, en las últimas versiones, ir a la opción de Información del documento y seleccionar el apartado <Proteger documento>



Y aparecerá las siguientes opciones:



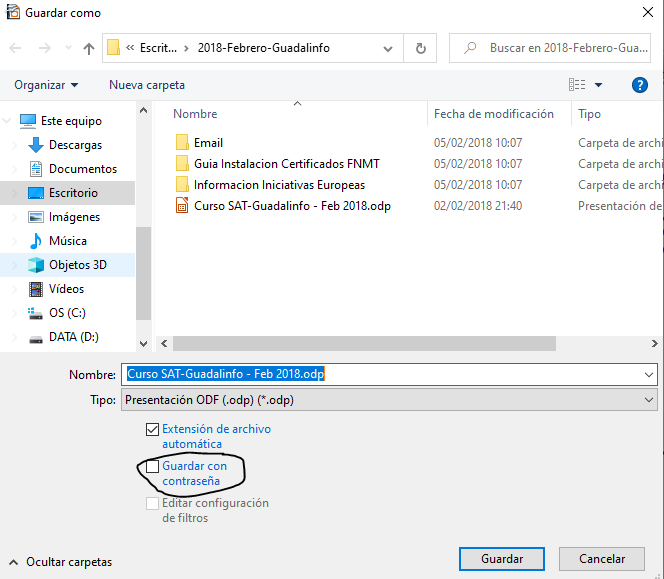
Seleccionar la opción <Cifrar con contraseña> y aparecerá una ventana para introducir la contraseña.



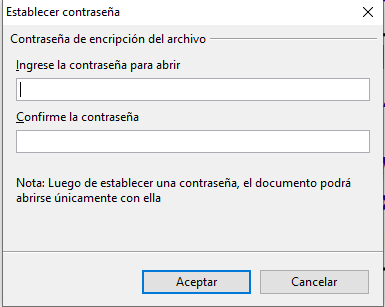
Si desea compartir el documento con otro usuario, o enviarlo por email a otro usuario, deberá proporcionarle la contraseña con la que poder abrir el documento.

# 7.- Protección de documentos con la suite OpenOffice o LibreOffice:

Para proteger documentos de las suites de distribución libre, OpenOffice o LibreOffice, se seleccionara la opción de <Guardar con Contraseña> cuando se vaya a guardar el documento, tal y como se muestra en la siguiente imagen:



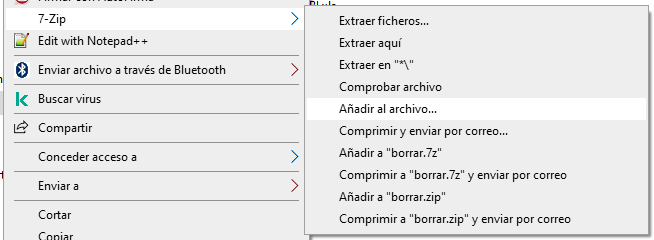
Y aparece una ventana para introducir la contraseña:



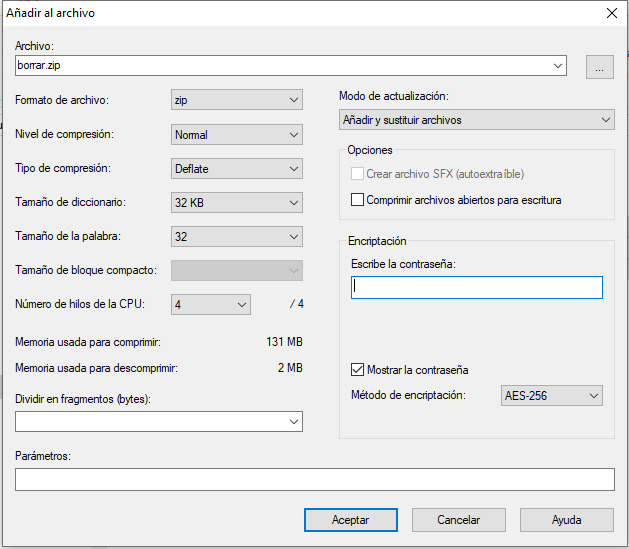
Si desea compartir el documento con otro usuario, o enviarlo por email a otro usuario, deberá proporcionarle la contraseña con la que poder abrir el documento.

# 8.- Protección de documentos con la aplicación de compresión 7-zip.

Para almacenar uno o varios documentos en un zip, con 7-zip y codificar con contraseña, se seleccionará los documentos que se desean guardar en el zip, y se pulas con el botón derecho del ratón y se selecciona, 7-zip y la opción de <Añadir al archivo>



Y aparecerá una ventana donde introducir la contraseña con la que se desea se codifique el archivo que se genere.

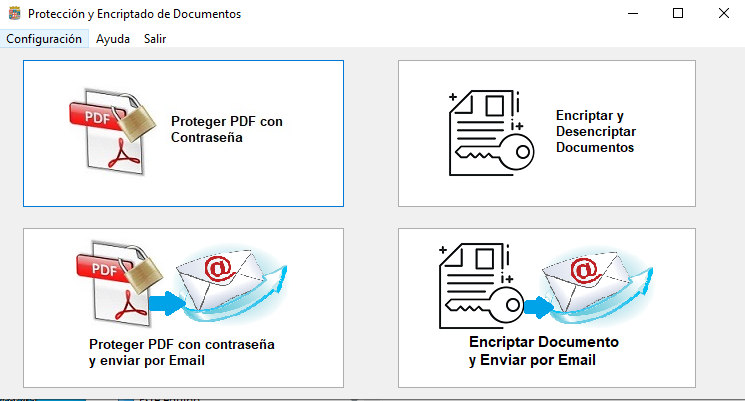


Si desea compartir el documento con otro usuario, o enviarlo por email a otro usuario, deberá proporcionarle la contraseña con la que poder abrir el documento.

# 9.- Protección de documentos PDF con contraseña.

Para proteger un documento PDF con contraseña, se puede utilizar la aplicación Adobe Acrobat, pero que tenga habilitada la opción para proteger que es una opción de pago, por lo que en Acrobar Reader no está activa esta opción, también se pueden utilizar otros programas alternativos para la gestión de documentos PDF.

La aplicación recomendada para poner contraseña a PDF es dipalCryp aplicación desarrollada por Diputación en java y que se ejecuta como herramienta de escritorio de Windows, y que previamente se debe de instalar (ver anexo de instalación de dipalCryp), al ejecutar la aplicación dipalCryp, aparece:

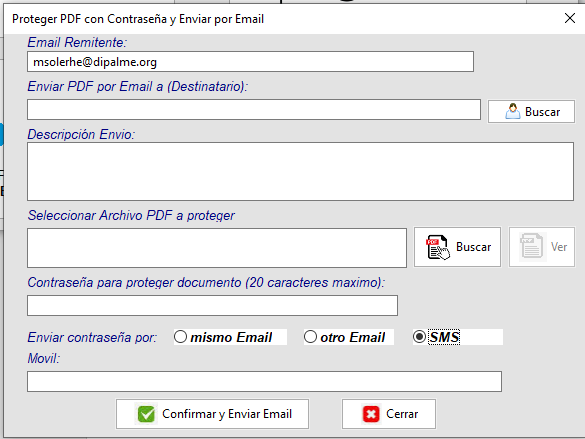


Para la protección de ficheros PDF con contraseña puede utilizar las siguientes opciones:

* **Proteger PDF con contraseña**: por esta opción se seleccionará el documento PDF a proteger y se guardará una copia protegida del PDF en la ubicación que desee. Y si se desea compartir o enviar por email el documento PDF protegido, es necesario proporcionar la contraseña al usuario con el que se desee compartir.



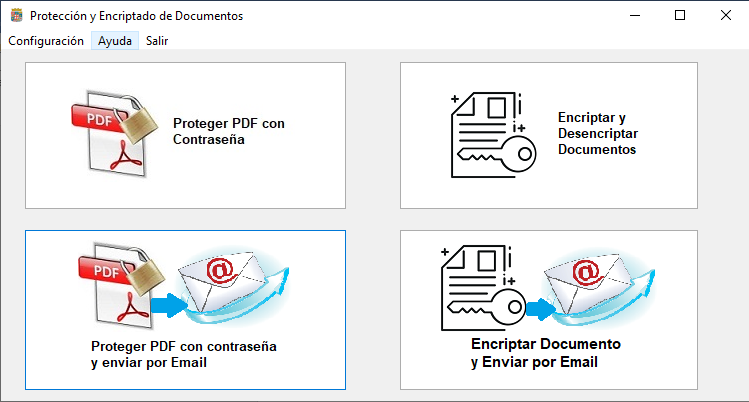
* **Proteger PDF con contraseña y enviar por Email**: por esta opción se seleccionará el documento PDF a proteger y una vez protegido con la contraseña se enviará por Email al usuario que se seleccione, y se enviara la contraseña con la que se ha protegido el documento con otro Email o con un SMS.



Para poder acceder al contenido del PDF solo es necesario abrir el documento con Acrobat Reader y se solicitara la contraseña que protege el documento para poder abrir el documento.

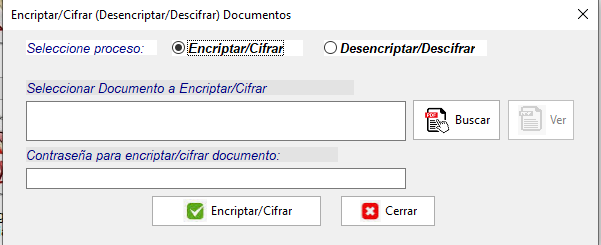
# 10.- Protección de cualquier documento con la aplicación dipalCryp.

Para proteger cualquier documento encriptándolo con dipalCryp, se ejecuta la aplicación y de las opciones que aparecen:

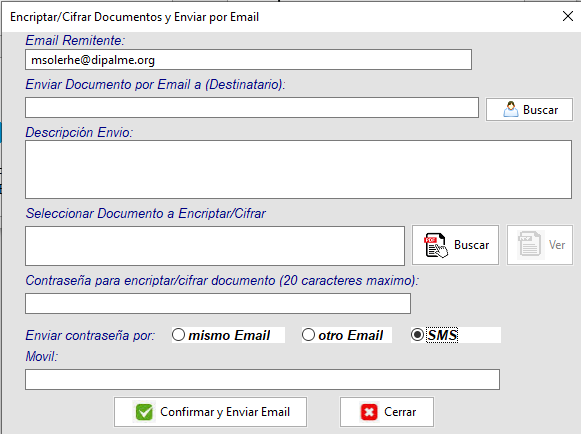


Se pueden utilizar las siguientes opciones:

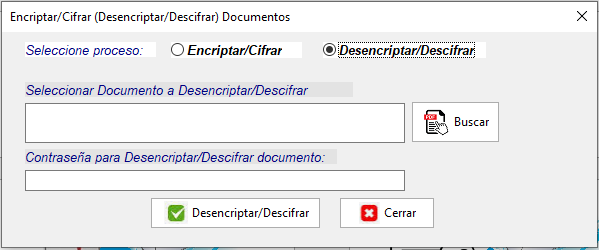
* Encriptar y Desencriptar Documentos: Por esta opción se puede realizar la Encriptacion del documento generando una copia del documento encriptado y guardándolo en la ubicación que se seleccione:



* Encriptar Documento y Enviar por email: Por esta opción además de Encriptar el documento se enviara por Email el Documento Encriptado, y la Contraseña se enviara también por Email o por SMS.



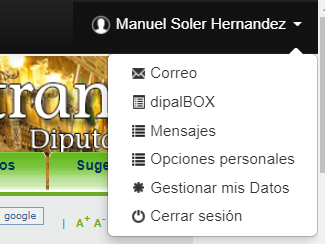
Para desencriptar los documentos encriptados con esta aplicación se seleccionará la opción de < Encriptar y Desencriptar Documentos> y una vez seleccionada se debe elegir la opción de Desencriptar, donde se seleccionar el documento a Desencriptar y se introducirá la Clave para Desencriptar y se guardará el documento desencriptado en la ubicación del disco que se seleccione:



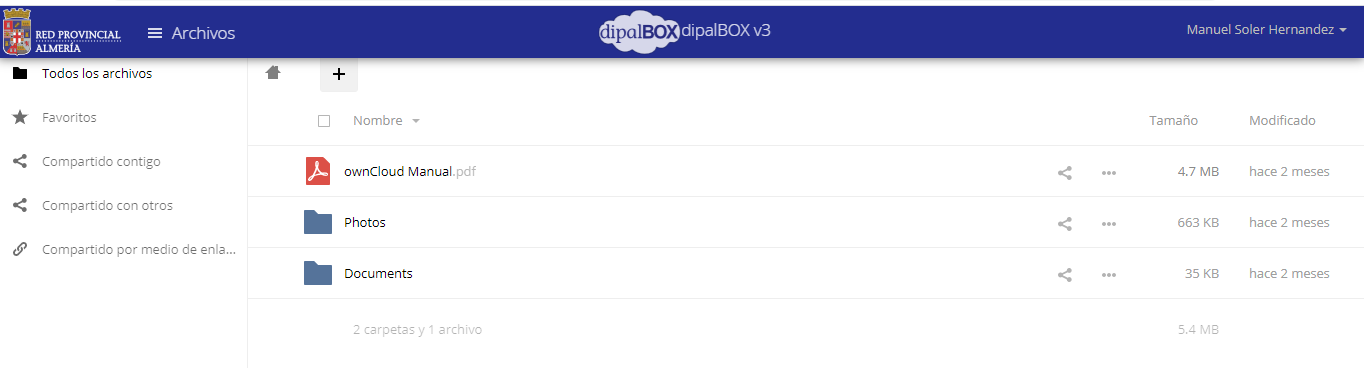
# 11.- Protección de cualquier documento con la aplicación en la nube de la RPC dipalBOX.

La aplicación de DipalBOX no es una aplicación para Encriptar o codificar documentos es una herramienta para gestión de documentos en la nube y se pueden compartir con una buena seguridad.

El acceso a la aplicación dipalBox se puede realizar a través de la Intranet, para ello una vez en la Intranet, se seleccionará en la parte superior derecha dela Intranet donde aparece el nombre del usuario, se selecciona la opción de dipalBOX:



Y se abre dipalBOX solicitando usuario y contraseña, una vez autenticado aparecerá el entorno web de la aplicación:



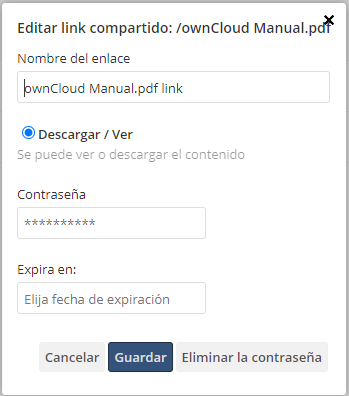
Si se desea compartir un documento en la aplicación, se puede realizar de las 2 siguientes formas:

* **Compartir con otros**: por esta opción se puede seleccionar el documento a compartir, así como los usuarios con los que compartir el documento:



Una vez seleccionado los usuarios y los permisos con los que se comparte, se puede enviar por Email una notificación la invitación a compartir el documento, los usuarios invitados deben autenticarse en la plataforma para poder acceder al documento.

* **Compartir con enlace publico**: por esta opción se puede seleccionar el documento a compartir, y generar una url que se podrá compartir por Email:



Una vez generada la url se puede enviar pinchado en compartir por Email, y se abrirá el cliente de Email para enviar los datos de la URL a compartir.

Existen aplicaciones clientes de dipalBOX para Windows, [Android App](https://doc.owncloud.org/android/) y IOS App, desde las que se puede realizar la gestión de los Documentos. Pero para mayor seguridad utilizar solo lo aplicación en la Web es mejor ya que no se duplican los documentos en los distintos clientes.

# 12.- Protección de cualquier documento con la aplicación en la nube de la RPC proDatos - Valija.

La aplicación de valija, es parecida a un sistema de correo electrónico, pero para la gestión del envió de documentos, que el sistema encripta de forma automática y desencripta en función de los permisos de los usuarios, y además el sistema gestiona el borrado de los documentos una vez caduquen, en función de los días que el usuario decida que los documentos estén vigentes.

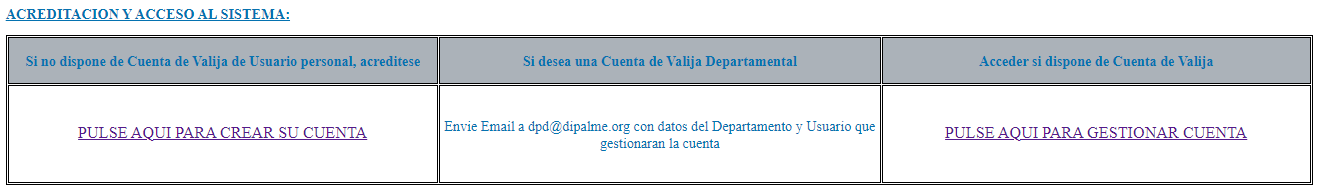
La aplicación para la gestión de Protección de Datos Personales proDatos, se abre a través de la Intranet, por la opción de <Protección de Datos> ,



Y una vez seleccionada aparece la página WEB de proDatos, y entre las opciones aparece la opción de <Valija de Documentos>.

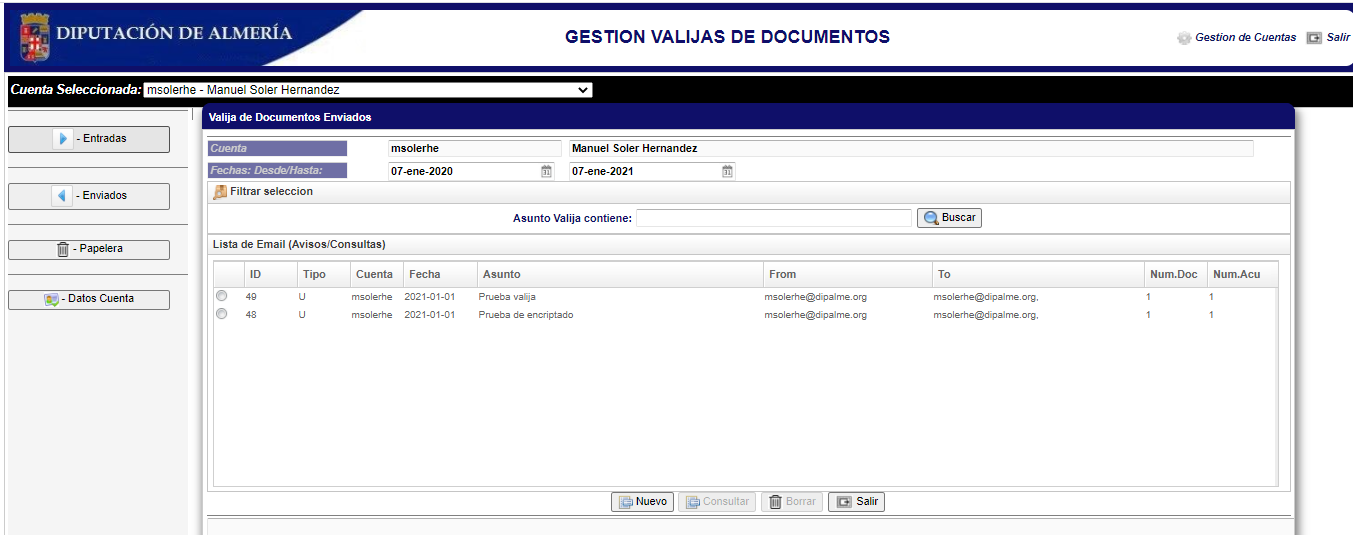


Si se pincha en la opción de Valija aparece una página indicando las opciones que se pueden utilizar:



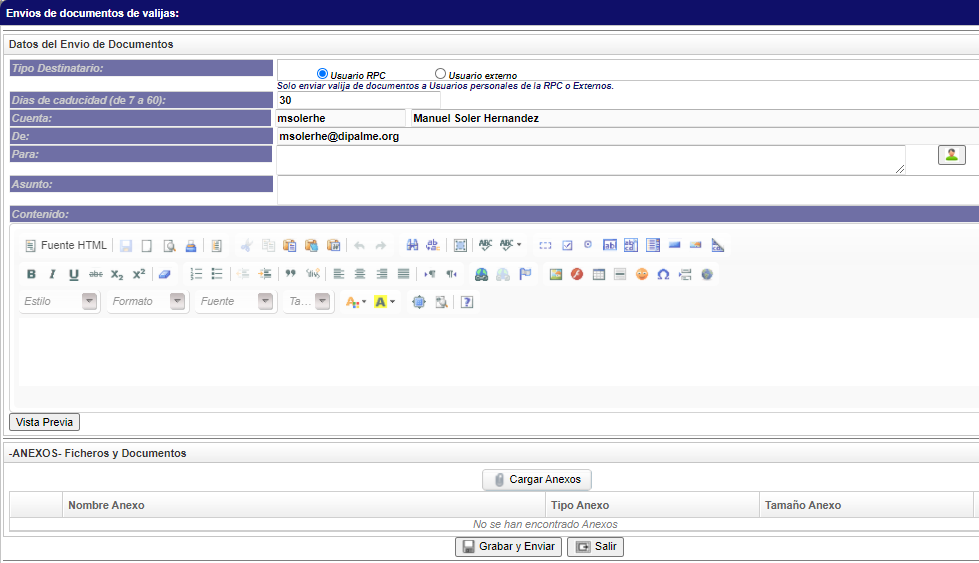
Para utilizar el sistema de valija y enviar documentos codificados hay que estar acreditado en el sistema. Cualquier usuario de la RPC se puede acreditar en el sistema, y además se pueden hacer cuentas departamentales donde se autorizan a varios usuarios para gestionarlas. Para cuentas de usuarios los propios usuarios pueden realizar la acreditación, pero para cuentas Departamentales es necesario solicitar la acreditación vía Email.

Una vez que un usuario ya está acreditado y tiene cuenta, podrá acceder a gestionar envíos de documentos, pinchando <GESTIONAR CUENTA> donde aparecerá una ventana para autenticarse, y tras la autenticación aparece:



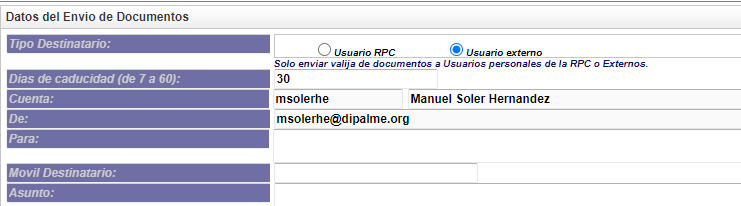
Aparece una vista de la bandeja de salido, con los documentos que se han enviado, y en la parte izquierda se puede navegar a las bandejas de entrada con los documentos que se han enviado al usuario, o a la papelera, así como a los datos de la Cuenta.

Si se desea realizar un envió, se pincha en el botón <NUEVO> y aparece:



Para él envió se rellenarán los datos como si de un Email se tratara y se anexan los documentos que se desean enviar encriptados, el sistema enviara un Email de Notificación y de invitación para acceder a los documentos, para ello el usuario a través del enlace en el email accederá al sistema de valija donde solo con ser usuario de la RPC podrá acceder con su usuario y contraseña de la Intranet, y si es usuario externo con los datos que se le envía en un SMS.

Así para el envió hay dos modalidades o Usuario de la RPC o Usuario Externo:



Para el envió a usuarios externos es necesario conocer un número de móvil del usuario externo donde se enviará un SMS con un código para acceder a los documentos.

# Anexo- Instalación de la aplicación dipalCryp.

Los pasos para instalar la aplicación son:

1.- Descargar la aplicación, desde el siguiente enlace:

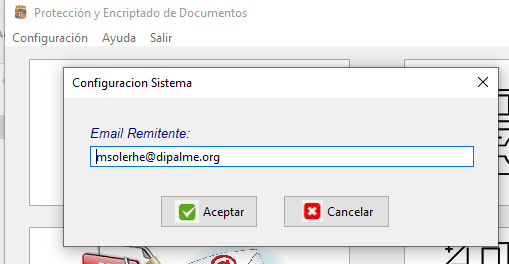
<https://app.dipalme.org/proDatos/paginaWeb.jsp?ppw_id=82&entidad=400000&descargar=S>

una vez acceda a la página descargue el documento de la Aplicación

2.- Crear una carpeta, ejemplo DIPALCRYP y copiar la aplicación dipalCryp.jar en el directorio.

3.- Ejecutar la aplicación para ello, cuando se pincha en dipalCryp.jar se debe selecciona abrir con JAVA(TM) Platform…

4.- Una vez se ejecute la aplicación, lo primero a cumplimentar es en la opción del menú Configuración, rellenar el Email para poner como remitente de los Documentos que se envíen.



5.- La aplicación ya está preparada para su utilización.