Guía de ciberseguridad para el trabajo en remoto

SEGURIDAD DE LA INFORMACIÓN

División de Transformación Digital

Marzo 2020

Uso Público

1 Introducción

La **crisis sanitaria del Covid-19** (Coronavirus) ha modificado nuestra sociedad en un cortísimo espacio de tiempo. Si bien estos cambios han afectado en muchos ámbitos, **el panorama laboral ha sido objeto de una drástica transformación** caracterizada en gran medida por el desplazamiento de la actividad presencial en las compañías, hacia los domicilios particulares del personal trabajador, **mediante la modalidad de trabajo a distancia** (acceso remoto o teletrabajo).

Esta nueva forma de trabajar y relacionarnos depende por completo del buen funcionamiento de las redes y sistemas de información de las organizaciones. Sin embargo, en este contexto un sinfín de **actores malintencionados del ciberespacio** (grupos de APT, grupos cibercriminales, ciberdelincuentes, grupos gubernamentales o paragubernamentales, ciberhacktivistas…) **tratan de sacar provecho de la situación** de muy diversas maneras.

Por ello, es fundamental que toda la sociedad en general y el personal de EMASESA en particular, conozca los **riesgos de ciberseguridad** que conlleva este nuevo escenario, así como las **pautas de seguridad** para enfrentarse a ellos con garantías.

EMASESA está firmemente comprometida con la creación de una sociedad digital más segura. Con esta finalidad, el presente documento se ha adaptado a partir de la correspondiente guía interna con objeto de que pueda ser utilizado pública y libremente por cualquier persona u organización interesada.

2 Top 10 fraudes en línea (Fuente: Instituto Nacional de Ciberseguridad)

1) Mil y un consejos para "frenar" el Coronavirus (WhatsApp): circulan cientos de mensajes con enlace a una gran variedad de páginas web, donde supuestos "expertos" ofrecen sus recomendaciones y soluciones ante el virus. Mucha atención pues una gran parte de estos mensajes contienen enlaces maliciosos o buscan desinformar. Incluso hay algunos que buscarán una compensación económica o nuestros datos a cambio de ofrecernos su supuesta ayuda.

2) Manda "Ayuda" al teléfono/email XXXX (redes sociales): otro tipo de estafa muy común es aprovecharse de la labor de los profesionales sanitarios, pidiendo que colaboremos para agradecer todo su trabajo y esfuerzo.

En muchos de estos casos nos pedirán que ingresemos algunos datos personales o incluso que realicemos alguna donación económica. Es una forma de recabar información personal de un gran número de usuarios de golpe. No significa que todas las iniciativas solidarias que circulan por Internet sean un fraude, pero sí habrá que ser cautos y contrastar la información para evitar problemas.

3) Corona-phishing (correo electrónico): en este fraude el ciberdelincuente suplanta la identidad de una institución de renombre, como puede ser la OMS o cualquier otra, que, aprovechándose de la preocupación global sobre el COVID-19, trata de ganarse nuestra confianza para hacerse con el control de determinados datos personales, como los datos bancarios o incluso infectarnos con un malware.

Por ejemplo, podríamos recibir un correo procedente de un supuesto hospital que nos informa de que podemos ser de los primeros en hacernos el test de diagnóstico pero que para ello debemos hacer clic en un enlace muy sospechoso.

4) Corona-smishing (SMS): un fraude muy popular es el envío a través de SMS haciéndose pasar, por ejemplo, por el Ministerio de Trabajo o la institución correspondiente de nuestra Comunidad, compartiendo un enlace donde se nos solicitarán una serie de datos personales. Aparentemente serán necesarios para tramitar una "solicitud de baja temporal en relación con el coronavirus". Se debe prestar mucha atención, ya que su carácter urgente puede confundirnos y hacernos caer en una trampa.

5)Estafas en la venta de material sanitario (compras online): una vez más los estafadores tratan de beneficiarse con los productos "estrella" relacionados con el coronavirus. Se han identificado varias estafas principalmente relacionadas con la venta online de mascarillas.

Por ejemplo, el vendedor asegura disponer de mascarillas especialmente preparadas para protegernos del virus, pero las víctimas, tras realizar la compra, no llegan a recibir lo que han comprado o, en su defecto, solo una parte o en unas condiciones muy distintas de las anunciadas.

6) Coronaware (ransomware): otro fraude muy extendido es el basado en un malware llamado "Coronavirus". ¿Quién no abriría un archivo de vídeo o un documento donde se incluyen instrucciones y alertas sobre cómo protegernos contra el COVID-19? Pues aquí está la trampa, pues no debemos confiarnos de todo lo que recibimos, ya que los archivos adjuntos pueden contener malware que termine por infectarnos y tomar control de nuestros equipos.

Esto es muy común a través del correo electrónico, aunque podría llegarnos también por aplicaciones de mensajería instantánea o incluso redes sociales.

7) El Gobierno reparte "corona-cheques": muchos usuarios están recibiendo a través de sus aplicaciones de mensajería instantánea un mensaje supuestamente de un Ministerio, en el que se les indica que el Gobierno regala una cantidad ¨X¨ de euros para sobrellevar mejor las consecuencias de la actual crisis sanitaria por el COVID-19. Para recibirlos, deberemos hacer clic en el enlace que viene adjunto. Mucho cuidado pues a día de hoy esta información es falsa.

Antes de hacer clic sobre cualquier enlace, una buena recomendación es confirmar si la fuente es fiable, podemos comprobarlo mediante sus canales de comunicación oficiales, en las redes sociales o en las webs oficiales de los distintos Ministerios.

8) Ofertas de trabajo fraudulentas: circulan falsas ofertas de empleo para elaborar material sanitario. Aprovechándose de esta difícil situación, los ciberdelincuentes tratarán de hacernos creer que nos encontramos ante una oferta de trabajo real para que compartamos con ellos nuestros datos personales e incluso que realicemos algún pago por adelantado en concepto de envío del material.

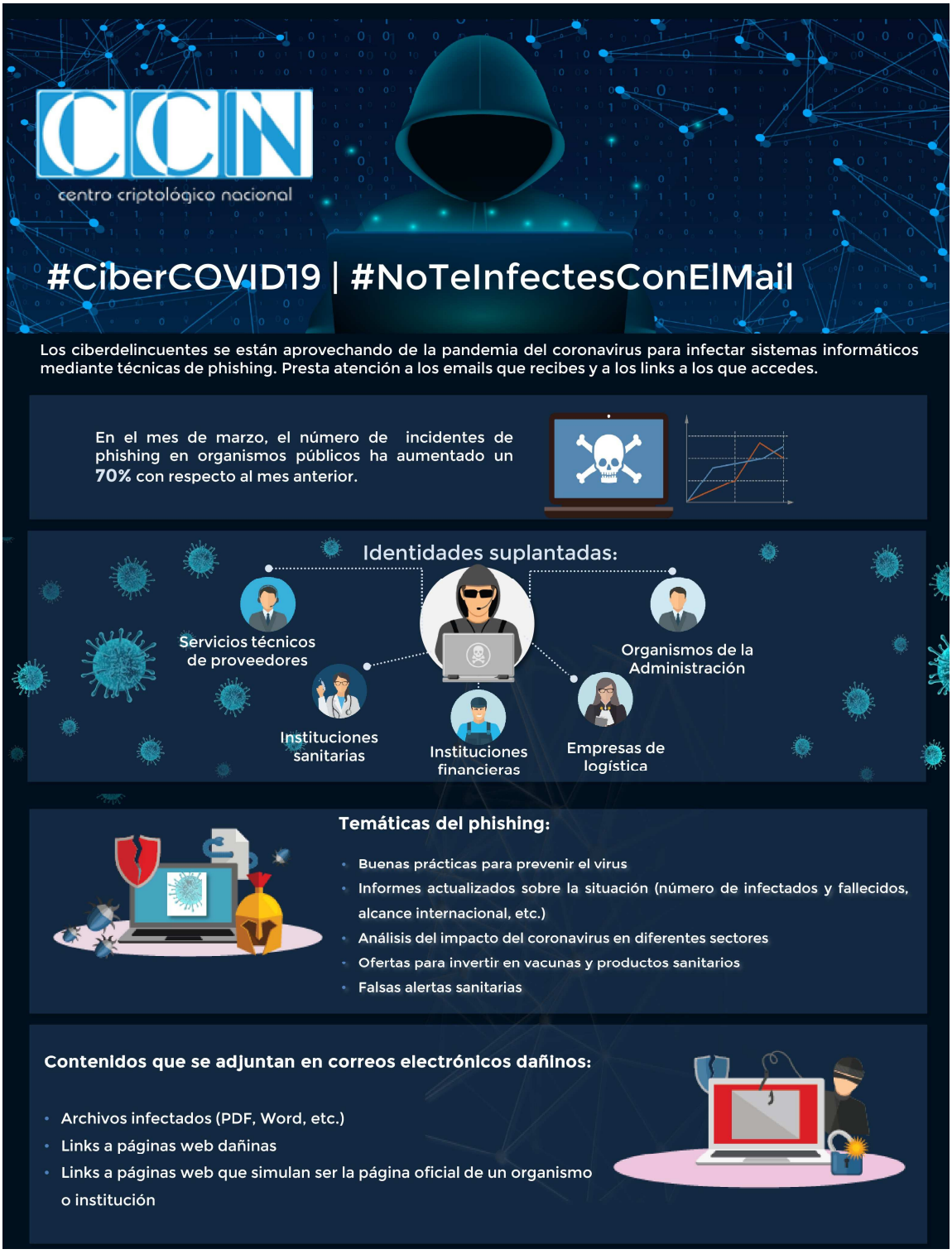
Ante una oferta de estas características, lo mejor es revisar todos los detalles del anuncio, contrastar la información y si algún detalle nos llama la atención o nos resulta raro, descartar la oferta, especialmente si proviene de un usuario desconocido o sin haberlo solicitado a ningún portal web de ofertas de trabajo.

9) Soporte técnico fraudulento (teléfono): los ciberdelincuentes, aprovechando la situación de cuarentena y teletrabajo, están poniendo en práctica algunas de sus engaños más clásicos. Recientemente se han notificado **denuncias de usuarios que afirmaban haber recibido llamadas de un supuesto "soporte técnico"** para colaborar mientras duren estas semanas de teletrabajo. Lamentablemente, tras seguir sus indicaciones, el ciberdelincuente acaba por **conseguir nuestras credenciales o que nos instalemos algún software malicioso** sin que nos demos cuenta.

10) Lleva mejor la cuarentena con estos "servicios gratuitos" (falsos cupones): en este momento, donde la mejor solución para vencer al virus es quedarnos en casa, es cuando aparecen los fraudes sobre supuestas promociones y suscripciones gratuitas o con descuentos.

Un ejemplo de mensaje que podemos recibir es el siguiente: "Disfruta de todos nuestros servicios de *streaming* de películas y series de forma totalmente gratuita". Los ciberdelincuentes buscarán que rellenemos algunos formularios con nuestros datos personales o que paguemos una pequeña cantidad bajo cualquier excusa. Lo primero que debemos hacer es revisar la URL, y si no estamos seguros, ir a la fuente oficial para confirmar o desmentir que estén ofreciendo este tipo de promociones.

3 Campañas de Phishing y desinformación: consejos del Centro Criptológico Nacional



CCN
centro criptológico nacional

#CiberCOVID19

Ante las campañas de malware y de desinformación que se están generando a raíz de la pandemia del coronavirus, te aconsejamos seguir las siguientes recomendaciones.

Phishing

- Presta especial atención a los emails que recibes. La cura del coronavirus no la recibirás por correo electrónico.
- Evita abrir documentos y archivos adjuntos sobre el COVID-19 en los correos electrónicos que recibas.
- No descargues aplicaciones no oficiales para conocer el alcance internacional del COVID-19.

Desinformación

- No difundas información que no provenga de medios y fuentes oficiales.
- No contribuyas a la difusión de contenido no contrastado.
- No compartas mensajes que puedan generar alarma en la población.

4 Servicios gratuitos en nube; riesgos para la seguridad de la información.

El uso de información corporativa en **servicios públicos para el intercambio, almacenamiento o tratamiento de archivos** (como Dropbox, WeTransfer, Google Drive, I Love pdf, etc.), también conocido como "el problema Dropbox", **implica importantes riesgos** para una organización. A continuación, describimos algunos de los más destacados.

- Las **condiciones de uso de estos servicios, suelen ser bastante confusas** e incluso, en ocasiones, se **atribuyen privilegios excesivos** a favor del propio prestador del servicio.

  Como ejemplo, en la siguiente captura se recoge parte de las condiciones de uso de Google Drive, por la que el usuario otorga al propio Google permisos prácticamente "ilimitados" sobre la información.


Google Drive

Al subir, almacenar, recibir o enviar contenido a Google Drive o a través del servicio, concedes a Google una licencia mundial para usar, alojar, almacenar, reproducir, modificar, crear obras derivadas (por ejemplo, las que resulten de la traducción, adaptación u otros cambios que realicemos para que tu contenido se adapte mejor a nuestros servicios), comunicar, publicar, ejecutar o mostrar públicamente y distribuir dicho contenido. Google usará los derechos que le confiere esta licencia únicamente con el fin de suministrar, promocionar y mejorar los servicios y de desarrollar servicios nuevos. Esta licencia seguirá vigente incluso cuando dejes de usar nuestros servicios, a menos que elimines tu contenido. Asegúrate de tener los derechos necesarios para concedernos esta licencia de cualquier contenido que envíes a Google Drive.

- Las **políticas de privacidad** de la mayoría de estos servicios de almacenamiento on-line incluyen por regla general cláusulas por las que **se reservan el derecho a acceder a determinados contenidos y compartir tus datos personales** con "terceros de confianza".


ECONOMÍA

Dropbox comparte datos de sus usuarios con Amazon y Google

La compañía actualiza su Política de Privacidad y se blinda ante el Brexit

- Por otra parte, y en cuanto a su seguridad, **si bien estos servicios deberían estar muy bien protegidos, no es menos cierto que también son muy atacados** (el "premio" en caso de sufrir una brecha de seguridad es "muy gordo"). Además, también **pueden tener fallos en su funcionamiento**. Aunque no ocurre de forma habitual, pueden producirse brechas de seguridad que dejan información de los usuarios expuesta.


TECNOLOGÍA

Google presenta un error que envió videos de usuarios a otros aleatoriamente

Algunos videos almacenados en cuentas de Google se enviaron a otros usuarios a causa de un error en Takeout de la app Fotos

por *LaVerdad*
09 de Febrero 2020 · 10:32 hs


24 JUN 2019 / TECNOLOGÍA

WeTransfer sufrió un error y envió archivos a las personas equivocadas

El incidente ocurrió la semana pasada y la compañía todavía no tiene certeza de qué lo provocó.

POR FERNANDA ARROS Comparte:

- En muchas ocasiones el usuario desconoce el uso correcto de las opciones de **sincronización y/o compartición**, lo que **puede llevar a exponer información sensible sin conocimiento del usuario**. Sirva de ejemplo el caso conocido como

"celebgate", que tuvo mucho impacto mediático a nivel mundial; en 2014 unos cibercriminales robaron y publicaron fotos íntimas de un elevado número de famosas (actrices, cantantes, etc.). Las víctimas no eran conscientes de que sus teléfonos móviles (de la marca Apple) realizaban copias de seguridad de las imágenes tomadas con su móvil en la nube del fabricante. Mediante ingeniería social los cibercriminales robaron las contraseñas con lo que pudieron acceder a esta nube y descargar todo el material, que luego publicaron. Este

'Celebgate': esta es la lista de las 100 famosas afectadas

EUROPA PRESS 02.09.2014 - 08:55H

- Debido a la repercusión del asunto, Twitter suspenderá las cuentas que compartan las imágenes.
- El hacker accedió al material gracias a un fallo de seguridad de iCloud.
- Las primeras imágenes ya han visto la luz, pero hay fotografías y vídeos de alrededor un centenar de famosas.
- Así hackearon y robaron las fotos de las famosas desnudas

Además, si se utilizan estos servicios desde un terminal móvil (Smartphone o Tablet) y este dispositivo cae en manos inadecuadas sin haber tomado las oportunas medidas de seguridad como el bloqueo de pantalla, podrán ver, compartir o borrar toda nuestra información.

- Es habitual que **los usuarios utilicen las mismas credenciales en diferentes servicios de internet**, **práctica totalmente desaconsejable**; de esta forma, cuando los ciberdelincuentes obtienen las credenciales por una brecha de seguridad en un servicio (habitualmente, el más "débil"), se hacen con las credenciales que utilizarán (las mismas credenciales o variaciones sobre estas) para acceder al resto de servicios (los más "fuertes"), quedando de nuevo expuesta la información.

- Desde el **punto de vista legal**, el **Reglamento General de Protección de Datos** de carácter personal **obliga al responsable** del tratamiento de los datos, **a cumplir determinados requisitos de seguridad** que a veces no quedan garantizados con este tipo de servicios de internet y que, en todo caso, tienen que quedar recogidos en un acuerdo legal. De subir datos de carácter personal a estos servicios sin garantizar estos requerimientos legales, se está expuesto a fuertes sanciones por parte de la autoridad.

También en el ámbito legal, los prestadores de estos servicios incluyen habitualmente en sus condiciones de uso **cláusulas por las que quedan exonerados de responsabilidad** alguna en caso de un incidente de seguridad, **recayendo esta exclusivamente en el usuario del servicio**.

Si utilizas estos servicios, ten siempre presente que:

"Cuando el producto es gratis… es que el producto eres tú"

4.1 Consejos para el uso seguro de estos servicios en el ámbito personal

Si en tu **ámbito personal** utilizas este tipo de servicios, te **recomendamos** las siguientes **pautas de seguridad**:

- Utiliza una **contraseña robusta** para acceder al servicio (mínimo 9 caracteres, combinando mayúsculas, minúsculas y caracteres especiales). Al terminar de usar el servicio, **cierra la sesión**. Si el servicio cuenta con **verificación en dos pasos** es recomendable **activarla** para dotar de mayor seguridad a la cuenta.

- **Utiliza siempre contraseñas diferentes para servicios diferentes**; un gestor de contraseñas (por ejemplo, Keepass) te puede resultar muy útil para esta tarea.

- **Ten siempre copia de seguridad de tus archivos**; de esta forma si el servicio de alojamiento en la nube deja de funcionar, no perderás tu información.

- **Presta atención a la sincronización**; si accidentalmente borras archivos en la carpeta de un equipo que tienes sincronizado, desaparecerá también la información de la nube.

- **Infórmate sobre el correcto funcionamiento de las opciones de compartición de archivos y carpetas** que nos ofrecen estos servicios para no mostrar información accidentalmente a quien no deberíamos

- En caso de que la **información** sea sensible, **almacénala en estos servicios siempre cifrada**; de esta forma estará protegida frente a ciberataques o fallos de funcionamiento que dejen tu información expuesta ya que esta no será legible

por terceros. **En el siguiente apartado te proponemos una forma sencilla para cifrar y proteger tus archivos**.

- **Lee las condiciones de uso y privacidad** atentamente, y utiliza exclusivamente aquellos servicios que te ofrezcan más seguridad y confianza.

4.2 Protección de un archivo mediante contraseña

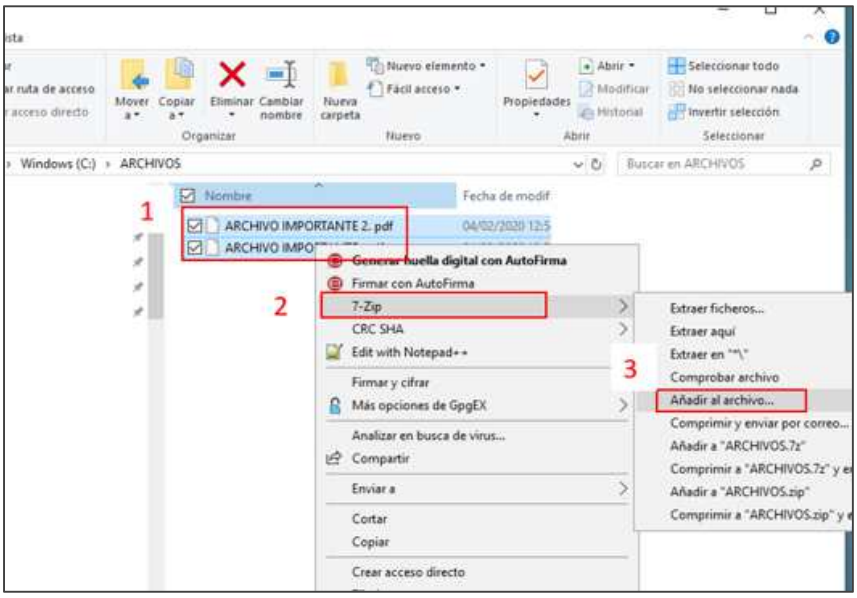
Los programas gratuitos para compresión de archivos (como 7zip), permiten habitualmente proteger el archivo de forma cifrada mediante una contraseña.

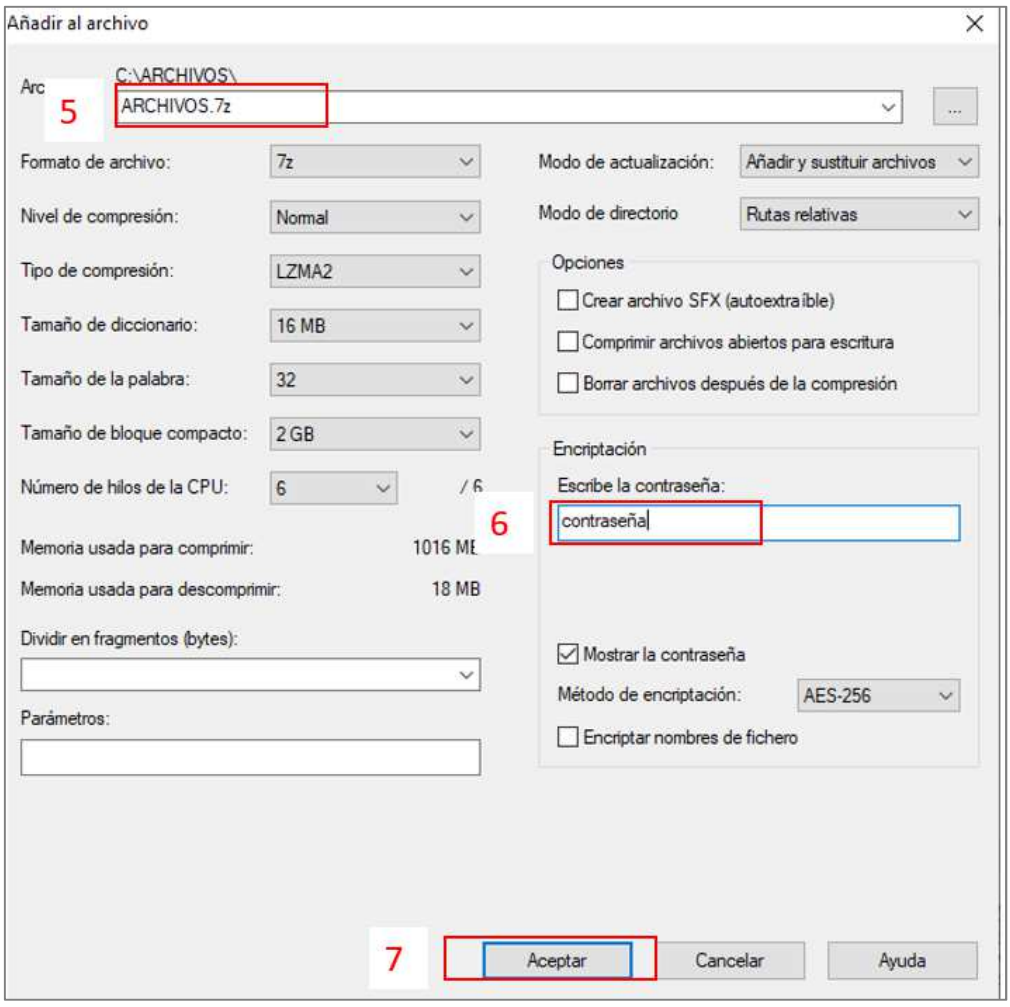
El proceso es muy sencillo. A continuación, te mostramos los pasos necesarios utilizando el programa 7zip.

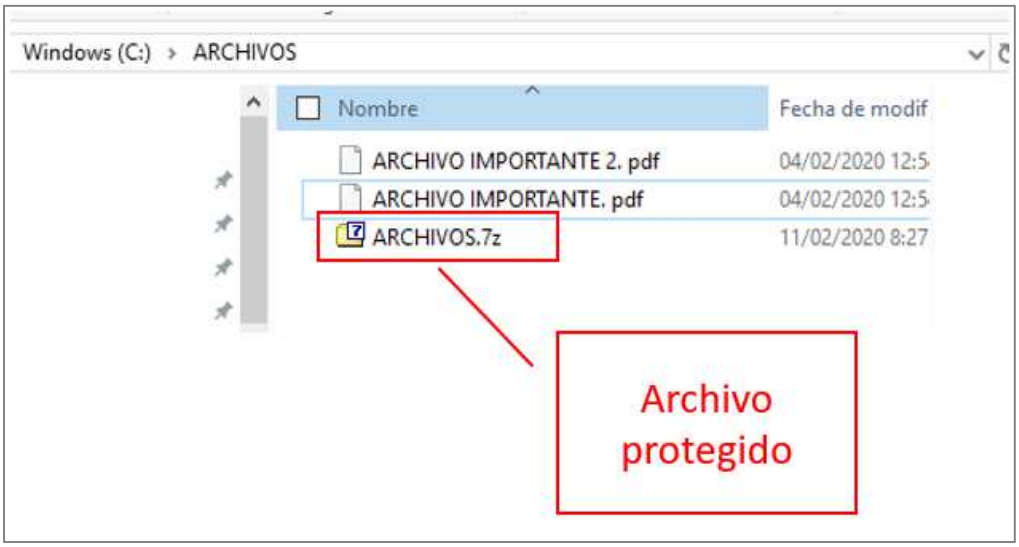
1. Selecciona el archivo o archivos que quieras proteger
2. Con el botón derecho del ratón, selecciona "7-zip"
3. En las opciones, selecciona "Añadir al archivo…"
4. Escribe el nombre con el que quieras que se cree
5. Escribe la contraseña y dale a Aceptar

En el explorador de Windows verás que se ha creado un nuevo archivo, de extensión ".7z", que contiene los archivos originales. Este archivo está cifrado y protegido mediante la contraseña que escribiste.

A continuación, se muestran los pasos indicados, mediante imágenes.




Añadir al archivo
Arc
C:\ARCHIVOS\
5
ARCHIVOS.7z
Formato de archivo:
7z
Nivel de compresión:
Normal
Tipo de compresión:
LZMA2
Tamaño de diccionario:
16 MB
Tamaño de la palabra:
32
Tamaño de bloque compacto:
2 GB
Número de hilos de la CPU:
6
/ 6
Memoria usada para comprimir:
1016 MB
Memoria usada para descomprimir:
18 MB
Dividir en fragmentos (bytes):
Parámetros:
Modo de actualización:
Añadir y sustituir archivos
Modo de directorio
Rutas relativas
Opciones
Crear archivo SFX (autoextraible)
Comprimir archivos abiertos para escritura
Borrar archivos después de la compresión
Encriptación
Escribe la contraseña:
6
contraseña
Mostrar la contraseña
Método de encriptación:
AES-256
Encriptar nombres de fichero
7
Aceptar
Cancelar
Ayuda


Windows (C:) › ARCHIVOS
Nombre
Fecha de modif
ARCHIVO IMPORTANTE 2. pdf
04/02/2020 12:5
ARCHIVO IMPORTANTE. pdf
04/02/2020 12:5
ARCHIVOS.7z
11/02/2020 8:27
Archivo protegido

5 Riesgos asociados al trabajo en remoto en una organización.

Las organizaciones proporcionan a sus empleados mecanismos de acceso remoto para realizar tareas relacionadas con el puesto de trabajo desde una ubicación externa. Sin embargo, la utilización del acceso remoto no está exenta de riesgos potenciales que deben ser conocidos y tenidos presente, siendo los principales:

- **Acceso no autorizado al equipo** y por medio de este, posibilidad de acceso también a los sistemas corporativos de la organización (en particular, mediante un posible robo de credenciales).
- **Ejecución de malware** en el equipo con capacidad para; registrar la actividad, grabar imágenes y sonido, robar información, credenciales, etc.
- La **comunicación** entre el equipo remoto y los sistemas de la compañía **podría ser interceptada**, distorsionada o manipulada por un atacante malintencionado.
- **Fugas o pérdidas de información** en caso de extravío o robo del equipo remoto desde el que se accede.
- **Corrupción de información sin salvaguarda** (copia de seguridad), en caso de avería en el equipo.

Para minimizar estos riesgos, es recomendable seguir estas pautas de seguridad.

5.1 Consejos de ciberseguridad para un teletrabajo seguro.

- **Cambia la contraseña** que trae **por defecto** el router Wifi. Además, desactiva la opción de WPS.

- **Utiliza una conexión WiFi robusta**; mínimo cifrado WPA2 con AES.

- **Utiliza contraseñas robustas** para todos tus servicios y equipos; mínimo de 9 caracteres, combinando mayúsculas, minúsculas, números y caracteres especiales.

- **Utiliza contraseñas diferentes** para cada servicio; para ello un gestor de contraseñas como Keepass te puede resultar de mucha utilidad. Ten en cuenta

que, si los ciberdelincuentes se hacen con la contraseña de un servicio, la irán probando en otros muchos.

- Asegúrate de que el equipo desde el cual accedes dispone de antivirus actualizado y activo, no presenta ningún signo de estar potencialmente comprometido, se encuentra debidamente actualizado (sistema operativo y aplicaciones) y cuenta con los parches de seguridad aplicados.

- Si estas teletrabajando, **cuando te ausentes activa el bloqueo de la sesión**. Activa también el bloqueo automático de sesión tras un período de inactividad.

- Si tu ordenador sale de casa, es muy aconsejable **cifrar el equipo**; de esta forma si te lo roban, se pierde o simplemente se te olvida en algún sitio, la información que contiene no podrá ser accedida por terceros. Las versiones modernas de Windows incluyen esta opción de forma nativa (Bitlocker).

- Ten **cuidado con las memorias USB**; estos dispositivos pueden contener o propagar malware muy fácilmente. Utiliza sólo dispositivos de los que estés seguro de su fiabilidad.

- **Realiza periódicamente copia de seguridad de tu información** importante en un **dispositivo aislado** (disco duro externo, memoria USB); te prevendrá de perder toda tu información ante averías o infecciones por ransomware.

Y, sobre todo:

“Aplica siempre el sentido común”