+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

RESGUARDO DE INFORMACIÓN:
¿CÓMO PRESERVAR EVIDENCIA DIGITAL?

+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

EVIDENCIA DIGITAL
¿QUÉ ES?

La evidencia digital es el conjunto de datos o información; como archivos, imágenes, videos, entre otros, cuyo contenido puede ser utilizado en un proceso judicial para esclarecer un hecho o incidente de seguridad informática. **Se trata de todo el material que pueda ser utilizado como prueba válida en un caso.**

HOY TE TRAEMOS RECOMENDACIONES A TENER EN CUENTA:

Realizar copia de resguardo/backup de la información en un dispositivo distinto al de uso habitual (por ejemplo: pendrive, disco externo u otra Pc), dado que contar con una copia exacta de la información permite a los investigadores acceder e inspeccionar los documentos asociados a un usuario, programas instalados y cuentas de usuarios existentes.

UN BUEN TIP PARA UN BACKUP CORRECTO, ES UTILIZAR LA ESTRATEGIA 3-2-1, LA CUAL INDICA:

3 Tener **3 copias de los archivos**: 1 original y 2 secundarias.

2 Contar con **2 tipos de formatos** de almacenamiento.

1 Poseer **1 copia fuera del lugar físico** (por ejemplo, en la Nube).

Existen diversas herramientas para cifrar información sensible y resguardarla en un dispositivo, como, por ejemplo: **Veracrypt (Anexo - Pag 11)** y **Bitlocker (Anexo - Pag 19).**

+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

RECOMENDACIONES GENERALES

Si el hostigamiento digital y/o amenazas se realizan a través de redes sociales, correos electrónicos y/o aplicaciones de mensajería instantánea, en primera instancia, **no es conveniente ni aconsejable bloquear el perfil, ni reportarlo como abusivo**.

EN TAL CASO RECOMENDAMOS:

- **Resguardar correctamente las direcciones URL** de los perfiles/cuentas de redes sociales y/o números telefónicos -exactos- involucrados. -Ver anexo "¿Cómo resguardar URL desde celular?" (pág 21)-.
- **No eliminar nada y preservar, sin modificar**, la evidencia digital disponible (Por ejemplo: realizando capturas de pantalla, grabaciones de voz y/o videos, etc).
- **Realizar copias** de los chats y comunicaciones recibidas.
- **Denunciar** a las entidades correspondientes.
- **Tampoco es aconsejable ceder al chantaje** ni responder los mensajes, sino finalizar la interacción.

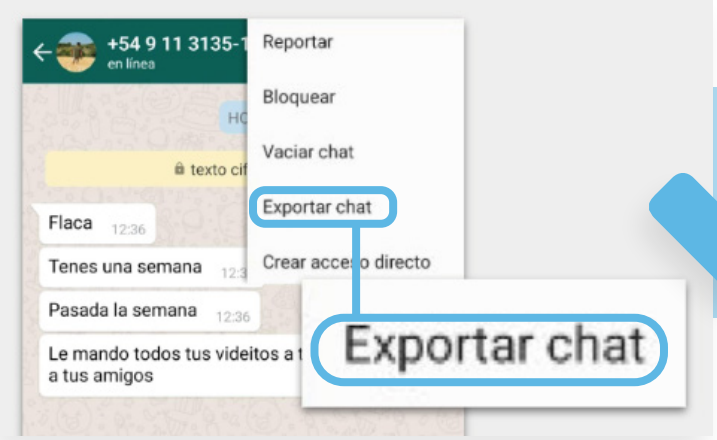
EN CASO DE QUE LA COMUNICACIÓN SEA MEDIANTE WHATSAPP:

- **No eliminar ningún contenido** que se haya intercambiando dentro de las conversaciones.
- En lo posible **que se visualice el número exacto y completo del remitente** de la comunicación, y no el nombre del contacto agendado. sino finalizar la interacción.

+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

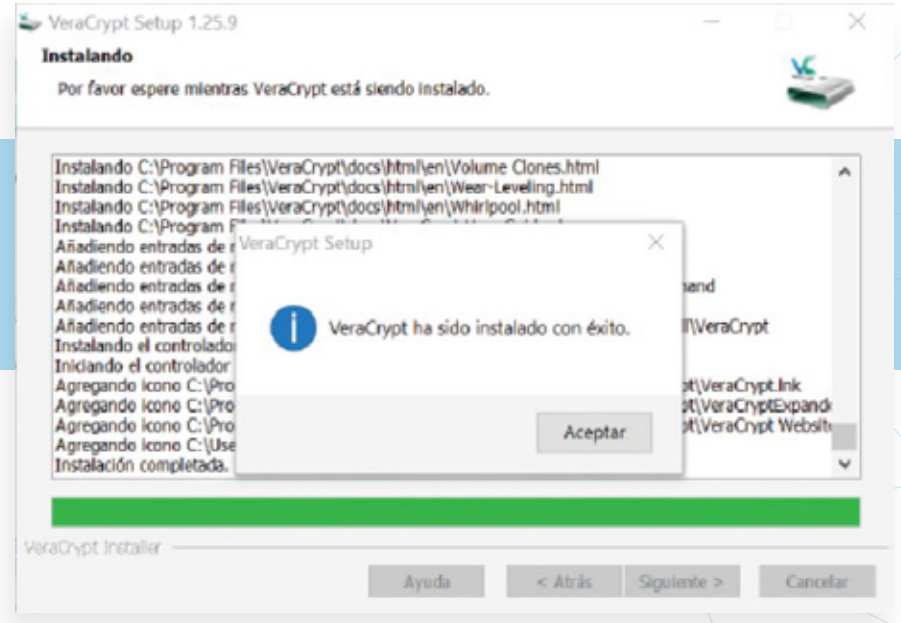
EN CASO DE QUE LA COMUNICACIÓN SEA MEDIANTE WHATSAPP:

- **Hacer copia de seguridad** de WhatsApp del historial completo de las conversaciones.
- **Exportar el chat** de WhatsApp.



EN CASO DE QUE LA COMUNICACIÓN SEA MEDIANTE CORREO ELECTRÓNICO:

- **Descargar** el/los correo/s electrónico/s en cuestión.
- **Extraer las cabeceras/encabezados** de los mismos en un archivo .txt.



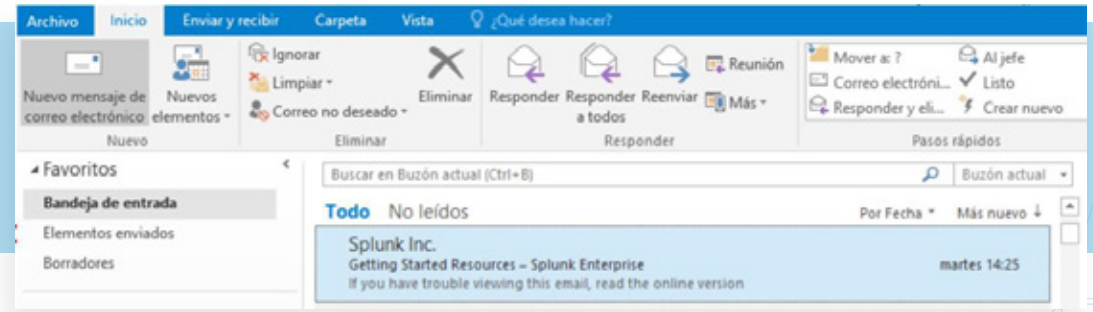
+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

EXTRACCIÓN DE CABECERAS DE CORREOS ELECTRÓNICOS PARA INVESTIGACIÓN

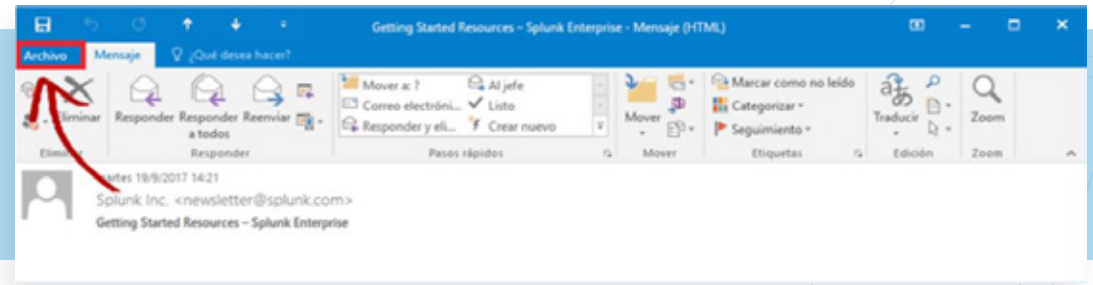
Uno de los principales puntos de entrada de los cibercriminales a los sistemas y equipos de las organizaciones y también de los ciudadanos, es a través del correo electrónico. Es decir, un email que puede llegar desde una dirección que no resulte conocida para así lograr engañar a la persona y/o empresa.
Aquellos casos en los que existe sospecha de haber recibido un correo electrónico falso o de dudosa procedencia, se puede solicitar el análisis del mismo. Para ello, es necesario descargar las cabeceras correspondientes dado que las mismas contienen la información acerca del lugar desde el cual ha sido enviado el correo y el origen del mismo.

1. MICROSOFT OUTLOOK

- Acceda a su cuenta de Outlook e ingrese al correo en cuestión para **abrirlo en una nueva ventana.**

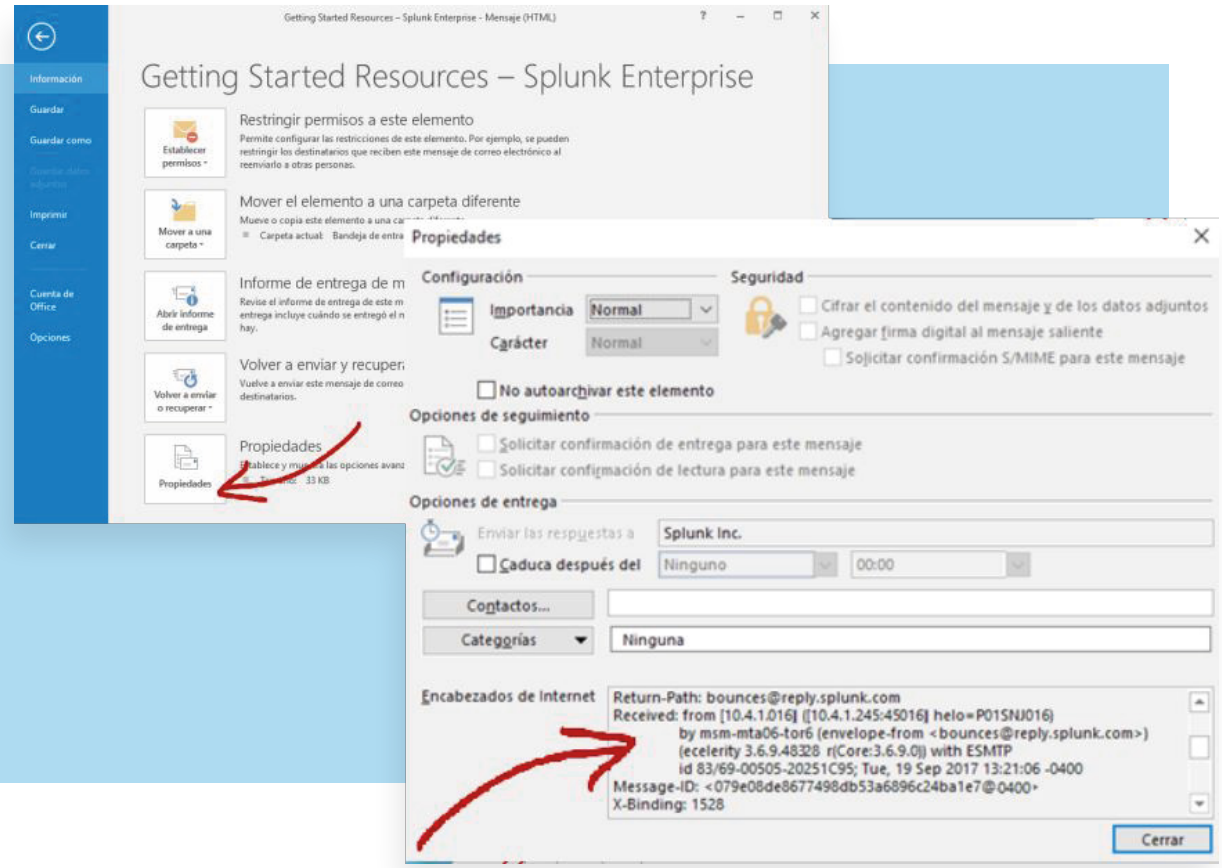


- Dentro del correo que le ha llegado, **debe seleccionar la opción "Archivo"** en la barra superior de la aplicación, tal como muestra la imagen.



Las cabeceras de los correos electrónicos **contienen información acerca del lugar desde el cual se ha enviado** un posible correo falso y engañoso o de dudosa procedencia.

- Por último, **seleccionar la opción "Propiedades"** dentro del menú desplegable.



- Los encabezados del email serán visibles **en el recuadro que se encuentra en la parte inferior de la ventana de "Propiedades"**.

- **Copie TODO el contenido de dicha ventana** arrastrando el cursor del mouse sobre el mismo.

- Abra un **nuevo correo.**

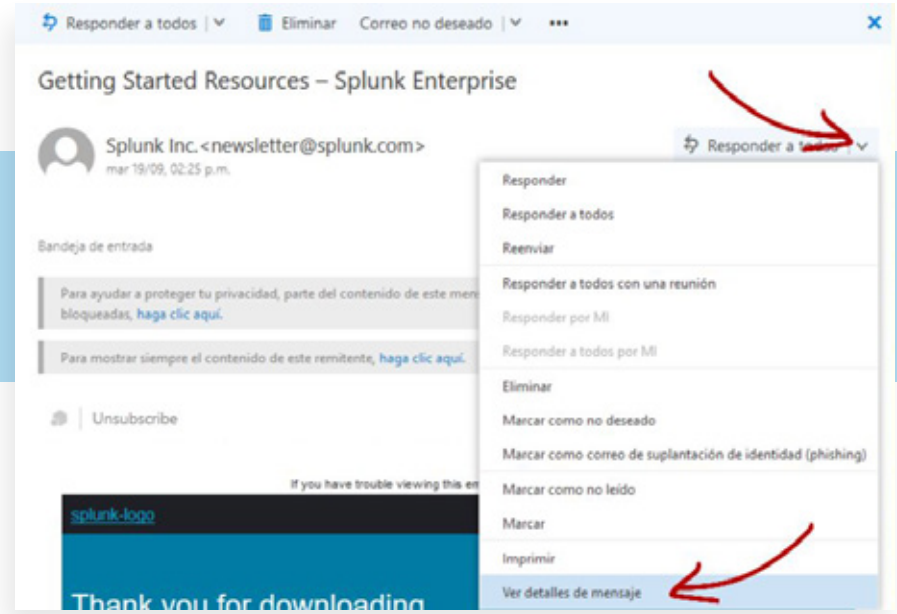
- En el campo "Para:" escriba la dirección **ciberseguridad@ba-csirt.gob.ar**, en el título del mensaje escriba "Información de mensaje N° (y el número que corresponda), y **en el cuerpo del mensaje pegue el contenido de la ventana que había copiado en el paso anterior.**

+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

1.1 OUTLOOK WEB/LIVE

- Acceda a su cuenta de Outlook WEB/ LIVE e ingrese al correo en cuestión para **abrirlo en una ventana independiente.**

- Desplegar el menú junto al botón “Responder” y seleccione la opción **“Ver detalles el mensaje”.**



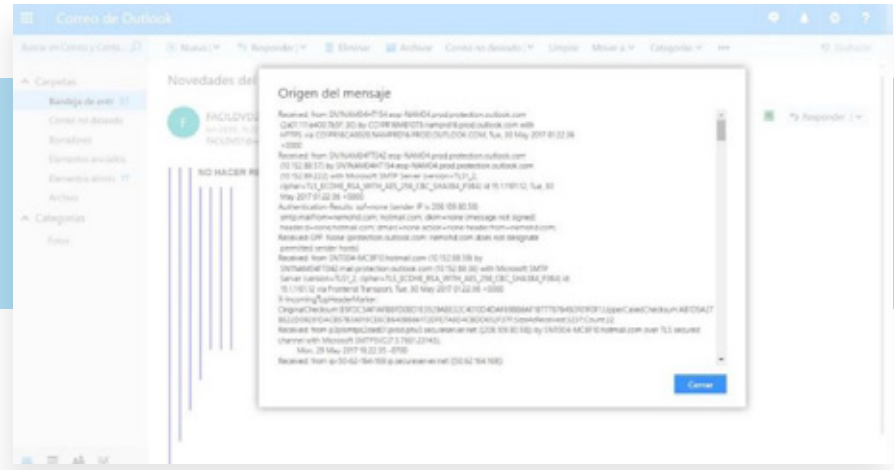
- **Se abrirá una nueva ventana** con contenido similar al de la siguiente imagen.

- **Copie TODO el contenido** de dicha ventana arrastrando el cursor del mouse sobre el mismo.
- Abra un **nuevo correo.**
- En el campo “Para:” escriba la dirección **ciberseguridad@ba-csirt.gob.ar**, en el título del mensaje escriba “Información de mensaje N° (y el número que corresponda), **y en el cuerpo del mensaje pegue el contenido de la ventana que había copiado en el paso anterior.**

1.2 HOTMAIL

- Acceda a su cuenta e **ingrese al correo en cuestión**.
- **Haga clic en la flecha** que aparece a la derecha del botón “Responder”.

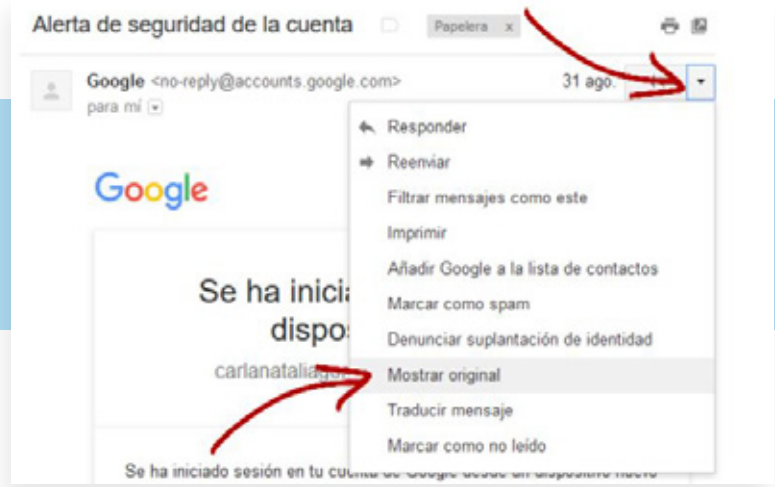
- Elija la opción **“Ver origen del mensaje”** del menú desplegable.



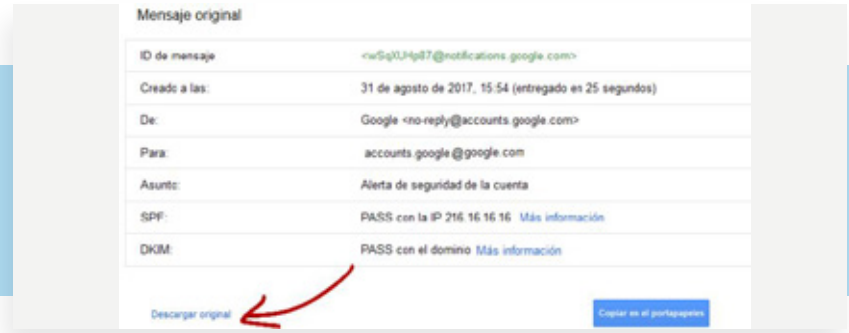
- **Copie TODO el contenido** de dicha ventana arrastrando el cursor del mouse sobre el mismo.
- Abra un **nuevo correo.**
- En el campo “Para:” escriba la dirección **ciberseguridad@ba-csirt.gob.ar**, en el título del mensaje escriba “Información de mensaje N° (y el número que corresponda), **y en el cuerpo del mensaje pegue el contenido de la ventana que había copiado en el paso anterior.**

2. GMAIL

- Ingresar al correo electrónico en cuestión y desplegar el menú junto al botón “Responder”. Luego, **seleccionar la opción “Mostrar Original”**.



- Se abrirá una nueva ventana. **Realizar clic en la opción “Descargar original”**

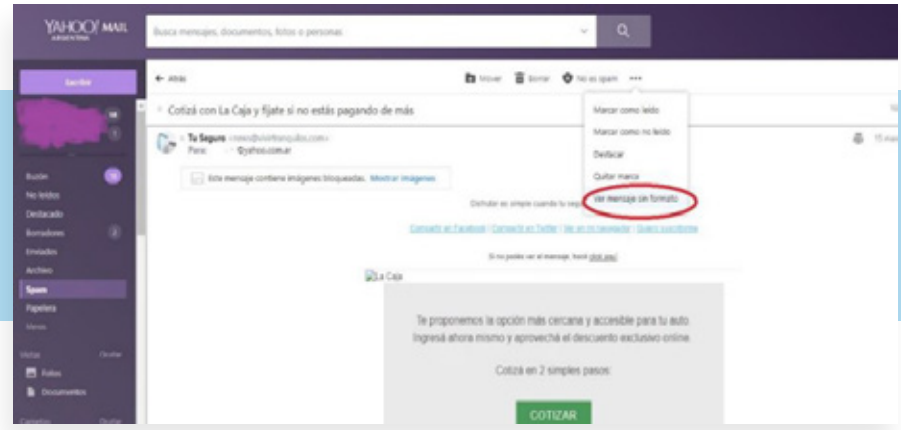


- **Guarde el archivo** y abra un nuevo correo.
- En el campo “Para:” escriba la dirección **ciberseguridad@ba-csirt.gob.ar**, en el título del mensaje escriba “Información de mensaje N° (y el número que corresponda), **y en el cuerpo del mensaje adjunte el archivo descargado en el paso anterior.**

+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

3. YAHOO

- **Ingresar al correo** electrónico en cuestión.
- Desplegar el menú "..." en la barra de tareas de Yahoo. Luego, **seleccionar la opción "Ver mensaje sin formato"**.



- A continuación, se mostrará una **ventana nueva con los encabezados del mensaje original.**

- **Copie TODO el contenido de dicha ventana** arrastrando el cursor del mouse sobre el mismo.
- Abra un **nuevo correo.**
- En el campo "Para:" escriba la dirección **ciberseguridad@ba-csirt.gob.ar**, en el título del mensaje escriba "Información de mensaje N° (y el número que corresponda), y **en el cuerpo del mensaje pegue el contenido de la ventana que había copiado en el paso anterior.**

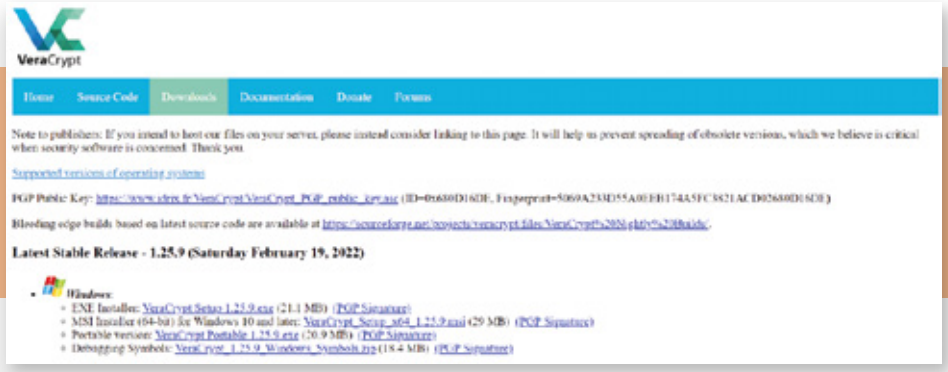
+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

ANEXOS

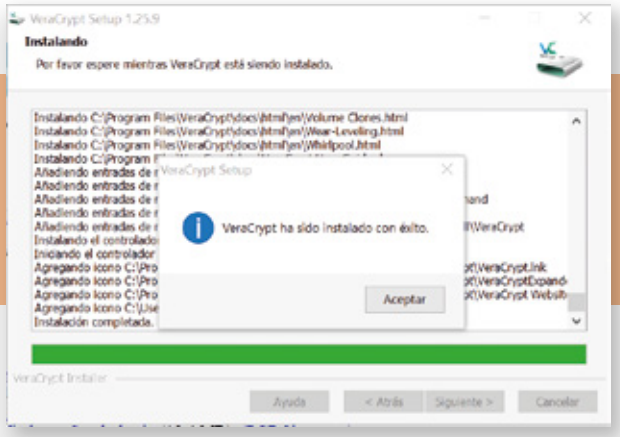
A continuación, especificaremos y explicaremos el uso de dos herramientas gratuitas, las cuales permiten tanto guardar como compartir información sensible, precisamente como lo es la evidencia digital:

1 USO DEL VERACRYPT

- **Descargar la aplicación** Veracrypt de su sitio oficial. https://www.veracrypt.fr/en/Downloads.html



- Una vez descargada la aplicación.EXE, **seguir el procedimiento por default** y finalizar la instalación.



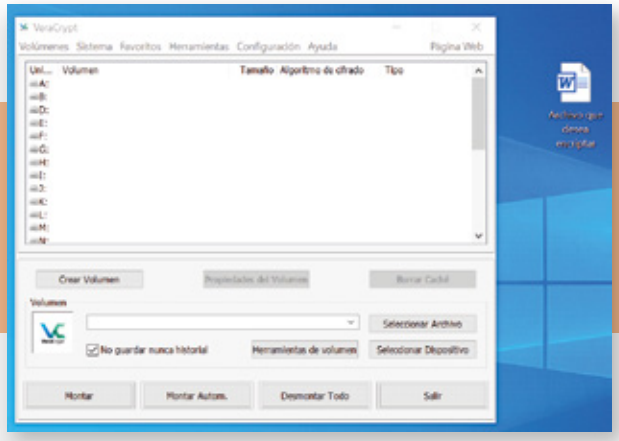
+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

VeraCrypt

- Una vez instalada la aplicación Veracrypt, **abrir el programa.**
  Para crear un nuevo archivo cifrado se debe tener previamente, el archivo vacío que será el utilizado por el programa, como contenedor. Por ejemplo: Un Word vacío, un Excel vacío, una imagen o un video cualquiera.
  Es recomendable que el archivo seleccionado sea elegido en base a lo que se desea guardar. Esto se debe a que el archivo que se encripte funcionará como contenedor "Estilo Pendrive" para que se aloje el resto de la información que queremos que esté segura.

1.2 PROCEDIMIENTO PARA CREAR UN ARCHIVO ENCRIPTADO

- Tener un documento vacío.
- Seleccionar Crear Volumen:

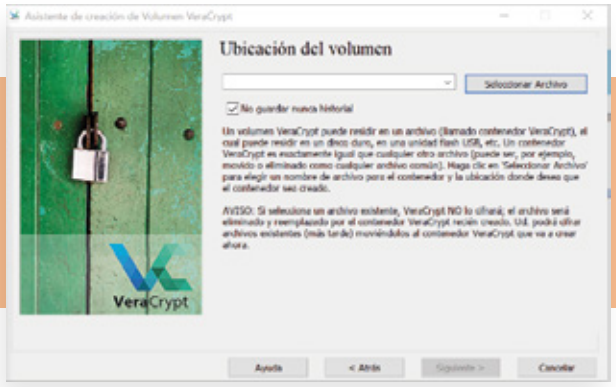


- Seleccionar "Crear un contenedor de archivos cifrado":

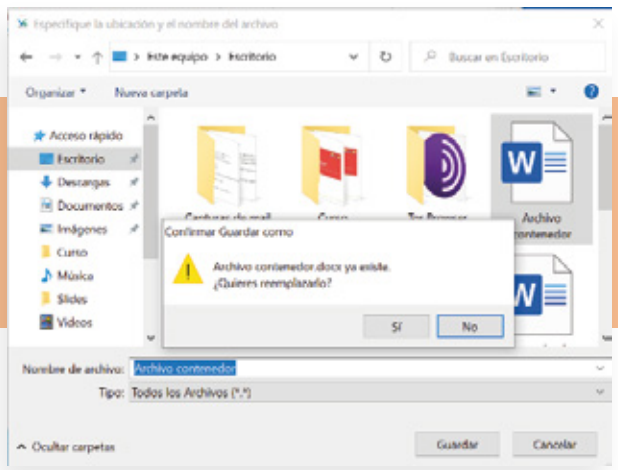
VeraCrypt

- Seleccionar "Volumen Veracrypt común":

- Seleccionar el archivo que se va a usar como señuelo: un archivo cualquiera que esté vacío.

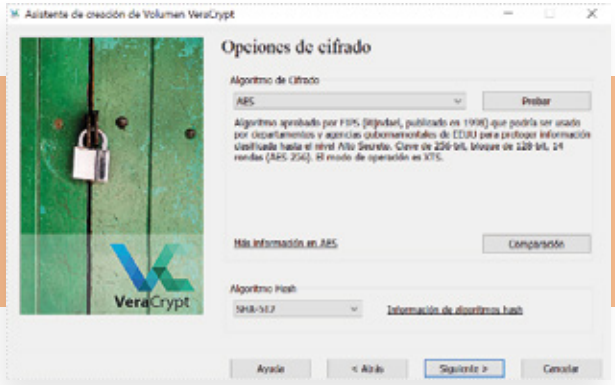


- Cargar el archivo contenedor. Luego de eso, le notificará al usuario si desea reemplazarlo, lo cual se debe aceptar.



VeraCrypt

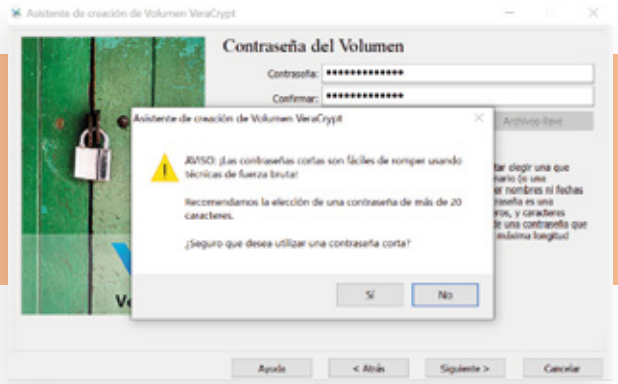
- En esta etapa, el usuario podrá seleccionar el tipo de cifrado que desea utilizar. En este caso es recomendable dejar el que viene por "Default", (Algoritmo de cifrado: AES – Algoritmo Hash: SHA-512).



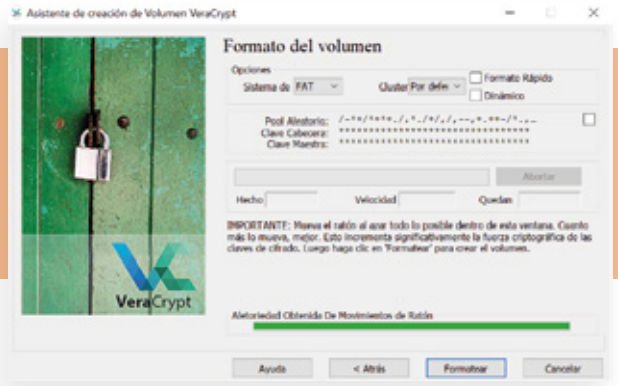
- Llegada esta instancia, el usuario debe seleccionar que espacio tendrá el archivo señuelo que será utilizado como contenedor. El espacio puede ser a elección, se recomienda elegir bien el espacio en base a lo que se desee guardar.

- Luego, se agrega la clave para el "archivo contenedor", el cual después será requerido cada vez que uno quiera abrir su contenido:

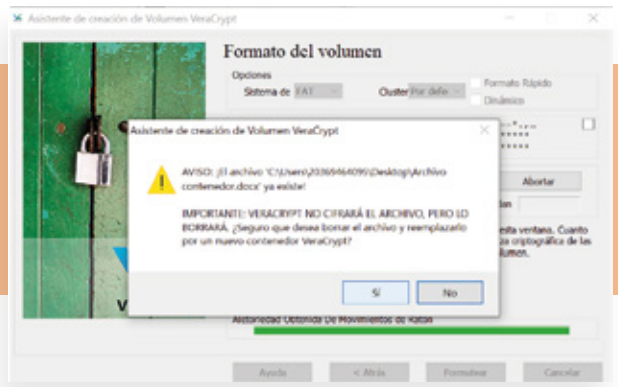
- Posteriormente, la aplicación le informará al usuario que debe utilizar una clave con mayor a 20 caracteres -se puede utilizar la clave que uno quiera- y se selecciona la opción “SI” para continuar con la encriptación.



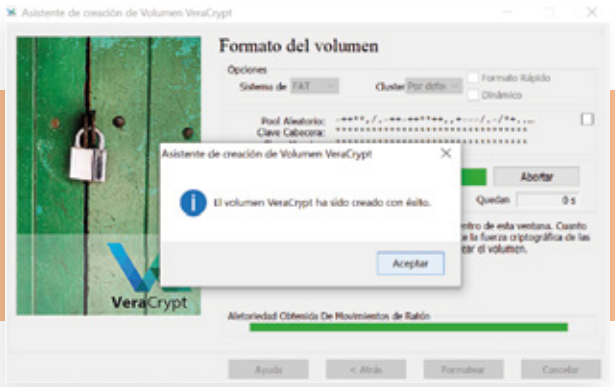
- Una vez realizado el paso anterior, se procederá a realizar un “pool” aleatorio que lo deberá realizar uno moviendo el mouse. Luego de haberse cargado la barra verde, se continua seleccionando la opción “Formatear”.



- En esta etapa, la aplicación Veracrypt le preguntará al usuario si desea sobre escribir el “archivo contenedor” y se debe aceptar esa opción.

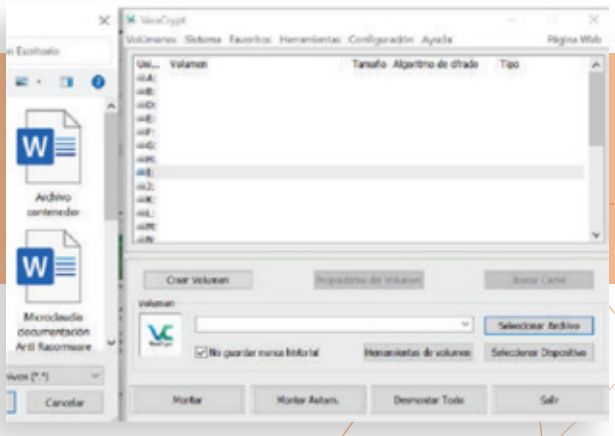


- Ahora ya se ha creado el volumen cifrado, el cual se podrá utilizar como un “pendrive virtual”.



1.3 PROCEDIMIENTO PARA MONTAR EL ARCHIVO CONTENEDOR, VISUALIZARLO COMO UN DISPOSITIVO DE ALMACENAMIENTO Y PODER GUARDAR INFORMACIÓN DENTRO:

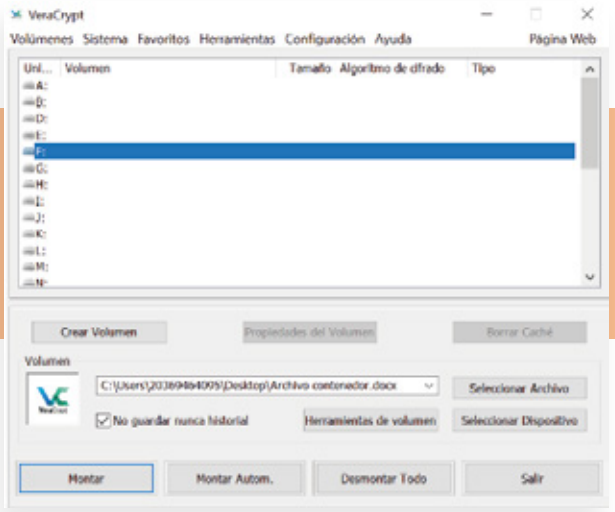
- Para poder montar el “archivo contenedor” y utilizarlo como un “pendrive virtual” -el cual se encuentra cifrado-, primero se debe seleccionar el archivo que utilizamos como contenedor. En este caso de ejemplo, sería el archivo contenedor.docx “WORD”.



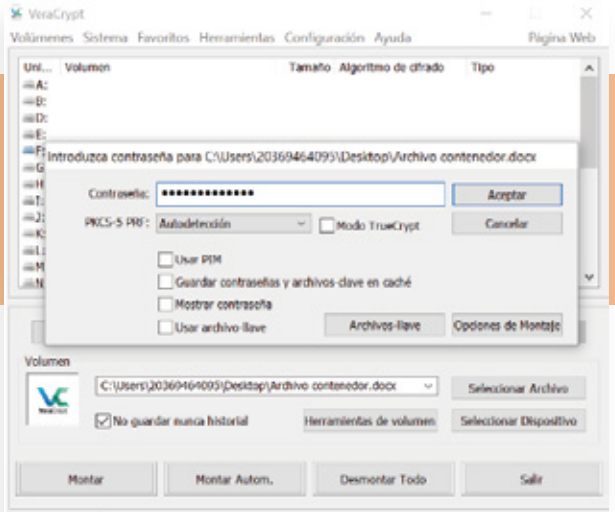
+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

VeraCrypt

- Una vez seleccionado el archivo, el usuario debe elegir con que letra lo quiere visualizar en el equipo. Sería la letra en la cual nos figura el "Pendrive". Puede ser la "F:", la "L:", la que uno desee. Posteriormente a estos pasos se debe seleccionar el botón "Montar".

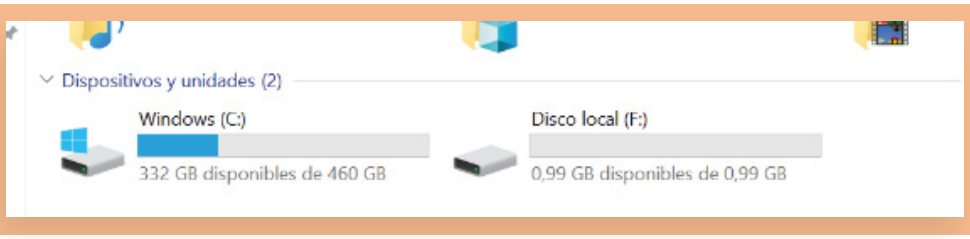


- Luego, le aparecerá al usuario una ventana solicitando la clave con la cual se encriptó anteriormente el archivo, y ahí se debe escribir la contraseña y clickear "Aceptar."

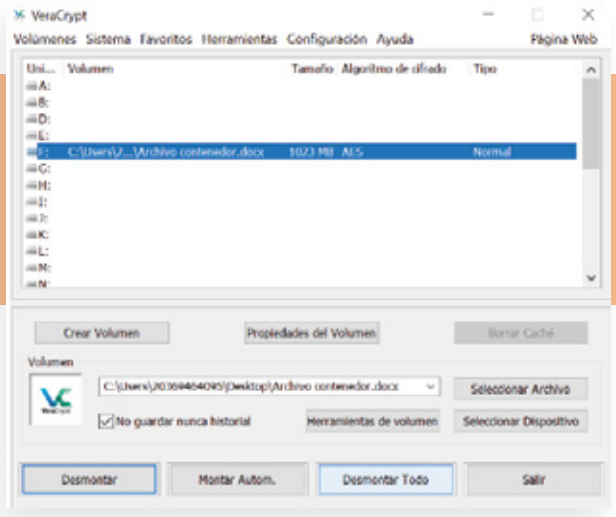


- Para finalizar y verificar se cargó correctamente el archivo cifrado como unidad de almacenamiento, se debe ir a la parte de "Este equipo" y ver al archivo contenedor como una unidad de almacenamiento (Pendrive – Disco externo).

  A partir de este momento, se podrá cargar archivos (copiar, cortar y/o pegar) dentro de esta unidad virtual.

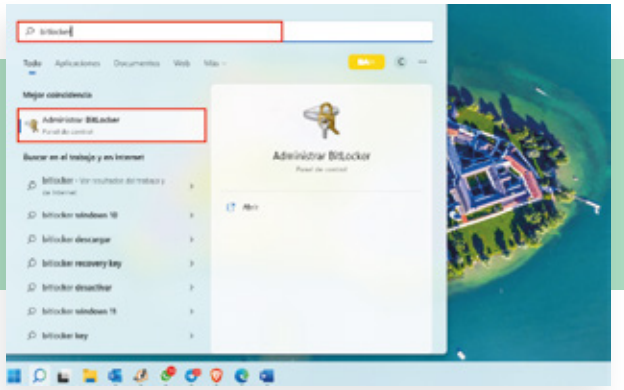


- Una vez cargado los archivos necesarios, se seleccionará la opción desmontar todo para que el archivo contenedor quede desconectado.

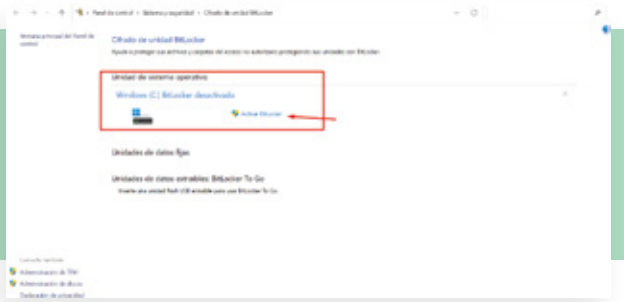


2 USO DE BITLOCKER

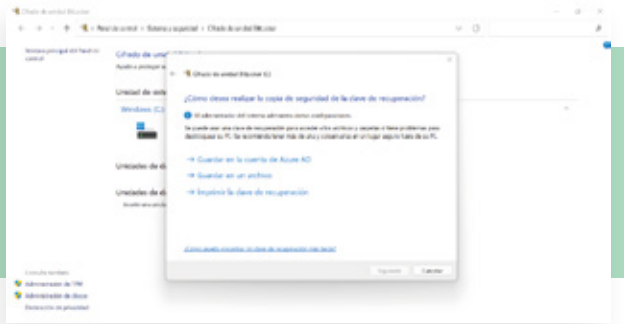
- Hacer click en el menú inicio y escribir "bitlocker" en la búsqueda de menú.
- Seleccionar la opción "Administrar Bitlocker".



- Hacer click en "Activar BitLocker".

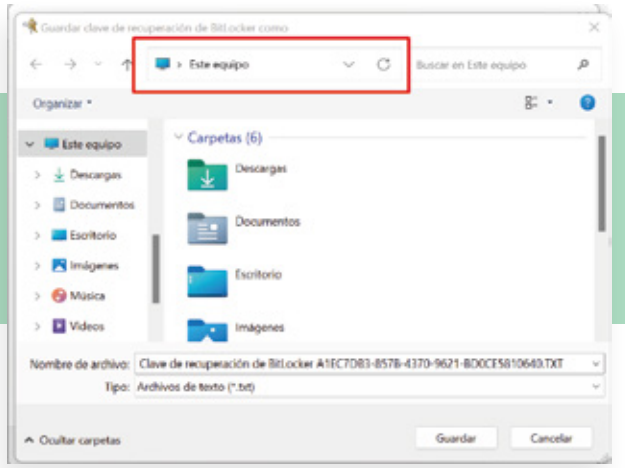


- Elegir donde se va resguardar la clave de recuperación. Deberá ser en un lugar diferente fuera de la PC, ya sea que se va a imprimir a resguardar en algún lugar remoto.

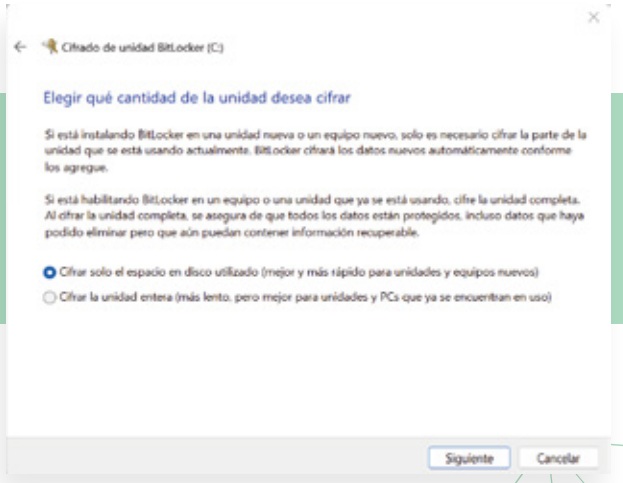


+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

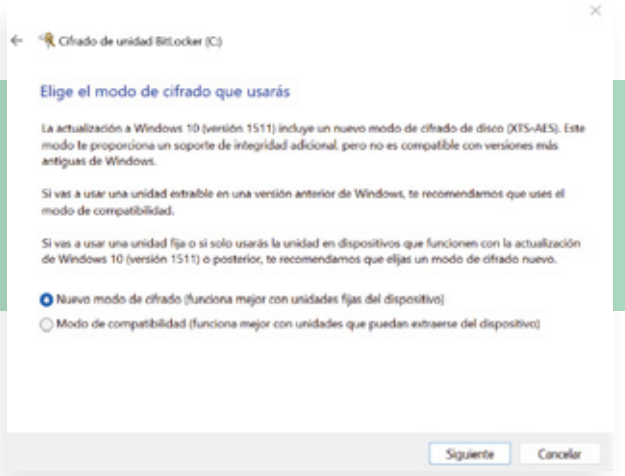
- Se debe optar por la opción “guardar en un archivo” y hay que elegir una ubicación diferente fuera del equipo.



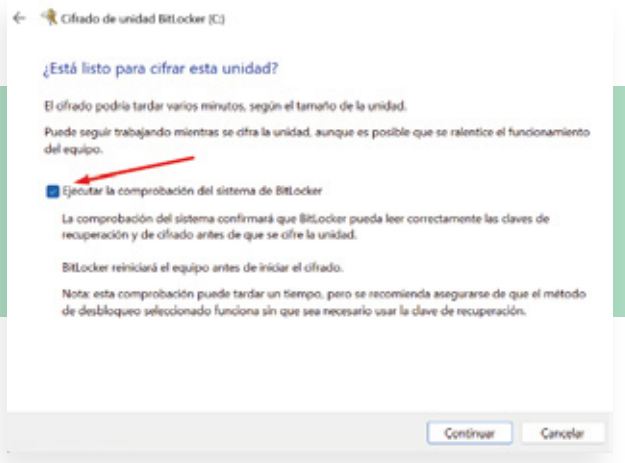
- A continuación, se elige cuanto del disco se quiere cifrar, tanto para equipos nuevos como para equipos que ya están en uso.



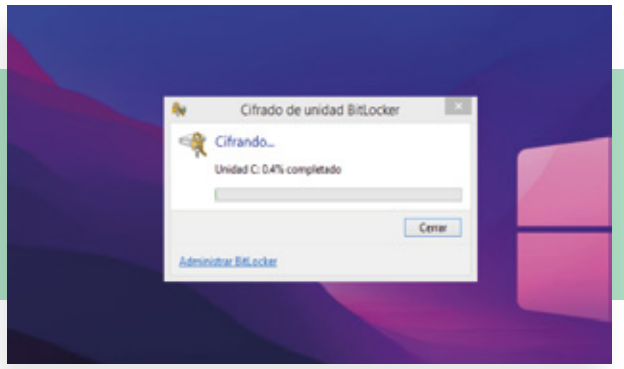
- En esta instancia, se le consulta al usuario el modo de cifrado que usará, donde estará cifrando además de su disco interno, uno externo. Es recomendable usar el tipo de compatibilidad para poder ser accedido en otros dispositivos con versiones anteriores de Windows.



- Ahora le pregunta al usuario si se encuentra listo para cifrar esta unidad. Recomendamos tildar la opción “Ejecutar comprobación del sistema Bitlocker” para garantizar un acceso completo a los archivos cifrados.



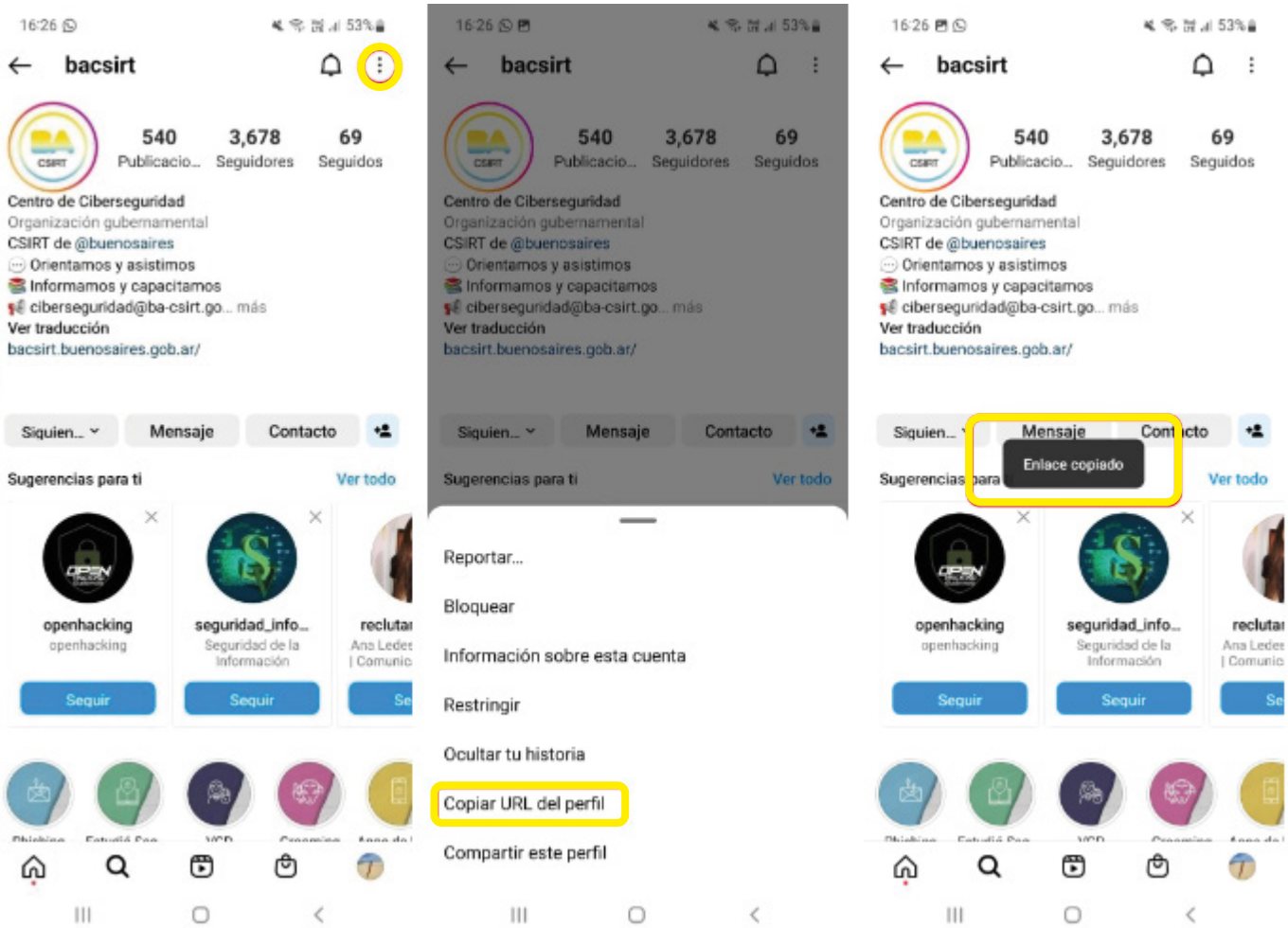
- Al reiniciar el equipo, aparecerá la siguiente pantalla donde le pedirá la clave de inicio de sesión para iniciar el cifrado de la unidad al iniciar la sesión. En el área de notificaciones aparecerá un mensaje diciendo que la unidad se está cifrando.



+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

CÓMO RESGUARDAR UNA

URL DESDE EL CELULAR



+54 (011) 4323-9362
https://bacsirt.buenosaires.gob.ar/
ciberseguridad@ba-csirt.gob.ar

RESGUARDO DE INFORMACIÓN:
¿CÓMO PRESERVAR EVIDENCIA DIGITAL?

Desde el BACSIRT, siempre hacemos hincapié en la importancia del resguardo y la correcta preservación de información y datos personales ya que, además de ser una de las estrategias más efectivas de prevención, es una herramienta de gran ayuda en caso de tener que mostrar evidencia digital frente a algún incidente tecnológico.