SEGURIDAD TECNOLÓGICA

Hospital Buen Samaritano

Departamento de Administración

Oficina de Proyectos Especiales

Jun 2015

USO APROPIADO DE LAS ESTACIONES DE TRABAJO

- En el Hospital Buen Samaritano de Aguadilla las computadoras provistas son para el uso exclusivo de las operaciones de nuestra institución, y no pueden ser utilizadas para propósitos ajenos a la misión de ésta corporación.

- Todos los miembros de la fuerza laboral del HBS somos responsables por el uso de nuestras estaciones de trabajo. El uso de las computadoras deberá ser apropiado, legal y ético.

USO APROPIADO DE LAS ESTACIONES DE TRABAJO

- El Administrador de sistemas asignará los accesos y cuentas de acuerdo a las funciones del usuario.
- El Departamento de Sistemas vigilará las actividades ejecutadas en las computadoras para asegurar el uso correcto.
- La información recopilada por el uso incorrecto de las estaciones podrá ser utilizada como evidencia en acciones disciplinarias o en acciones legales, si fuese necesario.

USO APROPIADO DE LAS ESTACIONES DE TRABAJO

- No se permiten anuncios, ni campañas políticas o religiosas.
- Se prohibe el uso de las computadoras para acceder o propagar material pornográfico, ver videos o entrar en cualquier red social.
- Se prohibe tomar fotos o videos del sistema, e imprimir información de pacientes o información del empleado sin autorización de la administración.
- Las computadoras no serán utilizadas para ninguna actividad ilegal. El HBS considera las siguientes actividades como “uso ilegal”:

    a. Acoso a otros usuarios

    b. Difamación de algún usuario

    c. Destrucción o daño de los equipos, programas o información bajo custodia del HBS.

USO APROPIADO DE LAS ESTACIONES DE TRABAJO

- Continuación:

  d. Interrupción o monitoreo sin autorización de las comunicaciones electrónicas.

  e. Copiar material con derechos reservados (derechos de autor) sin autorización.

  f. Guardar en las computadoras información ilegalmente adquirida.

  g. Violaciones a la confidencialidad y privacidad.

  h. Violaciones a las licencias de programas.

  i. Utilización del correo electrónico para usos no aprobados por la administración.

USO Y MANEJO DE CONTRASEÑAS

- Las contraseñas son un aspecto importante de seguridad en la tecnología. Ellas son la línea delantera de protección para el usuario y sus cuentas.

- Los usuarios son responsables del uso y mal uso de su identificación de acceso y contraseña (username + password).

- Los usuarios son responsables por todo el trabajo realizado bajo su cuenta de acceso, por lo que:

  a. Serán responsables de terminar sus sesiones de comunicación (desconectarse) apropiadamente.

  b. Asegurarse que nadie tenga acceso a su cuenta.

  c. Si piensa que alguien ha utilizado o aprendido su cuenta, deberá notificarlo inmediatamente a su supervisor y al personal de cómputos.

USO Y MANEJO DE CONTRASEÑAS

- No use la misma contraseña para las cuentas del HBS, como para cuentas personales.

- Nunca comparta la contraseña con sus compañeros de trabajo, supervisores, etc.

- Todo lo que un usuario realiza en el sistema, es monitoreado por el personal de cómputos, por lo que:

  *El uso y manejo inapropiado de las contraseñas puede ocasionar la desactivación temporal o permanente de la cuenta asignada.

USO Y MANEJO DE CONTRASEÑAS

- Una contraseña segura posee las siguientes características:

  a. Contiene caracteres en mayúsculas y minúsculas.

  b. Contiene letras y/o símbolos.

  c. Es de por lo menos 8 caracteres alfanuméricos.

  d. No son basadas en información personal, nombres de familiares, mascotas, etc.

  e. No son escritos o almacenados, ya que cualquier persona los podría ver.

- Ejemplo de una contraseña segura: Pepit@01

MALWARE

- Malware es el término en inglés para referirse a programas maliciosos. Es un término colectivo que incluye todo tipo de software perjudicial, como por ejemplo troyanos, programas espía y virus. El software instala programas sin su permiso para obtener su información personal o para usar su computadora para llevar a cabo actividades fraudulentas. Una vez instalado, el programa malicioso puede robar su información.

MALWARE

- Cómo los programas maliciosos entran en contacto con una computadora?

1. Usted no presta atención al instalar una aplicación de "buena reputación".

2. Ha instalado algo de una fuente poco fiable o desconocida.

3. Ya la computadora está infectada y no tiene el conocimiento, por lo tanto ese malware instalará más malware.

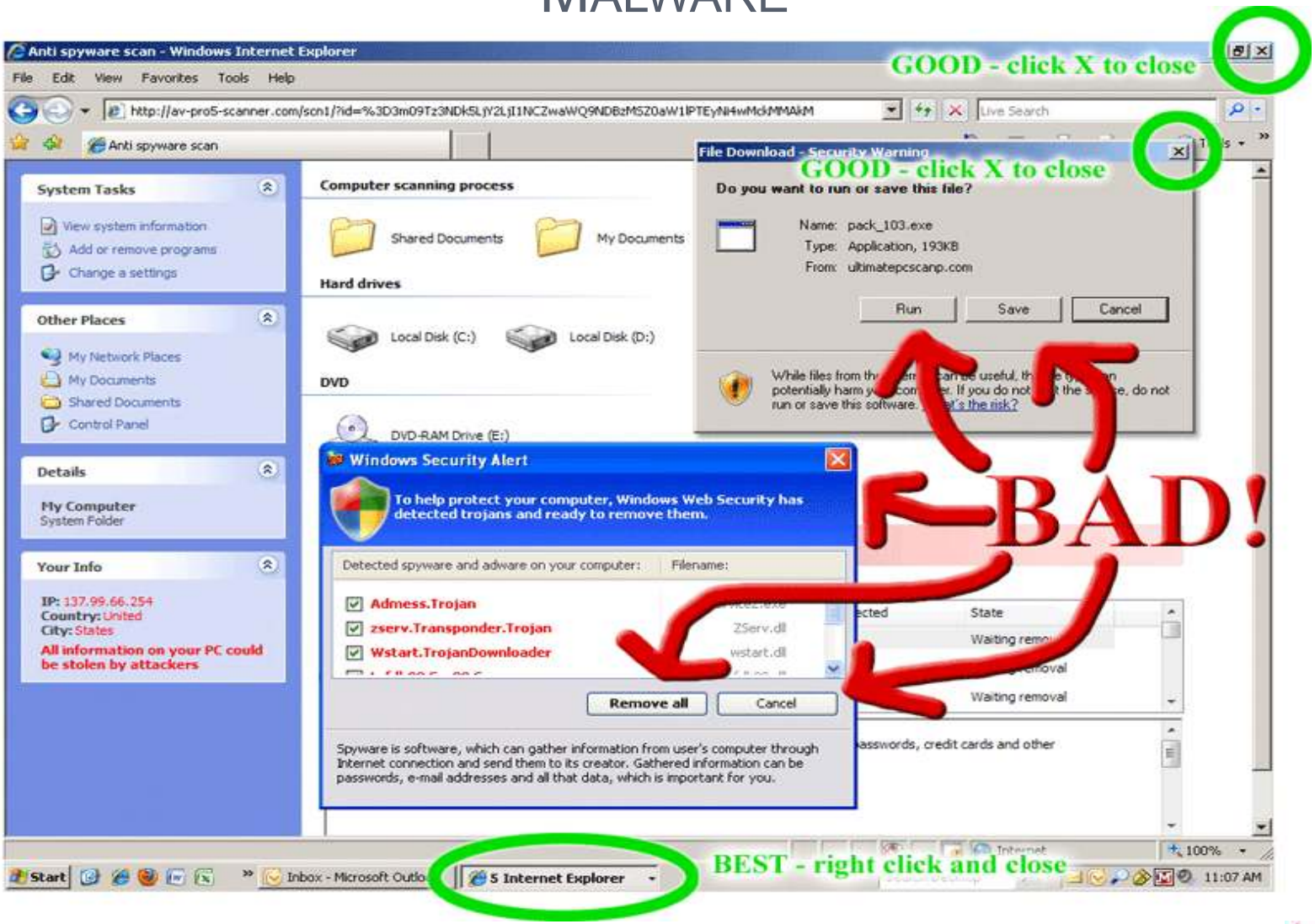
4. No está utilizando un programa Anti-virus o aplicación Anti-spyware de buena calidad, o no están actualizados.

5. Al visitar páginas web de dudosa reputación o desconocidas.

6. Ha contestado encuestas o promosiones aleatorias en el Internet.

7. A través del correo electrónico al abrir mensajes de remitentes desconocidos.

MALWARE



- En la pantalla vemos un ejemplo común que utilizan los cyberdelincuentes para infectar una computadora. La pantalla está diseñada para verse como un mensaje original del sistema Windows, pero es falsa. Si presionas en los lugares incorrectos, instalará malware en la computadora. La forma correcta para eliminar éstas pantallas, es dando “right click” en la ventana en el “task bar” y presionar “close”.

MALWARE

- Posibles síntomas de infección con Malware:

1. Un rendimiento deficiente del sistema (también pueden ser otros factores, no es necesariamente malware).

2. La computadora tarda más en iniciar o se vuelve “loca”.

3. El navegador se cierra de forma repentina o deja de responder.

4. Los enlaces no funcionan o llevan a páginas no relacionadas.

5. Aparecen ventanas emergentes con publicidad cuando el navegador no está abierto.

6. Se agregan barras de herramientas adicionales al navegador.

7. Los archivos desaparecen o son escondidos.

MALWARE

- Algunos métodos de protección contra Malware:

1. Si sospecha que tiene un programa malicioso en su computadora, deje de realizar actividades que impliquen el uso de nombres de usuarios y contraseñas.

2. Confirme que su software de seguridad esté funcionando y actualizado (Igualmente su navegador web y sistema operativo).

3. Tenga cuidado al abrir enlaces que vienen en correos electrónicos.

4. Descargue e instale software solamente de sitios web que conozca y en los que confíe.

5. Utilizar contraseñas de alta seguridad para evitar ataques de diccionario.

6. Tener instalado un buen Antivirus y un Firewall.

PROBLEMAS

- Si sospecha que su equipo pudiera estar infectado, es fundamental comunicarse con el Departamento de Sistemas para que evalúe la computadora lo antes posible.

- Para problemas con la computadora y el sistema comunicarse con el personal de cómputos:

- Sr. Jomar Rivera Ext. 1045, o realizar
- Sr. Ismael Ruíz Solicitud en la Intranet (ticket).
- Sr. Jorge Carmona

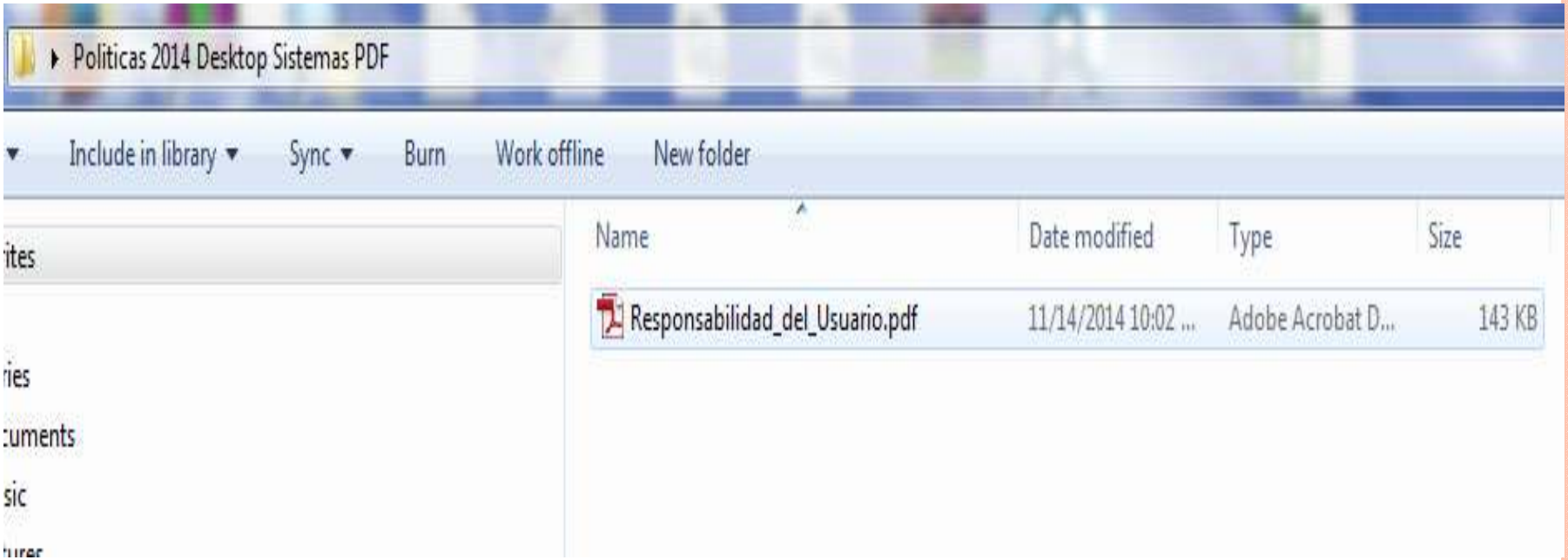
- Si tiene dudas sobre como utilizar una de las aplicaciones del sistema, comunicarse con:

- Sra. Aurora Nieves Ext. 1102
- Sra. Gisela González Ext. 2509

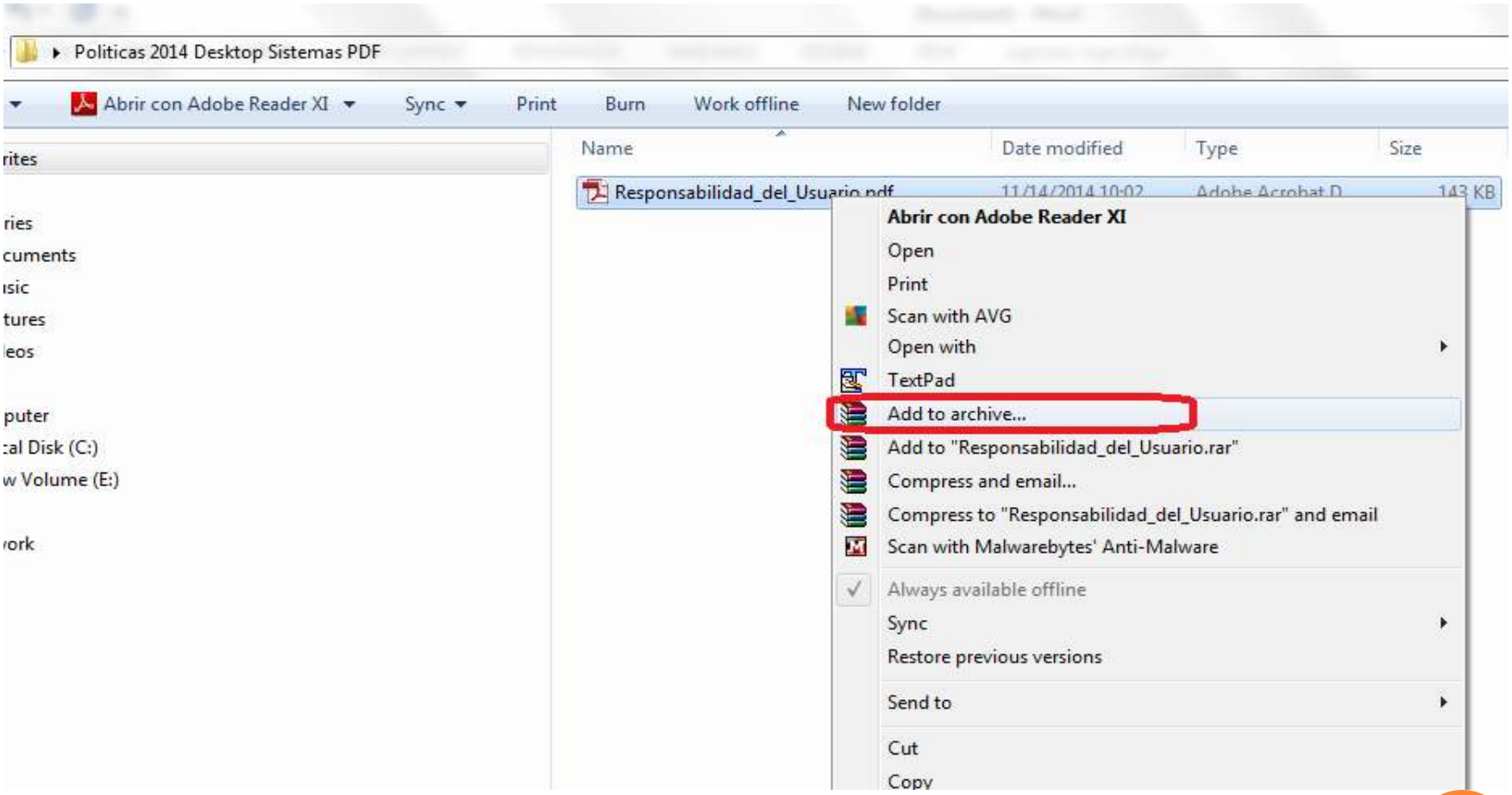
- Restart- si al momento no estás utilizando la computadora.
- Postpone- si estás realizando alguna labor.

COMO ENCRIPTAR DOCUMENTOS UTILIZANDO WINRAR?

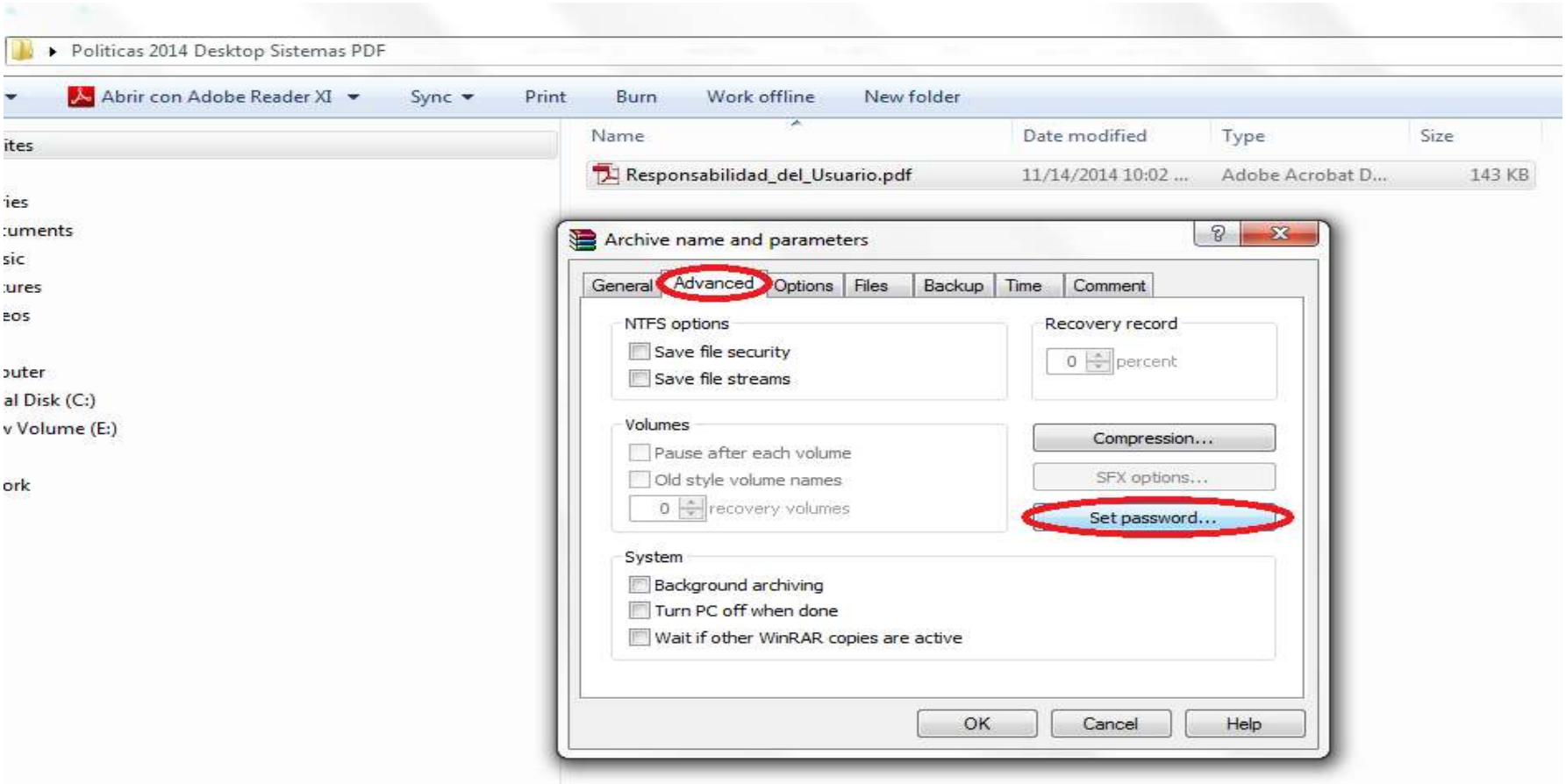
- **Paso 1:** Buscar el Archivo que desea proteger



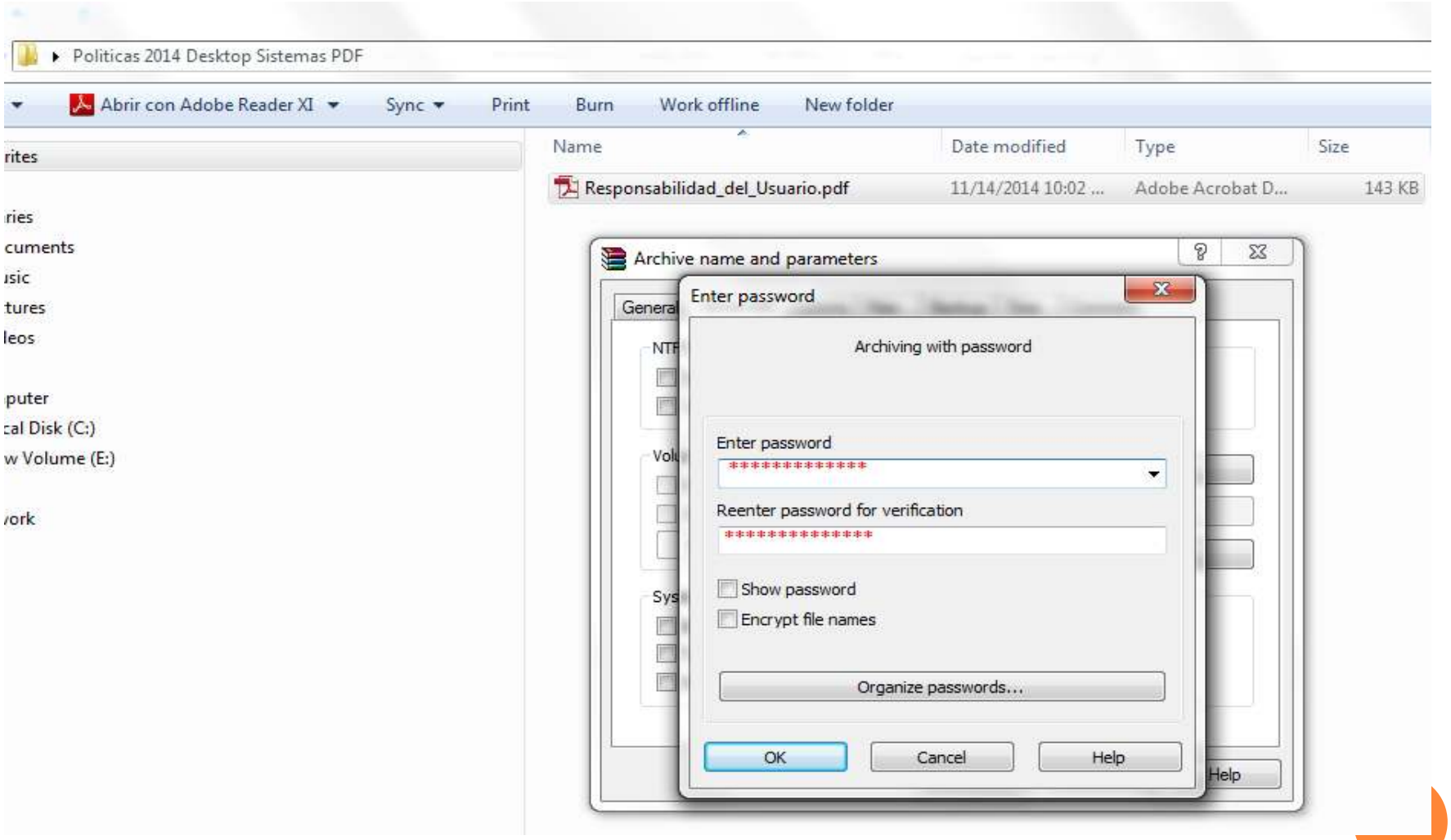
- **Paso 2:** Presionar el botón Derecho del “mouse” y seleccionar “Add to archive…”



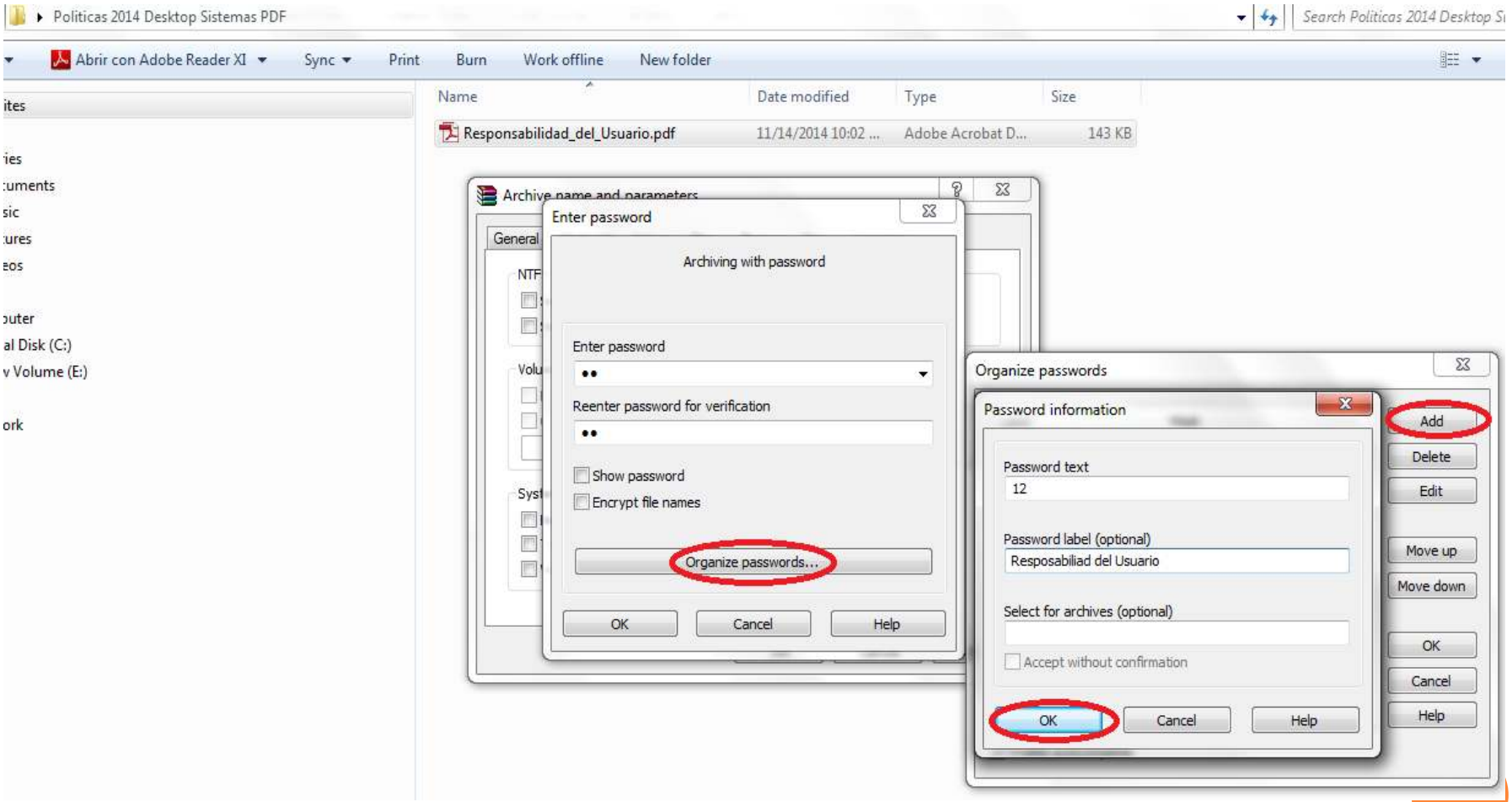
- **Paso 3:** Hacer un click encima de la pestaña de “Advanced” y luego en el botón “Set password…”



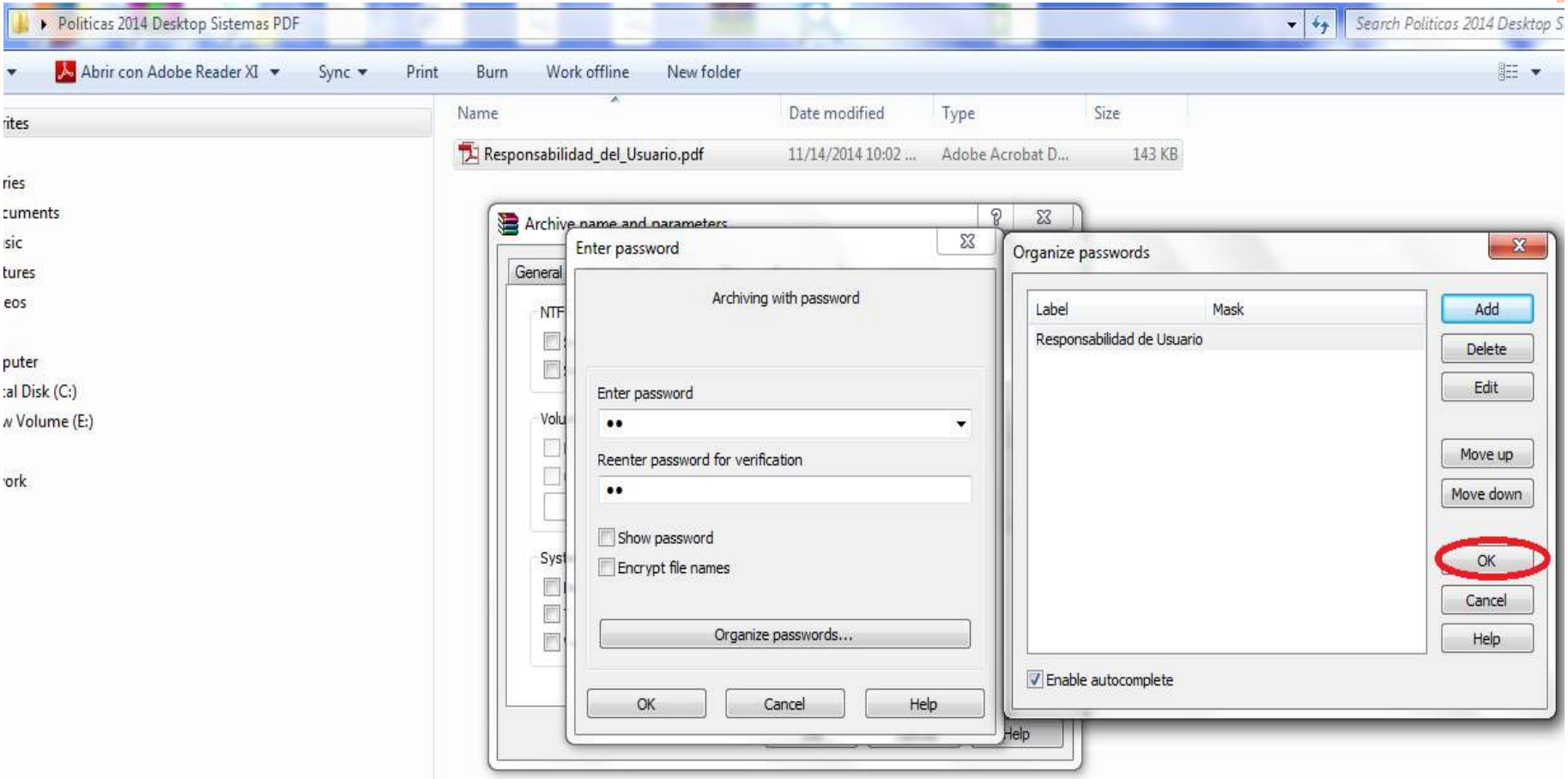
- **Paso 4:** Hacer un click encima de la pestaña de “Advanced” y luego en el botón “Set password…”. Favor de indicar la contraseña deseada.



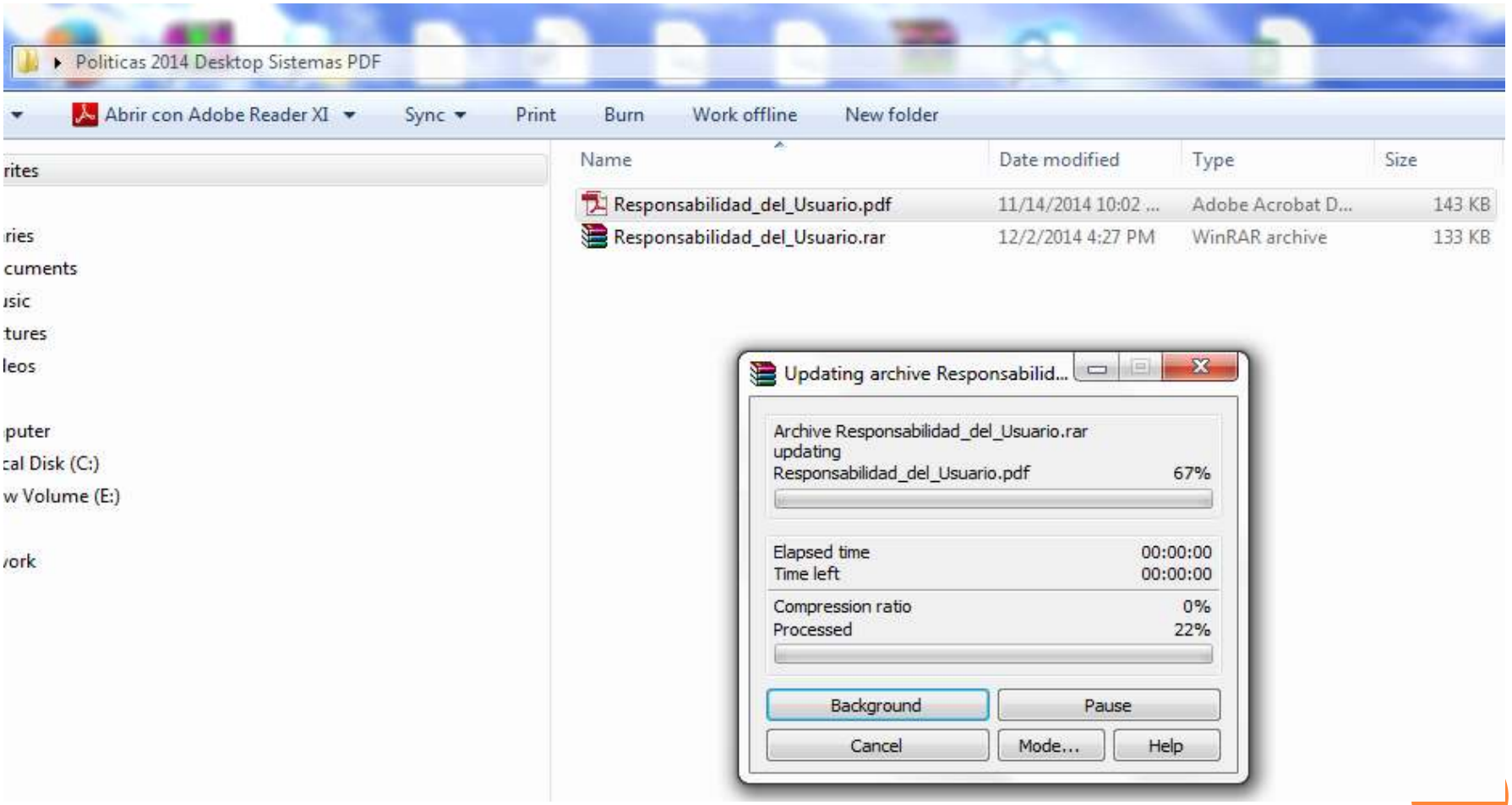
- **Paso 5:** *Manejo de las Contraseñas*: Para tener las contraseñas de forma organizada, el usuario puede hacer un click encima de “Organize Passwords”. Luego precionar el botón de “Add”. Se abrirá una pantalla la cual le permite colocar la contraseña y un etiquetado para recordar el archivo encriptado.



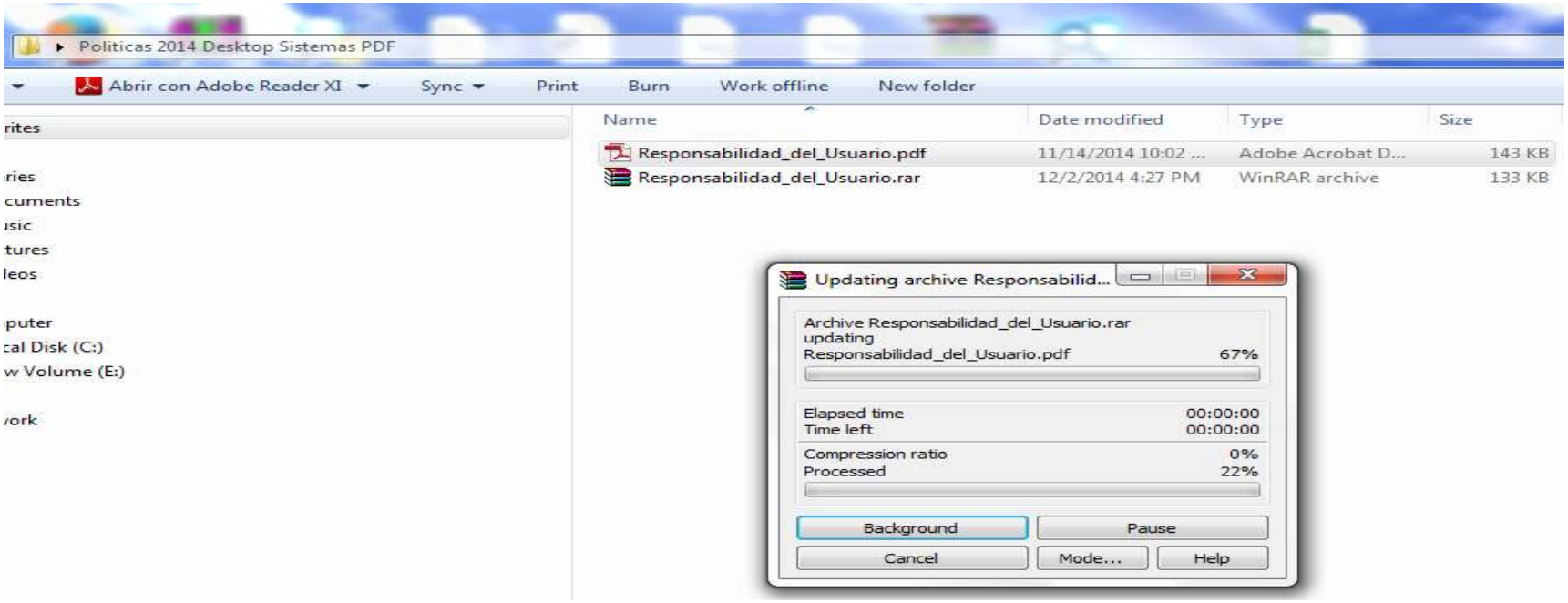
- **Paso 6: Manejo de las Contraseñas:** Si se te olvidó la contraseña, solo es cuestión de ir al botón que dice: “Organize Password…” Aquí aparecera el “Label” creado. Si le das al botón de “edit” seleccionando el archivo correspondiente podrás ver cual fue la contraseña utilizada.

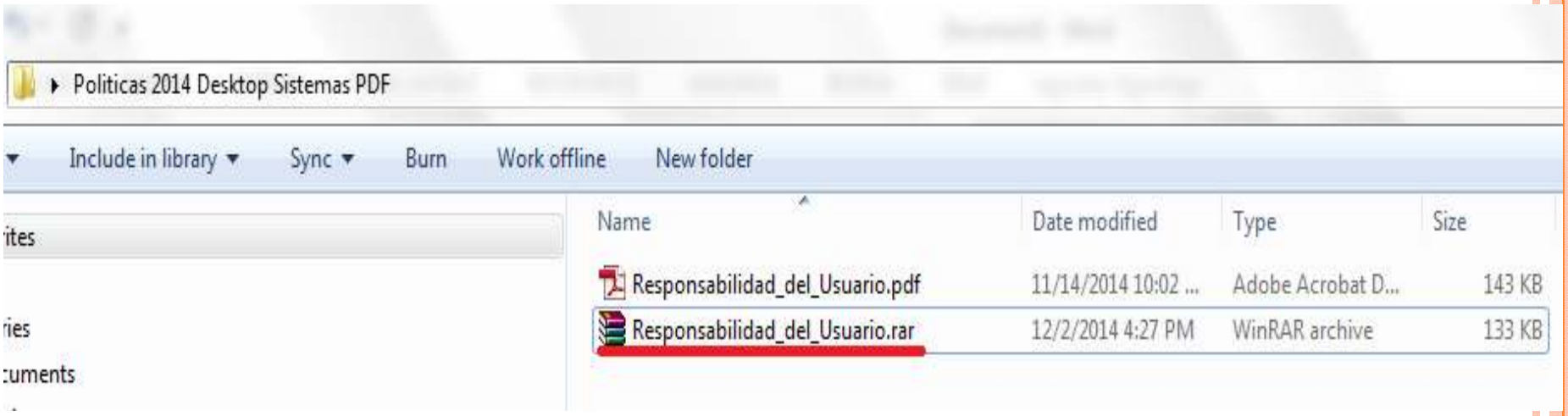


- **Paso 7:** En esta etapa del procedimiento se habrá creado otro archivo con un icono de libro. Este es el documento encriptado el cual será enviado por correo electrónico.

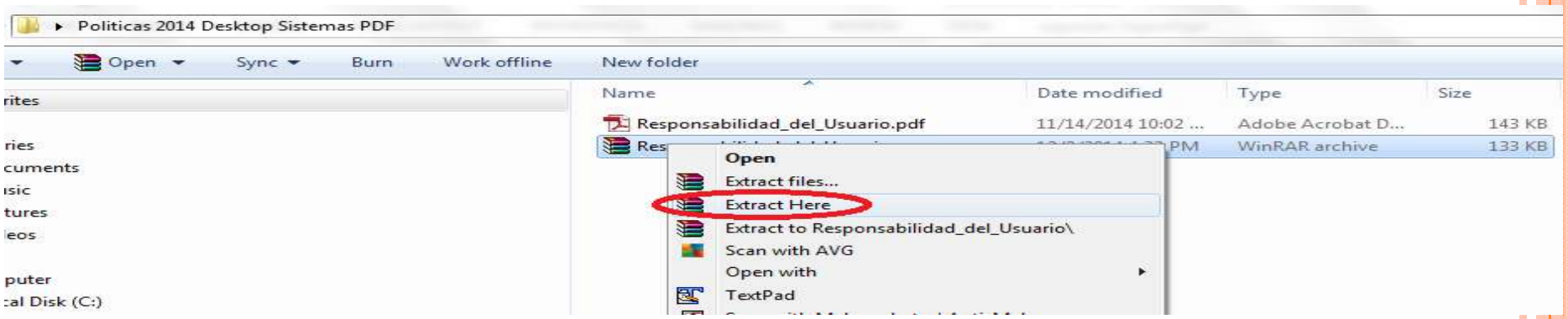


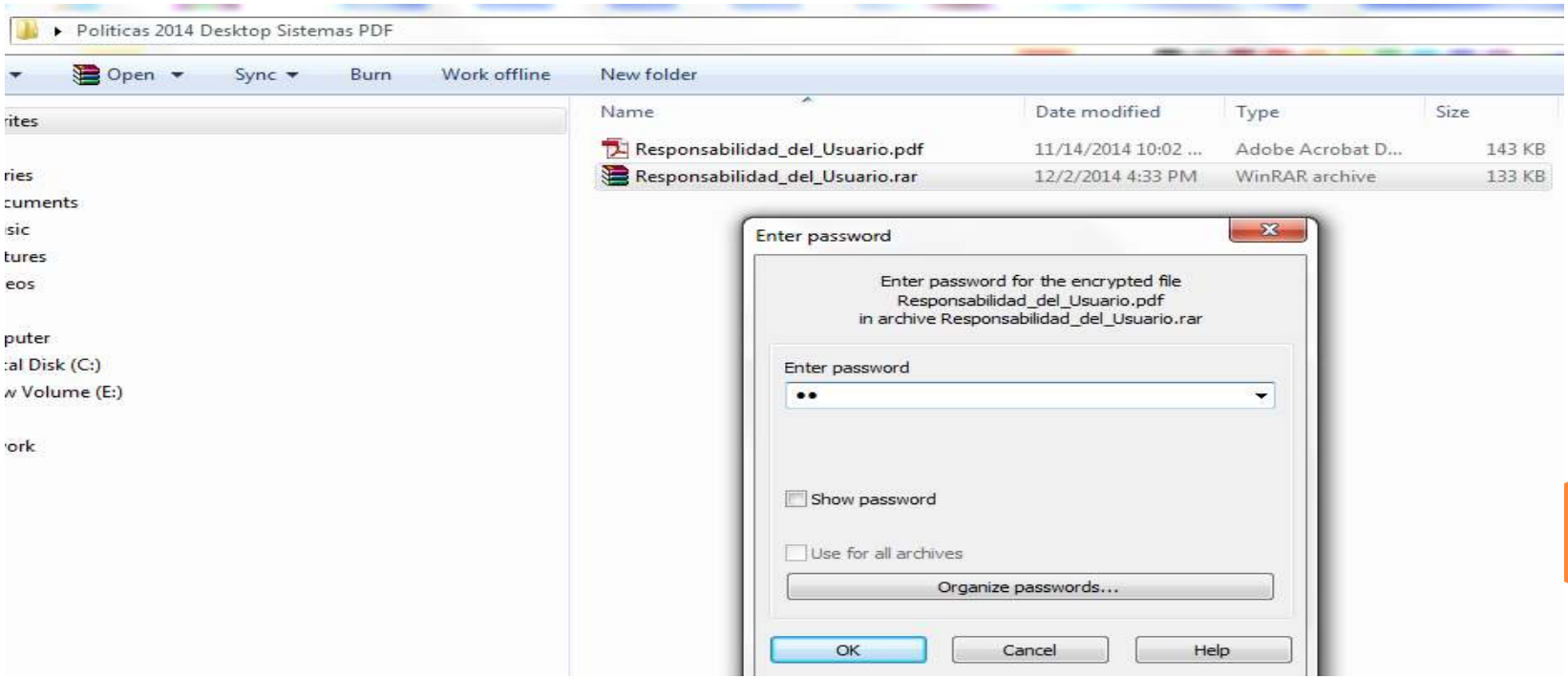
- **Paso 8:** En esta etapa del procedimiento se habrá creado otro archivo con un icono de libro. Este es el documento encriptado el cual será enviado por correo electrónico.





- **Paso 9:** Para Abrir un archivo encriptado debemos posicionarnos encima del documento, hacer un click con el botón derecho del mouse y seleccionar “Extract Here” . Aparecerá un recuadro para escribir la contraseña y le damos OK .





GRACIAS!

FAVOR DE COMPLETAR EL EXÁMEN ACCEDIENDO AL MENU PRINCIPAL DE SEGURIDAD TECNOLÓGICA EN NUESTRO PORTAL DE INTERNET: WWW.HBSPR.ORG