1.- Objetivo

Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.

Los dispositivos de almacenamiento con información sensible se deberían destruir físicamente o la información debe ser destruida, borrada o sobrescrita usando técnicas para hacer que la información original sea no recuperable y no simplemente usando la función normalizada de borrado (delete) o la función formato.

Los dispositivos dañados que contienen data sensible pueden requerir una evaluación de riesgos para determinar si es que los ítems deben ser destruidos físicamente en lugar de ser reparados o descartados.
La información puede ser comprometida a través de dispositivos descuidados o por el re uso del equipo.

El Objetivo es minimizar el riesgo de filtro de información sensible a personas externas con la eliminación segura de los medios. Se debería considerar los medios que contengan información sensible se almacenarán y eliminarán de forma segura, por ejemplo, incinerándolos, triturándolos o vaciando sus datos para usarlos en otra aplicación dentro de la organización;

2.- Alcance

Todas las reparticiones dependientes del Ministro de Economía.

3.- Modificaciones

Este documento es versión original PRO-BORR-01-V01.

4.- Definiciones y abreviaturas

N/A

5.- Responsables

Propietario:

Custodio:

6.-Clientes

Todos los medios de almacenamientos administrados por la DIME.

9.- Desarrollo

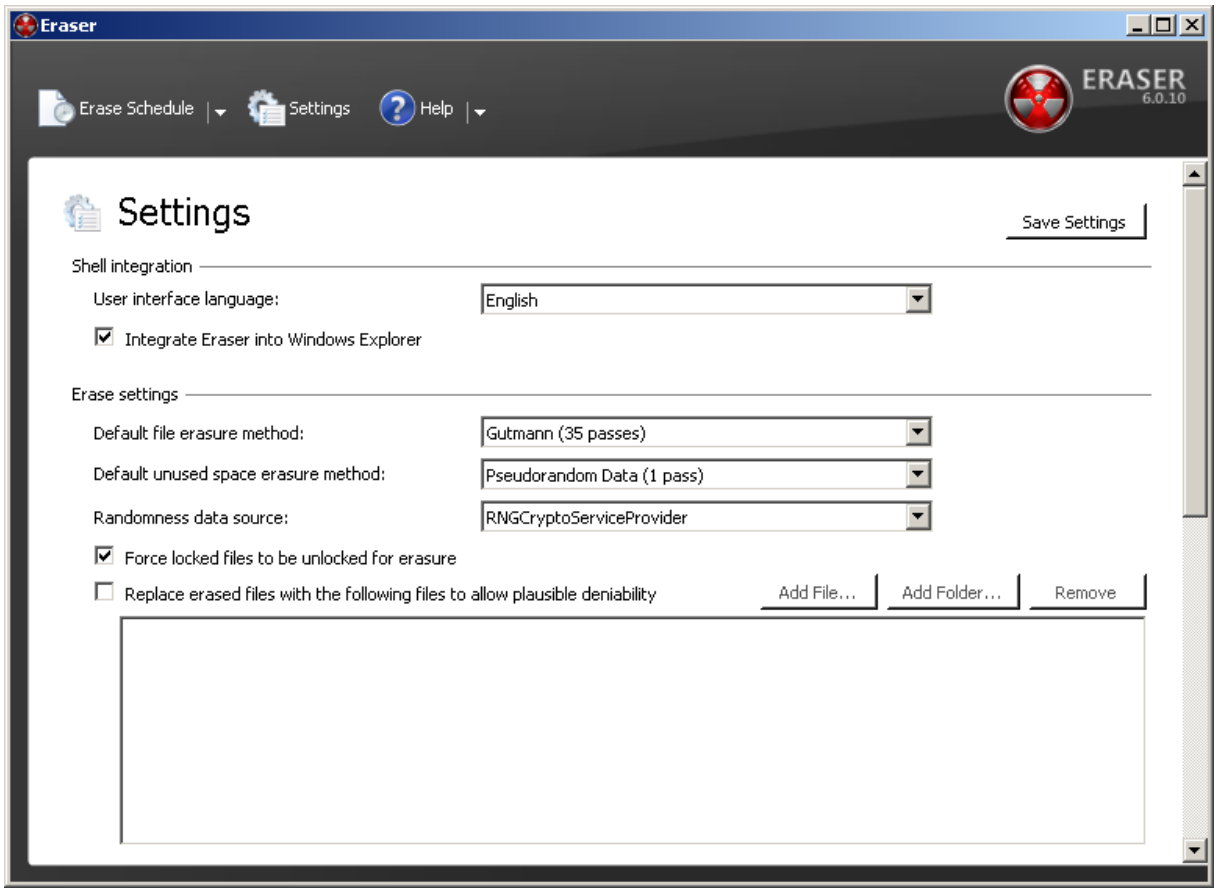
01	*Crear un directorio denominado **"ELIMINAR"** en el escritorio de la PC, donde cada usuario resguardará sus archivos y/o documentos que considera sensible y que desee* eliminar de forma segura de modo de minimizar el riesgo de filtrado de información.
02	En el caso de cambio de máquina, ingresar al panel de control y seleccionar la opción **"Agregar o Quitar Programas"** y desinstalar las aplicaciones con licencia de modo de liberar la misma, para poder reinstalarla en el nuevo equipo.
03	Bajar la aplicación ERASER de la página oficial de la DIME http://www.dime.gov.ar/Eliminar Seguir las instrucciones para su instalación.
04	Una vez finalizado el proceso de instalación posesiónese sobre el directorio "**ELIMINAR**", botón derecho del Mouse y seleccione la opción "**ERASE**" y elija la opción "**ERASE**". A través de esta acción **se eliminará en forma definitiva los archivos** del directorio, sin opción de recuperación de los mismos.
05	Ante consultas y/o dudas puede comunicarse a la DIME, teléfono 0381-4309316 interno 126 o bien a través de cuentas de correo oficial.

GUIA DE INSTALACIÓN

Muchas empresas utilizan destructores de documentos, trituradoras que hacen prácticamente imposible reconstruir el documento original, de manera que los datos que teníamos queden destruidos. Esta es una precaución básica, puesto que la mayoría de las fugas de datos que se detectan se realizan en papel. El equivalente a un triturador para los archivos informáticos sería una aplicación como **Eraser, que permite el borrado seguro de datos** de forma eficiente.

La instalación de Eraser es muy sencilla. Las técnicas que se utilizan en estos casos consisten en **borrar el archivo y sobreescribirlo**. Cuantas más veces se repita esta operación más seguro será el borrado, por lo que podemos hacerlo en este caso hasta 35 veces mediante el algoritmo Gutman.

ERASER, PERMITE EL BORRADO SEGURO DE DATOS



Una vez instalado, cuando queramos enviar un archivo a Eraser para su borrrado seguro sólo tenemos que **utilizar el menú contextual** con el botón derecho para que aparezcan las opciones de eliminación del archivo. Podemos eliminarlo directamente o programar su borrado para el próximo reinicio del equipo. El primer caso es recomendable para unidades externas como discos duros o memorias USB y el segundo caso es quizás mejor para los archivos que tengamos en los discos duros de nuestros equipos.

Hay que tener en cuenta que el **borrado seguro tarda bastante tiempo**, aunque todo dependerá del tamaño del archivo. No se producirá de forma instantánea como hacemos cuando borramos una archivo de la papelera, sino que el proceso de sobreescribir un archivo tardará su tiempo dependiendo del tamaño del mismo y el algoritmos que hayamos elegido.

Por último una cuestión a tener en cuenta es para qué tipo de archivos queremos utilizar este tipo de borrado. Sólo será necesario o recomendable para los documentos de carácter

más confidencial de nuestra empresa. Se trataría de llevar a lo digital las prácticas que realizamos en la destrucción de documentación física en nuestras empresas.

Debemos estar seguro de qué documento borramos puesto que éste no podremos recuperarlo.