RESOLUCIÓN ORGANIZACIONAL OGZ-0070 DE 2014

(agosto 29)

Diario Oficial No. 49.264 de 4 de septiembre de 2014

<Análisis jurídico en proceso>

CONTRALORÍA GENERAL DE LA REPÚBLICA

Por la cual se adopta el Instructivo de borrado seguro a través de formateo a bajo nivel en equipos de cómputo a dar de baja en la Contraloría General de la República.

LA CONTRALORA GENERAL DE LA REPÚBLICA,

en ejercicio de sus facultades constitucionales y legales, en especial las contenidas en el numeral 2 del artículo 35 del Decreto 267 de 2000 y,

CONSIDERANDO:

Que de conformidad con el artículo 6o del Decreto 267 de 2000, la Contraloría General de la República en ejercicio de su autonomía administrativa, debe definir todos los aspectos relacionados con el cumplimiento de sus funciones, en armonía con los principios consagrados en la Constitución Política.

Que el numeral 2 del artículo 35 del Decreto 267 de 2000 establece como función del Contralor General de la República la de “Adoptar las políticas, planes, programas y estrategias necesarias para el adecuado manejo administrativo y financiero de la Contraloría General de la República, en desarrollo de la autonomía administrativa y presupuestal otorgada por la Constitución y la ley”.

Que la Resolución Organizacional número OGZ-0001-2014 de fecha 3 de abril de 2014 “Por la cual se crea el Sistema de Información y Producción Normativa de Control Fiscal (SINOR) y se establece el procedimiento para la expedición de resoluciones de competencia de la Contraloría General de la República” establece en el numeral 3.5. del artículo 5o que a través de los actos administrativos denominados resoluciones organizacionales se regulan “asuntos internos o de funcionamiento de la Contraloría General de la República”.

Que el Consejo Nacional de Política Económica y Social de la República de Colombia mediante Documento Conpes 3701 del 14 de julio de 2011 fijó los lineamientos de la política para ciberseguridad y ciberdefensa, buscando generar mecanismos efectivos que permitan garantizar la seguridad de la información a nivel nacional.

Que a través de la Estrategia 2.0. del Programa Gobierno en Línea el Estado Colombiano adopta un modelo de seguridad de información basado en la necesidad de reconocer la seguridad informática como un factor primordial para la apropiación de las TIC a través de la aplicación de la norma técnica NTC: ISO/IEC 27001:2005.

Que a través del Sistema Integrado de Gestión y Control (SIGC) la Contralora General estableció el Plan Estratégico para la vigencia 2010-2014 denominado “Por un control fiscal oportuno y efectivo”, en el cual se fijó como visión de la Entidad la de “ser un referente a nivel nacional e internacional de transparencia, eficiencia y efectividad en la vigilancia y el control fiscal; con

recurso humano competente, ético e innovador, pionera en el desarrollo técnico y tecnológico; que genere en la ciudadanía confianza y credibilidad, sea promotora de transparencia, y contribuya al desarrollo de la ética pública y de las mejores prácticas de la gestión pública".

Que en Acta número 003 de fecha 29 de mayo de 2013 el Comité Directivo de la Contraloría General de la República aprobó la "Política de Seguridad de la Información", documento que contiene los criterios necesarios para garantizar en la Entidad la gestión y la administración de la información de forma segura con fundamento en los estándares internacionales de aseguramiento de activos tecnológicos e informáticos definidos por la Organización Internacional de Normalización (ISO).

Que la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (USATI), adscrita al Despacho del Contralor General, fue creada en virtud del artículo 128 de la Ley 1474 de 2011, reglamentada mediante Resolución Reglamentaria número 205 del 19 de diciembre de 2012, modificada por la Resolución Ordinaria número 7341 de 2013, con el fin principal de prestar apoyo profesional y técnico para la formulación y ejecución de las políticas y programas de seguridad de los servidores públicos, de los bienes y de la información de la entidad, así como llevar el inventario y garantizar el uso adecuado y mantenimiento de los equipos de seguridad adquiridos o administrados por la Contraloría; promover la celebración de convenios con entidades u organismos nacionales e internacionales para garantizar la protección de las personas, la custodia de los bienes y la confidencialidad e integridad de los datos manejados por la institución.

Que en desarrollo de sus funciones y de conformidad con la "Política de Seguridad de la Información", la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (Usati) evidenció la necesidad de crear un procedimiento para el borrado seguro de la información contenida en aquellos recursos informáticos de la Contraloría General de la República a ser dados de baja, a efectos de dar cabal cumplimiento a los deberes de custodia, cuidado y manejo exigidos por la ley.

Que la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (Usati) es la responsable de implementar los controles recomendados en la norma técnica colombiana NTC:ISO/IEC 27001:2005, así como a los anexos con derechos reservados por parte de ISO e Icontec que para este caso en específico corresponden a los controles 9. Seguridad Física y del Entorno/9.2. Seguridad de los equipos/9.2.6. Seguridad en la reutilización o eliminación de equipos de la norma.

Que a través de la presente resolución, se adoptará dentro del Sistema Integrado de Gestión y Control de Calidad (SIGCC) – Código: 80014/80018 – Versión 1.0 de fecha 1o de enero de 2014 el "Instructivo de borrado seguro a través de formateo a bajo nivel en equipos de cómputo para dar de baja en la Contraloría General de la República", documento elaborado conjuntamente por la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (Usati) y la Oficina de Sistemas e Informática (OSEI).

En mérito de lo expuesto;

RESUELVE:

ARTÍCULO 1o. Adoptar el "Instructivo de borrado seguro a través de formateo a bajo nivel en equipos de cómputo a dar de baja en la Contraloría General de la República", procedimiento mediante el cual se eliminará de forma segura de los dispositivos informáticos a ser dados de

baja en la Entidad, todo tipo de información institucional privilegiada, confidencial o sensible contenida en estos.

ARTÍCULO 2o. Asignar a la Oficina de Sistemas e Informática (OSEI) en conjunto con la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (Usati) la labor de evaluar y determinar con una periodicidad anual si las herramientas informáticas utilizadas en el proceso de borrado seguro requieren ser actualizadas acorde a la evolución de las TIC.

ARTÍCULO 3o. Otorgar a la Oficina de Sistemas e Informática (OSEI) y a la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (Usati) la potestad de actualizar, cuando a ello haya lugar y de conformidad con los resultados de la evaluación de que trata el artículo precedente, el "Instructivo de borrado seguro a través de formateo a bajo nivel en equipos de cómputo a dar de baja en la Contraloría General de la República".

PARÁGRAFO. La actualización del Instructivo no requerirá de acto administrativo que lo ordene, por tanto la Versión 1.0. adjunta a la presente resolución, así como las versiones que lo modifiquen, harán parte integral de la presente resolución.

ARTÍCULO 4o. Encargar a la Oficina de Sistemas e Informática (OSEI) y a la Dirección de Recursos Físicos de generar el Instructivo para la baja de equipos informáticos, el cual deberá estar acorde con la presente resolución, la Directiva Presidencial número 004 de 2012 (Eficiencia administrativa y lineamientos de la política cero papel en la administración pública), las políticas de Gobierno en Línea, los Lineamientos ITIL (Information Technology Infrastructure Library) y el Sistema Integrado de Gestión y Control de Calidad de la Contraloría General de la República.

ARTÍCULO 5o. La presente resolución rige a partir de su publicación y deroga todas las demás disposiciones que le sean contrarias.

Comuníquese, publíquese y cúmplase.

Dada en Bogotá D. C., a los veintinueve (29) días del mes de agosto de 2014.

La Contralora General de la República,

SANDRA MORELLI RICO.

SISTEMA INTEGRADO DE GESTIÓN Y CONTROL DE CALIDAD (SIGCC).

GESTIÓN DE RECURSOS DE LA ENTIDAD (GRE)

ADMINISTRACIÓN DE RECURSOS INFORMÁTICOS

INSTRUCTIVO DE BORRADO SEGURO A TRAVÉS DE FORMATEO A BAJO NIVEL EN EQUIPOS DE CÓMPUTO PARA DAR DE BAJA

INSTRUCTIVO DE BORRADO SEGURO A TRAVÉS DE FORMATEO A BAJO NIVEL EN EQUIPOS DE CÓMPUTO PARA DAR DE BAJA EN LA CONTRALORÍA GENERAL DE LA REPÚBLICA

CONTRALORÍA GENERAL DE LA REPÚBLICA

Unidad de Seguridad y Aseguramiento Tecnológico e Informático Oficina de Sistemas e Informática

USATI-OSEI

2014

TABLA DE CONTENIDO.

1. JUSTIFICACIÓN.

En la actualidad la desafectación segura de equipos así como la eliminación segura de información confidencial, privilegiada o sensibles, constituye un acto igual de importante que su almacenamiento de forma correcta y la restricción del acceso a esta, ya que de lo contrario esos datos confidenciales que han dejado de ser útiles pueden llegar a manos malintencionadas. Este trabajo, pretende resaltar la importancia de la gestión de recursos que ya no van a ser utilizados, no solo buscando el interés propio sino también no perjudicar a terceros

2. OBJETIVO.

3. GENERAL.

El ciclo de vida de la información consta de tres etapas: generación, conservación y destrucción. El objetivo principal de este trabajo se centra en la última fase de este proceso, en concreto la destrucción o eliminación de datos confidenciales, privilegiados o sensibles, no permitiendo que estos se puedan recuperar posteriormente. Estableciendo el manual de borrado seguro para los equipos a dar de baja.

4. ESPECÍFICOS.

-- Mitigar los riesgos relacionados con el acceso no autorizado y la confidencialidad de la información institucional.

-- Cumplir con los deberes de custodiar y cuidar, previstos en el Código Disciplinario Único.

-- Dar cumplimiento a los controles recomendados en la norma técnica colombiana NTC:ISO/IEC 27001:2005, relacionados con Seguridad Física y del Entorno, Seguridad de los equipos. Seguridad en la reutilización o eliminación de equipos de la norma.

5. GLOSARIO.

-- Hard Disk: En informática, un disco duro o disco rígido (en inglés Hard Disk) es un dispositivo de almacenamiento de datos no volátil que emplea un sistema de grabación para almacenar datos digitales.

-- Low Leve/Format: En informática, formato de bajo nivel (en inglés low-level format), este término se utiliza para lo que podría llamarse la reinicialización de un disco duro a su configuración de fábrica.

-- Backup: Una copia de seguridad, copia de respaldo o backup (su nombre en inglés) en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

-- Booteo: En informática, la secuencia de arranque, (boot o booting en inglés) es el proceso que inicia el sistema operativo cuando el usuario enciende una computadora. Se encarga de la inicialización del sistema y de los dispositivos.

-- Dar de baja un equipo: Sacar de producción, por daño, deterioro u obsolescencia tecnológica, un computador, disco duro y/o medio de almacenamiento removible. El equipo en cuestión, NO SERÁ utilizado más en la organización. El destino final es: La basura, o la venta (a un usuario o por chatarra)

6. ALCANCE.

Los equipos que se den de baja o se reciclen pueden contener información confidencial susceptible de ser recuperada por los nuevos propietarios. Esto aplica a computadores completos, discos duros, unidades de cinta y en general a cualquier medio de almacenamiento secundario. Antes de dar de baja un equipo o una parte, es responsabilidad de la dirección de sistemas garantizar que no hay información recuperable en dicha máquina o parte.

7. MARCO LEGAL.

Constitución Política de Colombia

Ley 734 de 2002 Código Disciplinario Único.

Ley estatutaria 1266 de 2008 hábeas data

Ley 1341 de 2009 Organización de las Tecnologías de la Información y las Comunicaciones

Ley 1450 de 2011 Plan Nacional de Desarrollo, 2010-2014.

Ley Estatutaria 1581 de 2012 protección de datos personales.

Decreto de Gobierno en línea (Decreto 2693 de 2012)

Manual 3.1 para la implementación de la Estrategia de Gobierno en línea Entidades del Orden Nacional.

8. DESARROLLO.

Consideraciones técnicas

Tecnología:

Para el borrado seguro de los equipos de cómputo que van a ser destinados para el proceso de bajas, se utilizará la herramienta gratuita Hard Disk Low Leve/**Format Tool**, la cual permite borrar la totalidad de la información contenida en el disco duro, independiente de las particiones que contenga ya que realiza un arranque virtual a través de Live CD.

En tal sentido, no se requerirá conexión a internet para realizar el proceso de borrado seguro; de igual manera, no se instalará ningún software en los discos duros, por lo cual no es requerido conocer el usuario y contraseña del equipo de cómputo para realizar el procedimiento como tal.

Requisitos mínimos para el borrado seguro:

a) Backup de la información, generado en el equipo de cómputo al cual se realizará el procedimiento de borrado seguro.

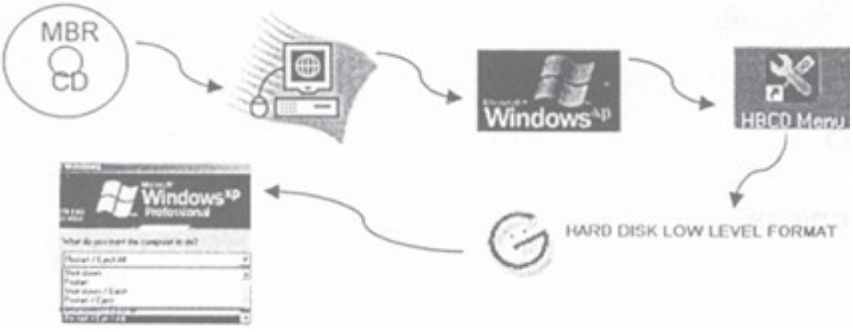
b) CD de gestión del MBR Master Boot Record.

c) Unidad de CD externa, si el equipo de cómputo no tiene.

Recuerde hacer backup de la información y ponerla a disposición del funcionario al cual pertenecía el equipo de cómputo que va a dar de baja.

9. PASO A PASO.

9.1. Esquema General



9.2. Descripción del proceso

Paso 1:

Booteo a través de CD. Inserte el CD en la unidad de CD; a través de las teclas de función que encuentra en el teclado (teclas F1 a F12), ingrese al menú de inicio del equipo de cómputo (boot

menú); para ello, prenda el equipo de cómputo y observe la parte inferior izquierda, en la cual se informará cuál es la tecla de acceso al booteo.

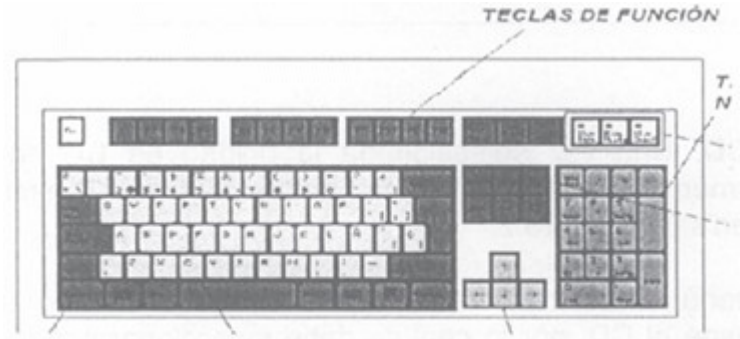


Imagen 1 – Teclas de función en el teclado.

Si no genera ese mensaje, reinicie el equipo tantas veces como lo requiera, y pruebe con las teclas F7, F8, F9 y F10 hasta que ingrese al menú de booteo.

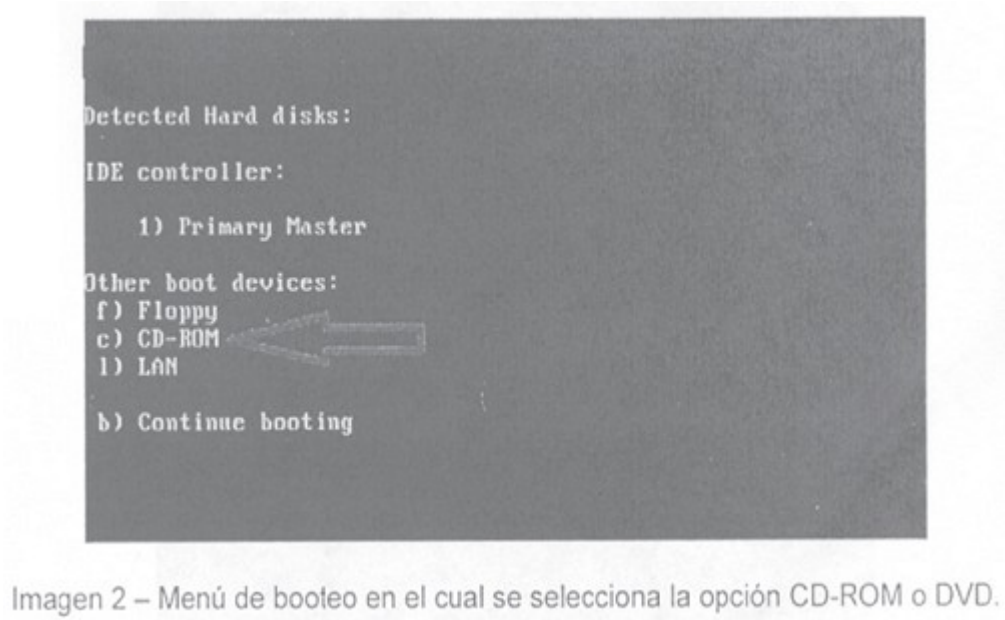


Imagen 2 – Menú de booteo en el cual se selecciona la opción CD-ROM o DVD.

Seleccione el booteo a través de CD-ROM, a fin de iniciar el CD Live y acceder al módulo del sistema requerido.

Si el CD no es reconocido por el equipo de cómputo, o este no tiene unidad de CD, conecte la unidad externa de CD, reinicie el equipo de cómputo y revise que en el menú de booteo se muestre esta nueva unidad.

Paso 2:

Ingreso al Live CD. Una vez seleccionada la unidad de CD en la cual ha insertado el CD, comenzará a ejecutar los comandos del Live CD hasta mostrar el menú inicial de Hiren›s BootCD 15.2.

Dentro de este menú, encontrará varias opciones de inicio; no obstante, es requerido iniciar desde el CD, por lo cual se debe seleccionar con las flechas de dirección del teclado la opción Mini Windows XP y presionar Enter.

Esto cargará un sistema operativo emulado de Windows XP, con las mínimas funcionalidades que son requeridas.

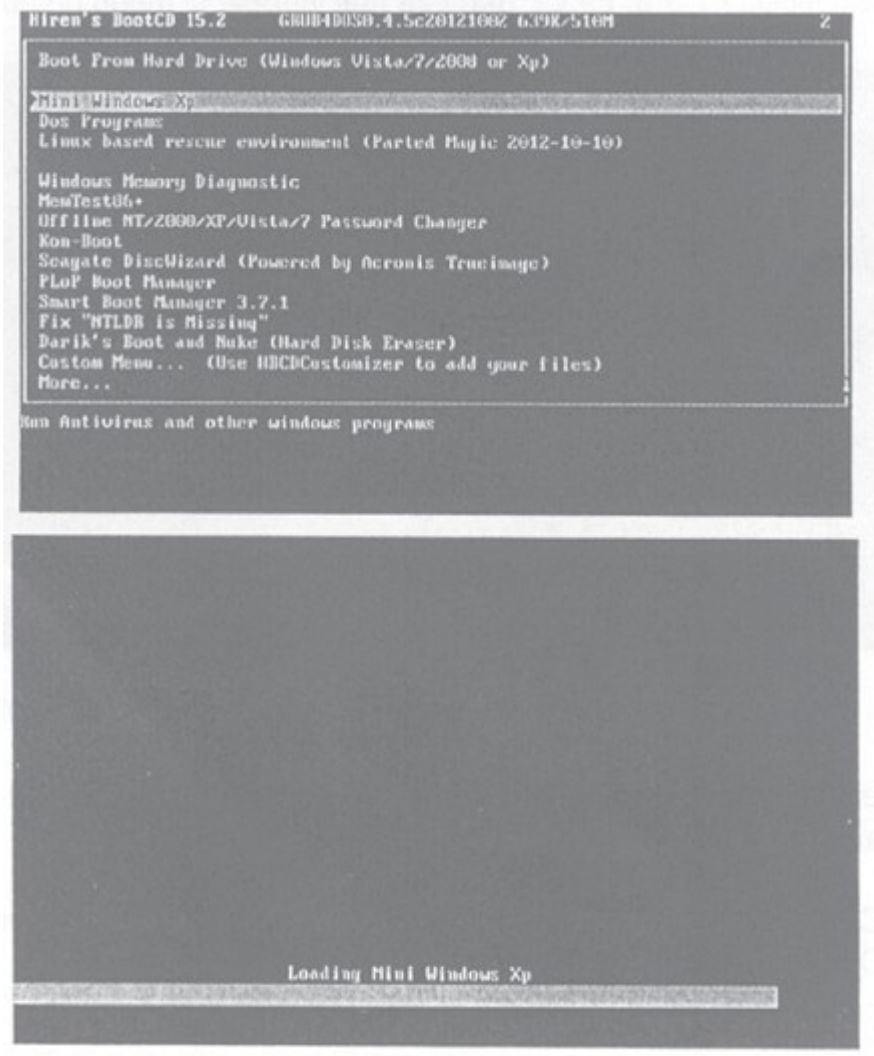


Imagen 3 – Selección y cargue de Mini Windows XP.

Paso 3:

Acceso al lanzador de programas de Hiren›s BootCD. Una vez ha ingresado a la versión ligera de Mini Windows XP, observará los íconos de acceso directo a los respectivos módulos de configuración del sistema.

Allí se debe seleccionar el ícono 

a fin de acceder al menú principal de los programas que contiene el CD, para que se puedan seleccionar de manera visual, bajo un Sistema Operativo conocido.

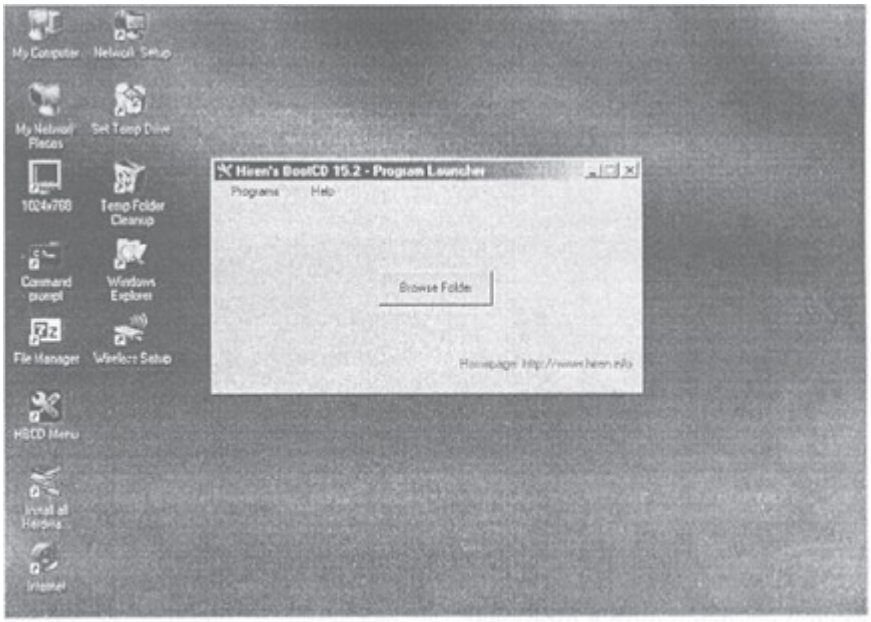


Imagen 4 – Acceso al menú principal de Hiren's BootCD.

Paso 4:

Acceso al módulo **Hard Disk Low Level Format Tool.** Ingrese al menú Programs y allí ubique el menú **Hard Disk/ Storage;** dentro de este menú encontrará el acceso al aplicativo **HDD Low Level Format,** al cual debe dar clic

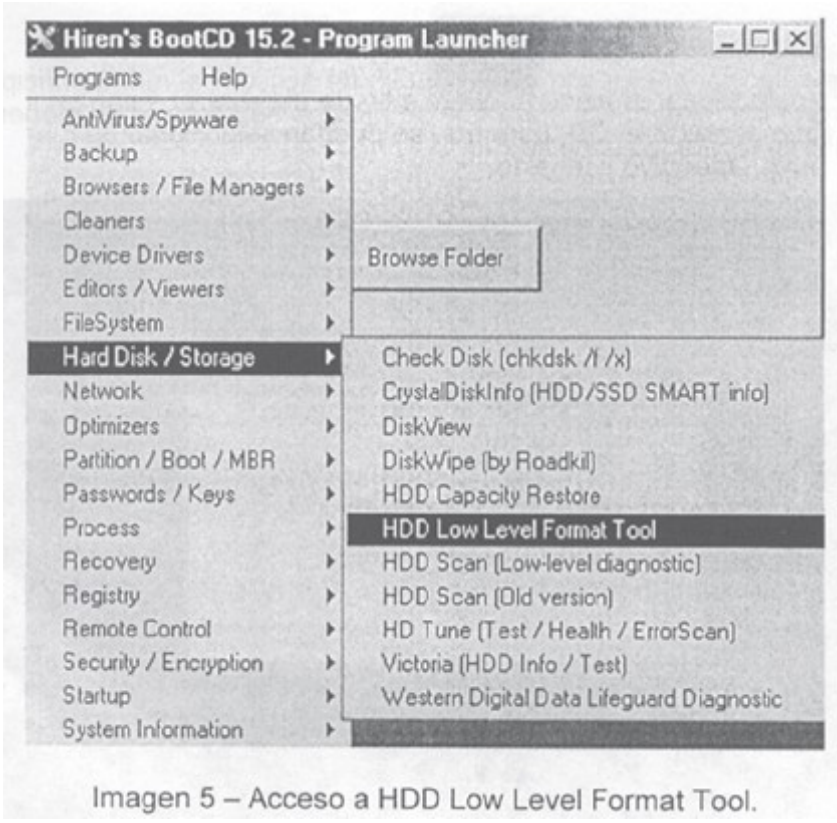


Imagen 5 – Acceso a HDD Low Level Format Tool.

Paso 5:

Selección del disco duro a formatear. Una vez acceda al aplicativo, se mostrará el disco duro físico o discos duros físicos; seleccione uno de ellos, y dé clic en el botón continue>> (Para el

ejemplo, el disco duro seleccionado es de 21.4Gb).

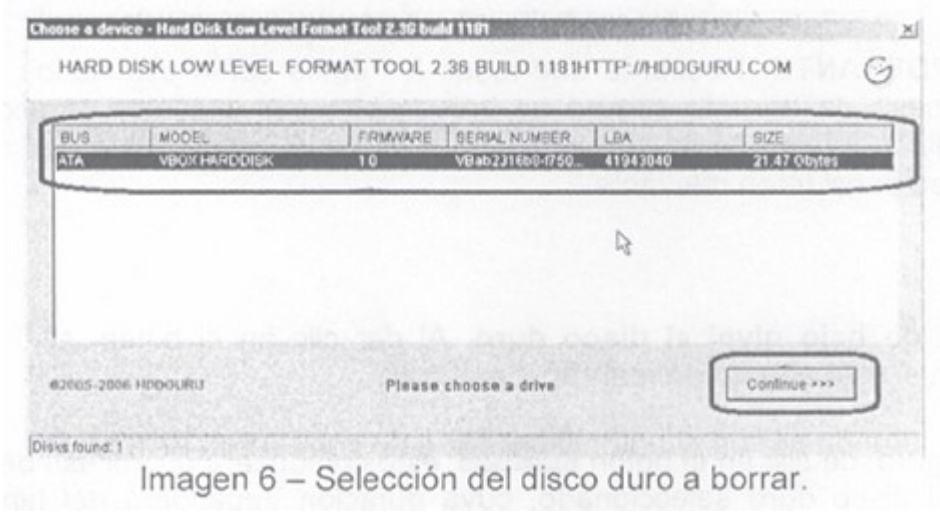


Imagen 6 – Selección del disco duro a borrar.

Paso 6:

Selección del formateo de bajo nivel. El sistema despliega una ventana con varias pestañas: la primera, contiene información sobre el Disco Duro físico, mientras que la segunda brinda el acceso al formateo de bajo nivel.

Vaya a la pestaña LOW-LWVEL FORMAT y dé clic en el botón FORTMAT THIS DEVICE puede aparecer movida la ventana, observando medio botón únicamente)

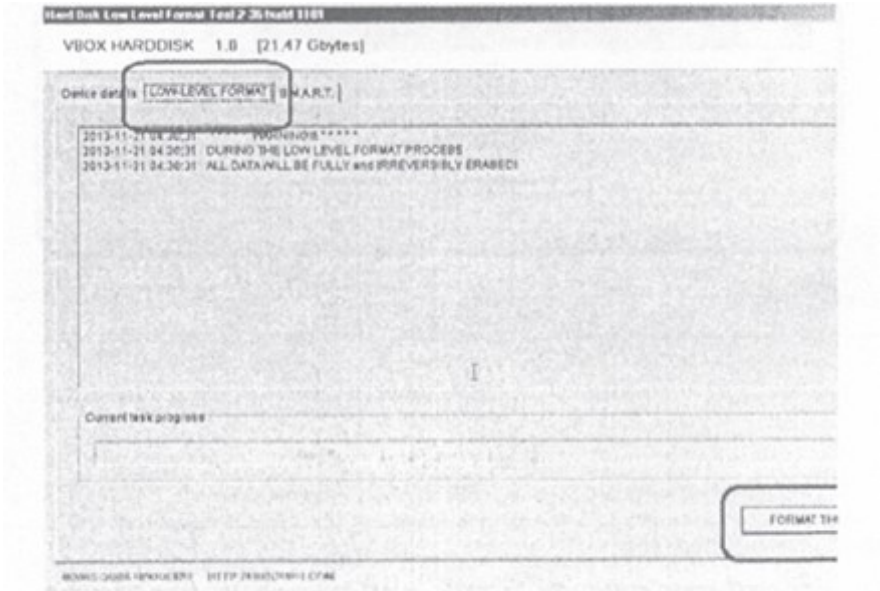


Imagen 7 – Selección del formateo de bajo nivel.

IMPORTANTE: Recuerde que todos los datos serán eliminados, y que el proceso de borrado seguro es irreversible; por lo tanto, es aconsejable realizar backup de la información que el usuario del equipo de cómputo o usted consideren relevante.

Paso 7:

Formateo de bajo nivel al disco duro. Al dar clic en el botón, el Sistema le preguntará si está seguro de realizar el proceso.

Si está seguro, dé clic en el botón Yes esto comenzará el proceso de borrado seguro del disco duro seleccionado, cuya duración dependerá del tamaño del disco (para un disco de 80 Gb, el proceso demora aproximadamente 40 minutos en concluir).

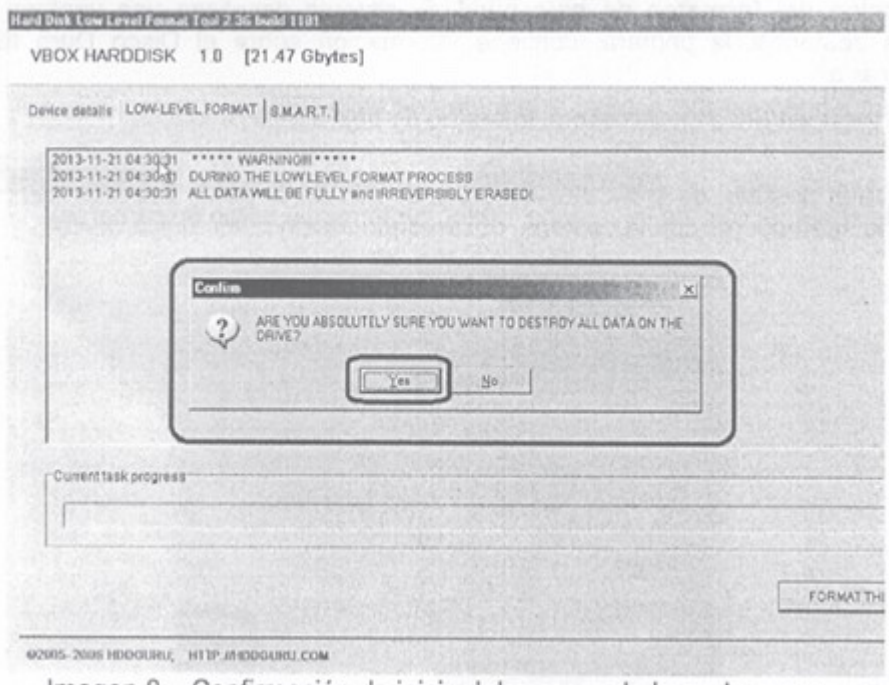


Imagen 8 – Confirmación de inicio del proceso de borrado seguro.

A medida que el proceso se desarrolla, observará una barra de estado azul en la parte inferior de la pantalla; esta se completará cuando el proceso de borrado seguro haya terminado.

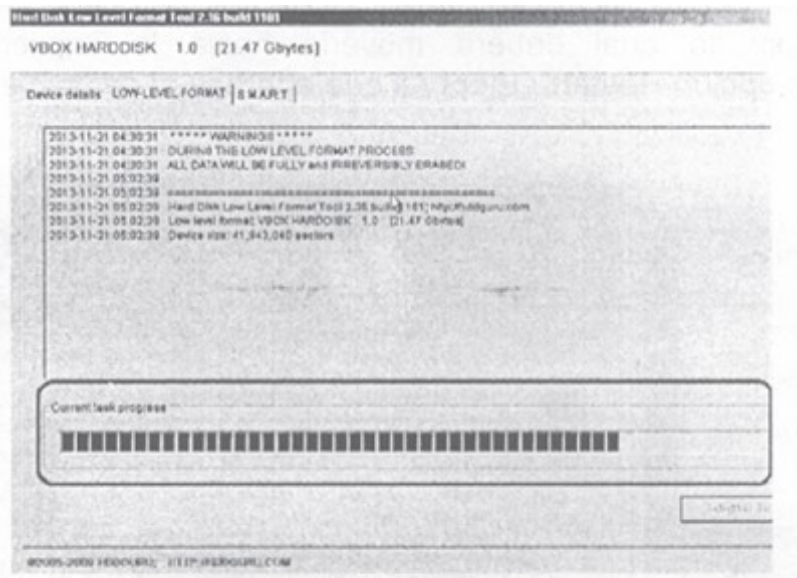


Imagen 9 – Avance del proceso de borrado seguro.

Espere hasta que termine el proceso, momento en el cual el Sistema le informará que el formateo de bajo nivel ya fue realizado, y que se pueden crear particiones y formatear el disco duro.

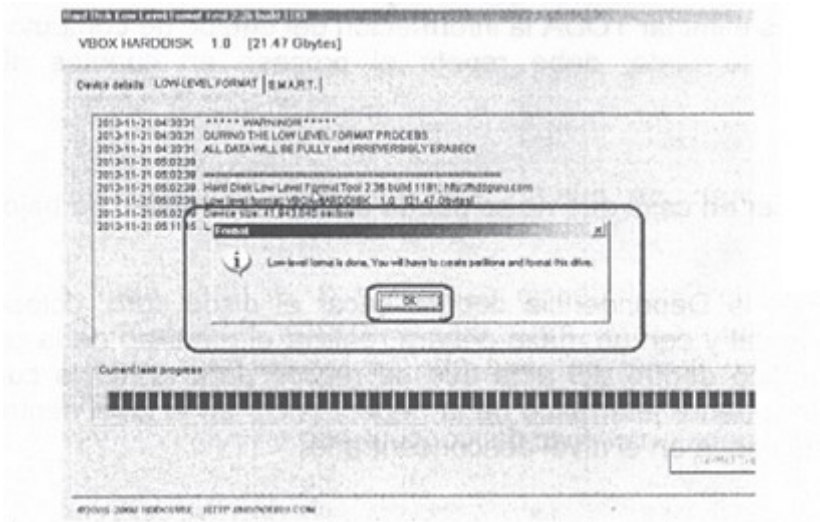


Imagen 10 – Finalización del proceso de borrado seguro.

Dé clic en el botón OK, cierre el aplicativo dando clic en la X que encuentra en la parte superior derecha del aplicativo (recuerde que puede mostrarse corrido el aplicativo, por lo cual deberá moverlo hacia la izquierda) y reinicie seleccionando a opción Restart/Eject All que aparece al dar clic en el botón Start / Shut Down

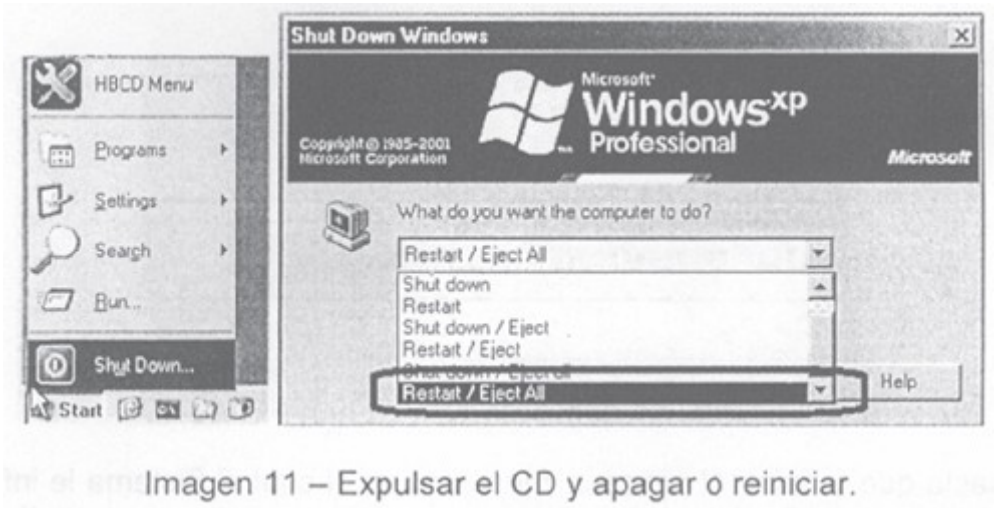


Imagen 11 – Expulsar el CD y apagar o reiniciar.

IMPORTANTE: Recuerde que el objetivo de realizar el proceso de borrado seguro, es eliminar TODA la información del equipo de cómputo para dar de baja; por lo tanto, debe repetir el proceso en cuantos discos duros aparezcan.

9.3. Qué hacer en caso que no se pueda aplicar el formateo de bajo nivel

El tecnólogo de la Dependencia deberá sacar el disco duro, colocarlo en una superficie de metal y con un mazo deberá realizar el martilleo de la caja, dejando registro fotográfico dentro del acta que se realice para tal fin la cual debe ser suscrita por el superior jerárquico de la dependencia en el nivel central, o por los Directivos Colegiados en el nivel desconcentrado.

10. CONTÁCTENOS.

Si tiene dudas o inquietudes sobre el aspecto técnico, contáctenos:

mesadeayuda@contraloria.gov.co

(1) 6 47 70 00 Ext. 1225

Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.
Normograma del Ministerio de Relaciones Exteriores
ISSN 2256-1633
Última actualización: 31 de marzo de 2018