

 <p>Unidad para las <b>Víctimas</b></p>	<b>GUÍA DE USO DE DISCOS DUROS CIFRADOS POR HARDWARE</b>	Código: 130.06.04-2
	PROCESO GESTIÓN DE LA INFORMACIÓN	Versión: 01
	PROCEDIMIENTO: GESTIÓN DE PRÉSTAMO DE DISCOS DUROS CIFRADOS	Fecha: 27/12/2017 Página <b>1</b> de <b>5</b>

### 1. OBJETIVO:

El objetivo de esta guía es dar las indicaciones para el buen uso de los discos duros cifrados por hardware, con el fin de proteger la información almacenada.

### 2. ALCANCE:

Esta guía está dirigida a los usuarios a quienes les ha sido asignado un disco duro cifrado, en ella podrá encontrar las generalidades asociadas a su uso, tales como: conectar el disco duro cifrado al equipo de escritorio, utilización del cable extensor, descripción del panel de actividades y descripción de la función bloquear y desbloquear el disco duro cifrado.

### 3. DEFINICIONES:

**Bloquear:** Propiedad con la cual el disco duro cifrado impide el acceso al equipo de escritorio, garantizando la confidencialidad de la información. Para desbloquearlo es necesario escribir la contraseña de la cuenta de usuario.

**Cifrado por hardware:** Es una tecnología utilizada para proteger la información, de manera que la transforma en un código ilegible que no puede ser descifrado con facilidad usando un hardware de encriptación para cifrar la información que va en un disco, evitando el acceso no autorizado a información almacenada y protegiendo el dispositivo contra ataques de arranque en frío, fuerza bruta y códigos maliciosos

**Confidencialidad:** Principio de seguridad de la información que garantiza que la información esté disponible únicamente, para las personas autorizadas. Estará protegida de la no divulgación.

**Disco Duro Extraíble Cifrado:** Medio de almacenamiento removible con un mecanismo de seguridad el cual permite cifrar la información almacenada dejándola no legible, de tal forma que, en caso de interceptación o robo, se mitigue el riesgo de uso y/o divulgación no autorizada de la misma al no tener la clave correspondiente o llave de acceso.

**Fuerza bruta:** Forma de recuperar una clave intentando todas las combinaciones posibles.

**Hibernar:** Esta opción es similar a suspender, la diferencia radica en que el ordenador guarda los archivos abiertos y el estado de sus programas ejecutados en el disco duro en vez de la memoria, apagando el equipo completamente. Cuando el equipo es encendido nuevamente, es recuperada la información del disco duro y restaura la sesión anterior.

**LED:** Diodo que emite luz. En el dispositivo se encuentra entre los símbolos desbloqueo  y bloqueo 

**AEGIS:** Marca comercial de los discos duros extraíbles adquiridos por La Unidad para la Atención y Reparación Integral a las Víctimas.

**PIN:** Contraseña o clave, forma de autenticación de información. La contraseña del disco debe cumplir con una longitud entre 7 a 16 dígitos, no puede contener números consecutivos (2345678 o 9876543), no puede repetir el mismo número más de dos veces, no puede ser

 <b>Unidad para las Víctimas</b>	<b>GUÍA DE USO DE DISCOS DUROS CIFRADOS POR HARDWARE</b>	Código: 130.06.04-2
	PROCESO GESTIÓN DE LA INFORMACIÓN	Versión: 01
	PROCEDIMIENTO: GESTIÓN DE PRÉSTAMO DE DISCOS DUROS CIFRADOS	Fecha: 27/12/2017 Página <b>2</b> de <b>5</b>

una contraseña de fácil deducción (fechas de nacimiento, número de teléfono, placas de vehículos, números de identificación personal etc.).

**SUSPENDER:** Opción de ahorro de energía del ordenador con la cual puede proteger el trabajo, ya que guarda los archivos abiertos, graba el estado de los programas que se están ejecutando en la memoria. Cuando el equipo vuelve a estar activo, necesita solo algunos segundos, para recuperar la información desde la memoria

#### 4. ACTIVIDADES:



**Generalidades:** El disco duro extraíble cifrado por hardware está diseñado para buscar un nivel más alto de seguridad. Cuenta con un diseño de teclado fácil de usar que es impermeable al polvo y partículas, con una configuración y operación de software libre, que le permite acceder a la unidad de forma fácil y sencilla con un PIN único.

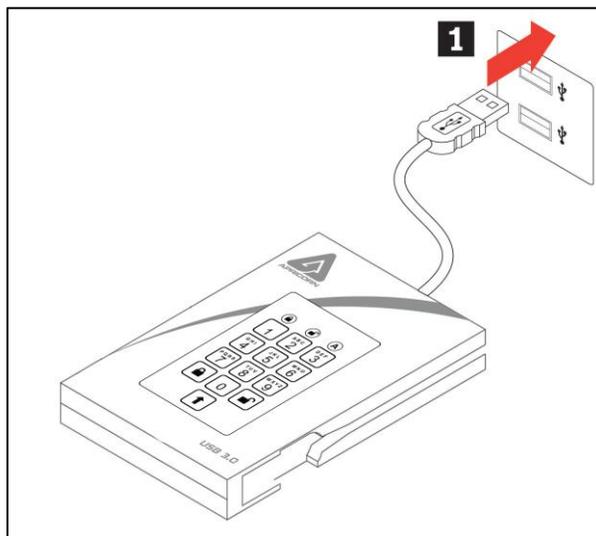
Nota: Recuerde guardar su PIN en un lugar seguro. Si se pierde u olvida, no hay manera de acceder al dispositivo.

##### 4.1. VERIFICAR LOS ACCESORIOS DEL DISCO DURO CIFRADO

Debe revisar la siguiente información antes de empezar a usar el dispositivo: Use solo los cables incluidos con el disco, ya que podría dañar el dispositivo si utiliza cables diferentes. El dispositivo está diseñado, para uso portátil sin necesidad de adaptadores externos de corriente alterna, en la mayoría de los casos será capaz de transferir la información con un solo puerto USB.

 <p>Unidad para las <b>Víctimas</b></p>	<b>GUÍA DE USO DE DISCOS DUROS CIFRADOS POR HARDWARE</b>	Código: 130.06.04-2
	PROCESO GESTIÓN DE LA INFORMACIÓN	Versión: 01
	PROCEDIMIENTO: GESTIÓN DE PRÉSTAMO DE DISCOS DUROS CIFRADOS	Fecha: 27/12/2017
		Página <b>3</b> de <b>5</b>

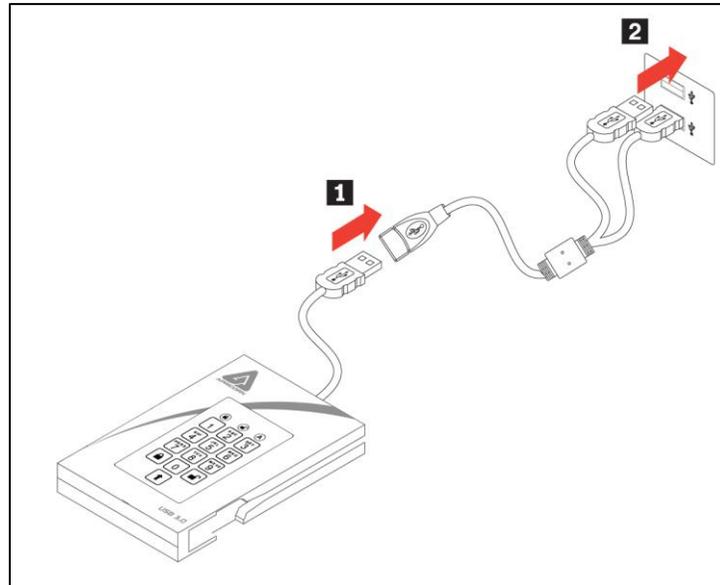
## 4.2. CONEXIÓN DEL DISCO DURO



1. Conecte el cable USB integrado al disco a un puerto USB disponible en su computadora, como se muestra en la imagen anterior. Si bien el funciona con cualquier puerto USB, para obtener las velocidades más rápidas, conéctese a un puerto USB 3.0 en su computadora.

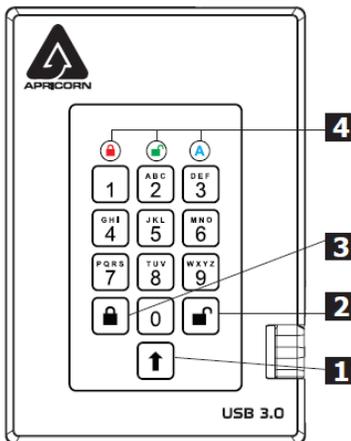
2. Al menos uno de los LED del debe encenderse, lo que indica que el disco está recibiendo energía. Si ninguno de los LED's se enciende, use el cable extensor que le fue entregado, de la siguiente forma:

1. Una el cable integrado del disco al conector hembra del cable USB extensor.
2. Conecte los dos conectores USB macho a dos puertos USB disponibles en su computador.
3. Al menos uno de los leds del dispositivo debe encenderse



### 4.3. PANEL DEL TECLADO

La siguiente imagen muestra la descripción de los botones e indicadores que se encuentran en el teclado del disco duro cifrado



- 1** Botón de SHIFT
- 2** Botón para Desbloquear
- 3** Botón para Bloquear
- 4** Indicadores LED

Cuando se conecta el dispositivo en el equipo de cómputo, la unidad va hacer su propia prueba, para verificar que los componentes estén trabajando correctamente.

Los LEDs pasaran por tres etapas (rojo, verde y azul). Cuando titila tres veces el LED de color verde la prueba fue exitosa, si es el caso contrario se encenderá varias veces el LED de color rojo

 <b>Unidad para las Víctimas</b>	<b>GUÍA DE USO DE DISCOS DUROS CIFRADOS POR HARDWARE</b>	Código: 130.06.04-2
	PROCESO GESTIÓN DE LA INFORMACIÓN	Versión: 01
	PROCEDIMIENTO: GESTIÓN DE PRÉSTAMO DE DISCOS DUROS CIFRADOS	Fecha: 27/12/2017 Página <b>5</b> de <b>5</b>

#### 4.4. BLOQUEAR EL DISCO DURO CIFRADO

Para bloquear el disco duro cifrado, debe hacer lo siguiente:

Pulse el botón de bloqueo  , si los datos todavía se están escribiendo, el dispositivo va a esperar hasta que todos los datos se hayan guardado correctamente en el disco duro y posteriormente se bloqueará.

**Nota:** El dispositivo no será reconocido por el sistema operativo en estado bloqueado.

#### 4.5. DESBLOQUEAR EL DISCO DURO CIFRADO

Ingrese la contraseña del usuario que estableció al momento en que le fue entregado el disco, pulse el botón de desbloqueo .

Nota: El dispositivo no será reconocido por el sistema operativo en estado bloqueado.

#### 4.6. BORRADO DE LA INFORMACIÓN DEL DISCO DURO CIFRADO

Seleccionar desde la ventana del explorador en la cual se visualizan los archivos que contiene el disco duro cifrado la información a eliminar y oprima la tecla SUPR del teclado del equipo de cómputo o de click derecho sobre los archivos seleccionados y en el menú emergente de click en eliminar.

Nota: Una vez eliminados los archivos, la información no puede ser recuperada.

### 5. ANEXOS

#### 6. Control de cambios

Versión	Fecha del cambio	Descripción de la modificación
1	27/12/2017	Creación del documento