

TOSHIBA

Leading Innovation >>>

Toshiba Encrypted USB Flash Drive User's Guide

594195-A0
GMAA00482010
06/14

Limitation of Liability

Toshiba assumes no liability for damage or losses due to fire, earthquake, third-party action or other accidents, the user's intent, negligence or misuse, or other kinds of use under unusual circumstances. Toshiba assumes no liability for damage or losses, lost profits or claims from third parties, etc. occurring from the use or inability to use, this product Toshiba assumes no liability for damage or losses occurring as a result of the manual instructions not being followed. Toshiba assumes no liability if destruction or loss of data occurs while using this product regardless of the cause or the type or scale of damage. Toshiba will not perform restoration or recovery of data. Toshiba assumes no liability for damage or losses occurring due to malfunctions, etc. resulting from a combination of connected devices and software not related to Toshiba.

FCC Information

FCC notice “Declaration of Conformity Information”

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- ❖ Reorient or relocate the receiving antenna.
- ❖ Increase the separation between the equipment and receiver.
- ❖ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- ❖ Consult the dealer or an experienced radio/TV technician for help.

NOTE

Changes or modifications made to this equipment, not expressly approved by TOSHIBA or parties authorized by TOSHIBA could void the user's authority to operate the equipment.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- 1 This device may not cause harmful interference.
- 2 This device must accept any interference received, including interference that may cause undesired operation.

IC Information

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

CE Compliance



This product is CE marked in accordance with the requirements of the applicable EU Directives. Responsible for CE marking is Toshiba Europe GmbH, Hammfelddamm 8, 41460 Neuss, Germany. A copy of the official Declaration of Conformity can be obtained from following website: <http://epps.toshiba-teg.com>.

Product specification, configurations, prices, system/component/options availability are all subject to change without notice. All other products and names are the property of their respective owners. Reseller/Retailer pricing may vary.

RoHS

This device is compatible with European Union Directive 2011/65/EU, Restriction of the use of certain Hazardous Substances in electrical and electronic equipment (RoHS), which restricts use of certain chemicals including, but not limited to, lead, cadmium, mercury, hexavalent chromium, PBB, and PBDE. Toshiba requires its computer component suppliers to meet RoHS requirements and verifies its suppliers' commitment to meeting RoHS requirements by conducting component sampling inspections during the product design approval process.

Copyright

This manual may not be reproduced in any form without the prior written permission of Toshiba. No liability is assumed with respect to the use of the information contained herein.

© 2014 by Toshiba America Information Systems, Inc. All rights reserved.

Notice

The information contained in this manual, including but not limited to any product specifications, is subject to change without notice.

TOSHIBA CORPORATION AND TOSHIBA AMERICA INFORMATION SYSTEMS, INC. (TOSHIBA) PROVIDES NO WARRANTY WITH REGARD TO THIS MANUAL OR ANY OTHER INFORMATION CONTAINED HEREIN AND HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH REGARD TO ANY OF THE FOREGOING. TOSHIBA ASSUMES NO LIABILITY FOR ANY DAMAGES INCURRED DIRECTLY OR INDIRECTLY FROM ANY TECHNICAL OR TYPOGRAPHICAL ERRORS OR OMISSIONS CONTAINED HEREIN OR FOR DISCREPANCIES BETWEEN THE PRODUCT AND THE MANUAL. IN NO EVENT SHALL TOSHIBA BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES, WHETHER BASED ON TORT, CONTRACT OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH THIS MANUAL OR ANY OTHER INFORMATION CONTAINED HEREIN OR THE USE THEREOF.

Trademarks

Microsoft, Outlook, Windows, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other brand and product names are trademarks or registered trademarks of their respective companies.

Safety icons

This manual contains safety instructions that must be observed to avoid potential hazards that could result in personal injuries, damage to your equipment, or loss of data. These safety cautions have been classified according to the seriousness of the risk, and icons highlight these instructions as follows:

⚠ DANGER Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.

⚠ WARNING Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

⚠ CAUTION Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

CAUTION Indicates a potentially hazardous situation which, if not avoided, may result in property damage.

NOTE Provides important information.

Contents

Introduction.....	8
Toshiba Encrypted USB Flash Drive features.....	9
LED indicators.....	10
Chapter 1: The User PIN.....	11
Changing the User PIN	11
Creating a new User PIN	12
Chapter 2: Unlocking and Locking the Flash Drive	14
How to Unlock the Flash Drive with a User PIN ..	14
How to Lock the Flash Drive.....	15
Chapter 3: Resetting the Flash Drive	16
How to Reset the Flash Drive	16
Chapter 4: Configuring the Flash Drive with Windows® after a Complete Reset	18
Configuring the Flash Drive.....	18
Chapter 5: Troubleshooting	21
Frequently asked questions.....	21
Chapter 6: Creating and Using the Admin PIN	23
Creating an Admin PIN	23

Unlocking the Flash Drive with an Admin PIN	25
Changing the Admin PIN	26
Index	28

Introduction

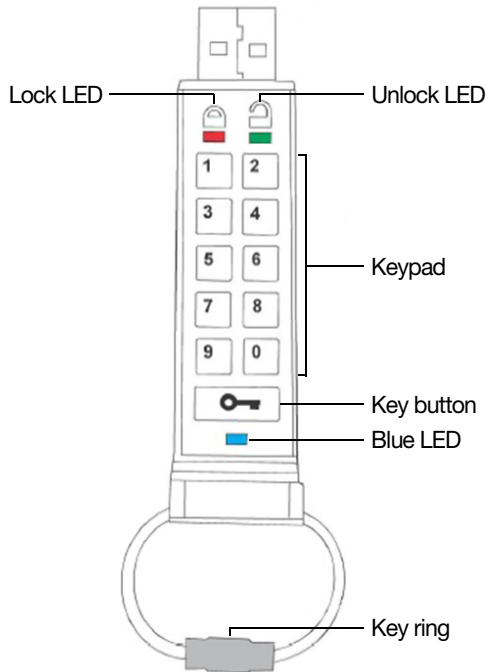
Thank you for purchasing the Toshiba Encrypted USB Flash Drive, a PIN activated, hardware Encrypted USB Flash Drive.

This Flash Drive uses military grade AES 256-bit hardware encryption, which encrypts all data stored on the Flash Drive in real-time. The Flash Drive requires no software and is OS and host independent. The Flash Drive incorporates a rechargeable battery allowing the user to enter a 7-15 digit PIN (Personal Identification Number) into the on-board keypad before connecting the Flash Drive to a USB port (e.g. on a computer). Should the Flash Drive get lost or stolen, the user can be assured that all data held on the Flash Drive is safe and cannot be accessed by any unauthorized person.

The Flash Drive can be Encrypted with both User and Admin PINs, making it perfect for corporate and government deployment.

As the Flash Drive is unlocked with the on-board keypad and not with the keyboard (e.g. on a computer), it is not vulnerable to software/hardware based key-loggers or brute force attacks.

Toshiba Encrypted USB Flash Drive features














(Sample Illustration) Features

Available LEDs and buttons:

- ❖ **Lock LED**—Standby with the Flash Drive locked
- ❖ **Unlock LED**—Flash Drive is unlocked when flashing
- ❖ **Keypad**—Use to enter PIN codes
- ❖ **Key button**—Allows you to activate the Flash Drive and enter PIN codes
- ❖ **Blue LED**—Illuminates when the Flash Drive is connected to a computer, and flashes when data is being transferred
- ❖ **Key ring**—Unscrew to add the Flash Drive to your key ring

LED indicators

	Blinking	The Flash Drive is unlocked, connect to a computer's USB port	 ON, solid	The Flash Drive is connected to a computer's USB port
	Blinking	The Flash Drive is locked	 ON, solid	The Flash Drive does not have a User PIN
	Blinking	Data is being transferred	 ON, solid	The Flash Drive is connected to a host computer
	Blinking alternately	Error	 ON, solid	The Flash Drive is accepting a new PIN code
	Blinking together	Accepting a User PIN	 Double-blinking	Accepting an Admin PIN
	Intensify	Security self testing		

CAUTION

Before disconnecting the Flash Drive, follow the user instructions of your laptop, computer or other compatible device for properly and safely ejecting USB drives. Disconnecting the USB drive from a device while data is being transferred may cause data corruption or loss.

NOTE



The Flash Drive's rechargeable battery will need to be charged prior to the first use. Connect the Flash Drive to a powered USB port (e.g. on a computer) for approximately 60 minutes to fully charge the battery.

NOTE

Unless otherwise noted, all INSTRUCTION steps need to be performed when the Flash Drive is not connected to a computer.

Chapter 1

The User PIN

The Flash Drive is shipped with the default User PIN  1-1-2-2-3-3-4-4  and although it can be used straight out of the box with the default PIN, for security reasons, it is highly recommended that you create a new User PIN immediately.

Changing the User PIN

CAUTION

If you forget your User PIN and no Admin PIN exists, or you forget both PINs, the Flash Drive will need to be reset and all data will be inaccessible. See [“How to Reset the Flash Drive”](#) on page 16.

NOTE

To protect against accidental data loss, back up your data frequently on multiple types of external storage media. With the passage of time, or after extended use, the Product may lose some or all of its functionality, including read/write and data deletion.














PIN requirements:

- ❖ Must be between 7-15 digits in length
- ❖ Must not contain repeating numbers/letters, (e.g. 3-3-3-3-3-3)

12 The User PIN

Creating a new User PIN

- ❖ Must not contain sequential numbers/letters, (e.g. 1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

Instructions	LED Activity	
1 Press the Key () button. 2 Enter the Default User PIN and press the Key () button.		LEDs blink together (factory default PIN: 1-1-2-2-3-3-4-4-4)
		LEDs illuminate together for approximately 4 seconds, and then:
		LED blinks to indicate a correct PIN entry
3 Press and hold the Key () button for approximately 3 seconds. 4 Enter a new PIN number (must be 7-15 digits).		LEDs are on
5 Press the Key () button to store the new PIN. 6 Re-enter the new PIN number.		LEDs illuminate together
7 Press the Key () button to confirm the new PIN.		LEDs illuminate together for approximately 4 seconds, and then:
		❖ LEDs blink if both PIN entries match. The Flash Drive is now ready to use.
		❖ LED blinks alternately if there is a PIN entry error. Return to step 3.

NOTE If a mistake is made while defining a new PIN or the procedure is not completed, the Flash Drive will retain the old PIN.

Creating a new User PIN










A new encryption key is automatically created under the following circumstances:

- ❖ After hacking detection has been triggered by 10 successive failed attempts to unlock
- ❖ The Flash Drive has been manually reset, see [“How to Reset the Flash Drive”](#) on page 16

When either of the above two scenarios occur, it will be necessary to create a new User PIN for the new Encryption key by following the instructions below.

User PIN requirements:

- ❖ Must be between 7-15 digits in length
- ❖ Must not contain repeating numbers/letters, (e.g. 3-3-3-3-3-3-3)
- ❖ Must not contain sequential numbers/letters, (e.g. 1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

Instructions	LED Activity	
1 Press and hold the Key () button for approximately 3 seconds.		LEDs are ON
2 Enter a new User PIN (must be 7-15 digits).		LEDs are ON
3 Press the Key () button to save.		LEDs blink together to indicate a correct PIN entry
4 Re-enter the new User PIN, and then press the Key () button.	  	LEDs illuminate together for approximately 4 seconds, and then: <ul style="list-style-type: none"> ❖ LED blinks to indicate a correct User PIN entry ❖ LEDs blink alternately if there is an Admin PIN entry error. Return to step 3.

NOTE










A user PIN can only be defined when the Red LED is lit in a constant state or changed when the Green LED is blinking (unlocked). User and Admin PINs cannot be created while the Flash Drive is connected to a host computer.

Chapter 2

Unlocking and Locking the Flash Drive

How to Unlock the Flash Drive with a User PIN

Once the User PIN is created, all data stored on the Flash Drive is encrypted, (in hardware) to the AES 256-bit CBC specification. In order to access the data stored on the Flash Drive, you must first unlock the Flash Drive with your User PIN, using the Flash Drive's keypad.

<i>Instructions</i>	<i>LED Activity</i>	
1 Press the Key () button.		LEDs blink together.
2 Enter your User PIN. (Factory default PIN: 1-1-2-2-3-3-4-4.)		
3 Press the Key () button.	  	LEDs illuminate together for approximately 4 seconds, and then: <ul style="list-style-type: none">❖ LED blinks to indicate correct PIN entry❖ LED blinks if an incorrect PIN is entered. Re-enter the PIN.
4 Insert your Flash Drive into the computer's USB port.	 	LED is ON LED is ON or blinks for activity

NOTE

Once unlocked, the Green LED blinks for approximately 30 seconds, within which time the Flash Drive needs to be connected to the computer's USB port. If no connection is detected within 30 seconds, the Flash Drive locks and you will need to start the process of unlocking it again. Return to step 1.

How to Lock the Flash Drive

The Toshiba Encrypted USB Flash Drive automatically locks when disconnected from the host computer or if the power to the USB port is turned off. Data is kept locked using AES 256-bit CBC encryption.

CAUTION

Before disconnecting the Flash Drive, follow the user instructions of your laptop, computer or other compatible device for properly and safely ejecting USB drives. Disconnecting the USB drive from a device while data is being transferred may cause data corruption or loss.

Chapter 3












Resetting the Flash Drive

How to Reset the Flash Drive

Follow the instructions in this chapter in the event that both the Admin and the User PIN have been forgotten, or if you would like to delete all data stored on the Flash Drive and create new User and Admin PINs. The reset process clears all PINs and encryption keys. This means a new User PIN will need to be defined in order to re-enable the Flash Drive. Also, since this will force the creation of a new encryption key, the Flash Drive must be reformatted, see [“Configuring the Flash Drive” on page 18](#).

NOTE To protect against accidental data loss, back up your data frequently on multiple types of external storage media. With the passage of time, or after extended use, the Product may lose some or all of its functionality, including read/write and data deletion.

CAUTION Resetting the Flash Drive renders all data on the Flash Drive inaccessible forever with no way to retrieve it. This may result in data loss.

<i>Instructions</i>	<i>LED Activity</i>	
1 Press the Key () button.		LEDs blink together
2 Press the Key () button again.		LED blinks
3 Press and hold the Key () button and the 2 () button for approximately 3 seconds.		LEDs blink together
4 Press the 9 () button 3 times (9-9-9), and then press the Key () button.		LEDs turn OFF
5 Press the Key () button.		LED is ON and solid

NOTE When the Red LED  is ON and solid, a new User PIN will need to be created prior to use.

Chapter 4

Configuring the Flash Drive with Windows[®] after a Complete Reset

Configuring the Flash Drive

In the event that hacking detection has been triggered by entering the incorrect PIN 10 times in succession or the Flash Drive has been reset, all data on the Flash Drive will be lost forever. Once a new User PIN has been created, the Flash Drive will need to be initialized and formatted.

NOTE To protect against accidental data loss, back up your data frequently on multiple types of external storage media. With the passage of time, or after extended use, the Product may lose some or all of its functionality, including read/write and data deletion.

To initialise your Flash Drive, perform the following procedure:

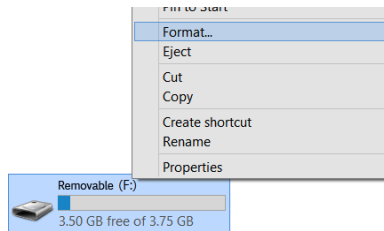
- 1 Create a new User PIN, see [“Creating a new User PIN” on page 12](#).
Entering the new User PIN and connecting to a computer unlocks the Flash Drive.
- 2 On the computer right-click or touch **My Computer**, and then click or touch **Manage**.

- 3 In the “Computer Management” window, click or touch **Disk Management**.

In the “Disk Management” window, the Flash Drive is recognized as a removable device in raw format.

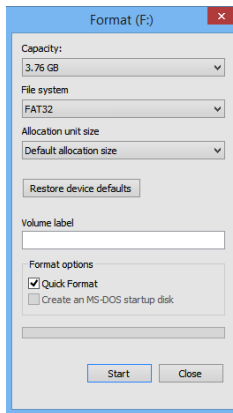
To have the Flash Drive recognized as a basic Flash Drive, perform the following procedure:

- 1 Right-click or touch **Removable Raw drive**, in the blank area under the unallocated section, and then select **Format**.



(Sample Image) Drive window

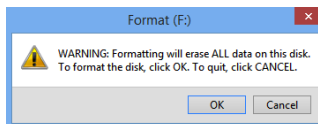
The “Format” window opens.



(Sample Image) Format window

- 2 Select **FAT32** or **NTFS** (depending on your requirements), and then click or touch **Start**.

The “Format warning” window appears.



(Sample Image) Format warning window

20 Configuring the Flash Drive with Windows® after a Complete Reset

- 3 Click or touch **OK**.

On the Flash Drive:

- ❖ The Blue LED flashes while the Flash Drive is formatting.
- ❖ The Blue LED is ON and solid when the process is finished. Your Flash Drive is now ready for use.

Chapter 5

Troubleshooting

Frequently asked questions

How do I unlock the Flash Drive if the battery is dead?

Your Toshiba Encrypted USB Flash Drive is supplied with a built-in rechargeable battery. If the battery is fully discharged, you may still continue to use the product by following the instructions below:

- 1** Connect the Flash Drive to a USB port on any computer.
- 2** While the Flash Drive is connected to the computer, enter the User or Admin PIN to unlock the Flash Drive.
- 3** While connected to the USB port, the internal battery automatically recharges. It is recommended that you keep the Flash Drive connected for approximately one (1) hour to fully charge the battery.

I forgot my PIN.

If you forget the User and/or Admin PINs, there is absolutely no way of gaining access to the data stored on the Flash Drive. There are no backdoors into the Flash Drive. You may continue to re-use the Flash Drive by resetting it, however by doing so all data previously stored on the Flash Drive will be lost.

See [“How to Reset the Flash Drive” on page 16](#) to reset the Flash Drive. Once that is done, the following occurs:

- ❖ The existing encryption key is deleted
- ❖ The original User and Admin PINs are deleted
- ❖ All data previously stored on the Flash Drive will be completely lost

I have detected a Brute Force Hack Defence Mechanism.

After 10 consecutive incorrect PIN attempts, the following occurs:

- ❖ The existing encryption key is deleted
- ❖ The User and Admin PINs are deleted
- ❖ All data previously stored on the Flash Drive will be completely lost

The Toshiba Encrypted USB Flash Drive, unlike other similar drives, is pre-loaded with an unlimited number of randomly generated encryption keys. Each time hacking is detected (i.e. the wrong PIN is entered a total of 10 consecutive times), the current encryption key is deleted and once a new User PIN is created the Flash Drive randomly generates a new encryption key. Because of this, the Flash Drive will have to be formatted after each time the defence mechanism is triggered.

Will unlocking the Flash Drive with the Admin PIN delete the User PIN?

Entering the Admin PIN to access a locked Flash Drive will clear the User PIN. If a user forgets their PIN, access to their Flash Drive is regained by defining a new user PIN. For security reasons, it is highly recommended that a new User PIN is created immediately once the Flash Drive has been unlocked using the Admin PIN.

The User PIN is deleted when:

- ❖ The Admin PIN is used to unlock the Flash Drive
- ❖ When the Admin PIN is changed

A new User PIN will need to be created.

Chapter 6

Creating and Using the Admin PIN

Creating an Admin PIN

An Admin PIN is a useful feature for corporate deployment, for example:

- ❖ Recovering data from the Flash Drive and configuring a new User PIN in the event an employee has forgotten their PIN
- ❖ Retrieving data from the Flash Drive if an employee leaves the company

NOTE











Entering the Admin PIN to access a locked Flash Drive will delete the User PIN. If you forget the PIN, access to the Flash Drive is regained by defining a new user PIN. For security reasons, it is highly recommended that you create a new User PIN immediately once the Flash Drive has been unlocked using the Admin PIN.

Admin PIN requirements:

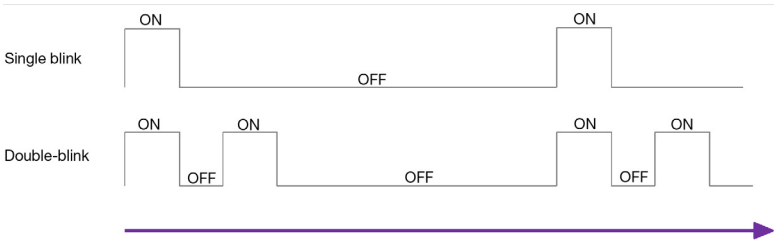
- ❖ Must be between 7-15 digits in length
- ❖ Must not contain repeating numbers/letters, (e.g. 3-3-3-3-3-3-3)
- ❖ Must not contain sequential numbers/letters, (e.g. 1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

24 Creating and Using the Admin PIN


If the Flash Drive has been reset or hacking detection has been triggered (i.e., no User or Admin PIN exists), follow the instructions in “Resetting the Flash Drive” on page 16. If a User PIN already exists, the Flash Drive must first be unlocked with the user PIN, see “How to Unlock the Flash Drive with a User PIN” on page 14. An Admin PIN can now be created by following instructions below:

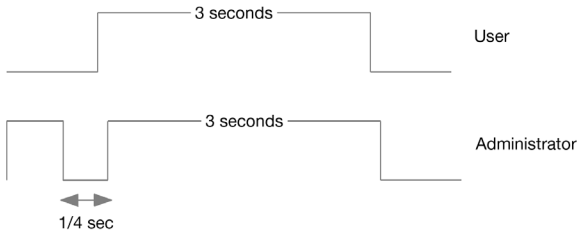
Instructions	LED Activity	
1 Press the Key () button two (2) times, holding the key for approximately 3 seconds on the 2 nd press.		LEDs blink one time, and then remain lit.
2 Enter a new Admin PIN (must be 7-15 digits).		LEDs are ON
3 Press the Key () button.		LEDs double-blink
4 Re-enter the new Admin PIN.		
5 Press the Key () button to confirm the new Admin PIN.	  	LEDs illuminate together for approximately 4 seconds, and then: <ul style="list-style-type: none">❖ LED blinks indicating correct Admin PIN entry❖ LEDs blink alternately if there is an Admin PIN entry error. Return to step 1.

The following image illustrates the Green LED blinking characteristics when the Flash Drive is opened in User mode vs. Admin mode.



(Sample Image) User mode single blink LED output vs. Admin mode double-blink









The following image illustrates the difference between pressing the **Key** () button to set the User PIN vs. setting the Admin PIN.



(Sample Image) Key entry for User/Admin mode selection

Unlocking the Flash Drive with an Admin PIN

NOTE Entering the Admin PIN to unlock the Flash Drive will delete the User PIN. For security reasons, it is recommended that a new User PIN is created immediately once the Flash Drive has been unlocked using the Admin PIN.

<i>Instructions</i>	<i>LED Activity</i>	
1 Double-press the Key () button.		LEDs double-blink together.
2 Enter the Admin PIN.		
3 Press the Key () button.	  	LEDs illuminate together, and then: <ul style="list-style-type: none"> ❖ LED double-blinks indicating a correct Admin PIN entry ❖ LED blinks if there is an Admin PIN entry error. Return to step 1.
4 Insert your Flash Drive into the computer's USB port within 30 seconds.		LED is ON
		LED is ON or blinks for activity

26 Creating and Using the Admin PIN

Changing the Admin PIN

NOTE The Green LED blinks for 30 seconds, within which time the Flash Drive needs to be connected to the computer's USB port. If no connection is detected within 30 seconds, the Flash Drive locks and you will need to start the process of unlocking it again. Return to step 1.








Changing the Admin PIN













NOTE To change the Admin PIN, the Flash Drive must first be unlocked with the Admin PIN, which will delete the User PIN. For security reasons, it is recommended that a new User PIN be created immediately once the Flash Drive has been unlocked using the Admin PIN.

Admin PIN requirements:

- ❖ Must be between 7-15 digits in length
- ❖ Must not contain repeating numbers/letters, (e.g. 3-3-3-3-3-3)
- ❖ Must not contain sequential numbers/letters, (e.g. 1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

Once an Admin PIN has been created, the Flash Drive needs to be unlocked by the administrator in order to change the Admin PIN. The Admin PIN *cannot* be changed from user mode.

Instructions	LED Activity	
1 Double-press the Key () button.		LEDs double-blink together
2 Enter the current Admin PIN.		LEDs illuminate together.
3 Press the Key () button.	  	LEDs illuminate together, and then: <ul style="list-style-type: none">❖ LED double-blinks indicating correct Admin PIN entry❖ LED blinks if there is an Admin PIN entry error. Return to step 1.

Instructions	LED Activity	
4 Press the Key () button two (2) times, holding the key for approximately 3 seconds on the 2 nd press.		LEDs remain lit.
5 Release the Key () button.		LEDs blink two (2) times, and then remain lit.
6 Enter the desired new Admin PIN.		LEDs illuminate together.
7 Press the Key () button.		LEDs double-blink
8 Re-enter the new Admin PIN.		LEDs double-blink
9 Press the Key () button.	  	LEDs illuminate together, and then: <ul style="list-style-type: none"> ❖ LED double-blinks indicating correct Admin PIN entry ❖ LEDs blink alternately if there is an Admin PIN entry error. Return to step 4.

Index

A

- Admin PIN
 - change 26
 - create 23

C

- Configure the Flash Drive
 - Windows® 18

F

- Flash Drive
 - features 9
 - reset 16
- Flash Drive features
 - Blue LED 9
 - Key ring 9
 - Keyboard 9
 - Lock LED 9
 - Unlock LED 9

I

- Icon
 - safety 5
- Introduction 8

L

- LED indicators 10
- Lock Flash Drive 15

S

- Safety
 - icons 5

T

- troubleshooting
 - Brute Force Hack Defence Mechanism 22
 - forgot PIN 21
 - recharge battery 21
 - unlocking with Admin PIN 22

U

- Unlock Flash Drive
 - Admin PIN 25
 - user PIN 14
- User PIN
 - change 11
 - create 12
 - requirements 13

TOSHIBA

Leading Innovation >>>

**Unidad de memoria
flash USB cifrada de
Toshiba
Manual del usuario**

Limitación de responsabilidad

Toshiba no asume ninguna responsabilidad por daños o pérdidas debidas a incendio, terremoto, acciones de terceros u otros accidentes, dolo, negligencia o mal uso por parte del usuario, u otros tipos de uso bajo circunstancias inusuales. Toshiba no asume ninguna responsabilidad por daños o pérdidas, pérdidas de ganancias o demandas por terceros, etc. que ocurran como consecuencia del uso o de la imposibilidad del uso de este producto. Toshiba no asume ninguna responsabilidad por daños o pérdidas que sean resultado de no seguir las instrucciones del manual. Toshiba no asume ninguna responsabilidad si se destruyen o pierden datos mientras se esté usando este dispositivo, independientemente de la causa o del tipo o magnitud del daño. Toshiba no llevará a cabo la restauración o recuperación de datos. Toshiba no asume ninguna responsabilidad por daños o pérdidas que ocurran debido a malos funcionamientos, etc. que resulten de la combinación de dispositivos conectados y software no relacionados con Toshiba.

Información de la Comisión Federal de Comunicaciones de Estados Unidos (FCC)

Aviso de la FCC “Información sobre la declaración de conformidad”

Este equipo se probó y se comprobó que cumple con los límites para dispositivos digitales de Clase B, en virtud de la parte 15 de las normas de la Comisión Federal de Comunicaciones de Estados Unidos (*Federal Communications Commission* o FCC). Estos límites están diseñados para proporcionar una protección razonable contra interferencias perjudiciales en una instalación residencial.

Este equipo genera, utiliza y puede irradiar energía de radiofrecuencia y, si no se instala y utiliza conforme a las instrucciones, puede provocar interferencias perjudiciales en comunicaciones de radio. Sin embargo, no hay ninguna garantía de que la interferencia no ocurra en una instalación en particular. Si este equipo provoca interferencias perjudiciales en la recepción de radio o televisión (lo que se puede determinar apagando y encendiendo el equipo), recomendamos al usuario que intente corregir la interferencia adoptando una o varias de las medidas siguientes:

- ❖ Cambiar la orientación o la ubicación de la antena receptora.
- ❖ Aumentar la distancia entre el equipo y el receptor.
- ❖ Conectar el equipo a un tomacorriente en un circuito diferente al que está conectado el receptor.
- ❖ Consultar al distribuidor o a un técnico especializado en radio y televisión para obtener ayuda.

NOTA

Los cambios o las modificaciones realizados a este equipo que no estén aprobados expresamente por TOSHIBA o por terceros autorizados por TOSHIBA, pueden invalidar el derecho del usuario a utilizar el equipo.

Requisitos de la FCC

Este dispositivo cumple con la Parte 15 de las normas de la FCC. Su funcionamiento está sujeto a las siguientes dos condiciones:

- 1 Este dispositivo no debe causar interferencias perjudiciales.
- 2 Este dispositivo debe aceptar cualquier interferencia recibida, incluidas aquellas que puedan comprometer su funcionamiento.

Información IC

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Declaración de conformidad de la UE



Este producto ostenta la marca CE de conformidad con las directivas pertinentes de la Comunidad Europea. La oficina responsable de la obtención de la marca en la Comunidad Europea es Toshiba Europe GmbH, Hammfelddamm 8, 41460 Neuss, Alemania. Una copia de la Declaración de conformidad oficial se puede obtener en el siguiente sitio: <http://epps.toshiba-teg.com>.

Las especificaciones del producto, las configuraciones, los precios y la disponibilidad de sistemas/componentes/opciones están sujetos a cambios sin previo aviso. Todos los demás productos y nombres comerciales pertenecen a sus respectivos propietarios. Los precios de los revendedores o distribuidores pueden variar.

RoHS

Este dispositivo cumple con la Directiva 2011/65/EU de la Unión Europea sobre la restricción del uso de ciertas químicas peligrosas en equipos eléctricos y electrónicos (*Restriction of the use of certain Hazardous Substances* o RoHS), la cual incluye pero no se limita al uso de plomo, cadmio, mercurio, cromo hexavalente, PBB y PBDE. Toshiba requiere que los proveedores de componentes para sus computadoras cumplan con la Directiva RoHS y verifica el cumplimiento de estas disposiciones llevando a cabo inspecciones de prueba de los componentes durante el proceso de aprobación del diseño del producto.

Derechos de autor

Este manual no puede reproducirse en forma alguna sin el permiso previo y por escrito de Toshiba. Toshiba no asume ninguna responsabilidad respecto al uso de la información incluida en este manual.

© 2014 por Toshiba America Information Systems, Inc. Todos los derechos reservados.

Aviso

La información contenida en este manual, incluyendo pero sin limitarse a las especificaciones del producto, está sujeta a modificaciones sin previo aviso.

TOSHIBA CORPORATION Y TOSHIBA AMERICA INFORMATION SYSTEMS, INC. (TOSHIBA) NO BRINDA NINGUNA GARANTÍA EN RELACIÓN CON ESTE MANUAL O CON CUALQUIER INFORMACIÓN EN ÉL CONTENIDA Y POR ESTE MEDIO SE LIBERA EXPRESAMENTE DE TODA RESPONSABILIDAD REFERENTE A CUALQUIER GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O ADECUACIÓN PARA UN FIN CONCRETO RELACIONADO CON CUALQUIERA DE LOS PUNTOS ANTES MENCIONADOS. TOSHIBA NO ASUME NINGUNA RESPONSABILIDAD POR LOS DAÑOS SUFRIDOS DIRECTA O INDIRECTAMENTE DEBIDO A ERRORES TÉCNICOS O TIPOGRÁFICOS U OMISIONES EN ESTE MANUAL NI POR DISCREPANCIAS ENTRE EL PRODUCTO Y EL MANUAL. TOSHIBA NO ASUME BAJO NINGUNA CIRCUNSTANCIA RESPONSABILIDAD POR DAÑOS INCIDENTALES, EMERGENTES, ESPECIALES O PUNITIVOS, YA SEA DERIVADOS DE ACTOS CIVILES ILÍCITOS, CONTRATOS U OTROS, QUE PUDIERAN DESPRENDERSE DE ESTE MANUAL O SE RELACIONARAN CON EL MISMO O CON CUALQUIER OTRA INFORMACIÓN EN ÉL CONTENIDA O CON EL USO QUE DE ELLA SE HICIERA.

Marcas comerciales

Microsoft, Outlook, Windows y Windows Media son marcas registradas o marcas comerciales de Microsoft Corporation en Estados Unidos y/u otros países.

Todos los demás nombres de marcas y productos son marcas comerciales o marcas registradas de sus respectivas compañías.

Íconos de seguridad

Este manual contiene instrucciones de seguridad que deben seguirse a fin de evitar posibles peligros que podrían tener como consecuencia lesiones personales, daños al equipo o pérdida de datos. Son advertencias de seguridad que están clasificadas de acuerdo con la gravedad del peligro y están representadas por íconos que distinguen cada instrucción como se muestra abajo:

PELIGRO

Este ícono indica la presencia de una situación inminentemente peligrosa que, de no evitarse, ocasionaría muerte o lesiones graves.

ADVERTENCIA

Este ícono indica la presencia de una situación potencialmente peligrosa que, de no evitarse, podría ocasionar muerte o lesiones graves.

PRECAUCIÓN

Este ícono indica la presencia de una situación potencialmente peligrosa que, de no evitarse, podría ocasionar lesiones menores o moderadas.

PRECAUCIÓN

Este ícono indica la presencia de una situación potencialmente peligrosa que, de no evitarse, podría ocasionar daños a la propiedad.

NOTA

Este ícono brinda información importante.

Contenido

Introducción	8
Características de la unidad de memoria flash USB cifrada de Toshiba	9
Luces LED	10
Capítulo 1: El NIP del usuario	11
Cambiar el NIP del usuario	11
Creación de un nuevo NIP del usuario	13
Capítulo 2: Desbloqueo y bloqueo de la unidad flash	15
Cómo desbloquear la unidad flash con un NIP del usuario	15
Cómo bloquear la unidad flash	16
Capítulo 3: Restablecimiento de la unidad flash	17
Cómo restablecer la unidad flash	17
Capítulo 4: Configuración de la unidad flash con Windows® después de un restablecimiento completo	19
Configuración de la unidad flash	19

Capítulo 5: Solución de problemas.....	22
Preguntas frecuentes.....	22
Capítulo 6: Creación y uso del NIP	
de administrador	25
Creación de un NIP de administrador.....	25
Desbloqueo de la unidad flash con un NIP de	
administrador	27
Cambiar el NIP de administrador.....	28
Índice	31

Introducción

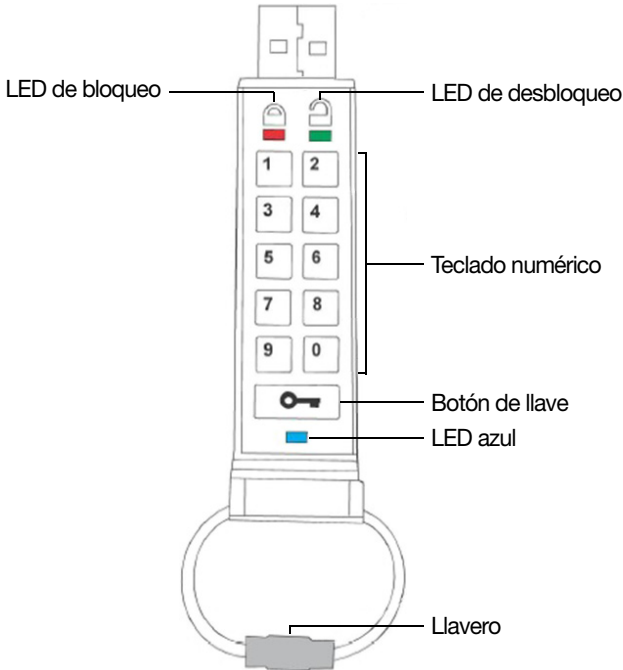
Gracias por adquirir la unidad de memoria flash USB cifrada de Toshiba, una unidad flash USB con hardware cifrado y un NIP activado.

Esta unidad flash usa un cifrado militar AES en hardware de 256 bits, y cifra todos los datos almacenados en la unidad flash en tiempo real. La unidad flash no requiere de ningún software y es independiente del anfitrión y del sistema operativo. La unidad flash incorpora una batería recargable que permite al usuario ingresar un NIP (número de identificación personal) de 7 a 15 dígitos en el teclado numérico integrado antes de conectar la unidad flash a un puerto USB (por ej. en una computadora). En caso de robo o pérdida de la unidad flash, el usuario puede sentirse seguro de que todos los datos almacenados en la unidad flash se encuentran protegidos y que ninguna persona no autorizada podrá acceder a ellos.

La unidad flash puede cifrarse con un NIP tanto de usuario como de administrador. Esto lo hace la unidad perfecta para ser usada a nivel corporativo o gubernamental.

Ya que la unidad flash se desbloquea con el teclado numérico integrado y no con el teclado (por ej. en una computadora), esta no es vulnerable a registradores de claves en software o hardware o ataques de fuerza bruta.

Características de la unidad de memoria flash USB cifrada de Toshiba














(Ilustración de muestra) Características

Luces LED y botones disponibles:

- ❖ **LED de bloqueo**—en modo de suspensión cuando la unidad flash está bloqueada
- ❖ **LED de desbloqueo**—cuando parpadea, la unidad flash está desbloqueada
- ❖ **Teclado numérico**—Úselo para ingresar los códigos NIP
- ❖ **Botón de llave**—Le permite activar la unidad flash e ingresar códigos NIP
- ❖ **LED azul**—Se ilumina cuando la unidad flash está conectada a una computadora y parpadea cuando se está efectuando una transferencia de datos
- ❖ **Llavero**—Desenrólquelo para agregar la unidad flash a su llavero

Luces LED

	Parpadeando	La unidad flash está desbloqueada, conéctela a un puerto USB	 ENCENDIDO, sólido	La unidad flash está conectada a un puerto USB de la computadora
	Parpadeando	La unidad flash está bloqueada	 ENCENDIDO, sólido	La unidad flash no tiene un NIP de usuario
	Parpadeando	Se está efectuando una transferencia de datos	 ENCENDIDO, sólido	La unidad flash está conectada a un equipo anfitrión
	Parpadeando de manera alterna	Error	 ENCENDIDO, sólido	La unidad flash está aceptando un nuevo código NIP
	Parpadeando al mismo tiempo	Aceptando un NIP de usuario	 Doble parpadeo	Aceptando un NIP de administrador
	Intensificación	Autocomprobación de seguridad		

PRECAUCIÓN

Antes de desconectar la unidad flash, siga las instrucciones de su computadora portátil, computadora de escritorio, o cualquier otro dispositivo compatible, para la extracción adecuada y segura de dispositivos USB. La desconexión de la unidad USB de un dispositivo mientras se está efectuando una transferencia de datos puede causar la corrupción o pérdida de los datos.

NOTA

La batería recargable de la unidad flash necesitará estar cargada antes de su primer uso. Conecte la unidad flash a un puerto USB en funcionamiento (por ej. en una computadora) por aproximadamente 60 minutos para cargar la batería por completo.

NOTA

A menos que se indique lo contrario, deben realizarse todos los pasos de las INSTRUCCIONES mientras la unidad flash no está conectada a una computadora.

Capítulo 1

El NIP del usuario

La unidad flash se envía con el NIP predeterminado del usuario ☐ 1-1-2-2-3-3-4-4 ☐ y aunque puede usar la unidad inmediatamente después de comprarla con el NIP predeterminado, por motivos de seguridad se recomienda encarecidamente crear un nuevo NIP del usuario de inmediato.

Cambiar el NIP del usuario

PRECAUCIÓN

Si olvida el NIP del usuario y no existe un NIP de administrador, o si olvida ambos, deberá reiniciar la unidad flash y perderá acceso a todos los datos. Consulte [“Cómo restablecer la unidad flash” en la página 17](#).

NOTA

Para protegerse en contra de la pérdida accidental de datos, haga copias de seguridad frecuentemente en diferentes medios de almacenamiento externos. Con el paso del tiempo, o después de su uso prolongado, el Producto puede perder funcionalidad total o parcial, incluyendo la de lectura/escritura y eliminación de datos.














Requisitos del NIP:

- ❖ Debe tener una longitud de 7 a 15 dígitos

12 El NIP del usuario

Cambiar el NIP del usuario

- ❖ No debe contener letras/números repetidos, (por ej. 3-3-3-3-3-3)
- ❖ No debe contener letras/números secuenciales, (por ej. 1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

Instrucciones	Actividad LED	
<p>1 Presione el botón de llave ().</p> <p>2 Ingrese el NIP predeterminado del usuario y presione el botón de llave ().</p>	  	<p>Las luces LED parpadean al mismo tiempo (NIP predeterminado de fábrica: 1-1-2-2-3-3-4-4)</p> <p>Las luces LED se iluminan al mismo tiempo por aproximadamente 4 segundos y después:</p> <p>La luz LED parpadea para indicar que el NIP fue ingresado correctamente</p>
<p>3 Presione y mantenga presionado el botón de llave () por aproximadamente 3 segundos.</p> <p>4 Ingrese un nuevo número de NIP (debe contener entre 7 y 15 dígitos).</p>		<p>Las luces LED están encendidas</p>
<p>5 Presione el botón de llave () para almacenar el nuevo NIP.</p> <p>6 Vuelva a ingresar el nuevo NIP.</p>		<p>Las luces LED se iluminan juntas</p>
<p>7 Presione el botón de llave () para confirmar el nuevo NIP.</p>	  	<p>Las luces LED se iluminan al mismo tiempo por aproximadamente 4 segundos y después:</p> <ul style="list-style-type: none"> ❖ Las luces LED parpadean si las dos entradas de NIP coinciden. La unidad flash está lista para el uso. ❖ La luz parpadea de manera alterna en caso de un error en la entrada del NIP. Regresar al paso 3.

NOTA Si se produjo un error al definir un nuevo NIP o si el procedimiento no se ha terminado, la unidad flash conservará el NIP anterior.

Creación de un nuevo NIP del usuario






Se creará una nueva clave de cifrado automáticamente bajo las siguientes circunstancias:

- ❖ Cuando después de 10 intentos fallidos consecutivos de desbloqueo se activa la detección de un ataque informático.
- ❖ Si la unidad flash ha sido restablecida manualmente, consulte [“Cómo restablecer la unidad flash” en la página 17.](#)

Cuando ha ocurrido una de las dos situaciones anteriores, será necesario crear un nuevo NIP del usuario para la nueva clave de cifrado siguiendo las instrucciones a continuación.



Requisitos del NIP del usuario:

- ❖ Debe tener una longitud de 7 a 15 dígitos
- ❖ No debe contener letras/números repetidos, (por ej. 3-3-3-3-3-3-3)
- ❖ No debe contener letras/números secuenciales, (por ej. 1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

Instrucciones	Actividad LED	
1 Presione y mantenga presionado el botón de llave () por aproximadamente 3 segundos.		Las luces LED están ENCENDIDAS
2 Ingrese un nuevo NIP del usuario (debe contener entre 7 y 15 dígitos).		Las luces LED están ENCENDIDAS
3 Presione el botón de llave () para guardar.		Las luces LED parpadean al mismo tiempo para indicar que el NIP fue ingresado correctamente

14 El NIP del usuario

Creación de un nuevo NIP del usuario

Instrucciones	Actividad LED	
<p>4 Vuelva a ingresar el nuevo NIP del usuario y luego presione el botón de llave ().</p>		<p>Las luces LED se iluminan al mismo tiempo por aproximadamente 4 segundos y después:</p> <ul style="list-style-type: none">❖ La luz LED parpadea para indicar que el NIP del usuario fue ingresado correctamente❖ Las luces LED parpadean de manera alterna en caso de un error en la entrada del NIP de administrador. Regresar al paso 3.

NOTA



Solo puede definirse un NIP del usuario cuando la luz LED roja está iluminada de forma constante o cambiarse cuando la luz LED verde está parpadeando (desbloqueada). No pueden crearse los NIP de usuario y administrador mientras la unidad flash esté conectada a un equipo anfitrión.

Capítulo 2

Desbloqueo y bloqueo de la unidad flash







Cómo desbloquear la unidad flash con un NIP del usuario

Una vez creado el NIP del usuario, se cifrarán todos los datos almacenados en la unidad flash, (en hardware) con base en las especificación AES de 256 bits en modo CBC. Para poder acceder a los datos almacenados en la unidad flash, primero deberá desbloquear la unidad con el NIP del usuario usando el teclado numérico.

<i>Instrucciones</i>	<i>Actividad LED</i>	
1 Presione el botón de llave ().		Las luces LED parpadean al mismo tiempo.
2 Ingrese su NIP del usuario (NIP predeterminado de fábrica: 1-1-2-2-3-3-4-4.)		

16 Desbloqueo y bloqueo de la unidad flash

Cómo bloquear la unidad flash

Instrucciones	Actividad LED
3 Presione el botón de llave ()	   Las luces LED se iluminan al mismo tiempo por aproximadamente 4 segundos y después: <ul style="list-style-type: none">❖ La luz LED parpadea para indicar que el NIP fue ingresado correctamente❖ La luz LED parpadea en caso de que el NIP ingresado sea incorrecto. Vuelva a ingresar el NIP.
4 Inserte su unidad flash en el puerto USB de la computadora.	  La luz LED está ENCENDIDA La luz LED está ENCENDIDA o parpadea para indicar actividad

NOTA

Una vez desbloqueada, la luz LED verde parpadea durante aproximadamente 30 segundos; durante ese tiempo la unidad flash necesitará estar conectada al puerto USB de la computadora. Si no se detecta ninguna conexión dentro de 30 segundos, la unidad flash se bloqueará y necesitará reiniciar el proceso de desbloqueo. Regresar al paso 1.

Cómo bloquear la unidad flash

La unidad de memoria flash USB cifrada de Toshiba automáticamente se bloquea cuando está desconectada del equipo anfitrión o si la alimentación del puerto USB está apagada. Los datos permanecen bloqueados por medio del cifrado AES de 256 bits en modo CBC.

PRECAUCIÓN

Antes de desconectar la unidad flash, siga las instrucciones de su computadora portátil, computadora de escritorio, o cualquier otro dispositivo compatible, para la extracción adecuada y segura de dispositivos USB. La desconexión de la unidad USB de un dispositivo mientras se está efectuando una transferencia de datos puede causar la corrupción o pérdida de los datos.

Capítulo 3

Restablecimiento de la unidad flash

Cómo restablecer la unidad flash

Siga las instrucciones en este capítulo en caso de haber olvidado tanto el NIP de administrador como el del usuario, o si desea eliminar todos los datos almacenados en la unidad flash y crear nuevos NIP del usuario y del administrador. El proceso de restablecimiento elimina todos los NIP y claves de cifrado. Esto significa que deberá definirse un nuevo NIP del usuario para poder rehabilitar la unidad flash. Además, ya que esto forzará la creación de una nueva clave de cifrado, deberá reformatar la unidad flash. Consulte [“Configuración de la unidad flash” en la página 19](#).

NOTA












Para protegerse en contra de la pérdida accidental de datos, haga copias de seguridad frecuentemente en diferentes medios de almacenamiento externos. Con el paso del tiempo, o después de su uso prolongado, el Producto puede perder funcionalidad total o parcial, incluyendo la de lectura/escritura y eliminación de datos.

18 Restablecimiento de la unidad flash


Cómo restablecer la unidad flash

PRECAUCIÓN

Si restablece la unidad flash, nunca más podrá acceder a los datos en la unidad flash y no tendrá ninguna forma de recuperarlos. Esto puede ocasionar la pérdida de datos.

Instrucciones	Actividad LED
1 Presione el botón de llave ()	 Las luces LED parpadean al mismo tiempo
2 Presione el botón de llave () nuevamente.	 La luz LED parpadea
3 Presione y mantenga presionado el botón de llave () y el botón del número 2 () durante aproximadamente 3 segundos.	 Las luces LED parpadean al mismo tiempo
4 Presione el botón del número 9 () 3 veces (9-9-9), y después presione el botón de llave ()	Las luces LED se APAGAN.
5 Presione el botón de llave ()	 La luz LED está ENCENDIDA y sólida

NOTA

Cuando la luz LED roja  está ENCENDIDA y sólida, deberá crear un nuevo NIP del usuario antes de poder usar la unidad flash.

Capítulo 4

Configuración de la unidad flash con Windows[®] después de un restablecimiento completo

Configuración de la unidad flash

En caso de que se haya activado la detección de un ataque informático después del ingreso consecutivo de 10 NIP incorrectos o si se ha restablecido la unidad flash, se perderán definitivamente todos los datos almacenados en la misma. Una vez que se ha creado un nuevo NIP del usuario, la unidad flash deberá inicializarse y formatearse.

NOTA

Para protegerse en contra de la pérdida accidental de datos, haga copias de seguridad frecuentemente en diferentes medios de almacenamiento externos. Con el paso del tiempo, o después de su uso prolongado, el Producto puede perder funcionalidad total o parcial, incluyendo la de lectura/escritura y eliminación de datos.

Para inicializar su unidad flash, realice el siguiente procedimiento:

- 1 Cree un nuevo NIP del usuario, consulte [“Creación de un nuevo NIP del usuario”](#) en la página 13.

La unidad flash se desbloqueará tras ingresar el NIP del usuario nuevo y conectarla a una computadora.

- 2 En la computadora, haga clic derecho o toque **Mi PC**, y después haga clic o toque **Administrar**.

20 Configuración de la unidad flash con Windows® después de un restablecimiento completo

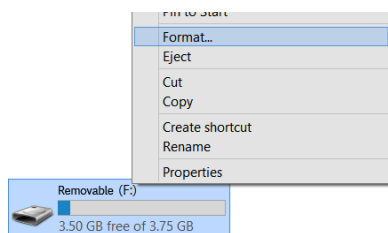
Configuración de la unidad flash

- 3 En la ventana de "Administración de equipos" haga clic o toque **Administración de discos**.

En la ventana "Administración de discos", la unidad flash se reconocerá como un dispositivo extraíble en un formato sin procesar.

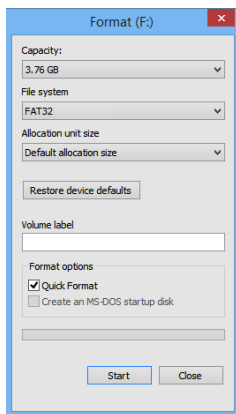
Para que la unidad flash sea reconocida como una unidad flash básica, realice el siguiente procedimiento:

- 1 Haga clic derecho o toque **Unidad extraíble en formato sin procesar**, en el área en blanco bajo la sección sin asignar, y después seleccione **Formateo**.



(Imagen de muestra) Ventana Unidad

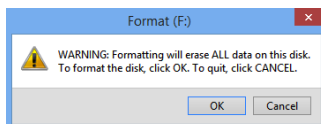
Se abre la ventana "Formateo".



(Imagen de muestra) Ventana de formateo

- 2 Seleccione **FAT32** o **NTFS** (dependiendo de sus requisitos), y luego haga clic o toque **Inicio**.

Aparece la ventana de "Advertencia de formateo".



(Imagen de muestra) Ventana de advertencia de formateo

- 3 Haga clic o toque **OK**.

En la unidad flash:

- ❖ La luz LED azul parpadea mientras la unidad flash se está formateando.
- ❖ La luz LED azul está ENCENDIDA y sólida cuando el proceso ha terminado. Su unidad flash está lista para usarse.

Capítulo 5

Solución de problemas

Preguntas frecuentes

¿Cómo desbloqueo la unidad flash si la batería está agotada?

Su unidad de memoria flash USB cifrada de Toshiba incluye una batería recargable integrada. Si la batería está completamente descargada, usted podrá continuar utilizando el producto siguiendo las instrucciones a continuación:

- 1** Conecte la unidad flash a un puerto USB de una computadora.
- 2** Mientras la unidad flash está conectada a la computadora, ingrese el NIP del usuario o administrador para desbloquear la unidad flash.
- 3** La batería interna se recarga de forma automática mientras la unidad está conectada al puerto USB. Se recomienda que mantenga la unidad flash conectada durante aproximadamente una (1) hora para cargar la batería por completo.

Olvidé mi NIP.

Si olvidó los NIP de usuario y/o administrador, no habrá ninguna forma de recuperar los datos almacenados en la unidad flash. No hay maneras subrepticias de ingresar a la unidad flash. Podrá

continuar reutilizando la unidad flash si la restablece; sin embargo, al hacer esto, se perderán todos los datos previamente almacenados.

Consulte [“Cómo restablecer la unidad flash” en la página 17](#) para restablecer la unidad flash. Una vez que esto se ha completado, ocurrirá lo siguiente:

- ❖ Se elimina la clave de cifrado actual
- ❖ Los NIP del usuario y del administrador originales son eliminados
- ❖ Todos los datos previamente almacenados en la unidad flash se perderán por completo

He detectado un mecanismo de defensa contra un ataque de fuerza bruta.

Después de 10 intentos consecutivos con un NIP incorrecto, ocurrirá lo siguiente:

- ❖ Se elimina la clave de cifrado actual
- ❖ Los NIP del usuario y del administrador son eliminados
- ❖ Todos los datos previamente almacenados en la unidad flash se perderán por completo

A diferencia de otros dispositivos, la unidad de memoria flash USB cifrada de Toshiba, viene pre-cargada con un número ilimitado de claves de cifrado generadas aleatoriamente. Cada vez que se detecta un ataque informático (es decir, cuando se ingresa el NIP incorrecto 10 veces consecutivas), se elimina la clave de cifrado actual y la unidad flash genera una nueva de forma aleatoria una vez que el nuevo NIP del usuario ha sido creado. Es por esto que la unidad flash deberá formatearse cada vez que se activa el mecanismo de defensa.

¿Se eliminará el NIP del usuario al desbloquear la unidad flash con el NIP de administrador?

Ingresar el NIP de administrador para acceder a una unidad flash bloqueada eliminará el NIP del usuario. Si un usuario olvida su NIP, podrá recuperar el acceso a la unidad flash tras definir un nuevo NIP del usuario. Por motivos de seguridad, se recomienda encarecidamente la creación de un nuevo NIP del usuario una vez que la unidad flash ha sido desbloqueada usando el NIP del administrador.

El NIP del usuario se elimina cuando:

- ❖ Se usa el NIP del administrador para desbloquear la unidad flash

- ❖ Se cambia el NIP del administrador

Necesitará crearse un nuevo NIP del usuario.

Capítulo 6

Creación y uso del NIP de administrador

Creación de un NIP de administrador

Un NIP de administrador es una función útil para que la unidad flash pueda usarse a nivel corporativo, por ejemplo:

- ❖ Recuperación de datos de la unidad flash y configuración de un nuevo NIP del usuario en caso de que un empleado haya olvidado su NIP.
- ❖ Recuperación de datos de la unidad flash en caso de que un empleado deje la compañía.

NOTA

El ingreso del NIP de administrador para acceder a una unidad flash bloqueada eliminará el NIP del usuario. Si olvida el NIP, podrá recuperar el acceso a la unidad flash tras definir un nuevo NIP del usuario. Por motivos de seguridad, se recomienda encarecidamente la creación de un nuevo NIP del usuario una vez que la unidad flash ha sido desbloqueada usando el NIP de administrador.










Requisitos del NIP de administrador:

- ❖ Debe tener una longitud de 7 a 15 dígitos
- ❖ No debe contener letras/números repetidos, (por ej. 3-3-3-3-3-3-3)

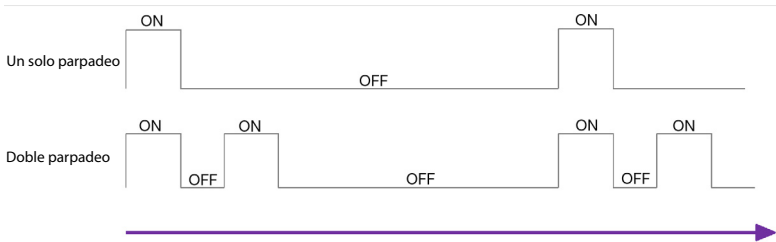
26 Creación y uso del NIP de administrador

- ❖ No debe contener letras/números secuenciales, (por ej. 1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)


Si la unidad flash ha sido restablecida o si se ha activado la detección de un ataque informático (es decir, no existe un NIP del usuario o de administrador), siga las instrucciones en [“Restablecimiento de la unidad flash” en la página 17](#). Si ya existe un NIP del usuario, la unidad flash deberá desbloquearse primero con el NIP del usuario, consulte [“Cómo desbloquear la unidad flash con un NIP del usuario” en la página 15](#). Ahora podrá crearse un NIP de administrador siguiendo las instrucciones a continuación:

Instrucciones	Actividad LED
1 Presione el botón de llave () dos (2) veces, y la segunda vez mantenga presionado el botón durante 3 segundos aproximadamente.	 Las luces LED parpadean una vez y permanecen iluminadas.
2 Ingrese un nuevo NIP de administrador (debe contener entre 7 y 15 dígitos).	 Las luces LED están ENCENDIDAS
3 Presione el botón de llave () 4 Vuelva a ingresar el nuevo NIP de administrador.	 Las luces LED parpadean dos veces
5 Presione el botón de llave () para confirmar el nuevo NIP de administrador.	   Las luces LED se iluminan al mismo tiempo por aproximadamente 4 segundos y después: <ul style="list-style-type: none">❖ La luz LED parpadea indicando que el NIP de administrador fue ingresado correctamente❖ Las luces LED parpadean de manera alterna en caso de un error en la entrada del NIP de administrador. Regresar al paso 1.

La siguiente imagen muestra las características del parpadeo de la luz LED verde cuando se abre la unidad flash en modo Usuario y no en modo Administrador.



(Imagen de muestra) Un solo parpadeo de la luz LED en el modo Usuario y doble parpadeo en el modo Administrador

La siguiente imagen muestra la diferencia entre presionar el botón de llave () para configurar el NIP del usuario y el NIP de administrador.





(Imagen de muestra) Entrada de la llave para la selección de modo Usuario/Administrador

Desbloqueo de la unidad flash con un NIP de administrador








NOTA

El ingreso del NIP de administrador para desbloquear la unidad flash eliminará el NIP del usuario. Por motivos de seguridad, se recomienda la creación de un nuevo NIP del usuario una vez que la unidad flash ha sido desbloqueada usando el NIP del administrador.

Instrucciones	Actividad LED
<p>1 Presione dos veces el botón de llave ().</p> <p>2 Ingrese el NIP de administrador.</p>	<div style="display: flex; align-items: center;">  <p>Las luces LED parpadean juntas dos veces.</p> </div>

28 Creación y uso del NIP de administrador

Cambiar el NIP de administrador

Instrucciones	Actividad LED	
3 Presione el botón de llave ().	   	Las luces LED se iluminan al mismo tiempo y después: <ul style="list-style-type: none">❖ La luz LED parpadea dos veces indicando que un NIP de administrador fue ingresado correctamente❖ La luz LED parpadea en caso de un error en la entrada del NIP de administrador. Regresar al paso 1.
4 Inserte su unidad flash en el puerto USB de la computadora dentro de 30 segundos.	 	La luz LED está ENCENDIDA La luz LED está ENCENDIDA o parpadea para indicar actividad

NOTA

La luz LED verde parpadea por 30 segundos; durante ese tiempo la unidad flash necesitará estar conectada al puerto USB de la computadora. Si no se detecta ninguna conexión dentro de 30 segundos, la unidad flash se bloqueará y necesitará reiniciar el proceso de desbloqueo. Regresar al paso 1.

Cambiar el NIP de administrador

NOTA














Para cambiar el NIP del administrador, la unidad flash deberá estar desbloqueada primero con el NIP del administrador, lo que ocasionará la eliminación del NIP del usuario. Por motivos de seguridad, se recomienda la creación de un nuevo NIP del usuario una vez que la unidad flash haya sido desbloqueada usando el NIP del administrador.

Requisitos del NIP de administrador:

- ❖ Debe tener una longitud de 7 a 15 dígitos
- ❖ No debe contener letras/números repetidos, (por ej. 3-3-3-3-3-3-3)





- ❖ No debe contener letras/números secuenciales, (por ej. 1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

Una vez que se ha creado un NIP de administrador, la unidad flash deberá desbloquearse por el administrador para poder cambiar el NIP de administrador. El NIP de administrador *no puede* cambiarse desde el modo usuario.

Instrucciones	Actividad LED	
1 Presione dos veces el botón de llave ().		Las luces LED parpadean juntas dos veces.
2 Ingrese el NIP actual de administrador deseado.		Las luces LED se iluminan juntas.
3 Presione el botón de llave ().		Las luces LED se iluminan al mismo tiempo y después: <ul style="list-style-type: none"> ❖ La luz LED parpadea dos veces indicando que el NIP de administrador fue ingresado correctamente ❖ La luz LED parpadea en caso de un error en la entrada del NIP de administrador. Regresar al paso 1.
4 Presione el botón de llave () dos (2) veces, y la segunda vez mantenga presionado el botón durante 3 segundos aproximadamente.		Las luces LED permanecen iluminadas.
5 Suelte el botón de llave ().		Las luces LED parpadean dos (2) veces y luego permanecen iluminadas.
6 Ingrese el nuevo NIP de administrador deseado.		Las luces LED se iluminan juntas.
7 Presione el botón de llave ().		Las luces LED parpadean dos veces
8 Vuelva a ingresar el nuevo NIP de administrador.		Las luces LED parpadean dos veces

30 Creación y uso del NIP de administrador

Cambiar el NIP de administrador

Instrucciones	Actividad LED	
<p>9 Presione el botón de llave ().</p>	  	<p>Las luces LED se iluminan al mismo tiempo y después:</p> <ul style="list-style-type: none">❖ La luz LED parpadea dos veces indicando que el NIP de administrador fue ingresado correctamente❖ Las luces LED parpadean de manera alterna en caso de un error en la entrada del NIP de administrador. Regresar al paso 4.

Índice

B

bloquear la unidad flash 16

C

cambio del

NIP de administrador 28

NIP del usuario 11

características

unidad flash 9

características de la unidad flash

LED azul 9

LED de bloqueo 9

LED de desbloqueo 9

llavero 9

teclado numérico 9

configuración de la unidad flash

Windows® 19

creación del

NIP del usuario 13

D

desbloqueo de unidad flash

NIP de administrador 27

NIP del usuario 15

I

ícono

seguridad 5

íconos de

seguridad 5

introducción 8

L

luces LED 10

N

NIP de administrador

crear 25

R

requisitos del

NIP del usuario 13

restablecimiento

Unidad flash 17

S

solución de problemas

desbloqueo con el NIP de

administrador 23

mecanismo de defensa contra

un ataque de fuerza bruta

23

NIP olvidado 22

recargar batería 22