



QUIPUS

# FUNCIONAMIENTO DEL PISO TECNOLOGICO Y KUAA

Manual Funcionamiento del Piso Tecnológico y KUAA

## Descripción breve

Este documento ha sido creado para entender el funcionamiento del piso tecnológico y equipos de computación modelo KUAA

Departamento de Tecnologías de información y Comunicación  
Empresa Pública Quipus

Versión: 1.0

JDTIC@quipus.gob.bo

# MANUAL FUNCIONAMIENTO DEL PISO TECNOLOGICO Y PISO TECNOLÓGICO

## INFORMACIÓN DEL DOCUMENTO

<b>Documento</b>	Manual Funcionamiento del Piso Tecnológico y KUAA		
<b>Elaborado por</b>	Alejandro Morales Pérez	<b>Versión del Documento</b>	v1.0
<b>Código:</b>	GAF-JDTIC-MF-M01		
<b>Fecha de elaboración</b>	15/08/2015	<b>Fecha de Aprobación</b>	22/08/2015

## CONTROL DE VERSIONES

<b>VERSIÓN</b>	<b>ELABORADO POR</b>	<b>REVISADO POR</b>	<b>OBSERVACIONES</b>
Versión 1.0	Alejandro Morales Pérez	Marcelo Eguino Burgoa	APROBADO

## INDICE

Funcionamiento del Piso Tecnológico y KUAA.....	3
1. PISO TECNOLÓGICO.....	3
2. ELEMENTOS MÁS IMPORTANTES QUE COMPONEN UN PISO TECNOLÓGICO.....	3
3. FUNCIONAMIENTO DEL PISO TECNOLÓGICO .....	6
4. FUNCIONAMIENTO DEL SISTEMA ANTIRROBO THEFT DETERRENT .....	10
5. COMPUTADORA KUAA GUÍA RÁPIDA DE INSTALACIÓN .....	22
6. INSTRUCCIONES DE SEGURIDAD .....	26

## Funcionamiento del Piso Tecnológico y KUAA

### 1. PISO TECNOLÓGICO

Se denomina piso tecnológico al conjunto de elementos necesarios (instalación, redes eléctricas, de datos y del equipamiento de red inalámbrica) para el funcionamiento del Programa denominado "Educación con Revolución Tecnológica" en las Unidades Educativas Fiscales y de Convenio del subsistema de educación regular.

Para que el Piso Tecnológico pueda funcionar se efectúan las siguientes tareas:

- Instalación de tablero eléctrico.
- Cableado y canalización de la Red Eléctrica.
- Cableado y canalización de la Red de Datos.
- Conexión del equipamiento suministrado por QUIPUS: Servidores/switch/UPS/Access Points (AP).
- Configuración de Servidor y Access Point.
- Conexión a Internet (sólo si la escuela tiene este servicio).
- Prueba integral de funcionamiento de la Red (conectividad).

### 2. ELEMENTOS MÁS IMPORTANTES QUE COMPONEN UN PISO TECNOLÓGICO

**Servidor:** Un servidor es una computadora más potente que las comunes que, formando parte de una red, provee servicios a otras computadoras denominadas clientes. El servidor brinda provisión y renovación de certificado de seguridad, aloja contenidos multimedia, brinda servicios de administración de web y permite compartir información entre alumnos y docentes, entre otras tareas.



**Switch:** es un dispositivo digital para la interconexión de redes de computadoras. Su función es interconectar dos o más elementos dentro de una red.

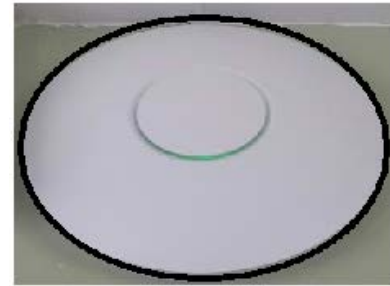


**Switch POE(Power Over Ethernet):**

Es un dispositivo que permite que la alimentación eléctrica se suministre a un dispositivo de red en este caso al Access Point .



**AP (Access point):** Un Access point o punto de Acceso es un dispositivo, capaz de transformar la señal de red en WIFI y viceversa. Un Access Point puede dar señal a unas 40 computadoras aproximadamente, con un alcance de entre 150 m en interior hasta varios centenares en exterior, dependiendo de las interferencias que reciba.



**Cable de red UTP CAT 6:** Son los cables utilizados para conectar dos dispositivos de red (computadoras, switch, AP o Routers, etc.) entre sí dentro de una red de área local (LAN).



**Cable canal:** En la instalación del piso tecnológico se utiliza el sistema de cable-canal para contener y proteger los cables de red Ethernet CAT 6, así como también los cables de alimentación para el servidor y los switches.



**UPS:** Un ups (en inglés Uninterruptible power Supply), es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.



**Rack:** Los Racks son un simple armazon Metalico destinado a alojar equipamiento Electronico, informatico y comunicaciones.

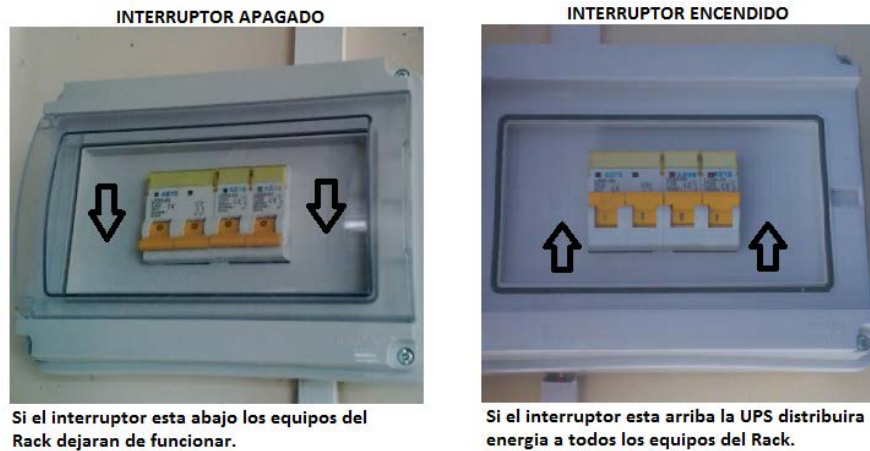


**Interruptor Termico Electrico:** Es un dispositivo capaz de interrumpir la corriente electrica de un circuito cuando esta tiene un corte electrico o cuando detecta altos voltajes.



### 3. FUNCIONAMIENTO DEL PISO TECNOLÓGICO

#### Interrupor térmico eléctrico



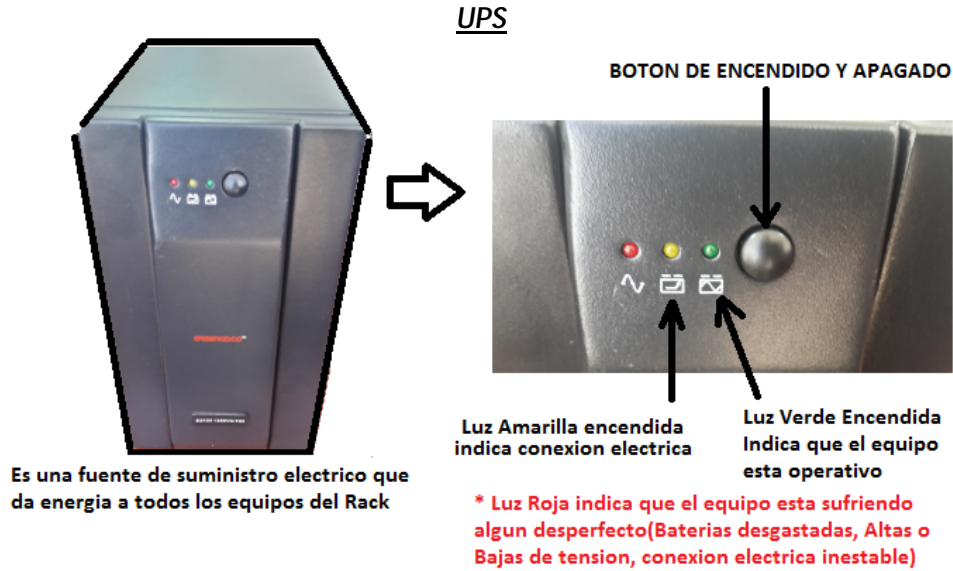
*Figura .1*

El equipamiento está configurado para encender automáticamente al subir los térmicos. Es importante aclarar que no se debe apagar el Piso Tecnológico desde esta opción puesto que puede ocasionar que el mismo deje de funcionar.

Para apagar el Piso Tecnológico debe abrir la puerta delantera del Rack y presionar el botón de Encendido/Apagado del servidor (Figura 3). Una vez hecho esto se debe esperar unos minutos hasta que el equipo se apague.

Posteriormente se de mantener presionado por 15 segundos el botón de encendido de la UPS (Figura 2.)

Después de esto recién se puede apagar el equipamiento restante a través del interruptor térmico (Figura 1)



*Figura .2*

En caso de que el equipo no tenga alimentación de energía, el mismo empezará a emitir un sonido, en cuyo caso se debe proceder a apagar el equipamiento de acuerdo a lo descrito en la sección del Interruptor Térmico para evitar que el equipo sufra un desperfecto.



El Rack para protección tiene puertas laterales y una puerta frontal las cuales previenen que el equipamiento interior se llene de polvo.

Se debe mantener las mismas cerradas a no ser que se necesite abrir las mismas para limpieza y/o mantenimiento.



### SERVIDOR



**Este tipo de equipo esta al servicio de las portatiles KUAA que le suministran todo tipo de informacion.**

*Figura .3*

En el servidor está instalado un sistema disuador de robos y administrador de activos denominado Theft Deterrent que es un sistema en línea que ofrece administración, control y seguridad física para activos tipo Classmate (KUAA).

Usando la red escolar, el servidor es responsable de administrar las computadoras KUAA a través de certificados que contienen información de la unidad, la red y políticas que de no ser cumplidas bloquean físicamente la maquina disuadiendo con ello el interés de ser robadas.

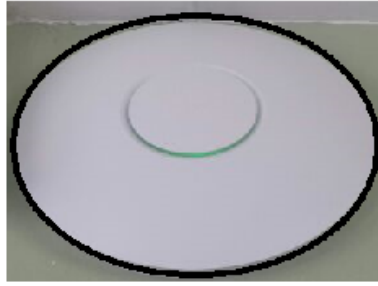
### SWITCH



**Dispositivo que permite la interconexion de los diferentes equipos del Piso Tecnologico**

Mediante este dispositivo podemos conectar todos los componentes de comunicación del piso tecnológico, está ubicado en el interior del Rack y sus ocho puertos son utilizados como puertas para enlazar otros dispositivos.

### Access Point



**Permite la conexión inalámbrica entre el servidor y la portatil KUAA**

Es un dispositivo de red que interconecta equipos de comunicación alámbrica para formar una red inalámbrica que interconecta dispositivos móviles o con tarjetas de red inalámbricas. La mayoría de los AP soportan la conexión de múltiples dispositivos inalámbricos a una conexión por cable

### INYECTOR POE



**Dispositivo que da energía y comunicación a la Antena WI-FI**

Es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre a un dispositivo de red (switch, punto de acceso, router, teléfono o cámara IP, etc) usando el mismo cable que se utiliza para la conexión de red.

### EQUIPO DE COMPUTACION KUAA



Este modelo de equipo de computación está diseñado exclusivamente para estudiantes de primaria y secundaria de Unidades Educativas con el fin de mejorar la calidad de aprendizaje.

#### 4. FUNCIONAMIENTO DEL SISTEMA ANTIRROBO THEFT DETERRENT

El Piso Tecnológico tiene un sistema antirrobo que es el Theft Deterrent que ofrece administración, control y seguridad física para activos tipo KUAA en un ambiente escolar.

Usando la red del aula donde instalaron el Piso Tecnológico, el servidor es el responsable de administrar las portátiles a través de certificados que contienen información de la unidad, la red y políticas de seguridad que de no ser cumplidas bloquean físicamente la maquina disuadiendo con ello el interés de ser robadas.

##### CONEXIÓN AL SERVIDOR

Conectamos un monitor en la parte de atrás del servidor.



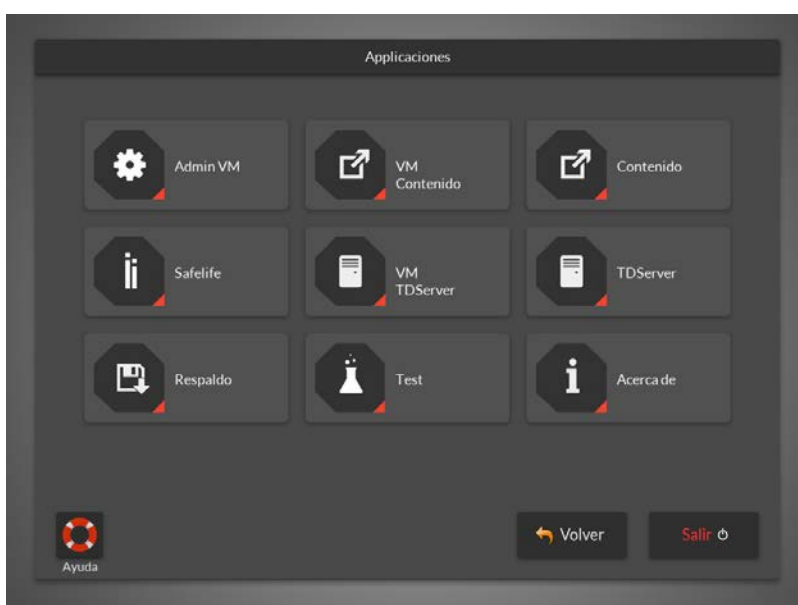
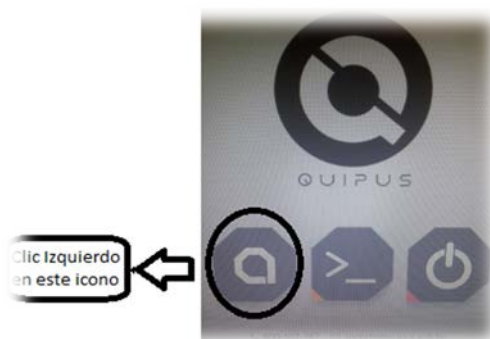
Conectamos un Teclado y Mouse



Cuando conectemos el monitor, Teclado y mouse, en la pantalla del monitor nos mostrara la siguiente pantalla de inicio donde ingresamos haciendo clic en el icono Admin el cual nos pedirá un password.



Una vez introducido el password nos mostrara la siguiente ventana donde le damos clic en el icono.



**Administración VM:** Ejecuta una ventana en la cual podemos acceder a la administración de las máquinas virtuales que se encuentran alojadas en el servidor.

**Máquina Virtual Contenido:** Ejecuta una ventana en la cual podemos acceder a la máquina virtual (contenidos) para realizar soporte.

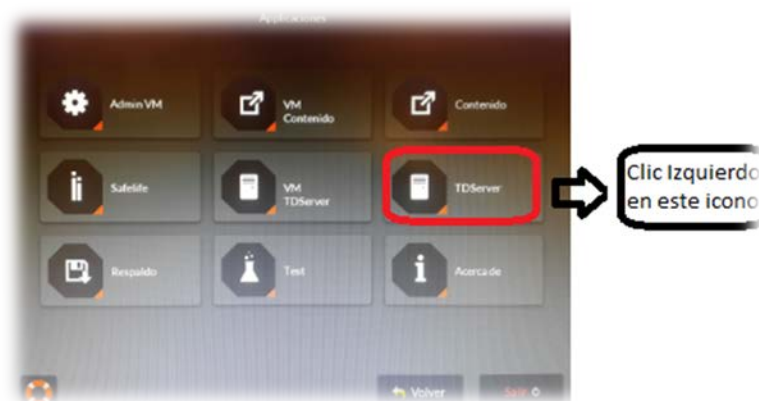
**Acceso al Contenido:** En esta opción se ejecutará una ventana en la cual se mostrará el contenido digital proporcionado por el Ministerio.

**Máquina Virtual TD:** Se ejecutará una ventana en la cual podemos acceder a la máquina virtual (TD Server) para realizar soporte.

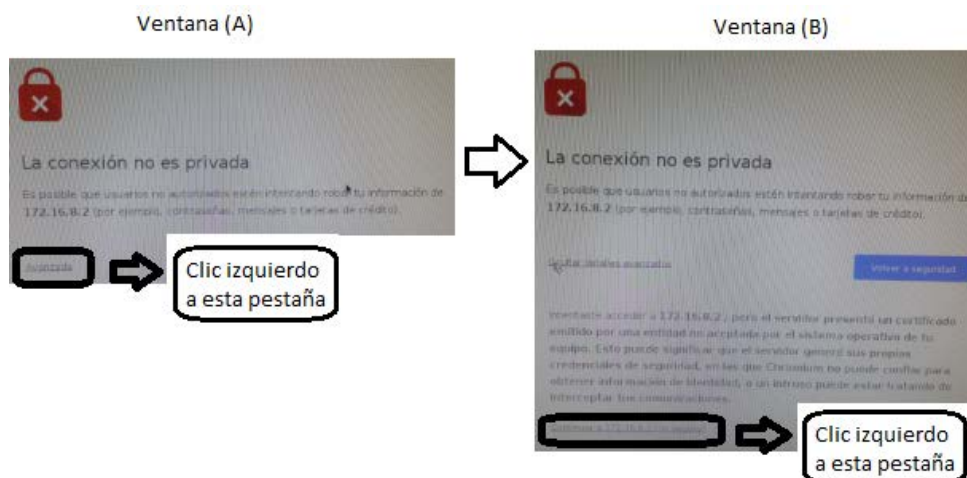
**Acceso a la Admin TD:** En esta opción se ejecutará una ventana en la cual se mostrará las opciones para la administración del TD.

**Menú de Respaldo:** Esta opción nos permitirá realizar y acceder a los backups que se generarán del TD Server.

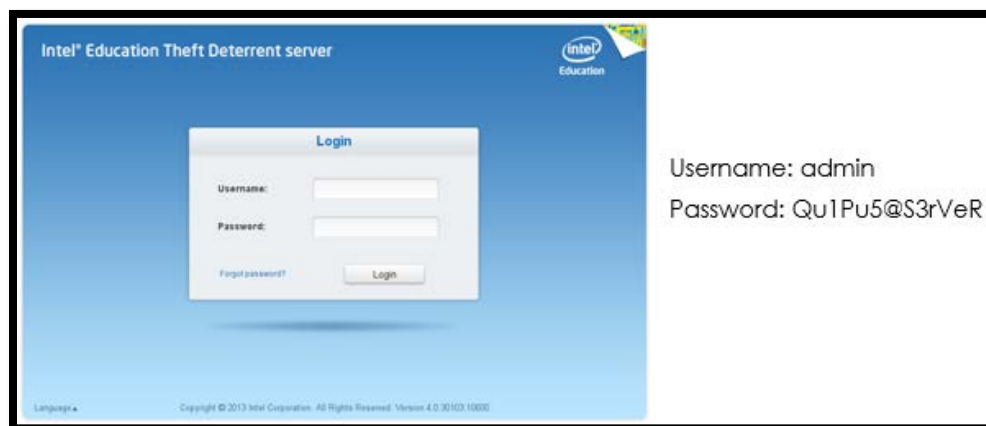
En la siguiente ventana abrimos el siguiente icono TDSerVer



Se abrirá una ventana de internet, en la ventana (A) le damos clic en la pestaña para que esta misma nos despliegue la ventana (B) como se muestra en la siguiente figura.



En esta nueva ventana ingresamos al Theft Deterrent Server donde introducimos el Username y el Password.



## PANTALLA PRINCIPAL DEL TD

**Theft Deterrent server**

? Bienvenido, admin | 🔄 Cerrar sesión

**Education**
**Inicio**
Inventario
Grupos y cuentas
Configuración

**Resumen de inventario**

Total de dispositivos gestionados: 1

Estado de dispositivo

Estado	Dispositivos
Normal	1
Permanente	0
A punto de expirar	0
Bloqueado	0
Bloqueo/Desbloqueo...	0
Otros	0

**Estadísticas dispositivo**

Días	Última protección	Bloqueados automáticamente	Bloqueados manualmente	Expirará en
1-7	1	0	0	0
8-30	0	0	0	0
31-60	0	0	0	0
61-90	0	0	0	0
>90	0	0	0	1

**Notificaciones**

**Buscar y filtrar**

[📄 Exportar informe](#)
[📖 Ver registros](#)

Último inicio de sesión: 2015-05-07 12:17; Última actualización: 2015-05-07 12:26

Idioma ▲

Copyright © 2013 Intel Corporation. All Rights Reserved. Versión 4.0.30103.10600

- Resumen de inventario: Se podrá observar el total de los dispositivos gestionados: bloqueados, a punto de expirar, permanente y normales.
- Notificaciones: Muestra la información de los movimientos que se hacen en el servidor, maquinas pendientes de aprobación, próximas a bloqueo, etc.

- Estadísticas dispositivo: En este cuadro se observa una estadística de los dispositivos por los días y las conexiones, es decir, última conexión y días restantes de certificado.
- Buscar y filtrar: Sirve para ubicar dispositivos en la lista general.

## Inventario

**Intel Theft Deterrent server**

Bienvenido, admin | Cerrar sesión

Education Inicio **Inventario** Grupos y cuentas Configuración

Gestión de dispositivos Pendiente de nuevos dispositivos (0)

**Todos los dispositivos** Seleccionar todos los 1 dispositivos

<input type="checkbox"/>	Id. de hardware	Grupo	Nombre de dispositivo	Modelo de hardware	Puerta de enlace	Última protección	Estado
<input type="checkbox"/>	7427EA8C8DDE		7427ea8c8ddb	Classmate PC desc	192.168.2.1	2015-05-07	Activo

Dispositivos seleccionados: 0 / 1

Página 1 de 1

**Buscar y filtrar**

Todos los dispositivos

Todos los estados

Especificar criterios.

**Acciones**

Asignar a grupo

Bloquear

Permitir desbloqueo

Generar códigos de desbloqueo

Más acciones

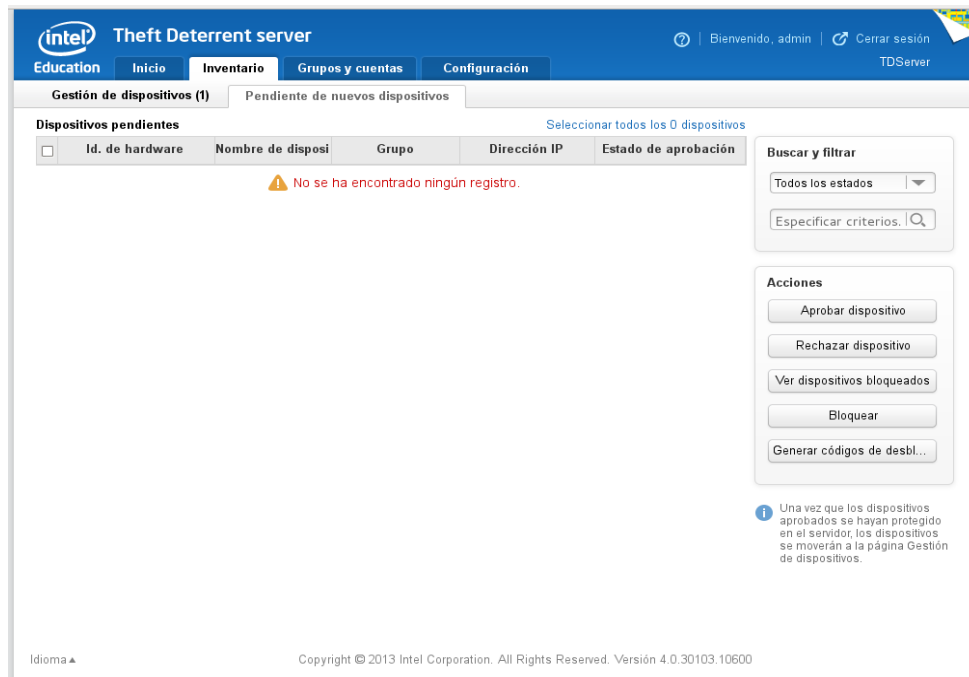
- Aprovisionar nuevo certificado
- Rechazar dispositivo
- Ver dispositivos bloqueados
- Exportar informe

Idioma

Copyright © 2013 Intel Corporation. All Rights Reserved. Versión 4.0.30103.10600

- Gestión de dispositivos: Listado completo de los dispositivos asociados al servidor. Se muestra ID. de hardware, Grupo, Nombre, Modelo, Última protección, etc.
- Asignar a grupo: Los dispositivos se pueden agrupar por grupos para su mejor administración.
- Bloquear: bloqueo de dispositivos manualmente.
- Permitir desbloqueo: Una vez bloqueado el dispositivo, con esta aprobación se puede pasar al paso de generación de códigos de desbloqueo.
- Generación de código de desbloqueo: Con el hardware ID y Boot tick, se genera un código que sirve para desbloquear el equipo, se puede ingresar tanto manualmente como a través de un pendrive.

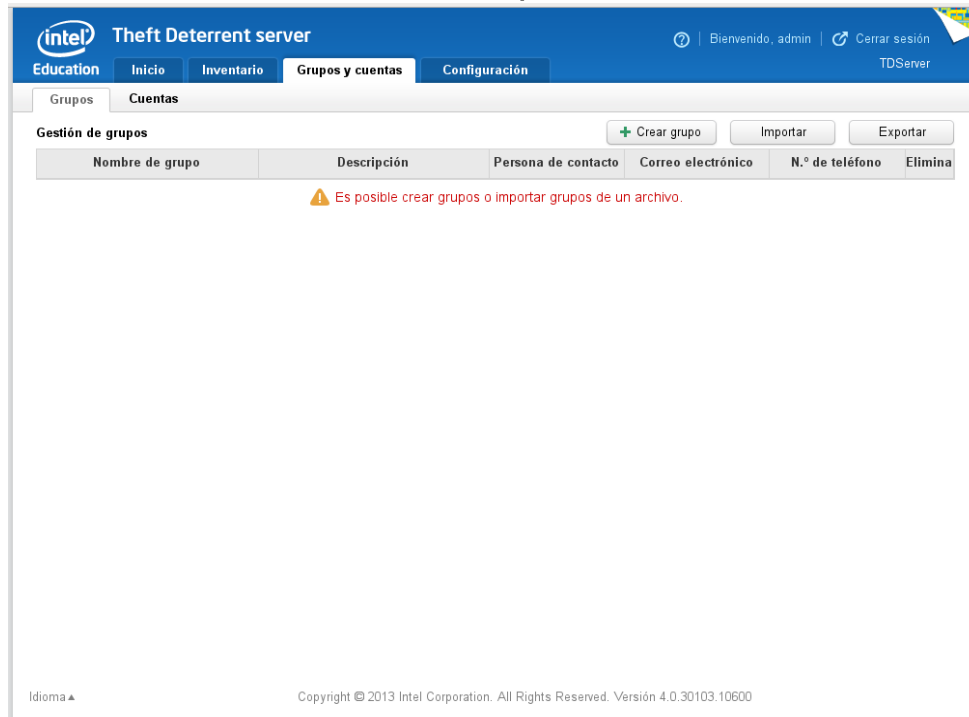
- Aprovisionar nuevo certificado: Setea nuevos valores de días y booteos para el equipo, también se puede generar una certificación donde el equipo queda liberado para siempre, es decir un certificado permanente.
- Rechazar dispositivo: El servidor rechaza el dispositivo, es decir, lo elimina de su lista.
- Ver dispositivos bloqueados: Te enseña la lista de los dispositivos bloqueados.
- Exportar informe: Exporta un listado con el estado de los equipos que sean seleccionados.



- Aprobar dispositivos: En esta pestaña se observarán los equipos que están a la espera de ser provisionados contra el servidor.



## Grupos



- En esta opción se permite la gestión de los grupos de equipos.
- En cuentas: se permite la integración de usuarios con diferentes permisos.

## Configuración

### General

**Configuración general**

Certificado de arranque sin conexión  
Puede exportar el certificado de arranque sin conexión para desbloquear un dispositivo que se haya activado de forma previa en la fábrica y se encuentre bloqueado antes de que se conecte con el servidor.

Id. de hardware:  (12 caracteres)

Boot Tick:

Modelo de hardware: ☐ Dispositivo Tableta ☒ Otros

[Exportar](#)

---

**Dispositivo de importación (s)**

Seleccione un archivo csv cruda o comprimida:

[Browse...](#) [Importar](#)

---

**Notificación por correo electrónico** ☒

Se debe enviar regularmente un informe de resumen a mi buzón de correo. Puede introducir varias direcciones de correo electrónico separadas por comas.

Correo electrónico:

Frecuencia: Cada  días

El servidor de correo electrónico no está disponible.

[Guardar](#)

---

**Notificación SMS** ☒

Enviar un informe resumido al teléfono móvil (s) con regularidad. Los números de teléfono pueden estar separados por comas. Por favor, consulte el [instrucciones sobre cómo configurar el entorno](#).

Código PIN:

Número de teléfono:

Frecuencia: Cada  días

[Guardar](#)

- Certificado de arranque sin conexión: Se utiliza para desbloquear equipos que hayan sido activados de forma previa y se encuentren bloqueados, con el Boot Tick y el Hardware ID.
- Dispositivo de importación: Aquí se puede importar una lista de dispositivos manualmente, el archivo debe ser csv.
- Notificación por correo electrónico: Se emite un mail al administrador cada cierta cantidad de días, informando el estado en que se encuentra el server.
- Notificación SMS: Enviar un informe cada cierta cantidad de días, en forma de mensaje de texto. Previamente se debe configurar número del receptor.

## Servidor

**intel Theft Deterrent server**

Education Inicio Inventario Grupos y cuentas Configuración

Bienvenido, admin | Cerrar sesión TDServ

General Servidor Cliente Seguridad Avanzado

### Configuración de servidor

**Difusión automática de servidor** ☒

Puede permitir que el servidor difunda su dirección para que los dispositivos en la misma red puedan detectar este servidor.

Frecuencia de difusión: cada  minutos

Guardar

---

**Aprobación automática de servidor** ☒

Puede permitir que el servidor apruebe automáticamente los dispositivos pendientes.

☒ Siempre aprobar automáticamente

☐ Aprobar automáticamente el:

Guardar

---

**Enviar correo electrónico a los usuarios** ☒

Puede configurar el servidor de correo electrónico para enviar por correo electrónico a los usuarios la información del servidor y de la cuenta de usuario.

Nombre de usuario de correo electrónico:

Contraseña de correo electrónico:

Servidor SMTP:

Puerto:

Modo de seguridad: ☒ Ninguno ☐ Soporte SSL ☐ Soporte TLS

Probar... Guardar

Idioma ▲ Copyright © 2013 Intel Corporation. All Rights Reserved. Versión 4.0.30103.10600

- Difusión automática: El servidor cada intervalo de tiempo envía un broadcast permitiendo que los equipos conectados en su red lo detecten.
- Aprobación automática: Aprueba automáticamente los equipos que se conectan al server.
- Enviar correo electrónico a los usuarios: Se configura el servidor de mail para poder enviar una mail informativo a cualquier usuario.

## Cliente

**Theft Deterrent server**

? Bienvenido, admin | 🔒 Cerrar sesión

Education
Inicio
Inventario
Grupos y cuentas
Configuración

General
Servidor
Cliente
Seguridad
Avanzado

**Configuración de cliente**

i Todos los cambios de configuración en esta página afectarán a todos los clientes en la próxima protección de clientes.

---

**Certificado global**

Puede configurar el certificado global para todos los dispositivos. Los dispositivos que están a punto de expirar solicitarán automáticamente el certificado global.

Duración de expiración de certificado:  días

Total de ciclos autorizados:  (no se aplica a dispositivos Tableta)

Umbral de advertencia de expiración:  días y/o  ciclos restantes

Límite de certificado de arranque:  veces dentro de  días

Guardar

---

**Intervalo de protección**

Puede configurar el intervalo para los dispositivos con diferentes estados para que se protejan automáticamente en el servidor.

Dispositivo en estado normal:  minutos

Dispositivo que está a punto de expirar:  minutos

Dispositivo que no se puede conectar con el servidor:  minutos

Guardar

---

**Protección de contraseña** ☒

Puede configurar una contraseña para proteger Theft Deterrent client de modo que los usuarios no autorizados no puedan configurarlo ni desinstalarlo.

Contraseña de cliente:  Mostrar caracteres

Guardar

---

**Código de desbloqueo de estudiante** ☒

Puede permitir que los estudiantes generen códigos de desbloqueo desde la página web para estudiantes de Theft Deterrent server. Además, puede establecer la cantidad de veces que un estudiante puede generar códigos de desbloqueo.

Límite de código de desbloqueo:  veces dentro de  días

☐ El nombre y correo electrónico del estudiante son obligatorios.

Guardar

---

**Desbloqueo Remoto de Dispositivo Desconocido** ☒

Puede habilitar la función de desbloqueo remoto para dispositivos de tableta que aún no están administrados por el servidor si los clientes están preactivados con una Public Key asociada con el servidor.

☒ Habilite la función para los dispositivos preactivados con una Public Key que no se encuentra en el almacén de claves del servidor.

La Boot Tick máxima admitida:

Guardar

- **Certificado global:** El certificado global es aquel que se le asigna a todos los equipos, cuando requieren un nuevo certificado.
- **Intervalo de protección:** Configurar intervalos de tiempo para la nueva provisión de los equipos.

- Protección con contraseña: Se le puede asignar una clave al TDAgent (cliente) para que los usuarios no puedan desinstalarlo.
- Código de desbloqueo de estudiante: Permite que los alumnos generen los certificados de desbloqueo.
- Desbloqueo Remoto de Dispositivo desconocido ( tablets) : Permite la asociación y desbloqueo de equipos que están pre activados.

## Seguridad

The screenshot shows the 'Configuración' (Configuration) page of the Intel Theft Deterrent server. The 'Seguridad' (Security) tab is selected. The page contains several sections for managing security settings:

- Configuración de seguridad:** Includes a warning about advanced user settings. It features buttons for 'Actualizar Public Key', 'Exportar', and 'Importar'.
- Sincronización de paquetes:** A section for synchronizing packages, with a 'Sincronizar paquetes' button.
- Paquete de recuperación tras bloqueo:** A section for recovery packages, including an 'Importar' button and a 'Provision Number' input field.

The footer of the page indicates 'Copyright © 2013 Intel Corporation. All Rights Reserved. Versión 4.0.30103.10600'.

- Public Key:
  - Actualizar Public Key: En esta opción se re-aprovisiona el servidor, generando un servidor diferente.
  - Exportar: Permite exportar la Public Key y el Root Key del servidor
  - Importar: Se permite la provisión de manera manual.
- Sincronización de paquetes: Actualiza y sincroniza la información de las classmates con el servidor.
- Paquete de recuperación tras bloqueo.

## Configuración Avanzada

**Configuración avanzada**

Use estos valores de configuración o herramientas solamente si es un usuario avanzado. Póngase en contacto con su representante de campo de producto para obtener soporte cuando sea necesario.

Dirección y nombre de servidor

Puede configurar el nombre y la dirección IP/URL para Theft Deterrent server.

Nombre de servidor:

Dirección IP/URL de servidor:

[Descarga de archivos de registro](#)

[Guardar](#)

Soporte de Central Server

Puede actualizar el servidor al modo de Central Server soportado. Esto habilitará más funciones en el servidor como la transferencia de dispositivos y el backup de servidor a través de Central Server.

Complete el [proceso de activación](#) para actualizar al modo de Central Server soportado.

[Activar servidor](#)

Si desea recuperar la activación de servidor, puede [reactivar](#) el servidor.

Backup de servidor

Puede realizar un backup de los datos de servidor manualmente o configurar un backup automático.

☐ Realizar un backup de los datos de servidor automáticamente cada  días

☐ Proteger los archivos de backup con contraseña:  [Mostrar caracteres](#)

**i** Solamente se conservarán los 3 últimos archivos de backup automático. Los archivos de backup anteriores se eliminarán automáticamente.

[Guardar](#)

Realizar un backup de los datos de servidor manualmente

[Realizar backup](#)

[Administrar los archivos de copia de seguridad del servidor](#)

Restauración de servidor

Puede restaurar los datos de servidor a un estado anterior desde un punto de restauración o un archivo de backup local.

**i** Después de que los datos del servidor se restauren correctamente, deberá reiniciar Theft Deterrent server.

[Restaurar](#)

Actualización de cliente inteligente

El servidor puede actualizar Theft Deterrent clients de forma automática a través de la red. Puede también usar un servidor de descarga independiente. Para obtener más información acerca de la actualización del cliente inteligente, consulte el [manual del usuario](#).

Habilitar	Habilitar descarga 3G	Nombre de paquete	Versión	SO	N.º total	N.º de correctos	N.º de fallidos	Eliminar
<a href="#">Configurar servidor de descarga...</a>								

[Cargar el paquete](#)

- Dirección y nombre de servidor: Darle un nombre y una dirección url para que las classmates tengan a donde apuntar.
- Soporte de Central Server: Contamos con un formulario el cual nos permitirá registrar nuestro servidor de TD en el Servidor Central.
- Backup de servidor: Esta opción permite al servidor realizar backups automáticamente, en un directorio específico dentro del servidor.
- Restauración del servidor: Con esto podremos restaurar uno de los tantos backups que realicemos del servidor.
- Actualización de cliente inteligente: Con esto podremos enviar a cada cliente una actualización, se realiza la carga del nuevo paquete y se envía.

## 5. COMPUTADORA KUAA GUÍA RÁPIDA DE INSTALACIÓN

1. Conectar el cable de alimentación al adaptador.(Figura .4)
2. Conectar el cargador de batería de la KUAA a la corriente de 220 volts.
3. Conectar el enchufe tipo plug a la computadora.(Figura .5)
4. Encender la computadora.

Cargador de Batería de la KUAA



**es un dispositivo utilizado para suministrar corriente eléctrica a una batería.**



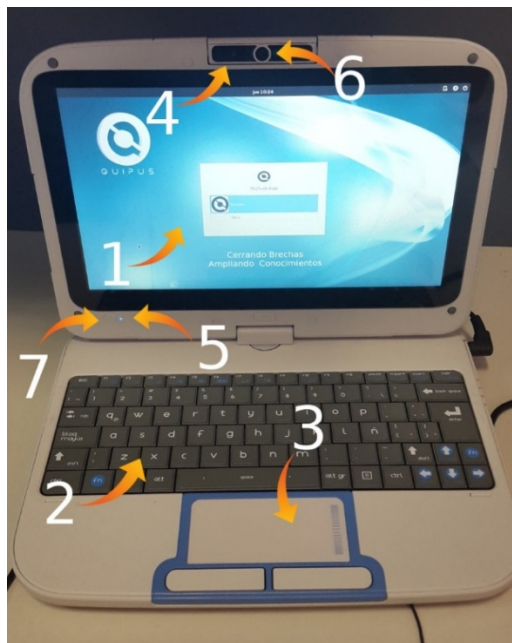
*Figura .4*



*Figura .5*

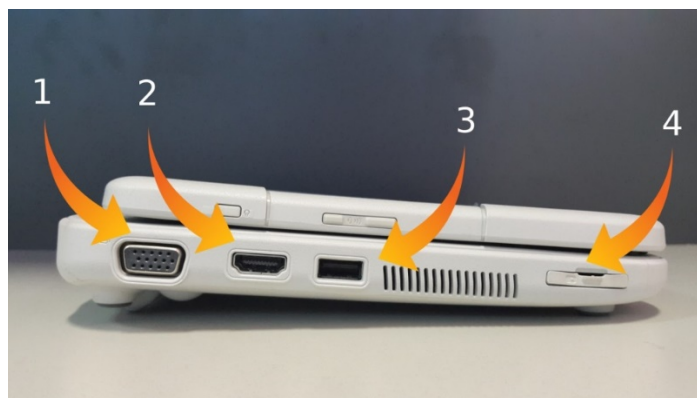
Nunca se debe apagar el equipo cuando el disco esté andando, ya que podría ocasionar pérdida de datos. **Encender y apagar el equipo en sucesiones rápidas podría dañarlo irreversiblemente.**

### Vista Frente



- 1) Display de LCD. Los contenidos del SO son expuestos aquí.
- 2) Teclado. Permite el ingreso de datos.
- 3) Touchpad. Panel táctil con dos botones correspondientes al mouse.
- 4) Micrófono. El micrófono incorporado permite que la computadora portátil reciba audio de entrada.
- 5) Indicadores de Led y Estado. Aquí se muestra el estado operacional.
- 6) Cámara. Permite tomar fotos y manejar aplicaciones de videoconferencia.
- 7) Botón de interrupción y suspensión. Maneja los estados del equipo.

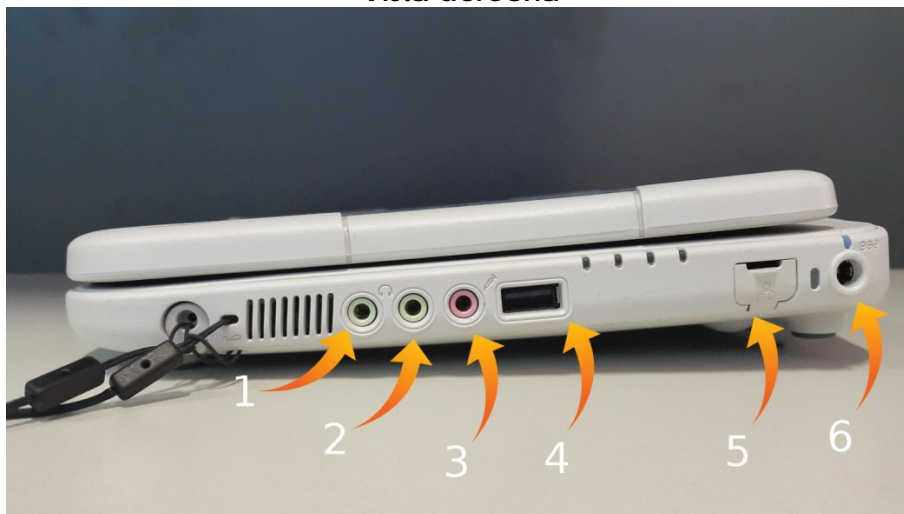
### Vista izquierda



- 1 y 2) Monitor. Permite conectar un monitor externo.
- 3) Usb1. Permite conectar dispositivos Usb.
- 4) Usb2. Permite conectar dispositivos Usb.



### Vista derecha



- 1 y 2) Salida de auriculares. Permite enchufar dispositivos como bocinas y/o audífonos.
- 3) Micrófono externo. Permite grabar con un micrófono.
- 4) Usb3. Permite conectar dispositivos Usb.
- 5) Cable de red. Permite conectar un cable de red externo.
- 6) Conector fuente de alimentación. Permite conectar la fuente.

### Vista posterior



- 1) Botón de extracción de batería. Permite quitar la batería.
- 2) Parlantes en estéreo. Permiten la salida del sonido.

## 5.1 OPCIONES DE TECLADO

El teclado del equipo tiene 84 teclas de acceso directo.

### Teclas de función.

Se sitúan en la parte superior del teclado alfanumérico, van del F1 al F12, y son teclas que aportan atajos en el uso del sistema. Por ejemplo, la tecla F1 permite recibir ayuda del programa, la tecla F5 permite actualizar las páginas web y la tecla F10 activa la barra del menú.

Además, las teclas contienen un símbolo dibujado en color. Dichos símbolos se utilizan manteniendo presionada la tecla Fn, que se encuentra en la parte inferior izquierda de su teclado.

### Controles de función (Teclas de acceso rápido).

Se presiona FN y la tecla designada.

F1: Enciende / Apaga la placa de red inalámbrica.

F2: Entra en modo de suspensión.

F3: Mudo / Sonido – Audio no mudo.

F4: Disminuye el volumen de altavoz.

F6: Cambia el modo de pantalla: Sólo monitor, sólo proyector • y monitor y proyector.

F7: Disminuye el nivel de brillo.

F8: Incrementa el nivel de brillo.

F9: Tecla sin funcionalidad.

F10: Bloqueo de panel táctil o touchpad.

### Teclas de control.

Algunas de las más importantes son :

1) Shift: representado por una flecha hacia arriba permite, mientras se mantiene pulsada, cambiar de minúsculas a mayúsculas y viceversa. También permite activar signos ubicados en las teclas con caracteres numéricos.

2) Enter: termina párrafos o introduce datos.

3) Cursores: mueve el cursor hacia el lugar deseado (indicado por las flechas).

4) BackSpace y Supr: sirven para borrar.

Back Space: borra campos en tablas y caracteres en procesadores, siempre y cuando estén a la izquierda del cursor.

Suprimir: borra campos en tablas y caracteres en procesadores, siempre y cuando estén a la derecha del cursor.

5) Esc: cancelar procesos y acciones en progreso. También sirve para cerrar cuadros de diálogo o ventanas.

6) Control: se utiliza en combinación con otras teclas para activar distintas funciones del programa. (Control + C es copiar, Control + X es cortar y Control + V es pegar en Windows).

7) Caps lock o "Bloq Mayús": activa el bloqueo de mayúsculas, lo que hace que todo el texto se escriba en mayúsculas (y que al pulsar Shift se escriba en minúsculas).

### Función de la tecla Alt Gr.

Algunas teclas en su computadora portátil, tienen un tercer símbolo en la parte superior derecha de la tecla.

### Panel táctil o Touch Pad.

Trabaja como cualquier otro mouse de escritorio, sólo se debe apoyar el dedo y deslizar hacia la dirección deseada.

Los botones derecho e izquierdo del mouse, tienen las mismas funciones que un mouse de escritorio.



## 6. INSTRUCCIONES DE SEGURIDAD

Siga las siguientes normas de seguridad para asegurar su protección y la de su computadora.

- No utilice su computadora portátil con la base directamente apoyada sobre el cuerpo por lapsos de tiempo extensos, ya que el calor podría acumularse en la base. El contacto prolongado con la piel podría causar molestias o, incluso, quemaduras.
- No intente revisar la computadora por su cuenta. Siempre siga las instrucciones de instalación cuidadosamente.
- A fin de evitar heridas causadas por descargas eléctricas o fuego:  
Apague la computadora completamente al realizar, una limpieza de ella, sus componentes o la carcasa; así como también al realizar operaciones que requieran de procedimientos similares. Para ello, apague el interruptor principal, quite la batería y, luego desconecte el adaptador (fuente de alimentación) de la toma corriente o de cualquier otro tipo de fuente de energía externo.
- No utilice la computadora cerca del agua, por ejemplo, cerca de una bañera, pileta de cocina o para lavar la ropa, en un sótano húmedo, junto

a una piscina o bajo la lluvia.

- No conecte ni desconecte ningún cable o realice un mantenimiento o reconfiguración de este producto durante una tormenta eléctrica.
- No coloque ningún objeto dentro de las salidas de aires o aberturas de su computadora o accesorios. Esta acción podría dañar los componentes internos y provocar un incendio o descarga eléctrica.
- Cuando se disponga a utilizar la computadora, colóquela sobre una superficie plana.
- Manipule los componentes con cuidado.
- Utilice la computadora dentro del rango de temperatura recomendado: 5°C a 35°C
- Guárdela a una temperatura de entre -20°C a +60°C.

Siga las siguientes normas de seguridad para el Piso Tecnológico.

- Mantener la temperatura del ambiente del servidor entre 15° y 28° C, asegurar una buena aeración y el límite de humedad no debe superar el 65% para evitar el deterioro.
- No conectar otros dispositivos eléctrico / electrónicos al distribuidor eléctrico del Rack.
- Es muy importante que el ambiente donde se encuentra el Piso Tecnológico haya una protección efectiva que imposibilite tanto el robo de los equipos y de sus componentes.
- Solo personal calificado y autorizado puede configurar o manipular los equipos del Piso Tecnológico.