



Latch

*AÑADE UN NIVEL ADICIONAL DE PROTECCIÓN
A TUS SERVICIOS DIGITALES*

Manual de uso paso a paso en la Universidad de Salamanca

Versión 7.1 – Noviembre 2016



CONTENIDO

1	Introducción	3
1.1	¿Qué es Latch?.....	3
1.2	Requisitos previos.....	3
1.3	Pasos para proteger con Latch una cuenta digital de un servicio	3
2	Cómo proteger con Latch una cuenta digital.....	4
2.1	Instalación de la aplicación Latch desde el dispositivo móvil.....	4
2.2	Creación de una cuenta de usuario en Latch	5
2.3	Acceso a Latch	7
2.4	Realización del pareado entre Latch y la cuenta digital	8
2.4.1	Acceso al pareado con Latch en la USAL	8
2.4.2	Generación del código de pareado en el dispositivo móvil.....	9
3	Ejemplos de utilización de Latch en la USAL.....	12
3.1	Ejemplo 1: Bloqueo total de la cuenta digital en la USAL.....	13
3.2	Ejemplo 2: Programar un bloqueo durante ciertas horas del día	15
3.3	Ejemplo 3: Configurar un autobloqueo por tiempo	15
4	Índice de imágenes	20
5	Recursos	30



**VNiVERSiDAD
D SALAMANCA**

CAMPUS DE EXCELENCIA INTERNACIONAL



1 Introducción

1.1 ¿Qué es Latch?

Básicamente, Latch es un servicio diseñado para proteger los accesos a las cuentas digitales de los usuarios.

La idea fundamental es la de limitar el tiempo de exposición de dichas cuentas digitales, ante un posible acceso no autorizado. Será el propio usuario el que decidirá si sus cuentas están BLOQUEADAS o DESBLOQUEADAS a la hora de poder acceder a ellas.

1.2 Requisitos previos

Para utilizar Latch el usuario debe disponer al menos de:

1. Un dispositivo móvil de tipo smartphone con la aplicación Latch instalada.
2. Una cuenta digital en alguno de los servicios que ya han integrado Latch.

1.3 Pasos para proteger con Latch una cuenta digital de un servicio

En este tutorial se realizará la protección de una cuenta de usuario en un servicio. Establecer esta protección con cualquier servicio sigue unos pasos muy definidos que se mostrarán con detalle a continuación:

1. Instalación de la aplicación Latch desde el dispositivo móvil.
2. Creación de una cuenta de usuario en Latch.
3. Acceso a Latch, con los datos de la cuenta anterior.
4. Realización del pareado entre dicha cuenta de usuario de Latch y el servicio que se desea proteger.

Una vez que se ha realizado el pareado, el usuario podrá establecer a través de Latch la protección de su cuenta digital en el servicio y bloquearla o desbloquearla, además de realizar distintas operaciones como son:

1. [Bloqueo y desbloqueo total de la cuenta digital.](#)
2. [Configurar un autobloqueo automático en un tiempo determinado.](#)
3. [Programar un bloqueo durante ciertas horas del día.](#)
4. [Establecer una contraseña de un solo uso para acceder a una cuenta digital.](#)
5. [Renombrar, agrupar, silenciar y observar los eventos realizados con cada cuenta digital.](#)

Los ejemplos de esta guía están basados en la aplicación Latch instalada en un dispositivo móvil con sistema operativo Android, por lo que las imágenes del dispositivo móvil y el proceso de instalación de Latch, se ajustan a este dispositivo.



En caso de que el dispositivo tuviera un sistema operativo **iOS, Windows Phone, Blackberry** o **Firefox OS** los pasos a realizar son exactamente los mismos, y el usuario podrá llevarlos a cabo igualmente. La excepción a esto último es la instalación de Latch, ya que cada sistema operativo utiliza una tienda distinta, aunque el proceso de instalación sea básicamente el mismo en todas. Asimismo Latch puede ser utilizado en dispositivos de tipo **Tablets** y **Apple Watch**.

2 Cómo proteger con Latch una cuenta digital

2.1 Instalación de la aplicación Latch desde el dispositivo móvil

Para utilizar Latch lo primero que hay que hacer es instalarla en el dispositivo móvil, la aplicación es gratuita, y puede descargarse desde la tienda correspondiente al tipo de dispositivo que se posea.

Los pasos que debe realizar el usuario para completar la instalación en un dispositivo móvil Android son:

1. Desde el dispositivo móvil, acceder al icono “Play Store” y pulsar sobre el mismo.
2. En la barra de búsqueda de la parte superior que aparecerá, debe escribir “Latch”.
3. Una vez hecho esto aparecerán varias aplicaciones relacionadas con la palabra “Latch”, siendo la de “Telefónica Digital España S.L.U.” la que hay que instalar. Para ello basta con pulsar el botón “INSTALAR”.

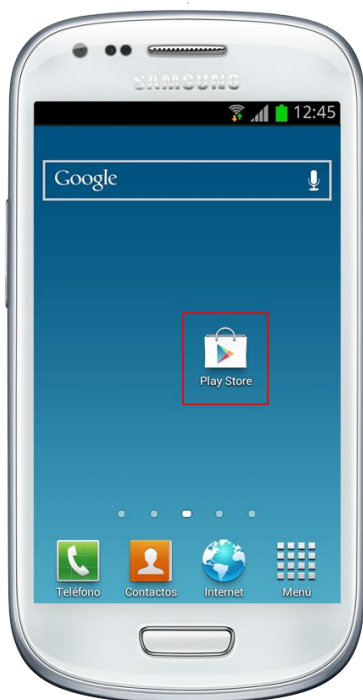


Imagen 01: Acceso a PlayStore.

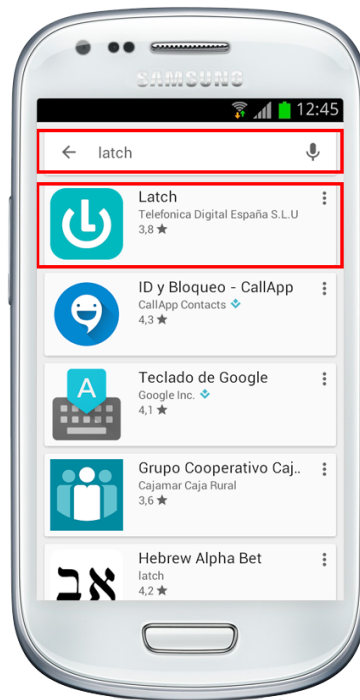


Imagen 02: Búsqueda de Latch.



Imagen 03: Instalación de Latch.

4. Tras pulsar el botón “INSTALAR” aparecerá una pantalla informando de los permisos que va a tener Latch en el dispositivo móvil, al pulsar el botón “ACEPTAR” comenzará la instalación propiamente dicha.
5. Tras unos segundos, la instalación habrá finalizado, y el usuario podrá abrirla directamente a través del botón “ABRIR”.
6. Al finalizar la instalación, aparecerá el icono de Latch en la pantalla inicial del dispositivo móvil, para que el usuario acceda a la aplicación cuando lo desee.

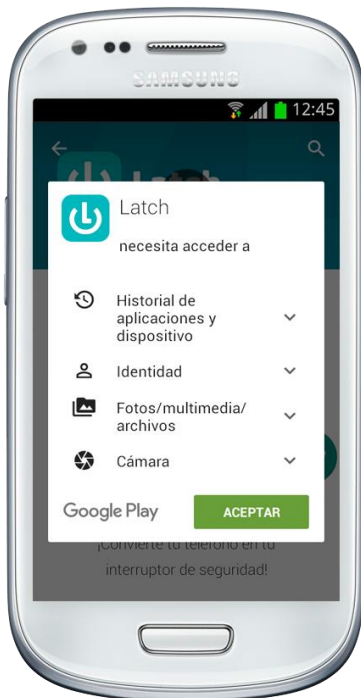


Imagen 04: Aceptar permisos.

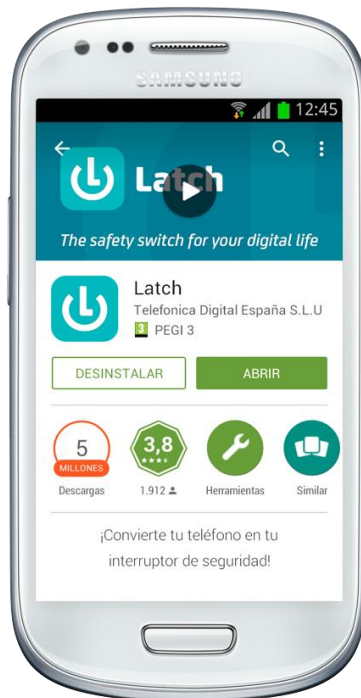


Imagen 05: Abrir Latch tras instalarlo.



Imagen 06: Icono de Latch.

2.2 Creación de una cuenta de usuario en Latch

Una vez instalada la aplicación, lo primero que tiene que hacer un usuario es abrirla desde su dispositivo móvil. En la primera pantalla aparecerá el logotipo de Latch, y unos textos indicativos (véase imagen 07).

Desde esta pantalla el usuario podrá hacer dos cosas:

- Deslizar la pantalla para acceder a un pequeño tutorial con las principales características de Latch (véase imagen 08), al final del cual se mostrará una pantalla desde la que podrán realizarse las siguientes acciones (véase imagen 09):
 - Registrarse en Latch a través del botón “No, regístrate”. En la siguiente página se muestra esto con más detalle
 - Iniciar sesión directamente a través del botón “Sí, inicia sesión”.
 - Contactar con el personal de soporte de Latch para consultar las dudas que pueda tener.
- Iniciar sesión directamente en caso de disponer de una cuenta. Para ello basta con pulsar sobre el texto “Inicia sesión” de la parte inferior de la pantalla, tal y como se puede apreciar en la imagen 07. Ese texto llevará al usuario a una nueva pantalla en la que podrá iniciar sesión (véase imagen 12).



Imagen 07: Pantalla inicial de Latch.



Imagen 08: Tutorial de Latch.



Imagen 09: Acceso al registro.

Al pulsar el botón “No, regístrate” mencionado anteriormente se abre un formulario en la aplicación, para que el usuario cree una cuenta en Latch. Para ello debe introducir una dirección de correo electrónico válida y una contraseña. Además deberá activar la casilla de verificación indicando que se está de acuerdo con los términos de uso de la aplicación, (pueden leerse dichos términos pulsando el botón “Leer las Condiciones de Uso”). Posteriormente debe pulsar el botón “Registrarme”, sito en la parte inferior de la pantalla.

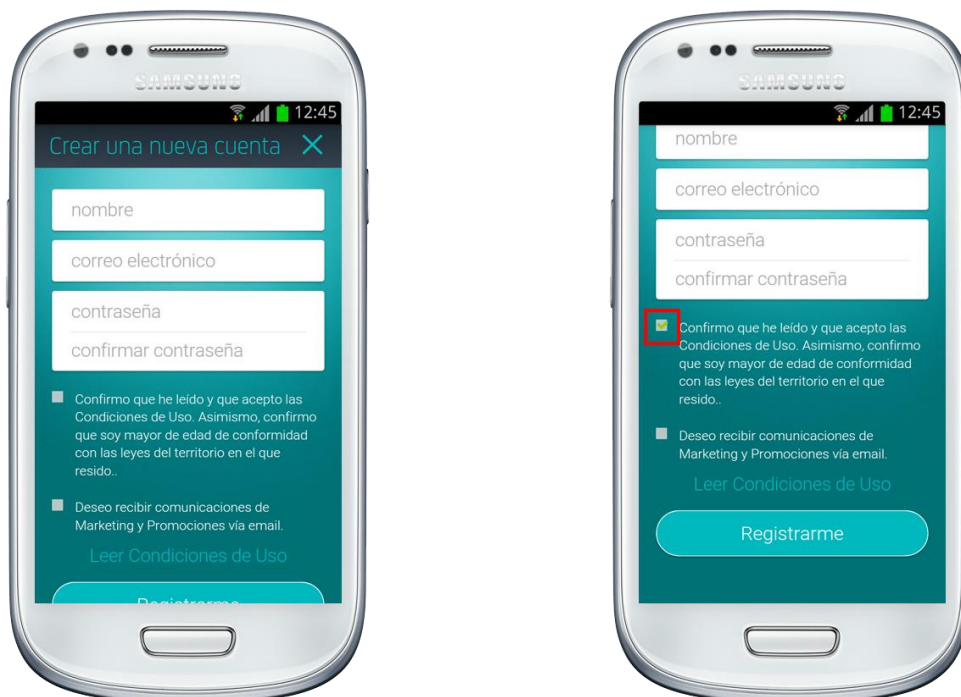


Imagen 10: Creación de una nueva cuenta en Latch.

Tras la introducción de dichos datos, se le habrá enviado al usuario un correo electrónico en la dirección indicada anteriormente, con un enlace que debe pulsar para darse de alta en Latch.

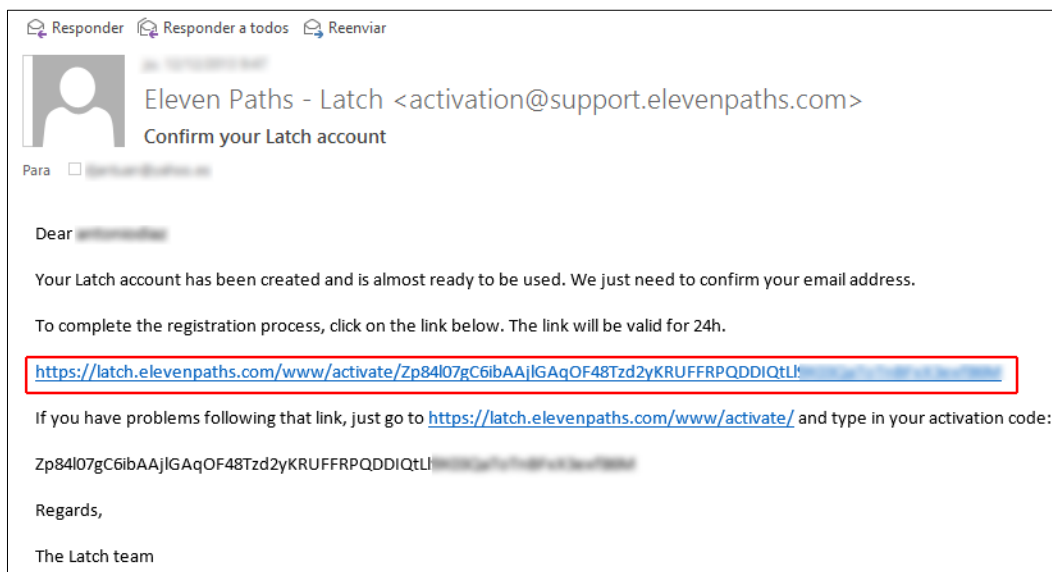


Imagen 11: Correo enviado al usuario con el enlace de activación de su cuenta en Latch.

Tras esta acción el usuario ya dispondrá de una cuenta en Latch, con lo que podrá acceder a la aplicación para proteger sus cuentas digitales.

2.3 Acceso a Latch

Una vez que el usuario ya dispone de una cuenta, deberá acceder a la aplicación a través del botón “Inicia sesión” mencionado anteriormente. Tras pulsar dicho botón, se mostrará una nueva pantalla, donde el usuario tendrá que introducir el correo electrónico y la contraseña con los que creó su cuenta en Latch, en el paso anterior.



Imagen 12: Acceso a la aplicación Latch.



Imagen 13: Pantalla de bienvenida de Latch.

En esta ventana además aparecerá el texto “¿Has olvidado tu contraseña?”, con el que podrá recuperar la contraseña en caso de que no la recuerde. Este proceso se hará mediante el envío por parte de Latch de un correo electrónico al usuario.

Una vez que el usuario ha entrado en la aplicación, aparecerán las cuentas digitales que el usuario tiene vinculadas con Latch. La primera vez que el usuario acceda a la aplicación no aparecerá ninguna, mostrando Latch un mensaje indicándolo: “Parea un nuevo servicio con Latch o bien protéjelo con Cloud TOTP: un PIN temporal de un solo uso”.

2.4 Realización del pareado entre Latch y la cuenta digital

Se llega ahora al paso fundamental. El usuario ya dispone de una cuenta en la aplicación Latch de su dispositivo móvil, y debe disponer de una cuenta digital en el servicio que quiere proteger (Universidad de Salamanca), por lo que el siguiente paso es realizar el pareado propiamente dicho entre las dos cuentas.

2.4.1 Acceso al pareado con Latch en la USAL

Para poder realizar el pareado, el usuario deberá iniciar sesión con sus credenciales en la Universidad de Salamanca y dirigirse al apartado correspondiente a sus datos personales, para ello deberá acceder a la aplicación “[MisDatos](#)”, y, o bien pulsar el botón “Protege tu identidad con Latch” situado en la parte superior de la sección “Mi Perfil” o bien el botón “LATCH” situado en el centro de la barra de herramientas.

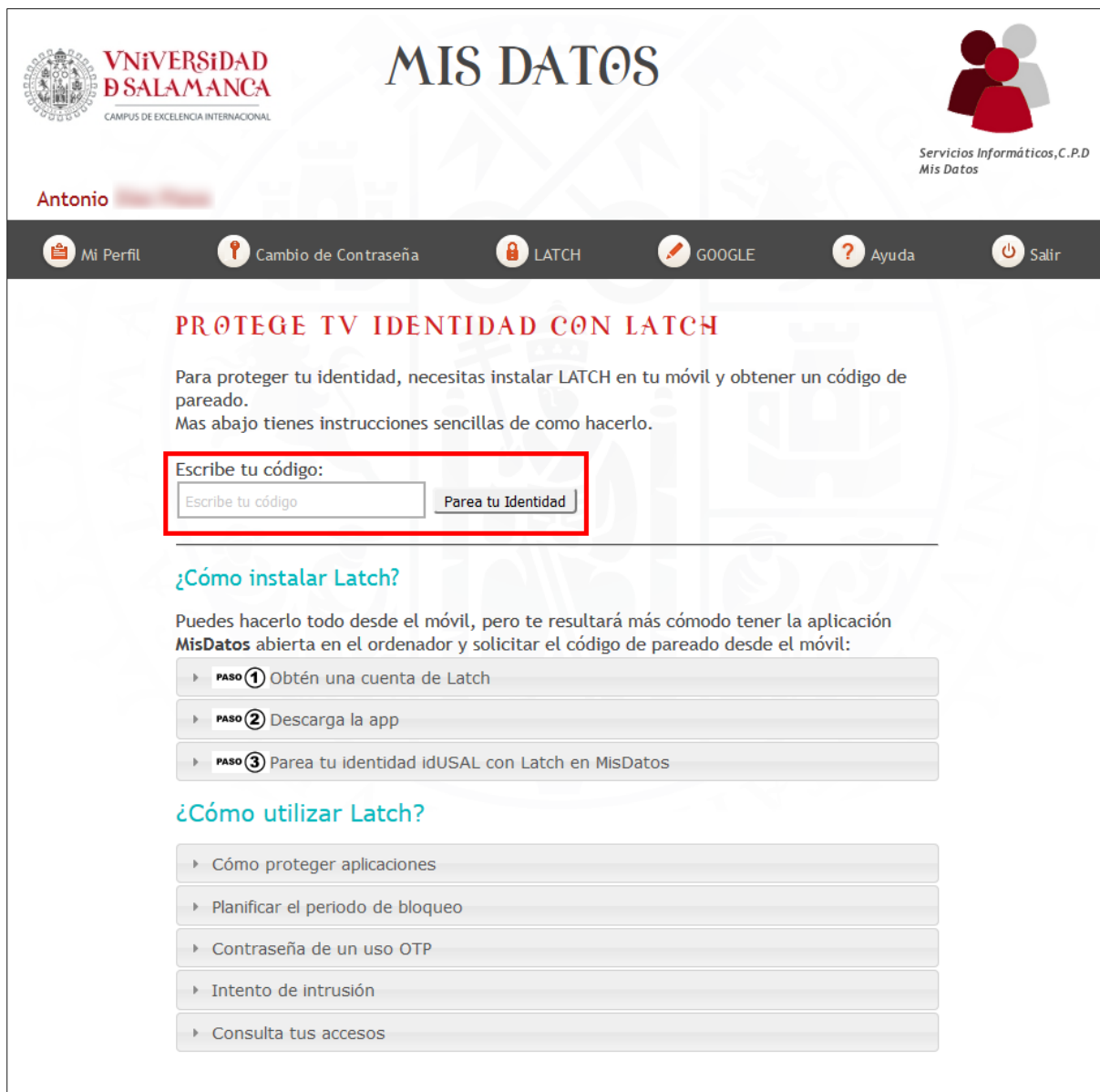
En cualquier caso se accederá al apartado donde se realizará el pareado.



Imagen 14: Acceso a la sección de Latch en la Universidad de Salamanca.

En esta página se describe qué es Latch, qué pasos tiene que seguir un usuario para instalárselo en su dispositivo móvil y además se muestra un resumen de sus principales características, cuyos detalles se pueden observar en este manual.

Esta ventana muestra también la caja de texto en la que el usuario deberá introducir el código de pareado para vincular su cuenta de Latch con su cuenta de la Universidad de Salamanca.



UNIVERSIDAD DE SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

MIS DATOS

Servicios Informáticos, C.P.D
Mis Datos

Antonio

Mi Perfil Cambio de Contraseña LATCH GOOGLE Ayuda Salir

PROTEGE TU IDENTIDAD CON LATCH

Para proteger tu identidad, necesitas instalar LATCH en tu móvil y obtener un código de pareado.
Mas abajo tienes instrucciones sencillas de como hacerlo.

Escribe tu código:

Escribe tu código Parea tu Identidad

¿Cómo instalar Latch?

Puedes hacerlo todo desde el móvil, pero te resultará más cómodo tener la aplicación **MisDatos** abierta en el ordenador y solicitar el código de pareado desde el móvil:

- ▶ PASO ① Obtén una cuenta de Latch
- ▶ PASO ② Descarga la app
- ▶ PASO ③ Parea tu identidad idUSAL con Latch en MisDatos

¿Cómo utilizar Latch?

- ▶ Cómo proteger aplicaciones
- ▶ Planificar el periodo de bloqueo
- ▶ Contraseña de un uso OTP
- ▶ Intento de intrusión
- ▶ Consulta tus accesos

Imagen 15: Zona de pareado.

2.4.2 Generación del código de pareado en el dispositivo móvil

Un “código de pareado” no es más que un conjunto de caracteres creados aleatoriamente. En Latch este código está compuesto por 6 caracteres que pueden ser números o letras, siendo estas mayúsculas o minúsculas. El siguiente paso por tanto es generar en el dispositivo móvil este código que la página web está demandando.

Para ello el usuario pulsará el botón “Añadir nuevo servicio” sito en la parte inferior de la pantalla del dispositivo móvil. En la siguiente pantalla deberá pulsar el botón “Generar nuevo código”. Tras pulsar dicho botón aparecerán unos caracteres, y una barra de desplazamiento correspondiente con una cuenta atrás de 2 minutos de duración.

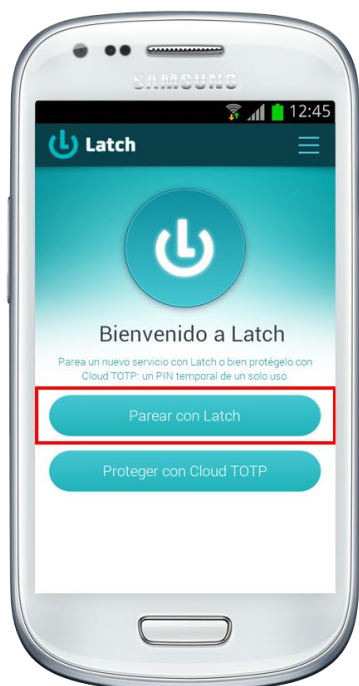


Imagen 16: Pantalla con el botón que da acceso a la siguiente imagen, donde se solicitará el código de pareado.



Imagen 17: Pantalla desde la que se solicita el código de pareado



Imagen 18: Código de pareado que se introducirá en la caja de texto mencionada anteriormente.

Los caracteres se corresponden con el código propiamente dicho. El usuario deberá introducirlos en la caja de texto de la página web mostrada anteriormente. Los caracteres deberán introducirse exactamente de la misma forma en que aparecen en el dispositivo móvil, respetando mayúsculas y minúsculas.



Imagen 19: Introducción del código de pareado en la web de la Universidad de Salamanca.

Si se introduce correctamente el código de pareado, en la página web se indicará mediante un mensaje, y en el dispositivo móvil aparecerá inmediatamente una pantalla indicando que la cuenta digital ya se ha pareado.



Imagen 20: Mensaje mostrando la cuenta digital que se ha pareado.

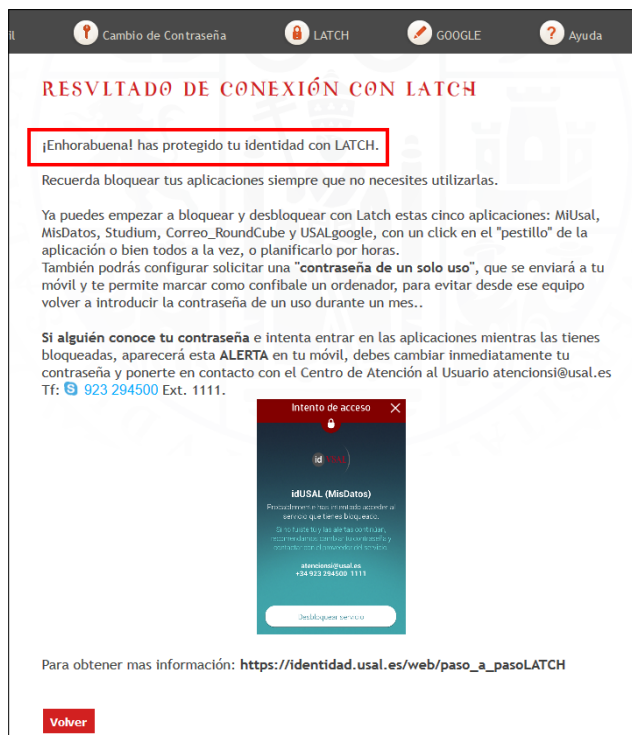


Imagen 21: Página web de la Universidad de Salamanca mostrando que la cuenta digital ha sido pareada.

Desde la pantalla del dispositivo móvil anterior, el usuario podrá acceder al listado de cuentas digitales pareadas pulsando el botón “*Configurar más tarde*”, sito en la parte inferior de la pantalla. Se mostrará entonces una nueva ventana con la cuenta digital recientemente pareada.



Imagen 22: Vista de Latch tras realizar el pareado con la Universidad de Salamanca, teniendo otra cuenta pareada.

3 Ejemplos de utilización de Latch en la USAL

Una vez que la cuenta digital de la Universidad de Salamanca está pareada con Latch, el usuario estará en condiciones de bloquear dicha cuenta para que el acceso a la misma esté limitado a sus necesidades.

La cuenta digital de la Universidad de Salamanca incluye actualmente una serie de operaciones independientes entre sí y que se relacionan directamente con algunos de los servicios ofrecidos por la Universidad de Salamanca.

El usuario podrá bloquear y desbloquear cada una de dichas operaciones a su elección, con lo que conseguirá que los servicios relacionados se bloqueen o desbloqueen. Cada una de las siguientes operaciones se corresponde con un servicio ofrecido por la Universidad de Salamanca:

- MiUsal.
- Studium.
- MisDatos.
- Correo_RoundCube.
- USALgoogle.

Para acceder a dichas operaciones desde Latch basta con pulsar el nombre o el icono de la cuenta “idUSAL” en el dispositivo móvil.

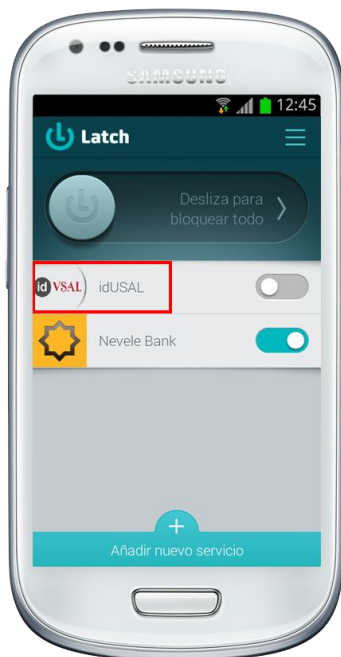


Imagen 23: Acceso a las operaciones de la Universidad de Salamanca protegidas con Latch.



Imagen 24: Operaciones incluidas en la Universidad de Salamanca que están protegidas con Latch.

Cada una de las operaciones incluye un control con el que el usuario podrá bloquear y desbloquear el servicio relacionado con la operación. Pulsando en el nombre de la operación, podrá acceder a la vista de detalles de la misma, desde donde podrá realizar ciertas configuraciones que se mostrarán a continuación.

En los siguientes ejemplos, se van a mostrar algunas de las posibles acciones que se pueden realizar con Latch, en las operaciones mencionadas.

3.1 Ejemplo 1: Bloqueo total de la cuenta digital en la USAL

En este primer ejemplo, el usuario desde Latch realizará un bloqueo total de su cuenta digital en la Universidad de Salamanca, siendo imposible acceder a dicha cuenta desde Internet y por tanto a ninguno de los servicios indicados anteriormente, a menos que el usuario no desbloquee la cuenta previamente desde Latch.

Para la demostración de este ejemplo, el usuario deberá, desde el dispositivo móvil, pulsar el botón gris perteneciente a la cuenta digital de la Universidad de Salamanca. Tras pulsar dicho botón, el color del mismo pasará a ser verde, lo que indicará que la cuenta digital de la Universidad de Salamanca estará bloqueada, y que no se podrá acceder a ninguno de sus servicios protegidos por Latch desde Internet.



Imagen 25: Cuenta de la Universidad de Salamanca desbloqueada.

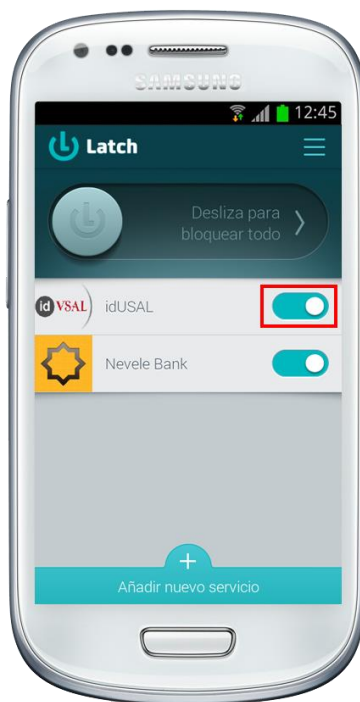


Imagen 26: Cuenta de la Universidad de Salamanca bloqueada.



Imagen 27: Operaciones bloqueadas al estar bloqueada la cuenta de la USAL.

Una vez que esté la cuenta digital de la Universidad de Salamanca bloqueada, el usuario deberá comprobar la imposibilidad de acceder a la misma. Para ello se dirigirá a cualquiera de los servicios que incluye la cuenta (*MiUsal*, *Studium*, *MisDatos*, *Correo_RoundCube* o *USALgoogle*), y en el formulario de acceso correspondiente intentará acceder indicando su nombre y su contraseña.

Las siguientes imágenes muestran:

- El bloqueo total de la cuenta digital de la Universidad de Salamanca que habrá realizado el usuario en el dispositivo móvil.
- El formulario de la página web en el que el usuario deberá introducir su usuario y contraseña para acceder a uno de los servicios protegidos de la cuenta digital.

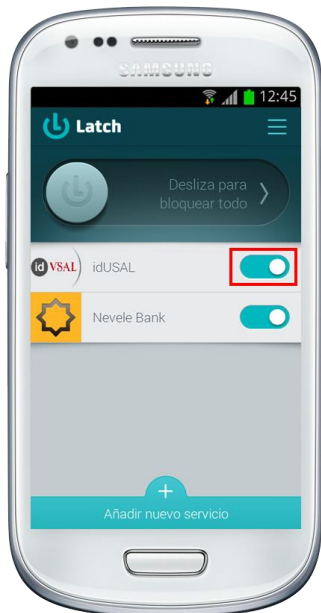


Imagen 28: Bloqueo de la cuenta digital de la Universidad de Salamanca.



Imagen 29 Intento de acceso a uno de los servicios protegidos de la cuenta digital de la Universidad de Salamanca.

En este ejemplo se va a intentar acceder al servicio “*Stodium*”, pero en caso de intentar acceder a cualquiera de los otros 4 servicios protegidos con Latch, el resultado sería el mismo, que el mostrado.



Imagen 30: Notificación recibida al intentar acceder a “*Stodium*”.



Imagen 31: Respuesta tras un intento de acceso estando el servicio bloqueado por Latch.

El resultado será que la Universidad de Salamanca no permitirá el acceso a través de Internet. En el dispositivo móvil el usuario recibirá una notificación indicando que se ha intentado realizar un acceso no autorizado a la cuenta digital de la USAL. En la página web se mostrará el mensaje “*ACCESO DENEGADO A ESTE SERVICIO DE LA USAL*” y unas indicaciones para que pueda hacerlo.

Para que el usuario pueda acceder a su cuenta digital, deberá desbloquearla desde Latch. Para ello deberá pulsar el botón verde para desbloquear el servicio, o directamente el botón “*Desbloquear servicio*” que aparece en la pantalla de notificación del dispositivo móvil (véase imagen 30). Es importante señalar que realizando cualquiera de estas 2 acciones se desbloquearán TODAS las operaciones incluidas, y no solo la que se quiere desproteger momentáneamente. En caso de realizar el desbloqueo desde la notificación se informará de esto último mediante un mensaje.

Una vez desbloqueada la cuenta digital, deberá accederse de nuevo al servicio protegido indicando el usuario y la contraseña tal y como se hizo anteriormente.

El resultado será, que ahora sí se puede acceder a la cuenta digital.



Imagen 32: Desbloqueo del servicio por parte del usuario en Latch.

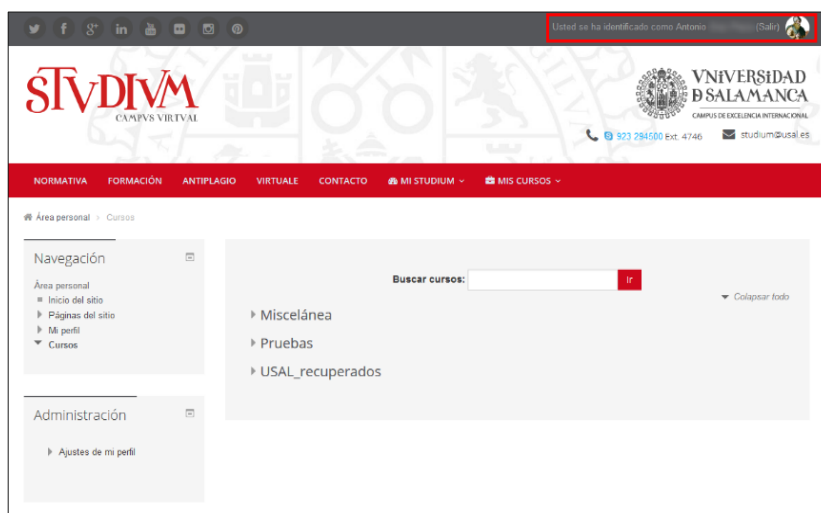


Imagen 33: Acceso correcto por parte del usuario.

3.2 Opciones referentes a bloqueos y desbloqueos.

Cada una de las operaciones mencionadas tienen a su disposición una serie de opciones que se mostrarán a continuación y que permiten personalizar los bloqueos y desbloqueos. Los siguientes ejemplos parten de la lista de operaciones relacionadas con sus respectivas prestaciones que aparecen en la imagen 24.

El usuario deberá pulsar el nombre de una operación y accederá así a la pantalla donde se podrán configurar otras opciones referentes a esta operación. Esta nueva pantalla (llamada **vista de detalles** en este manual) muestra los siguientes elementos:

- Un control deslizante en la parte superior que se utiliza para bloquear o desbloquear el acceso a la operación. En este caso tiene la misma funcionalidad que el botón que aparece en el nombre de la operación.
- Un elemento con el texto “*Autobloqueo por tiempo*”, utilizado para automatizar un bloqueo, se explicará en detalle en el ejemplo siguiente.
- Un elemento con el texto “*Programar bloqueo*”, que es el que se va a mostrar tras el anterior.

- Un elemento con el texto "Contraseña de un uso", utilizado para recibir una contraseña adicional en el smartphone y que se explica en detalle en el último punto.

3.2.1 Ejemplo 2: Configurar un autobloqueo por tiempo

En este ejemplo el usuario desde Latch establecerá un "Autobloqueo por tiempo" de un servicio. La funcionalidad de esta opción es muy simple: el servicio en cuestión se bloqueará automáticamente cuando transcurra un tiempo establecido por el usuario, sin que este tenga necesidad de bloquearlo manualmente.

La utilidad de esta funcionalidad viene dada en el caso en que el usuario olvide bloquear el servicio cuando finalicen sus gestiones en la página web de la Universidad de Salamanca. Gracias al "Autobloqueo por tiempo" Latch será capaz de bloquear el servicio en cuestión automáticamente para evitar posibles intrusiones.

El escenario que se presenta es que un usuario desbloqueará el servicio desde Latch y configurará un "Autobloqueo por tiempo" que durará 5 minutos, lo que quiere decir que durante esos 5 minutos el usuario será capaz de acceder a la página web del servicio, pero transcurridos los cuales este pasará al estado de "bloqueado" automáticamente, y ni el usuario ni un posible intruso serán capaces de acceder de nuevo al servicio hasta que se desbloquee de nuevo.

La configuración del tiempo de autobloqueo se realiza desde el menú de "Configuración", en el apartado "Tiempo de autobloqueo". Hay que señalar que el tiempo de autobloqueo que se establezca aquí será válido para todos los servicios y operaciones que utilicen esta opción, y que las opciones de "Autobloqueo por tiempo" y "Bloqueo programado" son autoexcluyentes en un mismo servicio u operación.

En este ejemplo se ha establecido un "Autobloqueo por tiempo" de 5 minutos al servicio "MiUsal".



Imagen 34: Vista de detalles.
"Autobloqueo por tiempo" establecido a 5 minutos.

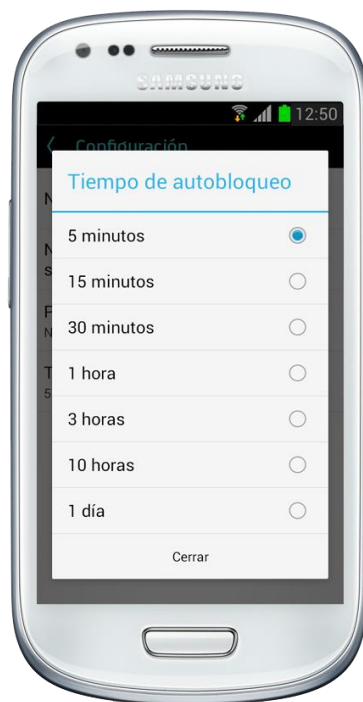


Imagen 35: Configuración del tiempo de autobloqueo.



Imagen 36: Bloqueo realizado transcurridos los 5 minutos.

3.2.2 Ejemplo 3: Programar un bloqueo durante ciertas horas del día

En este ejemplo el usuario desde Latch realizará un bloqueo durante un horario determinado, siendo imposible acceder a uno de los servicios de la Universidad de Salamanca incluidos en Latch desde Internet, durante dicho horario establecido por el usuario.



Imagen 37: Horario de 12:00 a 20:00 bloqueado.



Imagen 38: Horario de 00:00 a 12:00 desbloqueado.

Al pulsar sobre el botón situado junto al texto "*Programar bloqueo*" aparece una barra con unos números que hacen referencia a las horas del día, y dos botones circulares movibles, que se utilizan para configurar dichas horas. La franja horaria que hay entre dichos manejadores aparecerá resaltada en color azul, y el control deslizante de la parte superior cambiará de posición dependiendo si la hora actual está o no entre los límites de la hora programada por el usuario. Además bajo este control deslizante aparecerá el texto "BLOQUEO PROGRAMADO" y la franja horaria en la que este se ha establecido.

En la imagen 37 se puede apreciar que al programar el usuario un bloqueo desde las "12:00" hasta las "20:00", el control deslizante indica que el servicio está "*bloqueado*", debido a que las "12:45", que es la hora actual está incluida dentro de los márgenes establecidos. En la imagen 38 en cambio, se ha programado un bloqueo desde las "00:00" hasta las "12:00", siendo el estado actual en tal caso de "*desbloqueado*".

En caso de intento de acceso al servicio en las horas no permitidas el usuario recibirá una notificación en el dispositivo móvil similar a la de la imagen 30, siendo imposible acceder al mismo. Para poder acceder a su servicio el usuario deberá o bien cambiar el horario programado, o bien mover el control deslizante para desbloquear este servicio.

3.2.3 Ejemplo 4: Establecer una contraseña de un uso

En este ejemplo el usuario establecerá un nuevo factor de seguridad en la operación *Correo_RoundCube* por ejemplo. Dicho nuevo factor consiste en que la página web solicita una contraseña que acaba de enviar a la cuenta de Latch. En caso de que no se introduzca dicha contraseña en la página web, no se podrá realizar el acceso a la misma.

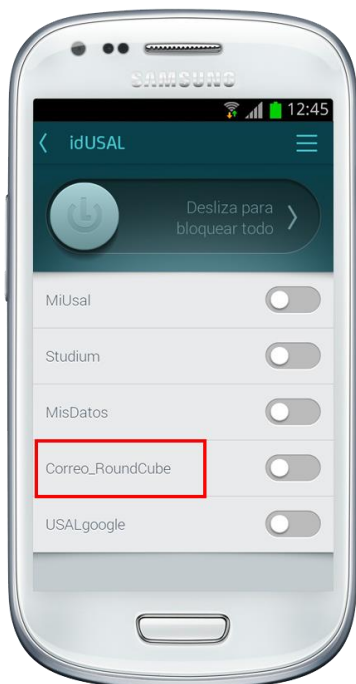


Imagen 39: Acceso a otras opciones de "InternationalTransfer".



Imagen 40: "Contraseña de un uso" en estado "Off".



Imagen 41: "Contraseña de un uso" en estado "On".

Para activar la "Contraseña de un uso" deberá pulsarse el botón resaltado de la imagen 40, lo que hará que aparezca un botón con el texto "Enviar contraseña de nuevo" bajo este elemento. Con este gesto ya se ha activado la "Contraseña de un uso", a partir de ahora si el usuario intenta acceder a *Correo_RoundCube* la página web mostrará una caja de texto donde el usuario deberá escribir la contraseña de un solo uso que ha recibido en su dispositivo móvil.




Imagen 42: Notificación de Latch con la contraseña de un solo uso.



Imagen 43: Petición de la contraseña de un solo uso por parte de la Universidad de Salamanca.



 Es importante tener en cuenta que para recibir la contraseña de un solo uso en el dispositivo móvil, el usuario debe tener su sesión iniciada en Latch. No es necesario (aunque sí recomendable) que esté la app en primer plano. En caso de que no haya iniciado sesión en Latch no recibirá la contraseña de un solo uso. Deberá en tal caso iniciar sesión en Latch, y pulsar el botón "Enviar contraseña de nuevo" (véase imagen 41), para volver a recibir la contraseña.

4 Opciones y personalización de Latch

4.1 Renombrar y reordenar servicios y operaciones

Es posible cambiar el nombre de los servicios y operaciones en el dispositivo móvil de dos formas distintas. Una de ellas es a través de la vista de detalles del servicio y, pulsando sobre el nombre del mismo que aparece en la parte superior, renombrarlo. En caso de que se desee modificar el nombre de una operación deberá accederse a la vista de detalles de la misma y pulsar sobre el nombre de la operación. Este cambio solo afecta al servicio u operación en la propia aplicación Latch. Si se volviera a palear el servicio más adelante, tanto este como sus operaciones volverían a tener el nombre original que tuvieron.

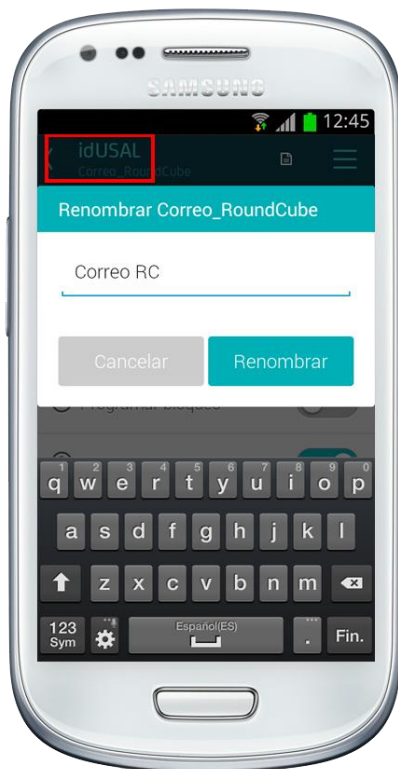


Imagen 44: Cambio de nombre de la operación Correo_RoundCube por "Correo RC" desde la vista de detalles del servicio.



Imagen 45: Reordenación de operaciones. Ubicación de "Correo RC" en la segunda posición.

Puede cambiarse la posición de un servicio u operación de un listado para colocarlos según elección propia. Para ello, simplemente hay que mantener pulsado el servicio u operación del listado y a continuación moverlo hacia arriba o hacia abajo.

4.2 Opciones contextuales de los servicios y operaciones

El acceso a estas opciones es ligeramente distinto según la plataforma que se esté utilizando:

- En Android, BlackBerry y Firefox OS se accede a estas opciones manteniendo pulsado durante unos segundos un servicio u operación.
- En iOS y Windows Phone se accede deslizando hacia la derecha un servicio u operación.

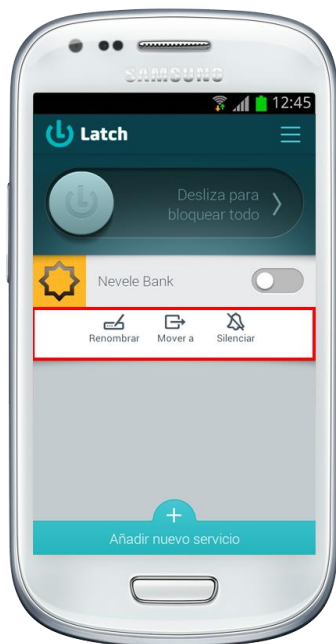


Imagen 46: Opciones contextuales del servicio idUSAL en Android.



Imagen 47: Opciones contextuales del servicio idUSAL en iOS.

Las opciones disponibles dependen de si se está accediendo desde un servicio o desde una operación. En caso de que sea un servicio, también varían las opciones en función de si este incluye o no operaciones. Las opciones disponibles son 4 (*Renombrar, Mover a, Silenciar y Log*).+

4.2.1 Renombrar

Es la otra forma de renombrar servicios y operaciones, y está disponible en ambos. En caso de indicar un nombre muy extenso aparecerán 3 puntos al final del mismo, y siempre debe incluir algún texto, de no ser así se mostrará el nombre original.

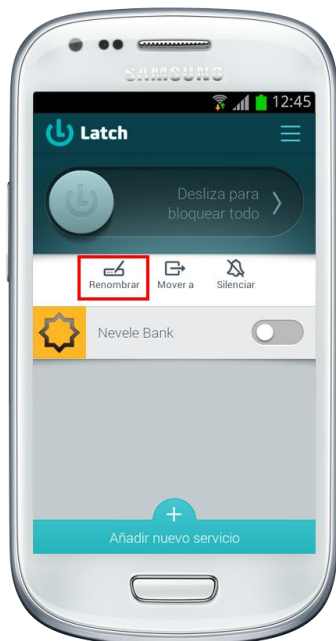


Imagen 48: Acceso a la opción "Renombrar".

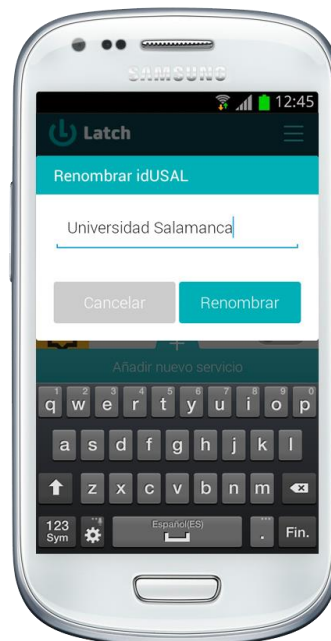


Imagen 49: Renombrado del servicio idUSAL por "Universidad Salamanca".

4.2.2 Mover a

Disponible en servicios únicamente, permite mover los servicios a grupos o crear grupos directamente. El objetivo es que el usuario tenga los servicios organizados según su propio criterio. Su funcionamiento es similar al existente entre archivos y directorios. No es posible crear grupos dentro de grupos y en caso de eliminar un grupo que incluyese servicios, estos simplemente quedarían fuera del grupo.

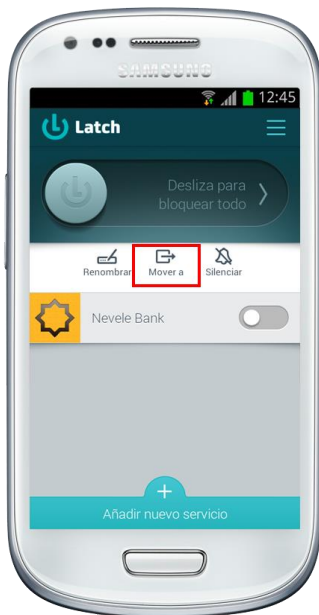


Imagen 50: Acceso a la opción "Mover a".

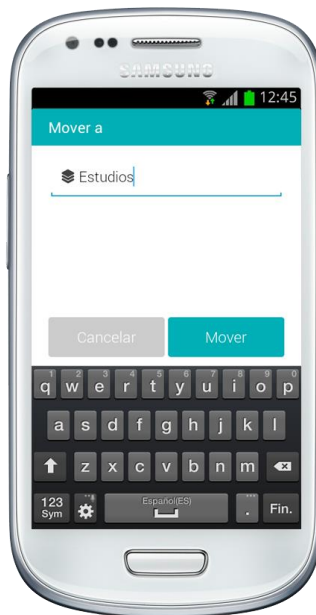


Imagen 51: Creación del grupo "Estudios".



Imagen 52: "Universidad de Salamanca" ya incluida en el grupo "Estudios".

4.2.3 Silenciar

Disponible tanto en servicios como en operaciones, en caso de que esté activo aparece un icono de una campana tachado junto al nombre. Con esta opción se impide que se reciban notificaciones de tipo "Intento de acceso" ni de "Servicio accedido" referentes a este servicio u operación.

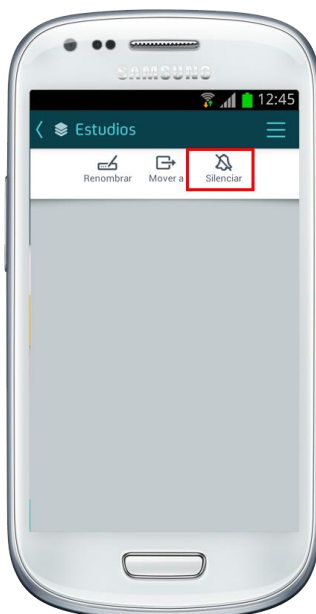


Imagen 53: Acceso a la opción "Silenciar".



Imagen 54: Icono representativo de "Silenciar".

4.2.4 Log

Disponible tanto en servicios sin operaciones como en operaciones, (siempre y cuando no incluyan a su vez operaciones internas). Esta opción permite mostrar un historial de los eventos realizados con el servicio u operación, y la cantidad de aquellos.

El acceso a la ventana *Log* se puede hacer bien desde el menú contextual o bien a través de un botón situado en la parte superior de la vista detalles.

La ventana *Log* se puede dividir en 3 partes bien diferenciadas:

- La parte superior incluye unos botones que permiten configurar el intervalo temporal y qué eventos se desean incluir en el historial. Por defecto se muestran todos los eventos del día en curso. Cada evento está identificado por un icono y un color.
- La parte central incluye un historial con cada uno de los eventos realizados, además de la fecha y hora en la que se produjo.
- La parte inferior incluye un botón para mostrar las estadísticas de uso. Básicamente muestra los datos del historial en modo numérico.

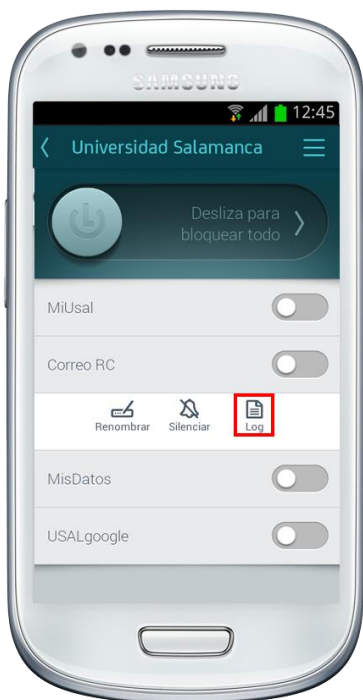


Imagen 55: Acceso a la ventana Log de la operación Studium desde el menú contextual.

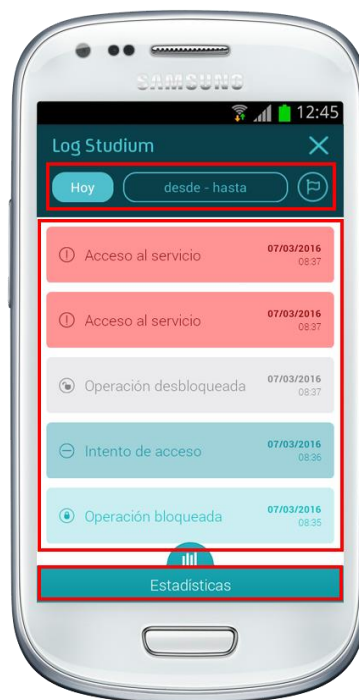


Imagen 56: Botones de la ventana Log, historial de eventos del día actual y botón Estadísticas.

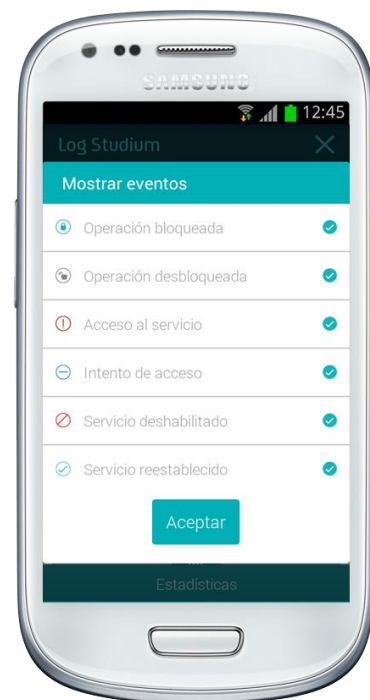


Imagen 57: Eventos disponibles accesibles a través del botón en forma de bandera.

4.3 El menú lateral de Latch

El menú lateral de Latch contiene principalmente opciones de configuración de Latch, e información acerca de su uso. Además muestra el nombre de sesión que se ha utilizado para acceder a Latch, y ofrece la oportunidad de cerrar la sesión, siendo necesario volver a introducir el usuario y la contraseña para volver a entrar.

A este menú se puede acceder desde múltiples pantallas de Latch, y siempre se hará desde el botón situado en la esquina superior derecha.

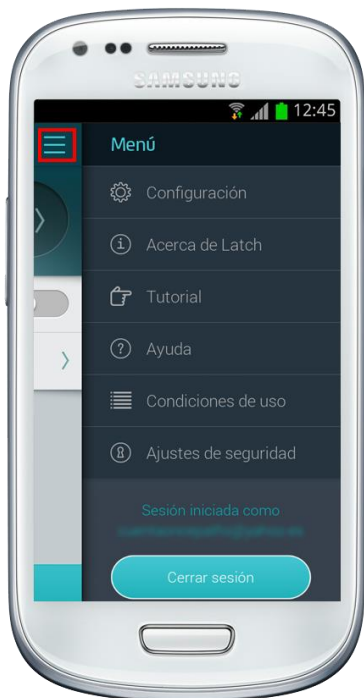


Imagen 58: Vista del menú lateral.



Imagen 59: Acceso desde la página de inicio.



Imagen 60: Acceso desde las cuentas pareadas.

Las opciones que muestra el menú lateral son las siguientes:

- **Configuración:** En la imagen siguiente se puede apreciar que se disponen de 4 apartados perfectamente definidos, que se explican a continuación:

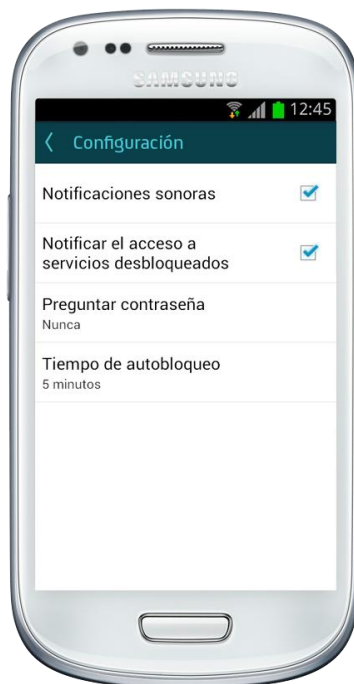


Imagen 61: Opciones disponibles en el apartado "Configuración".

1. **Notificaciones sonoras:** Activando esta opción, las notificaciones de Latch que se reciban cuando esté la sesión abierta y la aplicación en segundo plano emitirán un sonido. Estas notificaciones pueden ser de cualquiera de los tipos vistos en los ejemplos anteriores. Esta opción no está disponible en dispositivos Firefox OS.
2. **Notificar el acceso a servicios desbloqueados:** Activando esta opción se recibirá una notificación cuando se acceda a un servicio que esté pareado con Latch. En esta notificación aparecerá un icono con forma de advertencia bajo el logotipo del servicio y un botón para poder bloquearlo.

Gracias a esta opción el usuario será capaz de saber en todo momento los accesos que se están realizando a su servicio.



Imagen 62: Operación "USAL_Google" desbloqueada.



Imagen 63: Notificación recibida al acceder a la operación USAL_Google estando la operación desbloqueada.

3. **Preguntar contraseña:** Con esta opción se podrá indicar, cada cuanto tiempo Latch pedirá el nombre de usuario y la contraseña para acceder.

El valor por defecto es "Nunca", por este motivo cuando se accede a Latch por primera vez ya no se necesita volver a introducir el usuario y la contraseña, aunque se apague el dispositivo móvil. Gracias a esta opción se podrá añadir un nivel adicional de seguridad a la hora de acceder a la cuenta de Latch.

En caso de que se seleccione la opción "Siempre", se tendrán que introducir las credenciales de acceso cada vez que la aplicación vuelva al primer plano. Además en caso de que se reciba una notificación referente a un acceso, sea este autorizado o no, en la notificación no aparecerá ningún botón para realizar la acción correspondiente.

De esta forma el usuario se asegura de que no se pueda realizar ninguna acción sin que él haya accedido previamente a Latch.



Imagen 64: Opción para que Latch siempre solicite la contraseña.



Imagen 65: Petición de credenciales tras marcar la opción "Siempre".



Imagen 66: Notificación sin botón (compárese con la imagen 30).

4. Tiempo de autobloqueo: Esta opción se mostró anteriormente (véase imagen 35), sirve para establecer el tiempo de "Autobloqueo por tiempo" para todos los servicios.

- **Acerca de Latch:** Simplemente muestra un resumen acerca de la funcionalidad de Latch. También permite ver la versión del producto.
- **Condiciones de uso:** En esta pantalla se puede acceder a las páginas web de Latch, en las que se muestra la información legal disponible para todos los usuarios que deseen utilizar Latch. Esta información incluye las características de Latch respecto a sus aspectos legales.
- **Tutorial:** Este tutorial muestra una serie de 9 pantallas que resumen el funcionamiento de Latch.
- **Ayuda:** Contiene dos botones desde los que se podrá acceder a la solución de cualquier duda que se tenga respecto a Latch.

La respuesta a casi todas las dudas está en la página web de Latch, concretamente en la sección "Ayuda". Se puede acceder a esta sección en el dispositivo móvil desde el primero de los botones. En caso de que la sección "Ayuda" no resuelva las dudas, se puede contactar directamente con *Telefónica Digital Identity & Privacy* por correo electrónico para formular la consulta a través del segundo botón. En ese mismo correo electrónico se podrán enviar también sugerencias y opiniones acerca del producto.

- **Ajustes de seguridad:** Esta pantalla consta de 2 partes:
 1. **Gestión de sesiones:** Permite ver en qué dispositivos está actualmente iniciada la sesión con la cuenta de Latch del usuario. En la parte superior se mostrarán los datos del dispositivo móvil actual, estos datos incluyen el sistema operativo, y el tipo de dispositivo. A continuación se muestra el apartado "OTROS DISPOSITIVOS", que incluye un listado de dispositivos en los que la cuenta está activa actualmente, bien porque otro usuario haya iniciado sesión en ella o bien porque el propio usuario olvidó cerrar la sesión en dichos dispositivos.

Este listado muestra también el sistema operativo y el tipo de dispositivo en el que se inició sesión, y además cuándo fue su último uso. Desde cada uno de los elementos del listado, el usuario podrá cerrar la sesión en cada uno de esos dispositivos de forma remota utilizando el botón con forma de aspa. También será capaz de cerrar todas las sesiones de todos los dispositivos simultáneamente (excepto del suyo propio), a través del botón "CERRAR TODAS" de la parte inferior del listado.

- Cambiar contraseña:** Desde esta pantalla se podrá cambiar la contraseña de acceso a Latch. Esta contraseña es la misma que se indicó cuando se creó la cuenta. Para realizar el cambio de contraseña deberá introducirse la dirección de correo electrónico con la que se accede a Latch, y en la misma se recibirá información acerca de los pasos que deben realizarse.

Al cambiar la contraseña se cerrarán las sesiones que se tengan abiertas de Latch en TODOS los dispositivos móviles, y se tendrán que introducir las credenciales para acceder de nuevo.

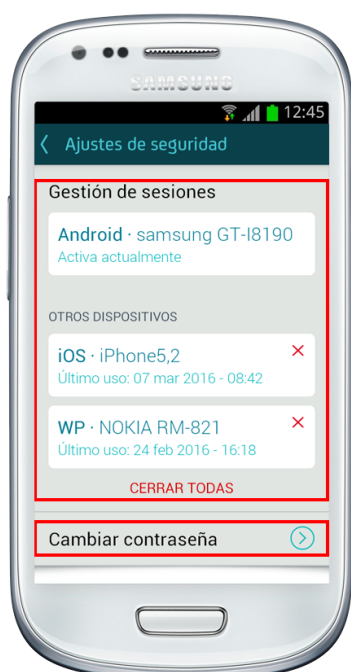


Imagen 67: Pantalla "Ajustes de seguridad" con las opciones "Gestión de sesiones" y "Cambiar contraseña".

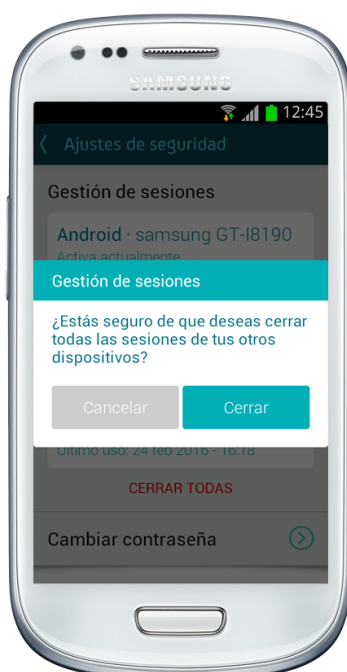


Imagen 68: Advertencia de que se van a cerrar las sesiones de los otros dispositivos.



Imagen 69: Pantalla "Cambiar la contraseña".

5 Índice de imágenes

Imagen 01: Acceso a PlayStore.	4
Imagen 02: Búsqueda de Latch.	4
Imagen 03: Instalación de Latch.	4
Imagen 04: Aceptar permisos.	5
Imagen 05: Abrir Latch tras instalarlo.	5
Imagen 06: Icono de Latch.	5
Imagen 07: Pantalla inicial de Latch.	6
Imagen 08: Tutorial de Latch.	6
Imagen 09: Acceso al registro.	6
Imagen 10: Creación de una nueva cuenta en Latch.	6
Imagen 11: Correo enviado al usuario con el enlace de activación de su cuenta en Latch.	7
Imagen 12: Acceso a la aplicación Latch.	7
Imagen 13: Pantalla de bienvenida de Latch.	7
Imagen 14: Acceso a la sección de Latch en la Universidad de Salamanca.	8
Imagen 15: Zona de pareado.	9
Imagen 16: Pantalla con el botón que da acceso a la siguiente imagen, donde se solicitará el código de pareado.	10
Imagen 17: Pantalla desde la que se solicita el código de pareado.	10
Imagen 18: Código de pareado que se introducirá en la caja de texto mencionada anteriormente.	10
Imagen 19: Introducción del código de pareado en la web de la Universidad de Salamanca.	10
Imagen 20: Mensaje mostrando la cuenta digital que se ha pareado.	11
Imagen 21: Página web de la Universidad de Salamanca mostrando que la cuenta digital ha sido pareada.	11
Imagen 22: Vista de Latch tras realizar el pareado con la Universidad de Salamanca, teniendo otra cuenta pareada.	11
Imagen 23: Acceso a las operaciones de la Universidad de Salamanca protegidas con Latch.	12
Imagen 24: Operaciones incluidas en la Universidad de Salamanca que están protegidas con Latch.	12
Imagen 25: Cuenta de la Universidad de Salamanca desbloqueada.	13
Imagen 26: Cuenta de la Universidad de Salamanca bloqueada.	13
Imagen 27: Operaciones bloqueadas al estar bloqueada la cuenta de la USAL.	13
Imagen 28: Bloqueo de la cuenta digital de la Universidad de Salamanca.	14
Imagen 29 Intento de acceso a uno de los servicios protegidos de la cuenta digital de la Universidad de Salamanca.	14
Imagen 30: Notificación recibida al intentar acceder a “Stadium”.	14
Imagen 31: Respuesta tras un intento de acceso estando el servicio bloqueado por Latch.	14
Imagen 32: Desbloqueo del servicio por parte del usuario en Latch.	15
Imagen 33: Acceso correcto por parte del usuario.	15
Imagen 34: Vista de detalles. “Autobloqueo por tiempo” establecido a 5 minutos.	16
Imagen 35: Configuración del tiempo de autobloqueo.	16

Imagen 36: Bloqueo realizado transcurridos los 5 minutos.	16
Imagen 37: Horario de 12:00 a 20:00 bloqueado.	17
Imagen 38: Horario de 00:00 a 12:00 desbloqueado.	17
Imagen 39: Acceso a otras opciones de "InternationalTransfer".	18
Imagen 40: "Contraseña de un uso" en estado "Off"	18
Imagen 41: "Contraseña de un uso" en estado "On".	18
Imagen 42: Notificación de Latch con la contraseña de un solo uso.	18
Imagen 43: Petición de la contraseña de un solo uso por parte de la Universidad de Salamanca.	18
Imagen 44: Cambio de nombre de la operación Correo_RoundCube por "Correo RC" desde la vista de detalles del servicio.	20
Imagen 45: Reordenación de operaciones. Ubicación de "Correo RC" en la segunda posición.	20
Imagen 46: Opciones contextuales del servicio idUSAL en Android.	21
Imagen 47: Opciones contextuales del servicio idUSAL en iOS.	21
Imagen 48: Acceso a la opción "Renombrar".	21
Imagen 49: Renombrado del servicio idUSAL por "Universidad Salamanca".	21
Imagen 50: Acceso a la opción "Mover a".	22
Imagen 51: Creación del grupo "Estudios".	22
Imagen 52: "Universidad de Salamanca" ya incluida en el grupo "Estudios".	22
Imagen 53: Acceso a la opción "Silenciar".	22
Imagen 54: Icono representativo de "Silenciar".	22
Imagen 55: Acceso a la ventana Log de la operación Studium desde el menú contextual.	23
Imagen 56: Botones de la ventana Log, historial de eventos del día actual y botón Estadísticas.	23
Imagen 57: Eventos disponibles accesibles a través del botón con forma de bandera.	23
Imagen 58: Vista del menú lateral.	24
Imagen 59: Acceso desde la página de inicio.	24
Imagen 60: Acceso desde las cuentas pareadas.	24
Imagen 61: Opciones disponibles en el apartado "Configuración".	24
Imagen 62: Operación "USAL_Google" desbloqueada.	25
Imagen 63: Notificación recibida al acceder a la operación USAL_Google estando la operación desbloqueada.	25
Imagen 64: Opción para que Latch siempre solicite la contraseña.	26
Imagen 65: Petición de credenciales tras marcar la opción "Siempre"	26
Imagen 66: Notificación sin botón (compárese con la imagen 30).	26
Imagen 67: Pantalla "Ajustes de seguridad" con las opciones "Gestión de sesiones" y "Cambiar contraseña"	27
Imagen 68: Advertencia de que se van a cerrar las sesiones de los otros dispositivos.	27
Imagen 69: Pantalla "Cambiar la contraseña".	27



6 Recursos

Para información acerca de cómo utilizar la app Latch, y probar gratuitamente sus múltiples características, puede consultarse la guía del usuario en español e inglés:

1. [Guía del usuario de Latch con Nevele Bank.](#)
2. [Latch user's guide for Nevele Bank.](#)

Además puede encontrarse la siguiente documentación constantemente ampliada:

- Manuales en español e inglés acerca de la integración y utilización de Latch con los plugins disponibles, en la propia [web de Latch](#) y en el canal de [Slideshare](#) de ElevenPaths.
- Vídeos subtítulos en español e inglés acerca de la integración y utilización de Latch con los plugins disponibles en los canales de ElevenPaths en [YouTube](#) y [Vimeo](#)
- Manuales acerca de la integración y utilización de Latch en las organizaciones que ya lo han implantado (Movistar, Tuenti, UNIR, USAL, etcétera), en la propia [web de Latch](#) y en el canal de [Slideshare](#) de ElevenPaths.
- Información acerca de la [API de Latch](#) en la propia web de Latch.

PUBLICACIÓN:**Noviembre 2016**

En ElevenPaths pensamos de forma diferente cuando hablamos de seguridad. Liderados por Chema Alonso, somos un equipo de expertos con inquietud para replantearnos la industria y gran experiencia y conocimiento en el sector de la seguridad. Dedicamos toda nuestra experiencia y esfuerzos en crear productos innovadores para que la vida digital sea más segura para todos.

La evolución de las amenazas de seguridad en la tecnología es cada vez más rápida y constante. Por eso, desde junio de 2013, nos hemos constituido como una start-up dentro de Telefónica para trabajar de forma ágil y dinámica, y ser capaces de transformar el concepto de seguridad anticipándonos a los futuros problemas que afecten a nuestra identidad, privacidad y disponibilidad online.

Con sede en Madrid, estamos presentes también en Londres, EE.UU, Brasil, Argentina y Colombia.

TIENES ALGO QUE **CONTARNOS, PUEDES HACERLO EN:**elevenpaths.comBlog.elevenpaths.com[@ElevenPaths](https://twitter.com/ElevenPaths)[Facebook.com/ElevenPaths](https://www.facebook.com/ElevenPaths)[YouTube.com/ElevenPaths](https://www.youtube.com/ElevenPaths)

La información contenida en el presente documento es propiedad de Telefónica Digital España, S.L.U. ("TDE") y/o de cualquier otra entidad dentro del Grupo Telefónica o sus licenciantes. TDE y/o cualquier compañía del Grupo Telefónica o los licenciantes de TDE se reservan todos los derechos de propiedad industrial e intelectual (incluida cualquier patente o copyright) que se deriven o recaigan sobre este documento, incluidos los derechos de diseño, producción, reproducción, uso y venta del mismo, salvo en el supuesto de que dichos derechos sean expresamente conferidos a terceros por escrito. La información contenida en el presente documento podrá ser objeto de modificación en cualquier momento sin necesidad de previo aviso.

La información contenida en el presente documento no podrá ser ni parcial ni totalmente copiada, distribuida, adaptada o reproducida en ningún soporte sin que medie el previo consentimiento por escrito por parte de TDE.

El presente documento tiene como único objetivo servir de soporte a su lector en el uso del producto o servicio descrito en el mismo. El lector se compromete y queda obligado a usar la información contenida en el mismo para su propio uso y no para ningún otro.

TDE no será responsable de ninguna pérdida o daño que se derive del uso de la información contenida en el presente documento o de cualquier error u omisión del documento o por el uso incorrecto del servicio o producto. El uso del producto o servicio descrito en el presente documento se regulará de acuerdo con lo establecido en los términos y condiciones aceptados por el usuario del mismo para su uso.

TDE y sus marcas (así como cualquier marca perteneciente al Grupo Telefónica) son marcas registradas. TDE y sus filiales se reservan todos los derechos sobre las mismas.