Memoria de la acción AYUDAS DE LA UNIVERSIDAD DE SALAMANCA PARA LA INNOVACIÓN DOCENTE

ANÁLISIS Y PROPUESTA DE DIFERENTES MÉTODOS DE AUTENTICACIÓN PARA EL ACCESO A LAS PLATAFORMAS DE FORMACIÓN ON-LINE Y AL SERVICIO DE CALIFICACIÓN DE ACTAS

Código del Proyecto: ID2016/106

Hablar de universidades online, **virtuales, es hablar de futuro,** así que es inevitable hacer un receso para admirar qué nos depara el futuro.

El desarrollo e implementación de las **tecnologías de la información y comunicación** (TIC), en todos los ámbitos de la vida cotidiana ha revolucionado y modificado, específicamente, el sistema de enseñanza tradicional. Parte de la enseñanza presencial ha pasado a tener una parte on-line o bien ha pasado a semipresencial o no presencial, llamada virtual; este nuevo tipo de formación debe apoyarse en el uso de las redes telemáticas y en los nuevos recursos TIC.

Relacionado con las TIC se viene desarrollando un nuevo espacio para la enseñanza y el aprendizaje: el Campus Virtual. **El Campus Virtual** es un espacio de docencia que se desarrolla a través de las redes telemáticas y que participa conjuntamente con el sistema de enseñanza convencional**. Su finalidad es doble: apoyar a la docencia universitaria presencial y extender la enseñanza superior a más alumnos mediante formación virtual.**

A la fecha de hoy, la herramienta más usada tanto para el apoyo de la docencia universitaria presencial como para la formación virtual es la plataforma Moodle. **Posiblemente la mayor problemática en la formación virtual es acreditar la identidad del estudiante,** es decir, saber que quien realiza la formación es quien dice ser.

Son muchos los métodos de autenticación: el identificador y contraseña, los certificados PKI sobre tarjeta inteligente o token USB, certificado software instalado en un navegador, métodos biométricos (reconocimiento facial, huella dactilar, …), etc.
El segundo factor de autenticación es un método de validación adicional de datos que, sumado a los métodos habituales, permite intensificar los niveles de seguridad; por poner un ejemplo a nivel bancario es muy frecuente utilizar *una tarjeta plástica* que tiene en el dorso una matriz de 9 filas y 9 columnas; cada celda contiene pares de datos (números), los cuales le serán solicitados al momento de la firma de cualquier operación monetaria o bien *el uso de una clave móvil*, que es una aplicación que puede ser instalada en cualquier dispositivo smartphone y que funciona como método de validación de datos, intensificando los niveles de seguridad y evitando el fraude electrónico, permitiendo generar claves de autenticación dinámica para la firma de operaciones.

Antes de haber iniciado este estudio, sospechábamos que la mayoría de los usuarios de la Universidad de Salamanca para el acceso a la plataforma de formación Studium utilizamos exclusivamente la autenticación por el método más inseguro, la contraseña que incluso la dejamos en nuestros ordenadores en modo recordatorio y cambiamos con poca frecuencia a lo largo del tiempo y en más de una ocasión hemos sospechado de que los alumnos intercambian las claves, acceden unos con las claves de otros e incluso que el acceso se lleva a cabo por profesores de academias que se ofrecen a realizar las tareas de los estudiantes.

Sin duda la situación anterior es preocupante y alarmante, pero aún más, los profesores hacemos uso de esa contraseña no sólo para acceder al correo electrónico y a la plataforma Studium, sino para grabar los documentos que dan fe de las competencias adquiridas por el estudiante, las actas

Objetivos

Por todo ello los **objetivos planteados** en este proyecto son:

- Conocer el porcentaje de uso de los diferentes métodos que dispone la USAL para acceder a Studium y al sistema de calificación de actas, por parte de los profesores participantes en este proyecto, de los alumnos de las asignaturas en las que se propone aplicar el proyecto y de los miembros de la Junta de Facultad de Ciencias.
- Analizar la seguridad o inseguridad de cada método.
- Estudiar el motivo por el que se utiliza uno u otro método.
- Analizar si los métodos utilizados son los adecuados.
- Proponer alternativas de autenticación con mayor nivel de seguridad. Formar a los participantes en los nuevos métodos.
- Poner en prueba estas alternativas de autenticación.
- Debatir si es necesario un segundo factor de autenticación. Analizar ventajas e inconvenientes.
- Conocer el porcentaje de usuarios que tienen activado el Latch que proporciona la Universidad.
- Estudiar qué método sería el adecuado como primer y/o segundo factor de autenticación para el acceso a plataformas de formación.
- Hacer una propuesta para la autenticación en el servicio de calificación de actas.

Impacto sobre la docencia

En la actualidad toda la formación Oficial en la universidad de Salamanca es presencial entendiendo que la mayor dificultad en la formación virtual es la acreditación del estudiante sobretodo en el momento de realizar la evaluación on-line. En la enseñanza presencial para la evaluación continua nos da miedo dar más peso a los cuestionarios o tareas realizadas por la plataforma de formación on-line por la inseguridad de quien lo ha realizado. **Por ello, si aumentamos el grado de certeza de quién es quién se está formando podremos apostar más por la formación virtual, por la semipresencial o presencial con mayor formación complementaria on-line.**

Beneficios obtenidos

- Conocer qué método de autenticación se utiliza mayoritariamente.
- Reflexionar sobre la inseguridad de utilizar un identificador y una contraseña.
- Concienciar de la necesitad de utilizar otros métodos de autenticación más seguros.
- Evaluar la dificultad que tenemos para utilizar estos otros métodos.
- Hallar propuesta para intensificar el nivel de seguridad para el acceso a la plataforma de formación y al sistema de calificación de actas.

Metodología de trabajo

Hemos seleccionado diferentes asignaturas en las que hemos pasado el formulario del **anexo I**, en concreto en las siguientes asignaturas:

- Programación I y II - 1er curso Grado en Ingeniería Informática. Facultad de Ciencias
- Informática teórica - 2º curso del Grado en Ingeniería Informática. Facultad de Ciencias
- Programación III - 2º curso del Grado en Ingeniería Informática. Facultad de Ciencias
- Protección de la información - 4º Grado en Información y documentación. Facultad de Traducción y Documentación

Hemos mantenido reuniones presenciales todos los miembros del equipo de trabajo y generado debate entre los participantes sobre el método de autenticación que están utilizado actualmente.

Para conseguir mayor generalidad hemos pasado el formulario del **anexo II** a todos los profesores de la facultad de Ciencias haciendo directamente la pregunta de si diferenciarían el acceso al servicio de calificación de actas del resto de servicios de la USAL. También hemos pasado el mismo formulario al personal de la secretaría de la Facultad de Ciencias y a los secretarios de los departamentos del mismo Centro.

Hemos puesto en común el resultado de las respuestas de los formularios y planteamos diferentes propuestas de autenticación para el acceso a las plataformas de formación y al servicio de calificaciones de actas

Recursos empleados

Para poder llevar a cabo el proyecto necesitaríamos contar con los siguientes recursos materiales:

Crypto kit lector Bit4id. Conjunto de lector y tarjeta inteligente. CryptoKIT tiene capacidad para generar claves públicas y privadas utilizadas para la firma electrónica y para la autenticación. La clave privada se genera dentro de la tarjeta criptográfica, lo que garantiza la imposibilidad de copiarla o de exportarla.

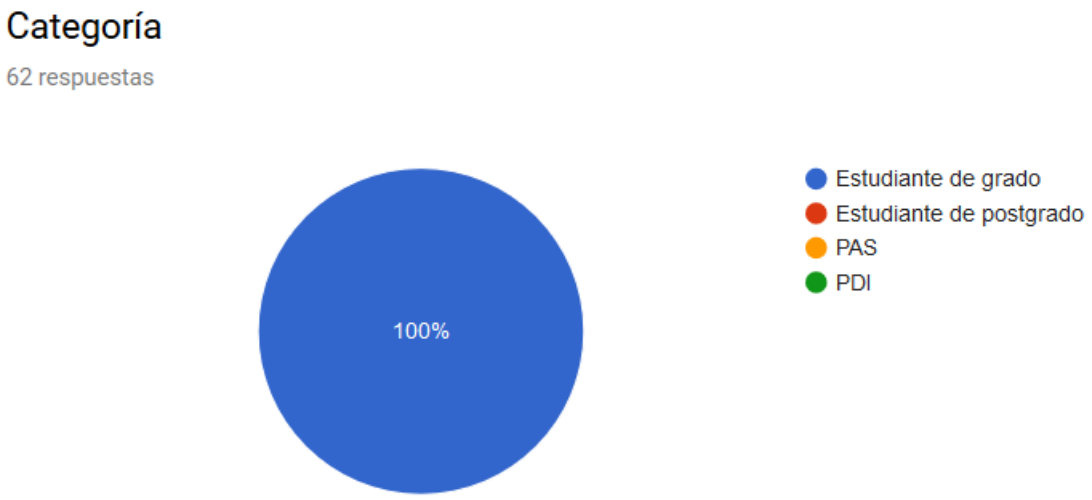
Lectores de DNIe. Hemos utilizado diferentes modelos en diferentes sistemas operativos.

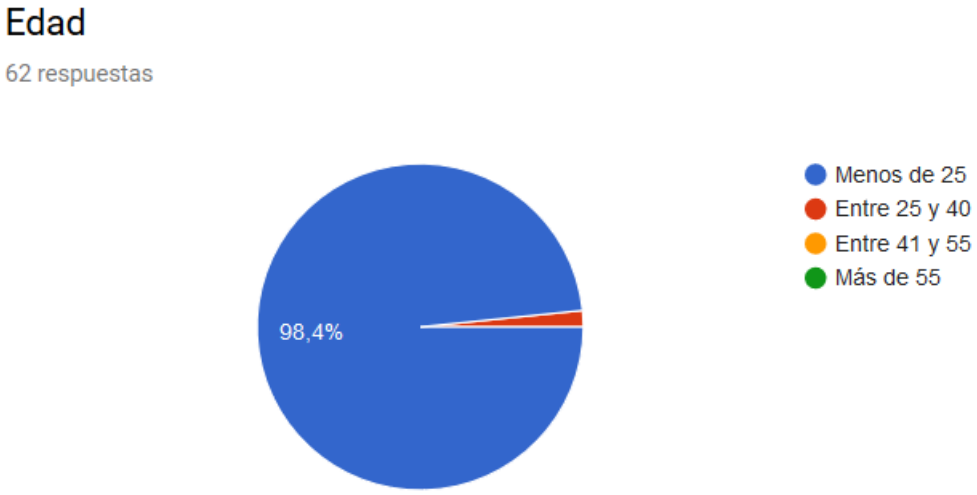
Smartphone. Utilizaremos los terminarles para leer tarjetas con autenticación por NFC.

El resultado de este proyecto busca una solución a la acreditación del estudiante para acceder a la plataforma desde la que recibirá la formación, evitando que otras personas accedan en nuestro nombre intencionadamente o falseando nuestra identidad. Ello conlleva la posibilidad de ofrecer formación virtual oficial: podremos hacer un seguimiento real al estudiante matriculado.

Las actas constituyen el documento con el que se da fe sobre el resultado de aprendizaje del estudiante por lo que tienen que tener un nivel de seguridad muy alto para tener la certeza de que reflejan la información veraz recabada por el profesor y no han sido manipuladas con posterioridad.

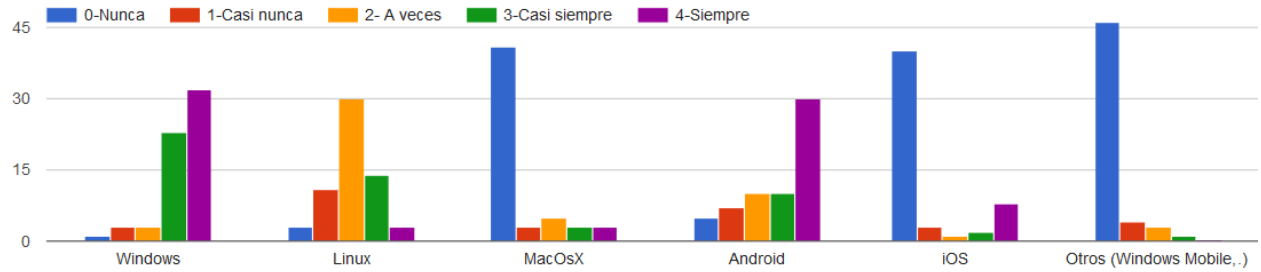
Resultado de encuesta pasada a estudiantes:



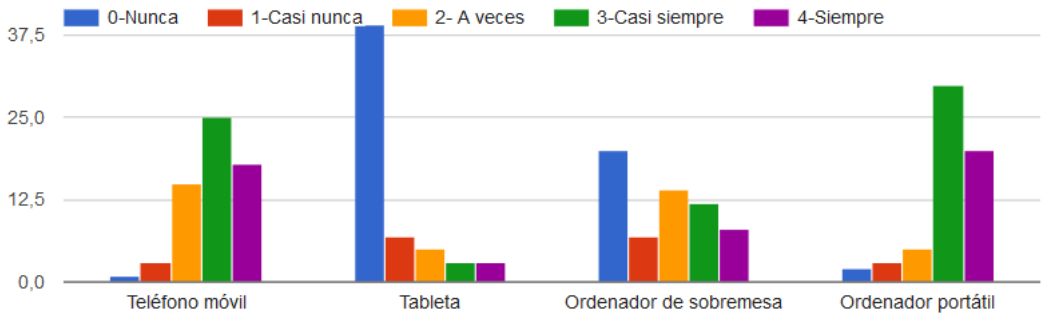


Forma de acceso a los servicios

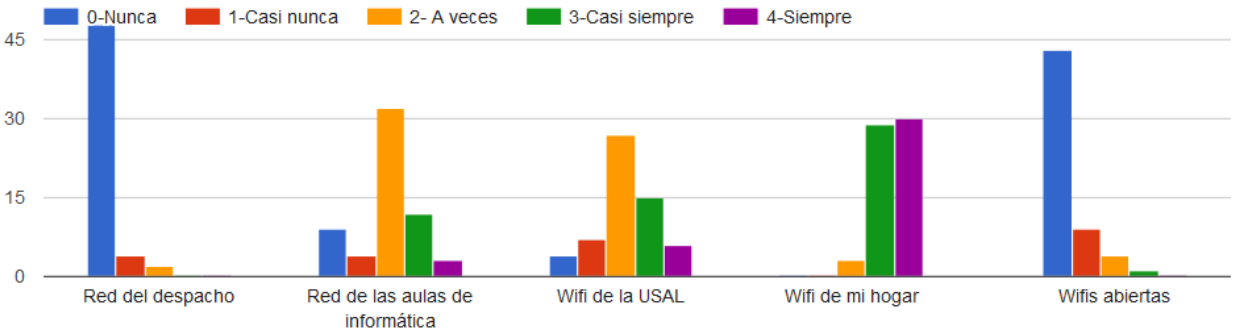
Sistemas operativos que utilizas



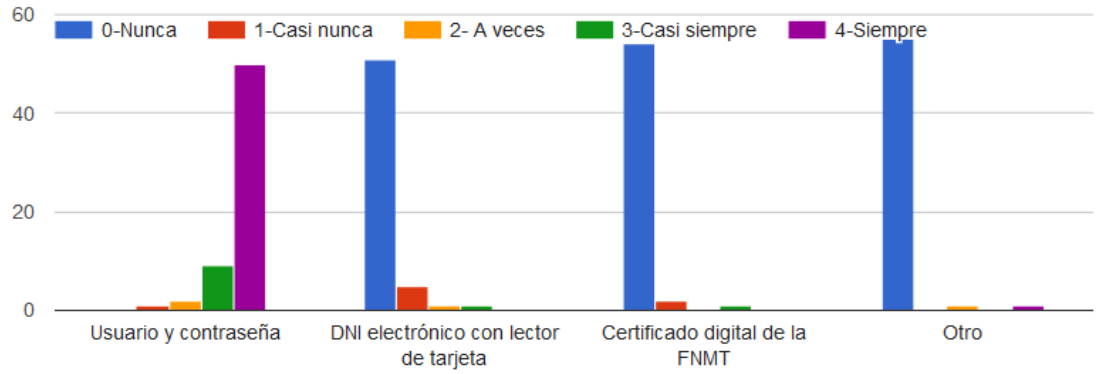
Dispositivos que utilizas para acceder



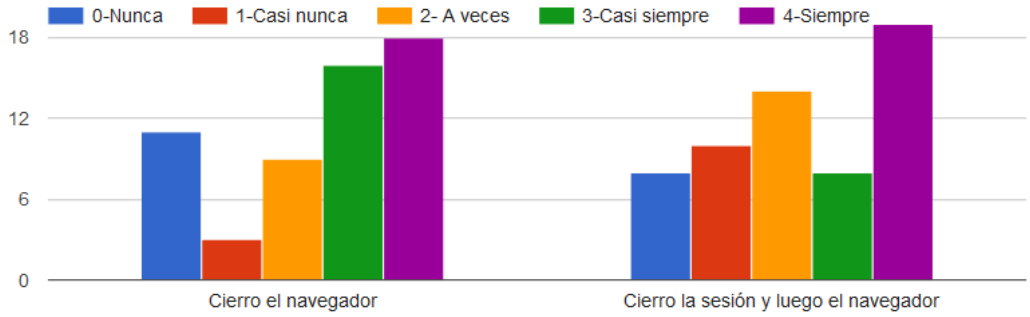
Método de acceso



Método para autenticación/validación de identidad



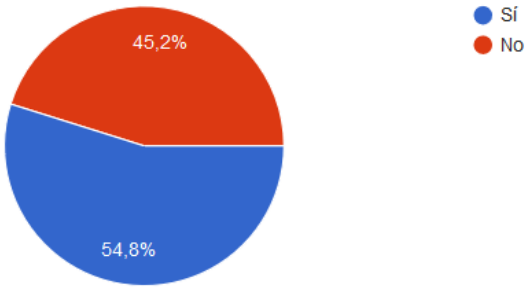
Cuando ya no deseas seguir trabajando desde el navegador



Uso del segundo factor de autenticación para acceder a los servicios de la USAL

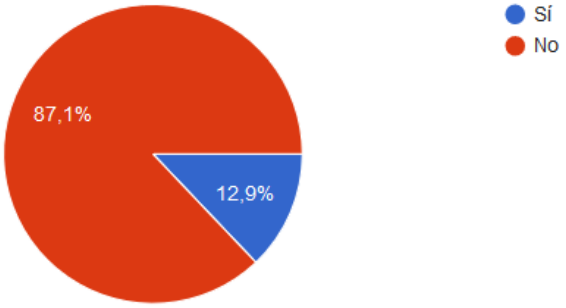
¿Conoces la existencia y la utilidad de la aplicación LATCH?

62 respuestas



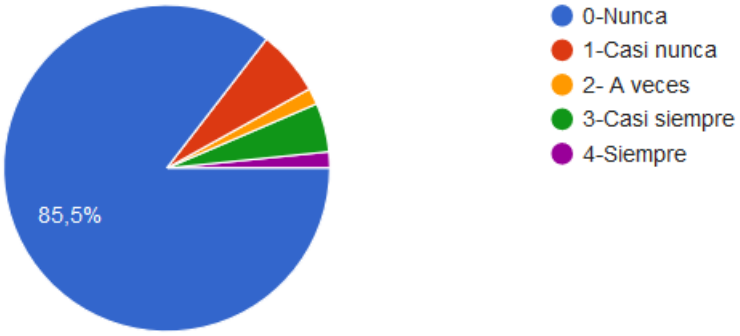
¿La tienes instalada?

62 respuestas

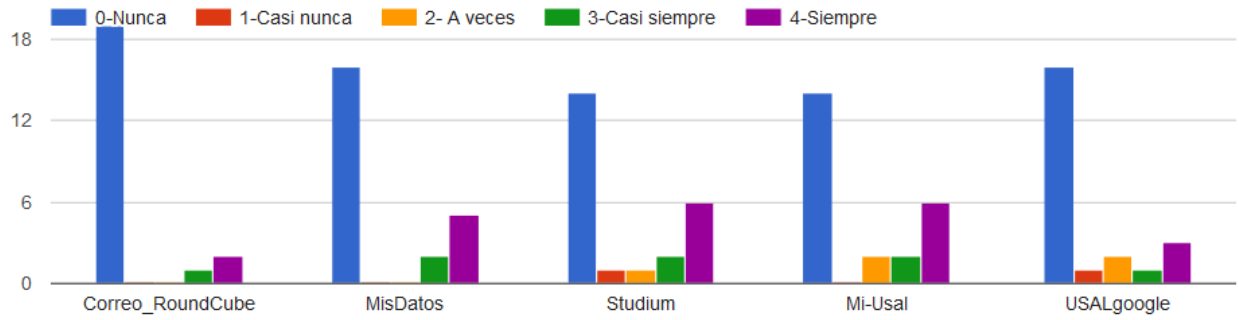


¿Con qué frecuencia la utilizas?

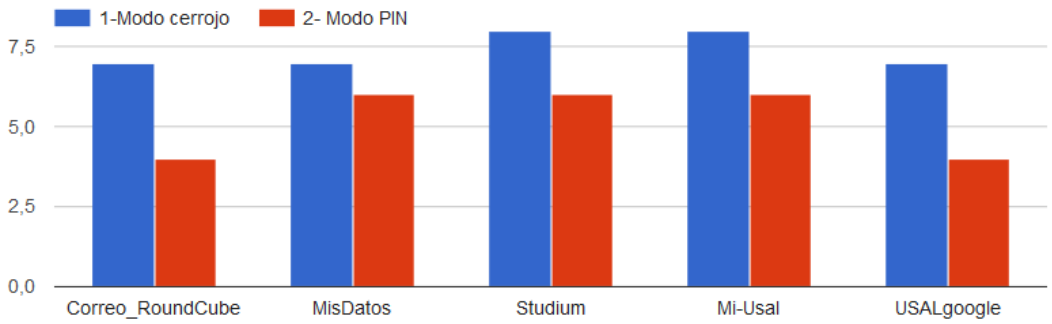
62 respuestas



En caso afirmativo, indica en qué secciones la usas



Método utilizado



Ventajas del uso de LATCH

7 respuestas

Mayor seguridad para tus cuentas
Te permite asegurarte de que nadie va a usar tu cuenta aunque te hayas dejado una sesion iniciada en un dispositivo que no es tuyo.
Mejor accesibilidad a los servicios de la usal
Mucha mayor seguridad de acceso
Te avisa al instante cuando se ha accedido a la cuenta.
Te avisa si alguien intenta entrar en tu cuenta.
Doble seguridad en el acceso a los servicios de la USAL, ya que además de ser necesario conocer las credenciales es necesario disponer de un objeto físico que normalmente sólo controla la persona dueña de la cuenta de la USAL.

Inconvenientes del uso de LATCH

5 respuestas

tiempo extra para entrar a tus cuentas
Es un poco molesto lo de tener que bloquear y desbloquear manualmente cada vez que quieres usar algún servicio. Estaría muy bien que para solucionar esto existiera un gadget para la pantalla de bloqueo para poder desbloquear y bloquear con mayor facilidad.
Es un paso más adicional
Cuando se utiliza el modo PIN, no da tiempo a acceder a la aplicación y después introducir el PIN en la cuenta. Desde el móvil, para introducirla en el ordenador sin ningún problema.
Pendiente de estar abriendo y cerrando el candado

En el caso de no usar LATCH ¿podrías indicar el motivo?

30 respuestas

Desconocimiento (3)
No lo conozco (2)
Aunque creo que es una buena aplicacion, no veo una imperiosa necesidad de proteger hasta ese extremo mis cuentas.
No me dió buena experiencia
No me he propuesto descargarla.
Utilizo Google Authenticator para la autenticación en dos pasos mediante PIN. Aunque tengo instalado LATCH no lo uso nunca para la USAL porque con Google Authenticator creo que es suficiente
Desconocimiento de la aplicación
Desconocimiento de la aplicación
No sé qué es
Acabo de enterarme de su existencia.
por pereza.
No sabía que existía
No se que es
Desconocimiento del funcionamiento
Desconocimiento y Pereza por informarme
Escaso de Informacion
no la conozco
No la conocía
No veo motivos suficientes para ello
No conocerla.
No se lo que es
Estoy tan liado que se me suele olvidar instalarla, pero quiero hacerlo.

La utilicé durante un par de meses, pero el hecho de tener que desbloquear (y bloquear) manualmente las cuentas me inclinó a desinstalarla. Si al menos hubiera un método más simple y rápido de desbloqueo / bloqueo, la volvería a utilizar.

No la conozco

Me parece engorroso

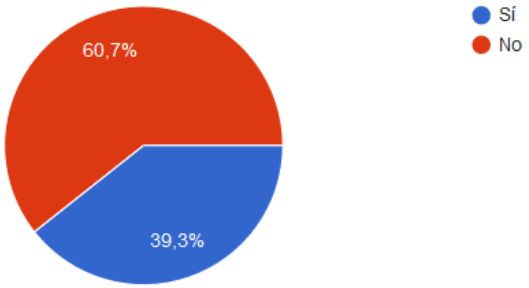
Que pereza configurarlo

No conozco la aplicación LATCH

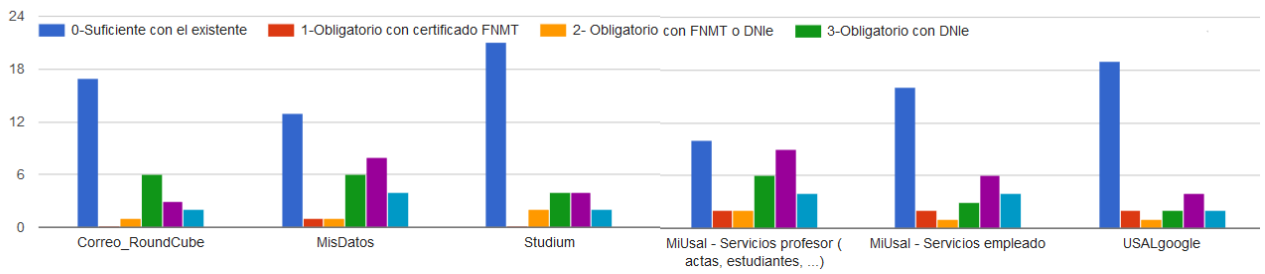
Opinión sobre el nivel de seguridad

¿Crees que es necesario aumentar los niveles de seguridad de acceso a algunas secciones?

61 respuestas

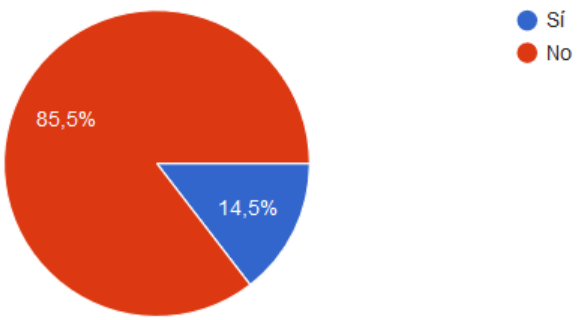


En caso afirmativo indica el método que consideras más adecuado:



¿Propones algún otro método de identificación para acceso a MI-USAL y al resto?

55 respuestas



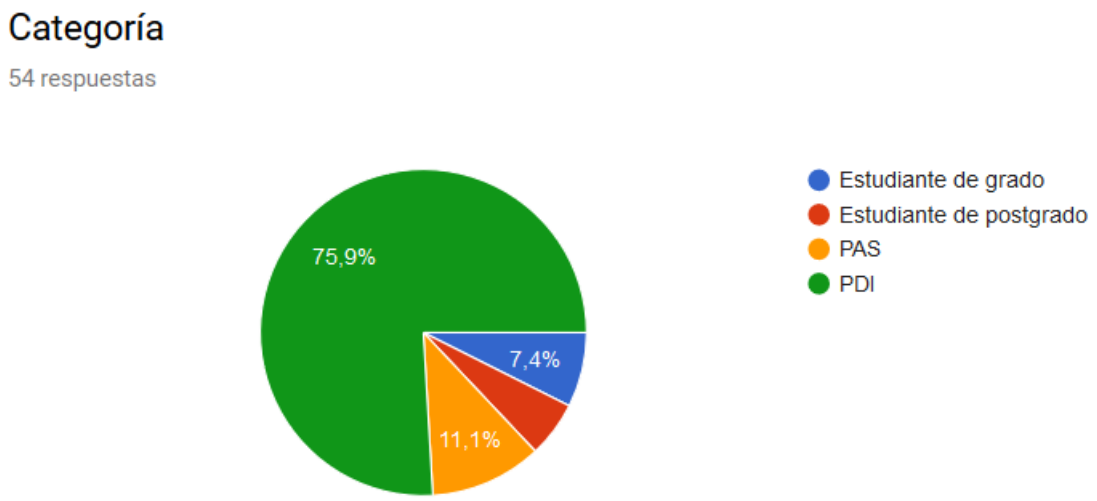
En caso afirmativo ¿aconsejarías alguno?

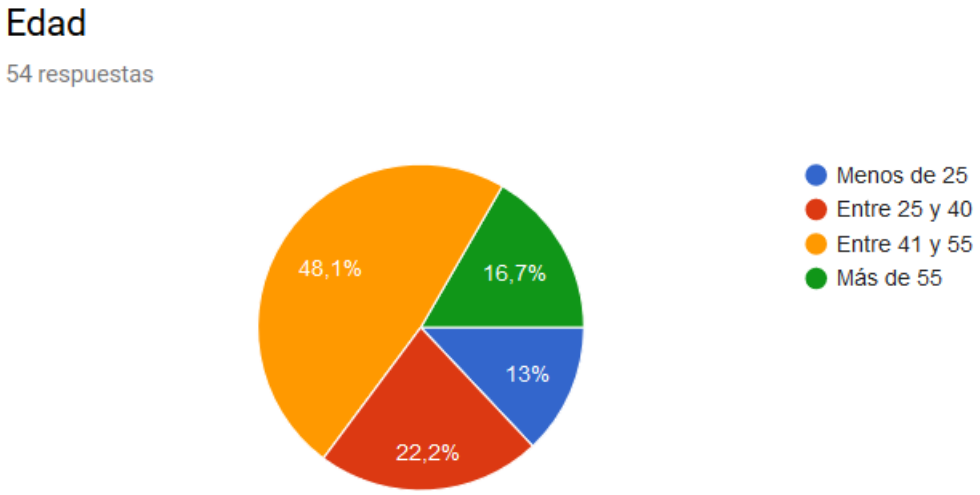
9 respuestas

Lector de huellas, es seguro, es fiable, es menos probable que alguien acceda en tu cuenta, y a diferencia de carnet de la usal no se te olvidara en casa nunca.
Estaría bien la posibilidad de autenticación en doble factor con huella dactilar para dispositivos móviles. Hoy en día cada vez más smartphones disponen de un lector de huellas, y es una forma muy fácil y rápida sin PINs adicionales.
El más usado por muchas páginas, sms al móvil.
Ahora ,él lector de huella esta presente en la mayoría de móviles .
Huella dactilar
Esto escapa a mi conocimiento.
Lector de carnet USAL.
usando el numero de la tarjeta universitaria, seria mas difícil de acceder a ese numero (o no), y seria algo mas personal, ya que cualquiera puede coger el numero del D.N.I. atreves de las calificaciones,(es una posibilidad, pequeña, pero real).
Código de acceso enviado a una aplicación del móvil o al correo electrónico asociado.

¡Gracias por colaborar! Tu opinión es muy importante para mejorar nuestra Universidad.

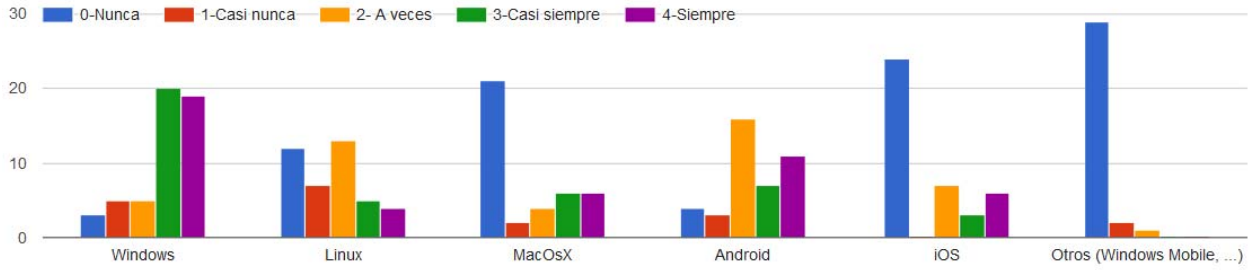
Resultado de encuesta pasada a miembros de la Junta de Facultad de Ciencias y al personal de Administración y servicios:



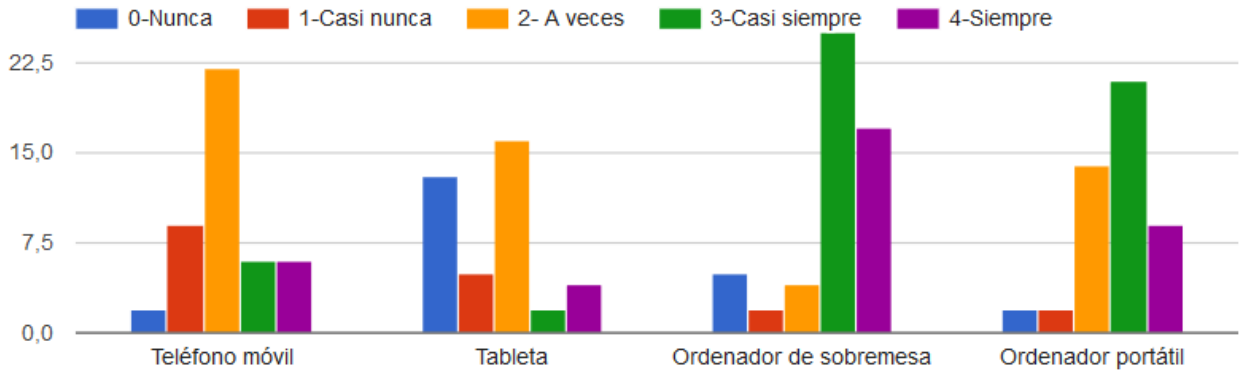


Forma de acceso a los servicios

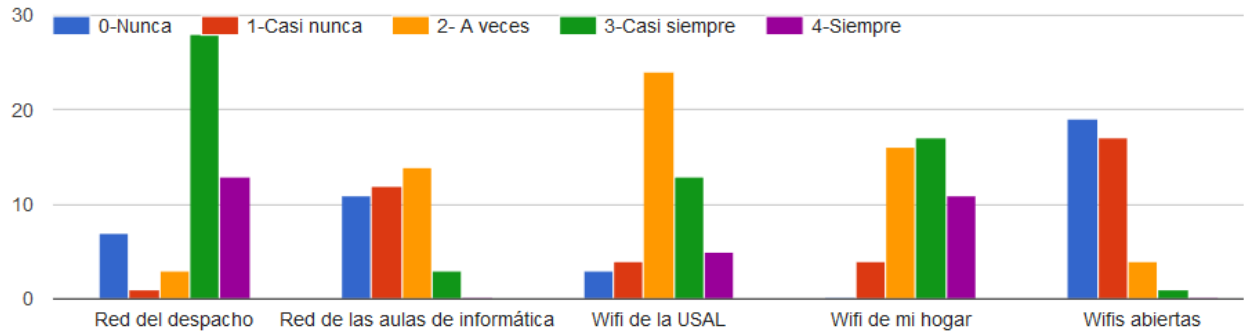
Sistemas operativos que utilizas



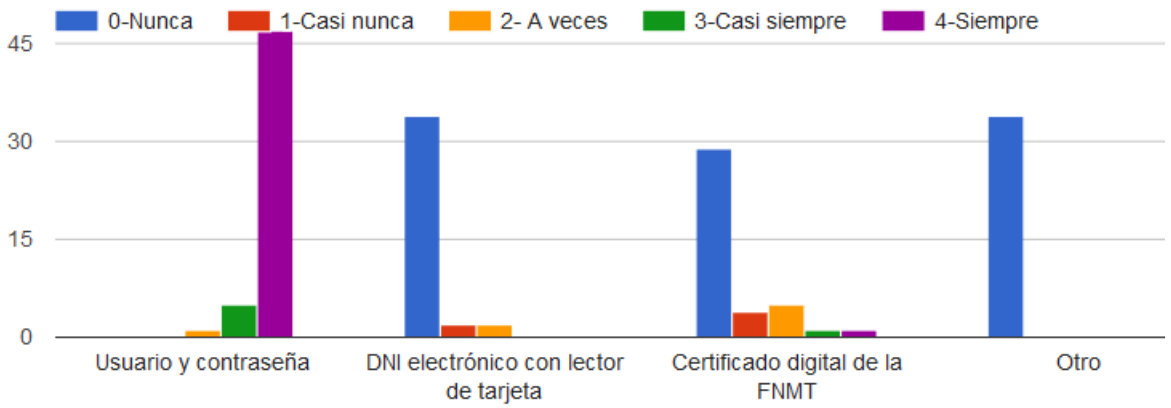
Dispositivos que utilizas para acceder



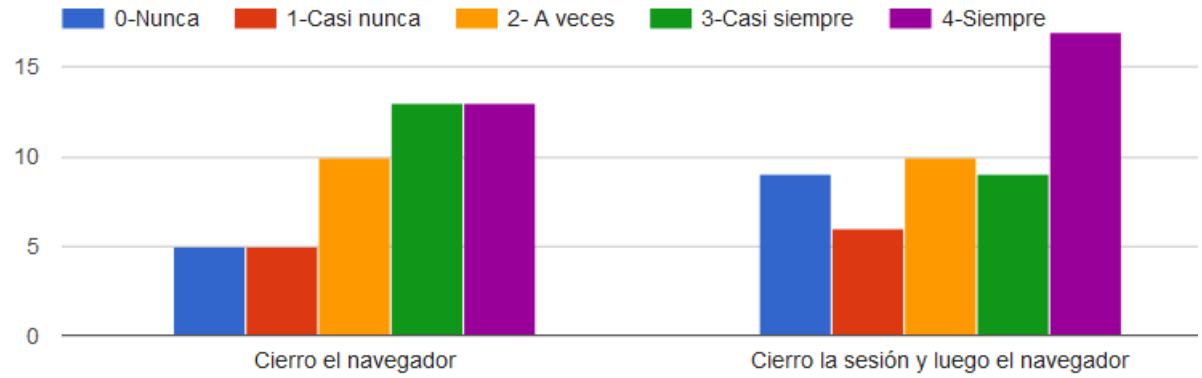
Método de acceso



Método para autenticación/validación de identidad



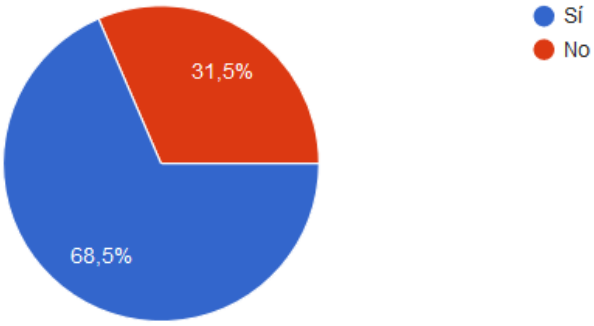
Cuando ya no deseas seguir trabajando desde el navegador



Uso del segundo factor de autenticación para acceder a los servicios de la USAL

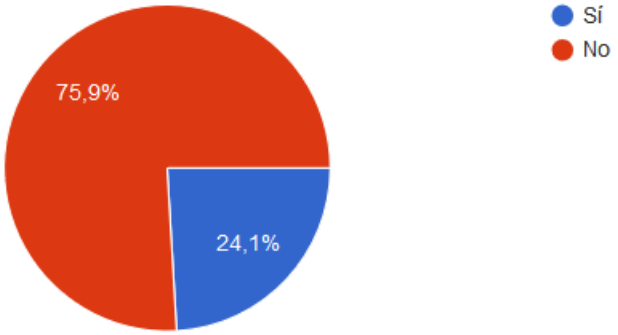
¿Conoces la existencia y la utilidad de la aplicación LATCH?

54 respuestas



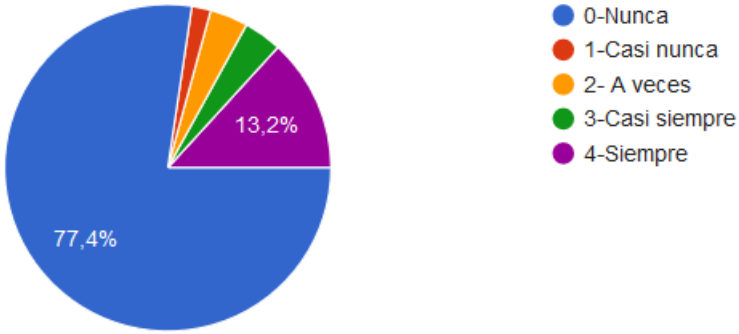
¿La tienes instalada?

54 respuestas

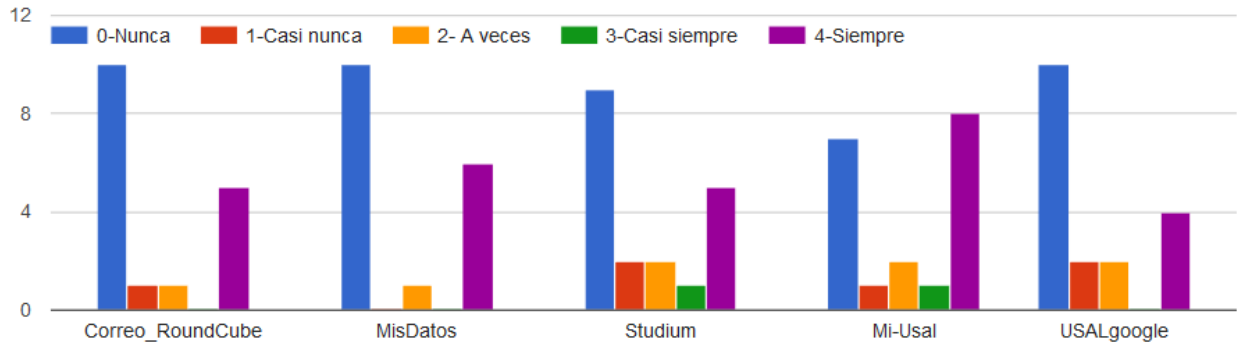


¿Con qué frecuencia la utilizas?

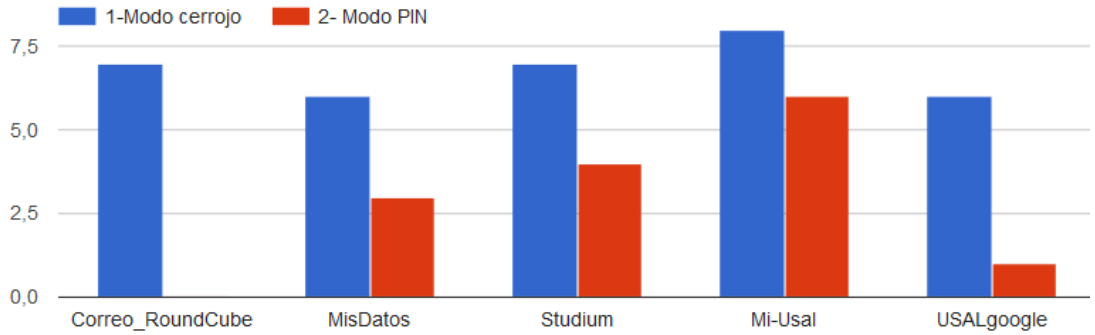
53 respuestas



En caso afirmativo, indica en qué secciones la usas



Método utilizado



Ventajas del uso de LATCH

13 respuestas

Ninguna (4)
seguridad (2)
Uso de segundo factor de autenticación. Servicio sólo activo por solicitud.
Sencillez
Aporta un grado mayor de seguridad
Aviso por intentos de acceso
Da más seguridad
Un escalón mayor de seguridad
Mayor seguridad frente a accesos externos

Inconvenientes del uso de LATCH

11 respuestas

Una acción más para acceder.
Desde el móvil la interfaz a veces no es clara
Suele dar errores.
Me parece engorroso
Hay que estar pendiente de la herramienta cada vez que se accede o dejar de usar MiUsal
si no tengo el móvil no puedo hacer nada
Tienes que tener telEfono mOvil
Muchas molestias
Es una herramienta del demonio. Te olvidas el teléfono en el despacho y ya no puedes dar la clase. Debería haber un segundo mecanismo de seguridad, con otra segunda contraseña o por código a través de una segunda cuenta de e-mail. Solucionaría todos los problemas que le encuentro.
Imposibilidad de uso sin batería
Tener que llevar el movil.

En el caso de no usar LATCH ¿podrías indicar el motivo?

29 respuestas

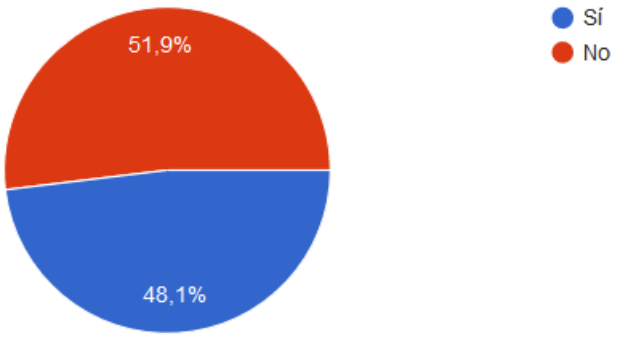
No me lo he planteado hasta este momento,
Pereza, falta de costumbre
Nunca conseguí que funcionara
La tuve instalada un tiempo, pero no acabé de ver su utilidad.
Quizas pereza
No me fio
Desconocimiento
No se qué es
Por no mezclar lo personal (teléfono móvil) con lo profesional (trabajo)
No tengo telEfono m0vil
Pereza
Es una aplicación externa, añade más peso al móvil y no me veo motivado para instalarla, pese a que el acceso a cualquier web con un usuario es más cómodo que el acceso a studium/miusal.
no le he visto utilidad
ignorancia
Muy molesto
Lo desconozco
Desconocimiento de la herramienta
Como estudiante no la veo muy necesaria, cuando la mayoria de las notas las suben en PFD con DNI (que acabas sabiendo si quieres) oincluso en casos con nombre y apellidos
Desconozco qué es ni qué ventajas puede tener
Porque si está bloqueado y tengo otro dispositivo me gusta igualmente poder acceder
No la conocía
Por pereza a configurarlo

No conocía la aplicación hasta ahora
No confío en Chema después del wannacry, y menos en telefónica
Charla de Chema Alonso en la USAL el año pasado: 100% publicidad de su herramienta.
Por los inconvenientes comentados
No me parece tan esencial, considero que la protección usual es suficiente para mí
Complica el acceso
No creo que sea necesario un segundo factor de autenticación si se usan contraseñas robustas

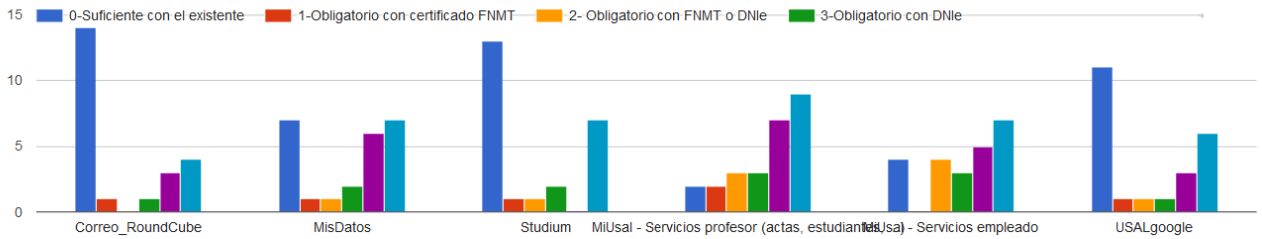
Opinión sobre el nivel de seguridad

¿Crees que es necesario aumentar los niveles de seguridad de acceso a algunas secciones?

52 respuestas

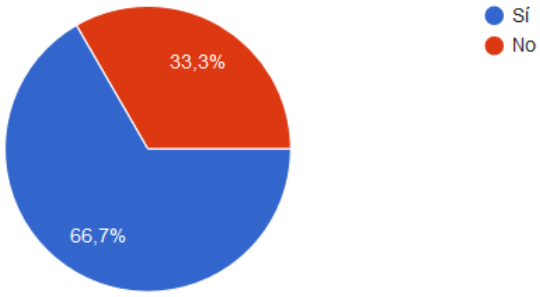


En caso afirmativo indica el método que consideras más adecuado:



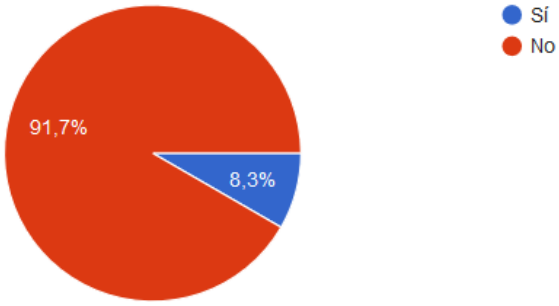
¿Consideras que habría que tratar por separado la identificación para acceder a los servicios del profesor (calificación de actas, mis estudiantes, ...) y al resto?

51 respuestas



¿Propones algún otro método de identificación para acceso a MI-USAL y al resto?

48 respuestas



En caso afirmativo ¿aconsejarías alguno?

5 respuestas

introducir un código de un sólo uso recibido por sms desde el servicio.
Doble factor, mensaje al móvil, combinación de varios métodos
Los que se proponen me parecen suficientes (FNMT, DNI-e,...)
Tarjeta de coordenadas
No sé cuál puede ser mejor

¡Gracias por colaborar! Tu opinión es muy importante para mejorar nuestra Universidad.

En la siguiente tabla presentamos un resumen:

	Alumnos	**Junta Facultad Ciencias y PAS**
Sistema operativo	Windows y Android	Windows y Android
Dispositivo para acceder	Portátil y teléfono móvil	Ordenador de sobremesa y portátil
Método de acceso	Wifi del hogar	Red del despacho – Wifi del hogar – Wifi de la USAL
Método de autenticación	Usuario y contraseña DNIe, en alguna ocasión	Usuario y contraseña Certificado FNMT, en alguna ocasión
Cierran sesión y el navegador	50%	60%
Conocen existencia de latch	54,8%	68,5%
La tienen instalada	12,9%	24,1%
Con qué frecuencia la utilizan	85,5%	77,4%
La usan mayoritariamente para	Studium	Mi USAL
Método utilizado cerrojo o pin	Ligeramente mayor cerrojo	Ligeramente mayor cerrojo
Ventajas	Seguridad, …	Seguridad – Ninguna, …
Inconvenientes	Tiempo extra, …	Suele dar errores, tener que tener teléfono móvil, …
Motivo por el que no uso Latch	Desconocimiento, pereza para instalarla, …	Desconocimiento, no tener móvil, …
Consideras necesario aumentar el nivel de seguridad	60,7%	48,1%
Consideras que hay que tratar por separado la identificación para acceder a los servicios del profesor?		66,7%
Propuesta de otro método de autenticación	Lector de huellas Lector de carnet de la USAL Código enviado al móvil	Código de un solo uso. FNMT, DNIe, Tarjeta de coordenadas

Conclusiones

Los resultados, por parte de los profesores y de los alumnos, se resumen en los siguientes ítems:

- La mayoría de los usuarios desconocen la **existencia de latch**.
- Hay usuarios que la tienen instalada y no la tienen activada.
- Los usuarios en la aplicación latch ven más inconvenientes que ventajas.
- Los estudiantes ven más necesario que los miembros de la Junta de Facultad de aumentar la seguridad.

Los miembros del equipo de este trabajo de investigación proponemos el uso de un segundo factor de autenticación y en función de presupuesto vemos varias vías:

- Crear en el CPD certificados propios para instalar en el navegador de cada profesor y obligatoriamente tener que hacer uso del mismo para determinados servicios.
- Validación por código enviado por un segundo canal, que sería canal telefónico vía sms, con validez limitada temporalmente. Sería necesario disponer de un teléfono con capacidad de recibir sms. En el caso actual, también valdrían los terminales de sobremesa que nos ha proporcionado la USAL.
- En casos extremos se podría aumentar muchísimo la seguridad simultáneando el uso del DNI y el teléfono: se introduce el DNI en el lector, y se envía un mensaje al teléfono asociado que recibe un código que se introduce en el ordenador.
- Como línea de trabajo futuro habría que explorar el uso de tokens NFS en combinación con lectores conectados a ordenadores de sobremesa o vía teléfonos móviles que soporten la tecnología.

Salamanca, 30 junio 2017

GONZALEZ ARRIETA MARIA ANGELICA - 06555917C

Firmado digitalmente por GONZALEZ ARRIETA MARIA ANGELICA - 06555917C
Nombre de reconocimiento (DN): c=ES, serialNumber=06555917C, sn=GONZALEZ ARRIETA, givenName=MARIA ANGELICA, cn=GONZALEZ ARRIETA MARIA ANGELICA - 06555917C
Fecha: 2017.06.30 23:44:06 +02'00'

Fdo.: Angélica González Arrieta