23-10-2014

Análisis de la seguridad en las contraseñas web

Estudio comparativo sobre la información, recopilación y almacenamiento de las contraseñas por parte de los sitios web españoles

Juan Carlos Vizner López
MÁSTER UNIVERSITARIO EN INFORMÁTICA DE SISTEMAS

Resumen

En los últimos años se vienen desarrollando trabajos tratando de estudiar la seguridad no sólo desde el punto de vista técnico, sino también económico y de usabilidad. En 2010 se presentó el artículo de Joseph Bonneau y Sören Preibusch, "The password thicket: technical and market failures in human authentication on the web" (en Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS), June 2010) y nos preguntábamos cómo serían las métricas que se describían allí para sitios populares en España. Este trabajo es una primera aproximación para tratar de responder a estas preguntas en lo referente a la creación y gestión de cuentas de usuario en comparación con las de otras partes del mundo.

Pensamos que sería beneficiosa una comparación clara y empírica sobre las medidas de seguridad adoptadas por los sitios web españoles frente a la identificación de sus usuarios, de modo que se puedan observar los puntos fuertes y débiles de dicha identificación.

Para ello hemos llevado a cabo una selección de los sitios web españoles más visitados y los dividimos en 3 categorías principales: sitios de identidad, de comercio electrónico y de contenido. Una vez hecho se recogen una determinada serie de datos relevantes y finalmente se comparan los resultados obtenidos de las distintas páginas web analizadas.

Contenido

1. Introducción

En los últimos años se vienen desarrollando trabajos tratando de estudiar la seguridad no sólo desde el punto de vista técnico, sino también económico y de usabilidad. En 2010 se presentó el artículo de Joseph Bonneau y Sören Preibusch, "The password thicket: technical and market failures in human authentication on the web" (en Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS), June 2010) y nos preguntábamos cómo serían las métricas que se describían allí para sitios populares en España. Este trabajo es una primera aproximación para tratar de responder a estas preguntas en lo referente a la creación y gestión de cuentas de usuario en comparación con las de otras partes del mundo.

Pensamos que sería beneficiosa una comparación clara y empírica sobre las medidas de seguridad adoptadas por los sitios web españoles frente a la identificación de sus usuarios, de modo que se puedan observar los puntos fuertes y débiles de dicha identificación.

Para ello hemos llevado a cabo una selección de los sitios web españoles más visitados y los dividimos en 3 categorías principales: sitios de identidad, de comercio electrónico y de contenido. Una vez hecho, se recogen una determinada serie de datos relevantes y finalmente se comparan los resultados obtenidos de las distintas páginas web analizadas.

2. Historia de las contraseñas

El uso de las contraseñas, se remonta a la antigüedad, cuando los vigías pedían el santo y seña a quien quisiera pasar. A día de hoy, en un solo día utilizamos multitud de contraseñas, por ejemplo al utilizar la tarjeta de crédito, iniciar sesión en el sistema operativo, encender el teléfono móvil o al autenticarnos en cualquier página web.

Normalmente, la seguridad de una contraseña y su facilidad para ser recordada son características opuestas, cuanto más compleja sea una contraseña, más difícil será que un posible atacante adivine cual es, pero a su vez, para el usuario también será más difícil de recordar.

Los factores que afectan a la seguridad de un sistema de contraseñas, podrían resumirse en los siguientes:

Posibilidad de que un posible atacante adivine la contraseña

El usuario deberá prescindir de contraseñas sencillas tales como "admin", "1234", "qwerty", etc, así como de nombres de familiares, mascotas, matrículas del automóvil o fechas de nacimiento. De este modo, si el sitio limita el número de intentos de un atacante por unidad de tiempo, será casi imposible que la contraseña sea descubierta mediante el uso de diccionarios o de la fuerza bruta.

Formas de almacenar las contraseñas

Los sitios web deben evitar el almacenamiento de las contraseñas en archivos de texto. De ese modo si un atacante se cuela en el sistema, no puede ver las contraseñas de todos sus usuarios.

Normalmente, los sitios web lo que almacenan es el hash de la contraseña, de modo que cuando un usuario se intenta autenticar, el sistema calcula el hash de la contraseña introducida y lo compara con el que tiene almacenado en la base de datos.

Método de transmisión de la contraseña entre el usuario y el sitio web

Usualmente, para evitar que un posible atacante capture nuestra contraseña mientras ésta es enviada a su destino, se implementa una capa de seguridad durante el transporte de los paquetes (TLS – Transport Layer Security). Los navegadores web suelen indicar que este tipo de cifrado está en uso mostrando un candado.

Procedimiento para renovar la contraseña

Todos los sistemas deben de proveer al usuario un modo de modificar su contraseña, y además dicho modo debe de ser seguro, ya que si durante la renovación de la contraseña, la transmitimos de forma no cifrada comprometemos nuestra seguridad.

Una forma alternativa de autenticación de un usuario, es el uso de los "Sistemas de Administración de Identidad", se basan en comprobar la identidad del usuario mediante la formulación de preguntas tipo, como por ejemplo ¿Dónde naciste? ¿Cuál es tu libro favorito? ¿Cómo se llamaba tu primera mascota? Este tipo de sistema de autenticación es poco recomendable ya que es muy vulnerable a la ingeniería social.

Vida útil de una contraseña

El hecho de renovar la contraseña de forma frecuente, no es muy recomendable. Los usuarios tienden a olvidar las contraseñas, y si estas se cambian frecuentemente a apuntarlas y dejarlas a la vista, y los atacantes, una vez descubren la contraseña de una cuenta con los suficientes privilegios, pueden manipular el sistema para que aunque posteriormente se cambie la contraseña sigan teniendo acceso.

Hay que considerar detenidamente todas las opciones antes de implementar algo así.

Número de usuarios por contraseña

No es aconsejable que varios usuarios compartan la misma contraseña, los usuarios suelen ser más responsables cuando saben que si sucede algo, la culpa va a ser de ellos.

3. Metodología

3.1 Preguntas a investigar

El principal objetivo de este artículo es comprobar qué tipo de protecciones son implementadas en las páginas web en todo aquello que esté relacionado con la autenticación de los usuarios mediante el uso de una contraseña. Todo esto nos suscita varias preguntas:

Pregunta 1: ¿Cómo varía la experiencia del usuario de un sitio a otro?

Pretendemos comprobar si la seguridad de los sitios web depende de la información de los usuarios que éstos recopilan, o del contenido y funciones que ofrecen.

Parecería razonable que un sitio web que almacene datos bancarios o datos sensibles de sus usuarios, debería tener unas mayores medidas de seguridad.

Pregunta 2: ¿Qué debilidades de implementación existen?

El objetivo de este artículo es evaluar los mecanismos utilizados en los sistemas de autenticación, su nivel de seguridad y con qué frecuencia es usado cada uno de esos mecanismos. También se evaluará cuando se opta por la usabilidad frente a la seguridad, o también el ahorro de recursos (tanto monetarios como de procesamiento) frente a la seguridad.

Un ejemplo de práctica poco segura en la que no influye la usabilidad, sería prescindir del uso de un protocolo de comunicaciones cifrado. Para un usuario la conexión con un servidor se realiza de forma transparente y apenas puede notar la diferencia entre usar un protocolo cifrado por ejemplo https o uno sin cifrar http. En cambio las ventajas del https frente al http en cuanto a seguridad son notables.

Pregunta 3: ¿Qué factores afectan a los sitios a la hora de implementar las opciones de recogida de contraseñas?

Estudiando los datos recogidos de los diferentes sitios web analizados en este artículo, esperamos encontrar qué factores influyen en la elección de contraseña. Podremos ver si en función del tipo de información ofrecida y requerida por la página web, los administradores de la misma exigen un mayor control y seguridad sobre sus contraseñas.

Pregunta 4: ¿Cómo afectan los requisitos de seguridad a las opciones de implementación de los sitios?

Los requisitos exigidos por los sitios web a la hora de elegir una contraseña varían mucho. Generalmente, si un sitio web almacena datos bancarios, debería tener una política de seguridad más estricta, por el contrario un periódico o una página web con recetas de cocina, podría permitirse tener una política de seguridad algo más laxa.

Vamos a comprobar si en la práctica esto es así.

Pregunta 5: ¿Por qué los sitios web deciden recopilar contraseñas?

Hay sitios web que realmente necesitan que te autentiques para poder desarrollar su actividad, un ejemplo serían los proveedores de correo electrónico, los comercios electrónicos o los bancos, en cambio hay otros donde la única función es personalizar la web. En dichos sitios se podría evitar todo este proceso y llevar a cabo el almacenamiento de los datos relativos a dicha personalización en el lado del cliente.

Intentaremos responder porqué en la amplia mayoría de los sitios web se sigue obligando a los usuarios a crear cuentas de usuario.

3.2 Selección de sitios

El objetivo inicial en este artículo ha sido recopilar los datos necesarios para el posterior análisis de una cantidad de sitios web suficiente, en nuestro caso hemos analizado 37, con la intención de disponer de una muestra de sitios variada con la cual poder hacer comparaciones.

Inicialmente utilizamos la lista de sitios web españoles más visitados obtenida de OJD[1], lista que posteriormente complementamos con otros sitios obtenidos de Alexa[2].

Hemos escogido una serie de sitios web muy visitados extraídos de ambas listas, otro requisito ha sido que todos los sitios web seleccionados almacenasen las contraseñas de sus usuarios. Los sitios web resultantes de ambas listas han sido clasificados en 3 grandes grupos:

Sitios de Identidad: Un ejemplo clásico sería Facebook o Gmail.

> Estos sitios permiten a sus usuarios crear su propia identidad y hacer uso de la misma para interactuar con otras personas. En este caso la contraseña se utiliza para evitar que dicha identidad pueda ser usurpada.
>
> Los ejemplos más importantes serían los emails, redes sociales y servicios de blogs, pero hay otros muchos tipos como páginas de juegos, foros o sitios de colaboración en línea como Wikipedia.
>
> Los usuarios de estos servicios habitualmente almacenan gran cantidad de datos personales en sus cuentas, así como conversaciones de carácter privado con otros usuarios.
>
> La financiación de las empresas propietarias de estos sitios, normalmente se realiza mediante la inclusión de publicidad, modos premium o la venta de parte de los datos recopilados a sus usuarios.

Sitios de comercio electrónico: Un ejemplo de esto sería ebay.

> El propósito de estos sitios es la compra/venta de productos. La mayoría ofrecen a los usuarios la posibilidad de crear una cuenta para almacenar listas de productos, gestionar sus pedidos, almacenar los datos de pago y envío o personalizar algunas opciones de la página.
>
> Dada la sensibilidad de los datos almacenados en este tipo de sitios, es importante que la seguridad sea mayor de lo habitual.
>
> No es habitual que en estos sitios los usuarios interactúen entre sí, al menos en el sentido de "red social", pero si es frecuente ver implementado un sistema de consultas para que los vendedores puedan resolver las dudas de sus clientes.

Sitios con contenido: Un ejemplo de esto sería cualquier periódico online.

[1] OJD realiza la labor de certificación sobre datos de recuento suministrados por distintos medidores, ofreciendo garantía de su adecuación a los estándares y prácticas admitidas en el mercado. La lista de medios online auditados es pública.

[2] Alexa.com provee información acerca de la cantidad de visitas que recibe un sitio web y los clasifica en un ranking. Recoge información de los usuarios que tienen instalado Alexa Toolbar, lo cual le permite generar estadísticas acerca de la cantidad de visitas y de los enlaces relacionados.

Hay numerosos sitios web en los que se permite a los usuarios crear una cuenta (con su correspondiente contraseña) sólo para personalizar el contenido que se muestra en dichas páginas.

El ejemplo más claro serían las webs de noticias, como El País. Estos sitios permiten personalizar las noticias que visualizas al visitar la página o los boletines que te envían al correo electrónico, entre otras cosas.

Normalmente en estos sitios web los usuarios no pueden interactuar entre sí, exceptuando los posibles comentarios que pueda hacer cada uno sobre las diferentes noticias que publica la web.

Dadas las últimas tendencias en páginas web, hay sitios que no encajan a la perfección en una única categoría. Lo más habitual es que en casi todas las páginas web los usuarios puedan interactuar entre sí, recomendarse noticias, enviarse correos, valorar mensajes, etc, etc. Hemos intentado escoger sitios web que se adecuen a los requisitos establecidos en las categorías. Por otro lado, también hemos intentado que dichos sitios web, reciban el mayor volumen de tráfico posible y para ello hemos recurrido a listas como las ofrecidas por Alexa o por OJD.

Durante la selección de sitios, hemos evitado las páginas web cuyas cuentas no eran gratuitas, o de acceso público. Esto limita la inclusión de algunos sitios con cierta relevancia, por ejemplo forocoches o Series.ly ya que requieren de una invitación previa por parte de un usuario de la web. También hemos prescindido de las páginas bancarias, por la dificultad de crear la cuenta. Los sitios pornográficos han sido excluidos.

3.3 Proceso de Evaluación

El proceso de evaluación que se ha llevado a cabo, ha sido un proceso manual en todos los casos, ha sido diseñado previamente, y se ha llevado a cabo para el análisis de todos los sitios.

1. **Registro**
   En todos los sitios web se han usado los mismos datos falsos. Para registrarse, se ha usado un único correo electrónico. Se ha dejado un periodo de al menos 24h entre los registros de cada página web, con el fin de identificar más fácilmente si dichos sitios generaban o no spam.
   Se han apuntado todos los datos requeridos por el sitio web, así como los consejos ofrecidos a cerca de qué contraseña elegir.
   Durante el registro se ha usado siempre una misma contraseña “muis2014”. Ha sido aceptada en todos ellos.

2. **Login/Logout**
   Una vez llevado a cabo el registro, y realizada la verificación del email si fuese necesario, se cierra la sesión y durante el Login se apuntan los detalles TLS (si los hubiese). También se toma nota de la existencia de cookies persistentes.
   Una vez iniciada la sesión nuevamente, se comprueba si el sitio puede almacenar datos de pago o si tiene la posibilidad de actualizar la cuenta a modo Premium.

3. **Actualización de la contraseña**
   Una vez completado el paso anterior, modificamos la contraseña de la cuenta mediante la interface del sitio web.

Los siguientes datos se han comprobado mediante el método de ensayo y error:

- Longitud mínima
- Longitud máxima no testeada. Si el sitio lo indica se anota.
- Se comprueba si se aceptan contraseñas tales como “1234”, “password” o “contraseña”. Si son aceptadas, se presupone que el sitio sólo comprueba la longitud de la contraseña, si son rechazadas, se entiende que se comprueban parámetros adicionales como combinar letras, números, símbolos o la pertenencia a un diccionario.
- Se comprueba si el sitio guarda un historial de contraseñas intentando utilizar una contraseña previa.
- Finalmente comprobamos si los cambios se notifican por correo electrónico.

4. **Reseteo de la contraseña**
   Cerramos la sesión, y comprobamos si al errar el login el sitio diferencia entre usuario erróneo y contraseña errónea.
   Comprobamos el protocolo de restablecimiento de contraseña. Normalmente se lleva a cabo mediante el envío de un email con la contraseña original, una nueva temporal o un vínculo para cambiarla.
   Para terminar anotamos si el protocolo obliga a cambiar la contraseña una vez iniciado el proceso.

5. **Sondeo de contraseña**
   Hemos llevado a cabo un ataque manual, utilizando un usuario válido y probando entre 10 y 15 contraseñas de forma consecutiva. Si pasado ese número de intentos el sitio no pide un tiempo de espera o requiere el uso de CAPTCHA se considera vulnerable.

Únicamente se han comprobado las medidas de seguridad anteriormente descritas. No se han comprobado ni las vulnerabilidades del servidor donde se aloja el sitio web ni el método de almacenamiento de los datos del usuario (como por ejemplo si las contraseñas se almacenan en la base de datos en texto plano). Tales comprobaciones en muchos casos no sería posible llevarlas a cabo de forma externa, y aunque si se pudiese, habría limitado mucho la muestra de sitios analizados.

4. Recolección de datos

La recolección de todos los datos pertinentes a este artículo ha sido llevada a cabo entre el 18 de Marzo del 2014 y el 21 de Agosto de ese mismo año.

4.1 Características de los Sitios

Como las categorías principales son bastante amplias, hemos agrupado los sitios web en función de diferentes características, dicha clasificación se puede apreciar en la tabla nº1.

Tabla 1: Características ofrecidas por los sitios web.

	Características	**Identidad**	**E-Comercio**	**Contenido**	**Total**
1	Noticias mostradas	1	0	26	27
2	Productos en venta	2	6	3	11
3	Almacenamiento de datos de pago	0	1	3	4
4	Redes Sociales	4	1	3	8
5	Disponibilidad de cuentas Premium	0	1	2	3
6	Proporcionan cuentas de Email	0	0	0	0
7	Foros de Discusión	2	1	7	10

Como se puede apreciar en los datos de la Tabla 1, se cumplen los requisitos básicos referentes a las categorías en las cuales están encasilladas las páginas, todas las webs de Identidad tenían funciones de red social, al igual que todas las páginas de E-Comercio vendían productos y todas las de Contenido mostraban noticias.

Al margen de los casos típicos que he mencionado también hay páginas que se salen del esquema general ofreciendo funciones de Red Social cuando a simple vista la página podría considerarse solo de Contenido.

Hemos prestado especial atención a los sitios con cuentas Premium o almacenamiento de datos de pago, ya que cabría esperar que tales páginas web tuviesen medidas de seguridad adicionales.

Tabla 2: Datos personales requeridos durante el registro.

	Características	**Identidad (5)**	**E-Comercio (6)**	**Contenido (26)**	**Total (37)**
1	Nombre y Apellidos	3 (60%)	6 (100%)	16 (61%)	25 (68%)
2	Correo electrónico	5 (100%)	6 (100%)	26 (100%)	37 (100%)
3	Nombre de Usuario (nic)	4 (80%)	4 (66%)	20 (77%)	28 (76%)
4	Código postal	1 (20%)	3 (50%)	6 (23%)	10 (27%)
5	Dirección	0 (0%)	2 (33%)	1 (4%)	3 (8%)
6	Número de Teléfono	1 (20%)	2 (33%)	2 (8%)	5 (14%)
7	Edad	3 (60%)	3 (50%)	9 (35%)	15 (41%)
8	Captcha	3 (60%)	1 (17%)	9 (35%)	13 (35%)

4.2 Requisitos del registro

4.2.1 Datos personales recolectados

A la hora de registrarse en una página web, debes introducir una cierta cantidad de datos. En la tabla 2, están representados y organizados en categorías los más relevantes.

Claramente los sitios de comercio electrónico, son los que solicitan más información a la hora de llevar a cabo el registro. Este hecho parece bastante razonable, ya que dado que se van a llevar a cabo transacciones comerciales parece normal tener más información de los usuarios implicados en las mismas. Por poner un ejemplo, si no tienen tu dirección, no pueden enviarte los productos que compres en la página web.

4.2.2 Verificación por Email

Una vez completado el registro, la mayor parte de los sitios web, nos enviaron un email al correo electrónico pidiendo que pulsásemos sobre un enlace que contenía el mismo, con el fin de verificar la existencia de dicho correo electrónico y así terminar de activar la cuenta.

De los 37 sitios analizados, 30 solicitaron dicha activación. De esos 30, 23 eran sitios con contenido, 3 eran de comercio electrónico y 4 eran sitios de identidad.

Prácticamente ningún sitio web envió la contraseña en texto plano a través de este email.

En mi opinión, hay sitios web donde la necesidad de verificar la dirección de correo electrónico es discutible, pero creo que es bastante razonable que el administrador de una web se quiera cerciorar de que al menos el email proporcionado por el usuario es veraz, más aun cuando dicho administrador se hace responsable legalmente de los comentarios que haga en su sitio web dicho usuario.

Tabla 3: Consejos sobre la contraseña utilizada.

	Características	**Identidad (5)**	**E-Comercio (6)**	**Contenido (26)**	**Total (37)**
1	Utiliza números	2 (40%)	0 (%)	5 (19%)	7 (19%)
2	Utiliza símbolos	1 (20%)	0 (%)	4 (15%)	5 (14%)
3	Indicador Gráfico de fortaleza	1 (20%)	1 (16%)	10 (38%)	12 (32%)
4	Sin palabras del diccionario	0 (%)	0 (%)	0 (%)	0 (%)
5	Cámbiala regularmente	0 (%)	0 (%)	0 (%)	0 (%)
6	Ninguno	3 (60%)	4 (66%)	14 (54%)	21 (57%)

4.3 Registro de la contraseña

4.3.1 Consejos dados

Tal y como se aprecia en la tabla 3, el 57% de los sitios web analizados, no ofrecen ningún tipo de consejo a sus usuarios a la hora de elegir una contraseña, y solamente el 14% aconseja usar algún tipo de símbolo no alfa-numérico.

Actualmente el robo de cuentas está a la orden del día, pero dados los datos recogidos en la Tabla 3, en mi opinión, no se están tomando las medidas oportunas para prevenirlo.

Ninguno de los sitios web analizados recomendó a sus usuarios no utilizar palabras que aparezcan en los diccionarios o que la contraseña sea cambiada regularmente.

Uno de los sitios web, “Central de reservas”, generó automáticamente la clave de la cuenta de usuario y la envió como texto plano al usuario junto al link de activación de la cuenta. La clave

eran 6 dígitos alfanuméricos. El sitio permitía al usuario elegir posteriormente su propia contraseña.

En ninguno de los sitios web analizados se permitía registrar una pista sobre la contraseña al modo “Windows 7” para facilitar al usuario recordar la contraseña en caso de ser necesario.

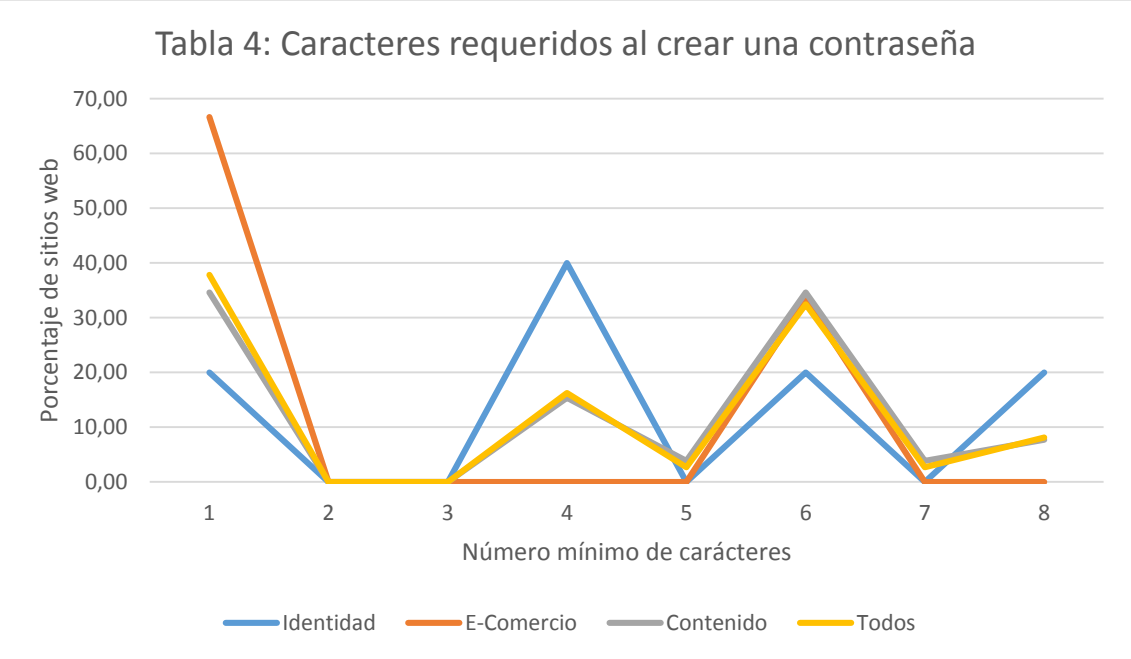
4.3.2 Requerimientos de la contraseña

La principal restricción que hemos encontrado a la hora de elegir una contraseña para un sitio web, ha sido la longitud mínima de la contraseña, el 62% tenía este requisito. Mayoritariamente, dicha restricción se sitúa en una longitud de 6 caracteres. Los sitios web cuya restricción a usar un número mínimo de caracteres era menor, fueron los de comercio electrónico, de los cuales el 66% toleraban contraseñas de un único carácter.

Dejando aparte la restricción de longitud, la mayor parte de los sitios analizados no tenían ningún otro requisito. Sólo dos de los sitios analizados (ElEconomista.es e infojobs.com) prohibían usar contraseñas tales como “password”, “1234” o “contraseña”.

Ninguno impuso otras restricciones tales como el uso de símbolos no alfanuméricos, la reutilización de la contraseña o el cambio regular de la misma.

Otra de las medidas de seguridad más útiles a día de hoy es la autenticación en dos pasos, consiste en vincular tu cuenta de usuario a un número telefónico o a un correo electrónico, de modo que cuando te vas a autenticar te llega un mensaje con un código o un link de verificación para autorizar dicho acceso. Ninguno de los sitios web analizados disponía de este sistema.



4.4 Login

4.4.1 Identificación

La mayoría de los sitios web analizados (25, 68%), durante la identificación piden al usuario que utilice su email. Algo menos de la mitad (18, 49%) permite al usuario identificarse mediante su Nick.

Cabe destacar que de los sitios de identidad analizados, el 80% pedían al usuario que utilizara su Nick, y que de los sitios de comercio electrónico analizados, el 100% pedían el email.

La razón para ello, podría responder a un intento por incrementar el nivel de seguridad, o a un intento por facilitar al usuario la tarea de recordar sus propios datos.

El hecho de que te identifiques con tu nick, facilita la tarea de recordar tus datos, debido a que la mayor parte de la gente, solamente utiliza un Nick a la hora de registrarse en las páginas web, especialmente en los sitios de identidad, esto es debido a que dichos usuarios se identifican con él, es por así decirlo, su segundo nombre. Por tanto el hecho de recordarlo es más fácil.

Por el contrario, el hecho de utilizar tu email para identificarte, podría incrementar tu nivel de seguridad, ya que hoy en día es fácil crearse varias cuentas de correo electrónico y reservar una sólo para registrarse en páginas serias, de modo que sea un dato “secreto” adicional, una especie de segunda contraseña, la cual también tendría que identificar un posible atacante.

De los 37 sitios analizados, 5 permitían usar indistintamente el Nick o el email durante la identificación.

4.4.2 Password Submision (presentación de la contraseña)

La gran mayoría de los sitios analizados (33, 89%), capturan la contraseña de los usuarios mediante una entrada HTML “imput= password”.

Sin embargo, hubo 4 sitios (11%) que capturaron la contraseña utilizando una entrada “imput= text”. Dichos sitios fueron: Telecinco, Cuatro, HogarUtil y La Nueva España Digital, todos pertenecientes a la categoría de contenido.

Durante el inicio de sesión, el 22% (9 sitios) llevaron a cabo las comunicaciones utilizando un enlace totalmente cifrado, un 16% (6 sitios) utilizó uno parcialmente cifrado y un 59% (22 sitios) no cifró las transmisiones.

Cabe destacar que de los sitios de comercio electrónico, el 33% llevó a cabo las transmisiones de datos sin cifrar.

4.5 Identidad Federada

La Identidad Federada, consiste en almacenar en un solo lugar la identidad y los datos referentes a un usuario, y recurriendo a dicha identidad poder identificarte en cualquier sitio web compatible con este sistema.

Durante años se han llevado a cabo diversos intentos de crear una Identidad Federada orientada a los usuarios domésticos (la idea original está más orientada a trabajadores de empresas). Los más conocidos actualmente serían los siguientes: Google+, Facebook, Twiter, OpenID, Linkedin y Live.

El uso/implantación de estos servicios se puede apreciar en la tabla 5.

Tabla 5: Identidad Federada

	Google+	**Facebook**	**Twiter**	**OpenID**	**Linkedin**	**Live**
Contenido (26)	5	12	3	0	1	3
E-Comercio (5)	0	0	0	0	0	0
Identidad (6)	0	2	2	0	0	0
Total (37)	5	14	5	0	1	3

De los 37 sitios analizados, 22 no permitían utilizar ningún tipo de identidad federada. Eso supone un 60% de las webs que han sido analizadas. Es un porcentaje muy elevado y revela la baja implantación de este sistema.

Como se aprecia en la tabla, el sistema de Identidad Federada más extendido es el de Facebook (93%), seguido de lejos por Twiter (33%) y Google+ (33%). El siguiente sería Live (20%). Linkedin sólo se admitía en un sitio y OpenID en ninguno.

En cualquier caso, la implantación de este sistema, dista mucho de ser mayoritaria.

La fundación Mozilla ha desarrollado una iniciativa parecida, se llama “Mozilla Persona”, y básicamente es lo mismo que las otras opciones, te registras en “Persona” y luego para registrarte en una web compatible con este sistema, sólo tienes que introducir tu email, ni contraseñas, ni datos personales de ningún tipo. En la bibliografía agrego un link con más información al respecto.

4.6 Actualizar Contraseña.

La totalidad de los sitios web analizados, permitían al usuario actualizar su contraseña. El problema de este tipo de opciones, es que un usuario pueda usurpar tu sesión, y modificar dicha contraseña, robándote tu cuenta de usuario.

La solución es sencilla y ha sido implementada por todos los sitios web analizados salvo uno “hogarutil.com”. Dicha solución consiste en requerir al usuario su contraseña actual a la hora de modificar los datos sensibles del perfil del usuario, como por ejemplo la contraseña o el email.

Otra buena práctica, es notificar por email al usuario el cambio de contraseña, dicha notificación solamente fue llevada a cabo por “MuyInteresante”, “ECartelera” y “CasaDelLibro”.

4.7 Recuperar Contraseña.

La totalidad de los sitios web analizados permiten recuperar la contraseña del usuario. Todos los sitios web analizados seguían el procedimiento basado en el envío de un email, aunque existen algunas variantes.

4.7.1 Recuperación basada en email.

El 100% de los sitios web analizados recurrieron al envío de un email al usuario. Dentro de este sistema, hay dos variantes que a su vez tienen algún pequeño cambio.

Las dos variantes principales son, o bien enviar directamente al usuario una nueva contraseña generada aleatoriamente, o bien enviar un link para acceder a una sección de la web donde crear una nueva contraseña.

Las variantes consisten en los posibles requerimientos para que dicho email sea enviado, y van desde escribir una captcha hasta escribir tu fecha de nacimiento.

Cabe destacar, que el sitio web “Shogun’s Fate” solicitó nuestra dirección de email, y nos envió nuestro usuario y nuestra contraseña en texto plano, de ahí se deduce que esos datos están almacenados en su base de datos y no solamente un código hash de los mismos.

4.7.2 Recuperación basada en pregunta personal

Este es otro sistema muy recurrente, pero que bien porque se está descartando o bien por pura coincidencia no existe en ninguno de los sitios analizados.

Normalmente éste sistema consistía en contestar una pregunta cuya respuesta había dado el usuario durante el registro. Podían ser preguntas predeterminadas o incluso una inventada por el usuario.

4.8 Limitar los intentos al usar una contraseña

En este estudio, hemos comprobado ligeramente la vulnerabilidad de los sitios web analizados frente a los intentos por adivinar la contraseña de un usuario que utilizan el método de ensayo y error.

Partimos del hecho de que disponemos del nombre del usuario/correo electrónico, y lo que queremos averiguar es la contraseña.

Si el sitio en cuestión, tras más de 5 intentos en un solo minuto, no nos redirige a otra página, nos exige introducir una captcha, o directamente nos bloquea los intentos de inicio de sesión desde nuestra IP, consideraremos que dicha web es vulnerable tanto a un ataque por fuerza bruta, como a uno por diccionario. El hecho de conseguir la contraseña, sólo dependería del tiempo.

Los resultados de estas pruebas, están en la Tabla 6.

Tabla 6: Vulnerabilidad a fuerza bruta y distinción entre usuario o email erróneo.

	Características	Identidad (5)	E-Comercio (6)	Contenido (26)	Total (37)
1	Sí es vulnerable a un ataque por fuerza bruta o por diccionario	3 (60%)	4 (67%)	23 (88%)	30 (81%%)
2	Al autenticarse de forma errónea sí se distingue entre usuario y contraseña	1 (20%)	1 (17%)	6 (23%)	8 (22%)

El 81% de los sitios web analizados, son vulnerables a un ataque por fuerza bruta. Cabe destacar, que aunque el porcentaje de sitios vulnerables en la sección de comercio electrónico es menor, sigue siendo de un 67%.

4.9 Prevención de sondeo de usuario

Es importante intentar proteger los intentos de sondeo de usuario registrado. Los usuarios habitualmente utilizan un mismo nombre de usuario (nic) así como un mismo email, para registrarse en diferentes páginas web.

Por tanto, se debería intentar evitar que un usuario sepa si en una página “A” existe un usuario “X”, ya que sino un posible atacante, podría intentar averiguar la contraseña del usuario “X” en una página “B”, “C” o “D”.

4.9.1 Login

La pantalla de autenticación del usuario, comúnmente conocido como login, es la forma más fácil de saber si un usuario está o no registrado en un sitio web.

El 22% de los sitios web analizados, al cometer un error durante el login, diferenciaban con su respuesta al usuario entre usuario/email erróneo y contraseña errónea.

De cara a la seguridad, tal y como se comenta en el apartado 4.9, es mejor que dicha diferenciación no se produzca. De cara a la satisfacción del usuario, le suele agradar más saber dónde ha cometido el error.

4.9.2 Registro

Otra forma que tienen los posibles atacantes de averiguar si un usuario determinado está o no registrado en un sitio web, es a través del registro de una nueva cuenta.

Si durante el registro de la cuenta, al atacante se le informa de que dicho usuario ya está en uso, dicho atacante ya ha obtenido la información que estaba buscando.

El único modo de evitar esto, o al menos de evitar la automatización de esta comprobación, es requerir al usuario que se está intentando registrar, que introduzca una CAPTCHA, así al menos descartamos el sondeo de usuarios automatizado.

De las 37 páginas analizadas, ninguna tenía implementada esta medida de seguridad.

4.9.3 Reset

Otro modo de comprobar si un usuario existe o no en un sitio web, es usar el restablecimiento de contraseña.

A la hora de restablecer una contraseña, el sitio web te pide que introduzcas el usuario o el email (en función del cual use esa página web como identificador).

Una vez introducido, al confirmar, el sitio web te informa de si se ha llevado a cabo correctamente (es decir el usuario/email existe) o si ha habido algún error (es decir el usuario/email no existe).

La solución es la misma que en el punto anterior, requerir al usuario una CAPTCHA.

De los 37 sitios web analizados, sólo 6 solicitaron al usuario que introdujera una CAPTCHA para poder llevar a cabo el reseteo de la contraseña.

De los 6, 5 eran sitios de contenido, y 1 de identidad. Ningún sitio de comercio electrónico solicito al usuario dicha CAPTCHA.

4.10 Cifrado y Autenticación

De los 37 sitios web analizados, solamente 9 (24%) implementaban TLS para proteger el envío de las contraseñas. Había 6 sitios web (16%) que implementaban TLS de una forma parcial, de modo que no protegían correctamente el envío de dichas contraseñas.

Esto nos deja con que el 60% de los sitios web analizados, no cifraban el envío de los datos del usuario durante la autenticación del mismo.

Cabe destacar, que de los 5 sitios de identidad analizados, sólo Tuenti utilizaba TLS, y de los 6 sitios de comercio electrónico analizados, 3 implementaban TLS de forma total, y 1 de forma parcial.

5. Análisis

Con el fin de simplificar y objetivar al máximo posible el proceso de calificación de la seguridad de cada uno de los sitios web que hemos analizado, hemos creado unas tablas donde se explican los criterios tenidos en cuenta para puntuar cada uno de los distintos aspectos analizados.

Hay que tener en cuenta que en este artículo, sólo se han analizado las características relativas a la seguridad más extendidas. Hay sitios web que pueden tener alguna medida de seguridad muy particular, y que no haya sido analizada.

Este test, solamente debe tenerse en cuenta como algo capaz de orientar al lector respecto al nivel de importancia que dan a su/tu seguridad cada uno de los sitios que hemos analizado.

Merece la pena resaltar, que al utilizar un sistema de puntuaciones, dos sitios con la misma calificación, podrían tener unas medidas de seguridad totalmente diferentes.

En esta sección, voy a comparar mis resultados, con los resultados obtenidos en el artículo "The password thicket: technical and market failures in human authentication on the web" (en Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS), June 2010).

5.1 Experiencia de Usuario

Volviendo a la **Pregunta 1**, en general, no hay grandes variaciones entre los datos y las medidas de seguridad de las diferentes páginas web, al menos de cara al usuario.

Entrada de la contraseña

En el 89% de los casos la contraseña fue capturada mediante una entrada HTML "imput= password". El 68% de los sitios, pedía que se utilizara el email como identificador de usuario. El 57% de los sitios web, no ofrecía ningún consejo a sus usuarios sobre cómo elegir la contraseña.

En mi opinión, eso podría demostrar dos cosas, o bien que los diseñadores dan por hecho que los usuarios ya saben por sí mismos cómo elegir una contraseña fuerte, o bien que no valoran lo suficiente la seguridad de dichos usuarios.

Lo datos obtenidos en el otro artículo son muy parecidos, el 87% de los sitios web acepta el email como identificador de cuenta, y el 78% proporciona asesoramiento sobre cómo crear la contraseña.

Consejos de seguridad y requerimientos, sin relación

No existe una relación clara entre que un sitio web ofrezca consejos o no sobre como diseñar una contraseña segura (4.3.1) y que después dicho sitio web también tenga unos mínimos requerimientos para la contraseña (4.3.2).

Hay todo tipo de casos, páginas con unos consejos muy amplios, pero que en la práctica no exigen a sus usuarios que los pongan en práctica, páginas que no dan consejos pero que si tienen requerimientos, y luego un tercer caso, las que ni aconsejan ni exigen nada.

Tampoco hubo un patrón claro en lo referente a otros mecanismos de seguridad, tales como TLS (4.10), o el modo de restablecer la contraseña mediante email (4.7). En ambos casos no se pueden sacar patrones diferenciadores entre los diferentes tipos de páginas web, en algún

caso concreto alguno de los segmentos tubo un porcentaje algo mayor, pero en mi opinión nada realmente diferenciador.

En mi opinión, dado que el usuario medio en general, aun no comprende ni la importancia ni el modo de crear una contraseña segura, los defectos de diseño e implementación anteriormente citados, resultan preocupantes.

5.2 Debilidades en la Seguridad

Volviendo a la **Pregunta 2**, nos damos cuenta de que hay múltiples debilidades de implementación, ya sea por dejadez, ineptitud o por falta de presupuesto de los diseñadores.

Las mejores prácticas están lejos de ser universales

La mayor parte de las mejoras en seguridad que aparecen en la literatura reciente, han sido ignoradas en la mayor parte de los sitios web analizados.

Un ejemplo sería el siguiente, el 76% de los sitios web mandaban las contraseñas sin utilizar TLS. Al sondeo de usuarios, de una u otra forma, fueron vulnerables el 100% de las páginas, y al tanteo de contraseñas sin restricciones de intentos fueron vulnerables el 81%.

Este tipo de prácticas, claramente son fallos de seguridad y deberían de ser solucionados.

En el otro artículo objeto de esta comparativa, el 57% de los sitios web no usaba TLS, el 83% eran vulnerables al sondeo de usuario y el 84% al de contraseña.

La mayor parte de los aspectos de una contraseña, no están estandarizados

No se ha llegado a ningún consenso en lo referente a los requisitos exigibles a un usuario de cara a crear una contraseña segura.

En general hay 5 conceptos básicos ordenados de mayor a menor importancia que se deberían manejar al crear una contraseña:

1. Longitud mínima.
2. Uso de mayúsculas y minúsculas
3. Uso de números
4. Uso de caracteres especiales
5. Excluir palabras del diccionario.

De las 37 páginas analizadas, sólo el 67% llegó a pedir el primer requisito, y la longitud mínima más común, fue de 6 caracteres en un 35% de los casos (4.3.2). Lo recomendable, sería una contraseña de más de 8 caracteres.

El número de sitios que llegan a exigir los demás requisitos va decreciendo hasta el punto de que ninguno de los sitios web analizados impidió usar palabras del diccionario.

Todos los sitios web, deberían ofrecer consejos útiles a sus usuarios a la hora de crear la contraseña, pero en la práctica, el 57% no ofreció ningún tipo de consejo (4.3.1).

El número de intentos erróneos de inicio de sesión debería de ser limitado, y el reseteo de la contraseña, debería de restringirse, o al menos implementarse bien para que no supongan un problema al usuario. Hay casos en los que directamente, sin comprobar la identidad del usuario, al realizar el reset (algo accesible para cualquiera que conozca tu identificador, es decir, tu usuario/email) te es enviada una nueva contraseña a tu email (y anulada la anterior).

Muchas políticas de seguridad, no tienen coherencia interna

La política de seguridad de muchas páginas, es inconsistente. Esto se aprecia especialmente en el uso/implementación de TLS. Un ejemplo de ello, sería el uso parcial de TLS (4.10).

Esto denota errores de los programadores a la hora de diseñar la web, y ya sea debido a la falta de preparación o a la falta de presupuesto, la consecuencia es la falta de seguridad para el usuario final.

En el otro artículo, han llegado a la misma conclusión.

5.3 Rendimiento en seguridad y posicionamiento en el mercado

Respondiendo a la **Pregunta 3**, y a la luz de los datos que hemos recogido, se llega a la conclusión de que no hay factores clave que indiquen o que garanticen que la página web tenga una cantidad mayor de medidas de seguridad.

En general, se podría decir, que las páginas web con mayor tráfico, tienen una seguridad mayor, o que los sitios web más populares, intentan que sus usuarios tengan una contraseña más robusta.

No hay diferencia entre que el sitio distribuya contenidos, venda productos o sea una web de identidad. Esas categorías no influyen directamente sobre la seguridad de la página.

Un ejemplo positivo en todo lo dicho anteriormente, sería Tuenti. Se corresponde con la categoría de identidad, es un sitio popular y tiene un tráfico considerable. Tiene implementadas el 86% de las medidas de seguridad que han sido analizadas en este artículo, y además tiene medidas adicionales tales como la autenticación en dos pasos o la comprobación de identidad mediante teléfono móvil.

Por el contrario, tendríamos El Corte Inglés, es un sitio de comercio electrónico, es popular, tiene tráfico, pero apenas tiene implementadas un 40% de las medidas de seguridad recogidas en el artículo.

Cabría esperar, que una web como la del Corte Inglés, fuese al menos tan segura como la de Tuenti. Ambas páginas web tienen un buen presupuesto (o la capacidad para tenerlo) y son populares, pero no es así.

Estos dos, no son los únicos ejemplos encontrados durante el análisis, por lo cual, vuelvo a la afirmación inicial, no hay factores clave que relacionen el posicionamiento en el mercado de un sitio web y su rendimiento en seguridad.

El otro artículo, no llega a la misma conclusión que el mío. Según ese artículo, a mayor tráfico, mayor presupuesto y mejores medidas de seguridad.

En mi análisis, (apéndice 3) solamente 6 de los 37 sitios analizados aprueban, el resto no llega a obtener ni si quiera 5 puntos sobre 10. Dentro de los sitios que aprueban, los hay grandes y los hay pequeños.

5.4 Motivaciones en Seguridad

De los 37 sitios analizados, sólo 5 almacenaban datos de pago del usuario. De esos 5 sitios, había 3 que pertenecían a la categoría de Contenido, 2 que pertenecían a la de Comercio electrónico y ninguno que perteneciese a la de Identidad.

Las puntuaciones obtenidas por los sitios serían las siguientes:

Sitio Web	Categoría	Nota
El Economista	Contenido	4
Hola	Contenido	4
El Diario.es	Contenido	5
Casa del Libro	Comercio	8
Central de reservas	Comercio	4

Las puntuaciones se han establecido de acuerdo a los criterios adjuntos en el Anexo 1.

Con una muestra tan pequeña sería arriesgado afirmar que los sitios de Comercio tienen una seguridad mayor que la de las otras dos categorías, sobre todo, cuando hay otras páginas analizadas de la categoría de Comercio (no incluidas en esta sección por no almacenar datos de pago) y que tienen una puntuación inferior a 4.

La calificación máxima que se podía sacar en el análisis, era de 15 puntos, así que todos los sitios web estarían suspendidos, menos “Casa del libro” que aprobaría con un 5,3.

Respondiendo a la **Pregunta 4**, no está claro que haya un patrón entre el hecho de que una página web albergue datos bancarios, y que automáticamente ésta tenga un mayor nivel de seguridad.

El otro artículo sigue discrepando con este, y afirma que los sitios de contenido son los que peor puntuación en seguridad tienen.

5.5 Motivaciones para desarrollar la contraseña

Respondiendo a la **Pregunta 5**, hoy en día los usuarios navegan por internet desde múltiples plataformas, tres ejemplos podrían ser el ordenador de casa, el del trabajo y el teléfono móvil. Si las personalizaciones de cada página se almacenasen en cada dispositivo, el usuario tendría que llevarlas a cabo en todos ellos, con el consiguiente tiempo perdido.

Con la aparición de servicios de sincronización en la nube como Dropbox, Copy, Google Drive o BitTorrent Sync, sería posible sincronizar dichos perfiles entre todos los dispositivos, pero esto requeriría de unos conocimientos informáticos de los que no disponen todos los usuarios.

La opción más simple, es almacenar el perfil en cada página web. Para ello es necesario que el usuario cree su propia cuenta en dicha página.

Se especula con que algunos de estos sitios después venden a terceros la información recopilada sobre el usuario durante el registro. Dicha acción es un delito ya que viola la ley de protección de datos.

La única luz que puede aportar este artículo al respecto (ya que no se centraba en este asunto) es afirmar que en la cuenta de correo electrónico usada para crear las cuentas de usuario, no sé ha recibido spam de terceras personas, es decir, los correos provenían de la propia web con publicidad, ofertas y novedades de la misma.

6. Interpretaciones económicas

Los principales problemas observados en la seguridad de las contraseñas se pueden explicar y agrupar en dos, la delegación en el usuario por parte de las empresas en elegir y recordar su contraseña, y el hecho de reutilizar por parte de los usuarios la misma contraseña una y otra vez en diferentes sitios web.

El primer problema, delegar la elección y memorización de las contraseñas al usuario, provoca que habitualmente la seguridad de las mismas sea muy reducida. El usuario tipo, normalmente busca contraseñas fáciles de recordar, y eso suele implicar que también sean fácilmente descifrables por un posible atacante.

El segundo problema causa que por muy buenas medidas de seguridad que adopte una página web, si el usuario repite la misma contraseña en todas aquellas páginas en las cuales está registrado, un posible atacante, la capture en una página web de baja seguridad y luego la pueda utilizar en una de alta seguridad.

A continuación examinamos estos problemas y sus posibles soluciones, así como la vertiente económica del problema.

6.1 El problema de memorizar contraseñas

Los usuarios tienen una capacidad de memorizar contraseñas limitada, y cada vez es necesario registrarse en más sitios web para poder utilizarlos o para poder disfrutar de todas sus características.

Esto necesariamente lleva al usuario medio hasta dos posibilidades, o bien simplificar la contraseña o bien reutilizarla.

Dado que hay sitios que dificultan al usuario el uso de contraseñas simples y poco seguras añadiendo restricciones de caracteres especiales, uso de números y demás medidas de seguridad analizadas anteriormente, los usuarios puestos a tener que recordar múltiples contraseñas y además algunas de ellas complejas, optan por tener una única contraseña segura y reutilizarla.

A causa de esto, una contraseña segura utilizada en una página web segura y con unas restricciones de uso de contraseña estrictas, es vulnerable, ya que el posible atacante, en lugar de intentar obtener la contraseña en esa página web, lo hará cuando el usuario la utilice en una página web insegura.

6.2 La seguridad de la contraseña dependiente de agentes externos

Tal y como comentábamos en el punto 6.1, la memoria de los usuarios es limitada, y por tanto tienden a reutilizar la misma contraseña una y otra vez en los diferentes sitios web en los cuales se registran.

También es habitual, que dichos usuarios utilicen la misma dirección de correo electrónico como identificador en dichos sitios web.

La consecuencia es que un supuesto atacante, en lugar de tener que vulnerar la seguridad del sitio al cual quiere acceder, sólo tiene que burlar la del sitio con una seguridad menor en el cual se haya registrado el usuario objetivo.

6.3 Posibles soluciones reguladoras

En nuestra opinión el mercado ha fallado en su intento de regularse así mismo en lo referente a la seguridad de las contraseñas de los sitios web.

No se han tenido en cuenta, o si se ha hecho, no de la forma apropiada, los dos aspectos fundamentales y ya comentados en puntos anteriores

En primer lugar, la capacidad de memoria limitada de los usuarios. En casi cualquier sitio web se le pide al usuario que cree una cuenta y por tanto que memorice una contraseña. En segundo lugar, y como derivado del punto anterior, la reutilización de contraseñas. El usuario reutiliza sus contraseñas así que la seguridad de la misma es igual a la seguridad del peor sitio web donde haya sido utilizada.

Proponemos las siguientes medidas para paliar estos problemas

Restringir la reutilización de contraseñas

Una opción, podría ser establecer un nivel de seguridad a las contraseñas en función del nivel de seguridad requerido por el sitio web.

Es decir, un sitio con un nivel de seguridad bajo, véase cualquier sitio web de contenido estándar, podría tener una limitación máxima al tamaño de contraseña de 6 caracteres. En cambio, un sitio con un nivel de seguridad alto, como por ejemplo cualquiera que almacene datos bancarios, podría tener una limitación de un mínimo de 7 caracteres para su contraseña.

De este modo, las contraseñas quedarían forzosamente segmentadas y un usuario no podría usar la misma contraseña en una web de baja seguridad y otra de alta.

Problemas, internet es “libre” y “global”, no es fácil acordar este tipo de estándares ya que cada administrador web, puede hacer lo que quiera, especialmente si dicha web está alojada en países con una legislación laxa. Otro problema, sobre todo inicialmente, sería que a los usuarios les causaría cierta confusión recordar qué sitio es de alta o de baja seguridad.

Estándares técnicos

Sin lugar a dudas esta sería la mejor opción, tanto por resultados finales, como por facilidad de implantación.

Consistiría en crear kits de desarrollo para la generación de contraseñas y todo lo relacionado con la gestión de las cuentas del usuario.

Se podrían crear con diferentes estándares de seguridad, e incluso crear una marca comercial asociada para que tanto los usuario como los desarrolladores tuvieran una referencia sobre la seguridad real de lo que tienen entre manos.

Otra ventaja de usar un sistema así, sería que se estandarizaría también todo el popurrí de consejos/requisitos que sufren los usuarios cada vez que se registran en una web.

Si se crease como software libre, a los sitios web pequeños, no les supondría un costo elevado diseñar su página web respetando unos mínimos estándares de seguridad.

Identidad Federada

Una última opción, sería utilizar una Identidad Federada Global, algo así como la opción desarrollada por Mozilla, “Persona”, pero estandarizado a nivel mundial, y financiado

apropiadamente. Consistiría en una identidad “global” que serviría para identificarnos en cualquier sitio web sin necesidad de utilizar una contraseña. La contraseña sólo la utilizaríamos al identificarnos en el servidor de “Persona” y luego él se encargaría de las gestiones para el registro y la autenticación con el resto de los sitios web.

Un posible problema sería que si un usuario busca privacidad no querría usar este sistema, ya que según cómo fuese diseñado podría servir para controlar casi cualquier tipo de actividad que realizasen los usuarios en internet.

7. Conclusiones

En el estudio que hemos llevado a cabo, se ha analizado de una forma práctica, el modo en el cual se implementa la seguridad en la contraseña.

Nuestras observaciones respecto a los fallos detectados, se pueden agrupar en 2 campos, y los voy a explicar a continuación:

Fallos Técnicos

El análisis llevado a cabo confirma nuestras suposiciones iniciales. Todo lo relacionado con la implementación de una contraseña de acceso, al menos la parte de cara al usuario, mayoritariamente, se hace de forma insegura.

La implementación de estos sistemas varía mucho de unos sitios web a otros y ello provoca inconsistencias y fallos de seguridad.

Para solucionar esto, lo más sencillo sería desarrollar un estándar de referencia con código fuente de libre acceso para los desarrolladores, de modo que cada uno de ellos no tenga que desarrollar desde cero cada implementación de estos sistemas.

Ello evitaría los problemas de seguridad debidos a los fallos de los desarrolladores y también estandarizaría los consejos y los requisitos mínimos exigidos a los usuarios a la hora de crear una contraseña.

En cuanto a qué consejos o qué requisitos mínimos exigir, hay documentación abundante en internet, y en este mismo artículo.

Fallos del Mercado

Dado el alto número de casos de robo de cuentas o de robo incluso de intrusión en servidores de compañías con el consiguiente robo de cientos de contraseñas a la vez, sorprende ver que las empresas no hacen gran cosa al respecto.

Las páginas web españolas analizadas, en general, tienen una seguridad en la contraseña bastante baja.

Esto se debería de solucionar a corto plazo. No veo viable una regulación al respecto por parte del estado, ya que aparte de la complejidad y posiblemente imposibilidad legal de hacerlo, a la gente no le gusta que el gobierno intente regular internet.

La solución más plausible, sería desarrollar algo similar a OpenID o Persona. Pero el mercado no parece estar a favor de esto, ya que OpenID está casi desaparecido y la implantación de Persona es casi inexistente. Se podría intentar financiar inicialmente con algún tipo de

subvención estatal, pero dejando su gestión a una organización sin ánimo de lucro. Con un sistema así, el problema de los fallos de seguridad por la mala elección de la contraseña, o por el robo de la misma, desaparecería, o al menos quedaría reducido a algo muy puntual.

Mi opinión personal y valoración del artículo

La realización de este artículo me ha parecido una tarea interesante, ya que ha cambiado significativamente mi percepción respecto a la seguridad de los sitios web. Dados los habituales casos de robo masivo de cuentas y contraseñas, ya incluso recogidos por la prensa y los informativos, creía que la seguridad sería mayor. Pero dada la baja puntuación obtenida por la amplia mayoría de los sitios web aquí analizados, sólo aprueban el 16% y sólo un sitio saca más de un 8 sobre 10, he comprendido la baja seguridad que hay en la mayoría de los sitios.

Sería interesante que el estudio se volviese a realizar dentro de unos años, para comprobar la evolución de las medidas de seguridad, pero viendo los resultados de la comparativa que ha sido hecha entre éste y el de 2010, no parece que la evolución vaya a ser muy positiva. Por citar un ejemplo de esto, en la sección 5 apartado 1 de este artículo, los resultados comparados con el artículo de 2010, han ido a peor. No se puede afirmar que se deba solamente al paso del tiempo, ya que el método llevado a cabo para la selección de los sitios web analizados es diferente, pero en cualquier caso, a mí personalmente me preocupan esos resultados.

Para terminar, me gustaría resaltar especialmente la solución propuesta tanto en este artículo como en el anterior referida a las identidades federadas. Puede que no sea una solución definitiva, pero dados los resultados actuales, creo que sería algo fácilmente aplicable a corto plazo. A largo plazo apostaría más por la solución de las herramientas estandarizadas para desarrolladores.

Bibliografía

The password thicket: technical and market failures in human authentication on the web" (en Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS), June 2010)

Contraseña https://es.wikipedia.org/wiki/Contrase%C3%B1a

Identidad Federada https://es.wikipedia.org/wiki/Identidad_federada

Mozilla Persona https://support.mozilla.org/es/kb/que-es-y-como-funciona-mozilla-persona

Apéndices

Apéndice 1. Criterios de evaluación de la seguridad de los sitios web analizados.

Sección	Característica	Puntuación
	Registro	
4.3.1	Recomendaciones de contraseña	+1pt
4.3.2	Tamaño mínimo de contraseña	+1pt
4.3.2	Prohibición del uso de palabras de diccionario	+1pt
4.3.2	Requerir el uso de números o símbolos	+1pt
4.9	Proteger la lista de usuarios	+1pt
4.2.2	Enviar en texto plano la clave al email del usuario	-1pt
	Login	
4.4.2	Cifrado de la contraseña antes del envío	+1pt
4.8	Límite de pruebas al introducir la contraseña	+1pt
4.9	Proteger la lista de usuarios	+1pt
4.5	Aceptar login mediante uso de Identidad Federada	+1pt
	Actualización de contraseña	
4.6	Requerir la contraseña original durante el proceso	+1pt
4.6	Notificar el cambio al usuario por email	+1pt
	Recuperación de contraseña	
4.7	Requerir cambiar la contraseña tras recuperarla	+1pt
4.7.1	Envío por email de la contraseña en texto plano	-1pt
4.9	Proteger la lista de usuarios	+1pt
	Transmisión Cifrada	
4.10	Uso total de TLS para la transferencia de contraseñas	+2pt
4.10	Uso de TLS sólo al usar POST	+1pt

Apéndice 2. Lista de sitios web analizados.

1) El Mundo, www.elmundo.es
2) El País, www.elpais.com
3) As, www.as.com
4) ABC, www.abc.es
5) 20 Minutos, www.20minutos.es
6) Telecinco, www.telecinco.es
7) RTVE, www.rtve.es
8) El Economista, www.eleconomista.es
9) Hola, www.hola.com
10) Páginas Amarillas, www.paginasamarillas.es
11) InfoJobs, www.infojobs.net
12) Público.es, www.publico.es
13) Fotocasa, www.fotocasa.es
14) Mis-Recetas, www.mis-recetas.org
15) Cuatro, www.cuatro.com
16) Hogar útil, www.hogarutil.com
17) ElDiario.es, www.eldiario.es
18) Muy Interesante, www.muyinteresante.es
19) FormulaTV, www.formulatv.com
20) La Nueva España, www.lne.es
21) E-Cartelera, www.ecartelera.com
22) serPadres.es, www.serpadres.es
23) VerTele!, www.vertele.com
24) AutoBild.es, www.autobild.es
25) Computer Hoy, www.computerhoy.es
26) Hobby Consolas, www.hobbyconsolas.com
27) El Corte Inglés, www.elcorteingles.es
28) Casa del Libro, www.casadellibro.com
29) Mumumio, www.mumumio.com
30) Central de Reservas, www.centraldereservas.com
31) Cooking Hacks, www.cooking-hacks.com
32) Aceros de Hispania, www.aceros-de-hispania.com
33) Tuenti, www.tuenti.com
34) Shogun's Fate, www.shogunsfate.com
35) Bitácoras, www.bitacoras.com
36) Partigi, www.es.partigi.com
37) HTCMania, www.htcmania.com

Apéndice 3. Resultados de los sitios web analizados al aplicar los criterios de evaluación del apéndice 1.

Sitios Web	Registro						Login				A.C.		R.C.			T.C.		P. Totales
	+1pt	+1pt	+1pt	+1pt	+1pt	-1pt	+1pt	+1pt	+1pt	+1pt	+1pt	+1pt	+1pt	-1pt	+1pt	+2pt	+1pt	Max 15pt
El Economista	Si	Si	No	No	No	No	Si	No	Si	No	No	No	Si	Si	No	No	-	4
Hola.com	No	No	No	No	No	No	Si	No	Si	No	No	No	Si	Si	No	Si	-	4
El Diario.es	No	Si	No	No	No	No	Si	No	Si	No	No	No	Si	No	No	No	Si	5
Casa del Libro	Si	No	No	No	No	No	Si	Si	No	No	Si	Si	Si	No	No	Si	-	8
Central de Reservas	No	Si	No	No	No	Si	Si	Si	No	No	No	No	Si	Si	No	Si	-	4
El Mundo	Si	No	No	No	No	No	Si	No	No	No	No	No	Si	No	No	Si	-	5
El País	Si	Si	No	Si	Si	No	Si	No	Si	Si	Si	No	Si	No	No	Si	-	11
As	Si	Si	No	No	Si	No	Si	No	No	No	No	No	Si	No	No	No	No	5
ABC	Si	No	No	No	No	No	Si	No	Si	No	No	No	Si	Si	No	No	No	3
20 Minutos	Si	Si	No	Si	No	No	No	No	Si	Si	Si	No	Si	Si	Si	No	No	7
Telecinco	No	Si	No	No	Si	No	Si	No	Si	Si	No	No	Si	No	Si	No	Si	8
RTVE	No	Si	No	No	Si	No	No	No	No	Si	No	No	Si	No	No	No	Si	5
Páginas Amarillas	No	Si	No	No	Si	No	Si	No	Si	Si	No	No	Si	No	Si	Si	-	9
InfoJobs	Si	Si	No	Si	No	No	Si	Si	Si	No	Si	No	Si	No	Si	Si	-	11
Público.es	Si	Si	No	No	No	No	Si	No	No	No	Si	No	No	Si	No	No	Si	4
Fotocasa	Si	Si	No	No	Si	No	Si	No	Si	No	No	No	No	Si	Si	No	No	4
Mis-Recetas	No	Si	No	No	No	No	Si	No	Si	Si	Si	Si	No	No	No	No	Si	7
Cuatro	No	Si	No	No	No	No	No	No	Si	No	No	No	Si	No	No	No	No	3
Hogar útil	No	No	No	No	No	No	No	No	Si	No	No	No	No	Si	No	No	No	0
Muy Interesante	No	Si	No	No	Si	No	Si	Si	Si	No	No	No	Si	No	No	No	No	6
FormulaTV	No	No	No	No	No	No	Si	Si	No	No	No	No	Si	No	No	No	No	3
La Nueva España	No	Si	No	No	No	No	No	Si	Si	Si	Si	No	Si	Si	No	No	No	5
E-Cartelera	No	Si	No	No	No	No	Si	Si	No	Si	No	No	Si	No	No	No	No	5
serPadres.es	No	Si	No	No	Si	No	Si	Si	Si	Si	No	No	Si	No	No	No	No	7
VerTele!	No	No	No	No	No	No	Si	No	Si	Si	Si	No	Si	No	No	No	No	5
AutoBild.es	Si	No	No	Si	Si	No	Si	No	Si	No	No	No	Si	Si	Si	No	No	6
Computer Hoy	Si	No	No	Si	No	No	Si	No	Si	Si	Si	No	Si	No	No	No	No	7
Hobby Consolas	Si	No	No	Si	No	No	Si	No	No	Si	No	No	No	No	No	No	No	4
El Corte Inglés	No	Si	No	No	No	No	Si	No	No	Si	Si	No	Si	Si	No	Si	-	6

Mumumio	No	No	No	No	No	No	Si	No	Si	No	Si	No	Si	No	No	No	No	4
Cooking Hacks	No	Si	No	No	No	No	Si	No	Si	No	Si	No	Si	No	No	No	No	5
Aceros de Hispania	No	No	No	No	Si	No	Si	Si	Si	No	Si	No	Si	No	No	No	Si	7
Tuenti	Si	Si	No	Si	Si	No	Si	Si	Si	No	Si	Si	Si	No	Si	Si	-	13
Shogun's Fate	Si	Si	No	No	No	Si	Si	No	No	No	Si	No	No	Si	No	No	No	2
Bitácoras	No	Si	No	No	Si	No	Si	No	Si	Si	Si	No	Si	Si	No	No	No	6
Partigi	No	Si	No	No	No	No	Si	No	Si	Si	No	No	No	No	No	No	No	4
HTCMania	No	No	No	No	Si	No	Si	Si	Si	No	Si	No	No	No	No	No	No	5