

Ibex Softworks

Improving your ideas

Reporte de seguridad web

ParkPlatz puede automatizar, gestionar, y brindar servicios de estacionamientos a los usuarios de la zona urbana, es decir, se divide en dos partes fundamentales, el conductor y el estacionamiento, donde ambos podrán reportar fallos en el sistema, y cuenta con un administrador global del sistema.

El estacionamiento cuenta con una herramienta de dibujo de modelado para que pueda crear el esquema de como es el estacionamiento, a su vez, puede publicar servicios adicionales, tarifas, su ubicación y lugares disponibles.

Por otro lado el conductor puede consultar los estacionamientos más cercanos a su ubicación, así como, ver la ruta por la que se puede desplazar para llegar a él, agregarlo como estacionamiento favorito para futuras visitas, ver los estacionamientos que ha visitado recientemente, ver los lugares disponibles, tarifas y servicios adicionales.

El administrador del sistema puede revisar los fallos reportados, así como, la gestión de los estacionamientos y brindarle las actualizaciones necesarias para su buen funcionamiento, en ambas cuestiones, el estacionamiento y el sistema en sí.

Se puede realizar las acciones necesarias para darse de alta y configuración de las cuentas de usuario, conductor, estacionamiento y administrador

Se le brinda al estacionamiento herramientas para diseñar, modificar y eliminar objetos pertenecientes al esquema del inmueble, así como, la posibilidad de cambiarle la disponibilidad a los lugares de aparcamiento mediante sensores o manualmente , publicar, servicios, tarifas, limitaciones que ofrece, y posicionamiento de mapa en la red de estacionamientos.

El conductor, desde la aplicación web, puede localizar los estacionamientos más cercanos a su ubicación, consultar una guía para llegar a él, marcar sus estacionamientos preferidos, ver, los estacionamientos que recientemente ha visitado, ver las tarifas que ofrece el estacionamiento, así como, los servicios adicionales y limitaciones del mismo.

El administrador desde la aplicación web puede gestionar los estacionamientos registrados en la red, dar seguimiento a las quejas y sugerencias que los usuarios aporten y llevarlos a cabo.

La [seguridad](http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml) en la web es un [proceso](http://www.monografias.com/trabajos14/administ-procesos/administ-procesos.shtml#PROCE) o [acción](http://www.monografias.com/trabajos35/categoria-accion/categoria-accion.shtml) para prevenir el uso desautorizado de su [computadora](http://www.monografias.com/trabajos15/computadoras/computadoras.shtml) y no sufrir invasión a la privacidad teniendo en cuenta los peligros que los usuarios pueden tener si no están bien informados.

La seguridad en la web es una característica prominente de la red asegurando [responsabilidad](http://www.monografias.com/trabajos33/responsabilidad/responsabilidad.shtml) ,confidencialidad , integridad y sobretodo protección contra muchas amenazas externas e internas tales como [problemas](http://www.monografias.com/trabajos15/calidad-serv/calidad-serv.shtml#PLANT) basados en email de la

seguridad de red ,[virus](http://www.monografias.com/trabajos5/virus/virus.shtml), [spam](http://www.monografias.com/trabajos28/nueva-modalidad-spam/nueva-modalidad-spam.shtml), los gusanos ,los troyanos e intentos de ataques de seguridad , etc. La [información](http://www.monografias.com/trabajos7/sisinf/sisinf.shtml) sobre los diversos tipos de prevención debe de estar actualizados de acuerdo para garantizar su funcionamiento.

El no tener una buena seguridad en la red implica que un [hacker](http://www.monografias.com/trabajos/hackers/hackers.shtml) pueda acceder fácilmente a la red interna .Esto habilitaría a un atacante sofisticado, leer y posiblemente filtrar correo y [documentos](http://www.monografias.com/trabajos14/comer/comer.shtml) confidenciales; equipos [basura](http://www.monografias.com/trabajos11/recibas/recibas.shtml), generando información; y más. Por no mencionar que entonces utilice su red y [recursos](http://www.monografias.com/trabajos4/refrec/refrec.shtml) para volverse e iniciar el ataque a otros sitios, que cuando sean descubiertos le apuntarán a usted y a su [empresa](http://www.monografias.com/trabajos11/empre/empre.shtml), no al hacker. Debemos tener en cuenta que tampoco es muy fiable conformarse con un [antivirus](http://www.monografias.com/trabajos12/virus/virus.shtml) ya que a no son capaces de detectar todas las amenazas e infecciones al [sistema](http://www.monografias.com/trabajos11/teosis/teosis.shtml) además son vulnerables desbordamientos de búfer que hacen que la seguridad del sistema operativo se vea más afectada aún, A veces los [métodos](http://www.monografias.com/trabajos11/metods/metods.shtml) mas óptimos para la seguridad de [redes](http://www.monografias.com/Computacion/Redes/) son muy incómodos ya que dejan a los usuarios sin muchos permisos.

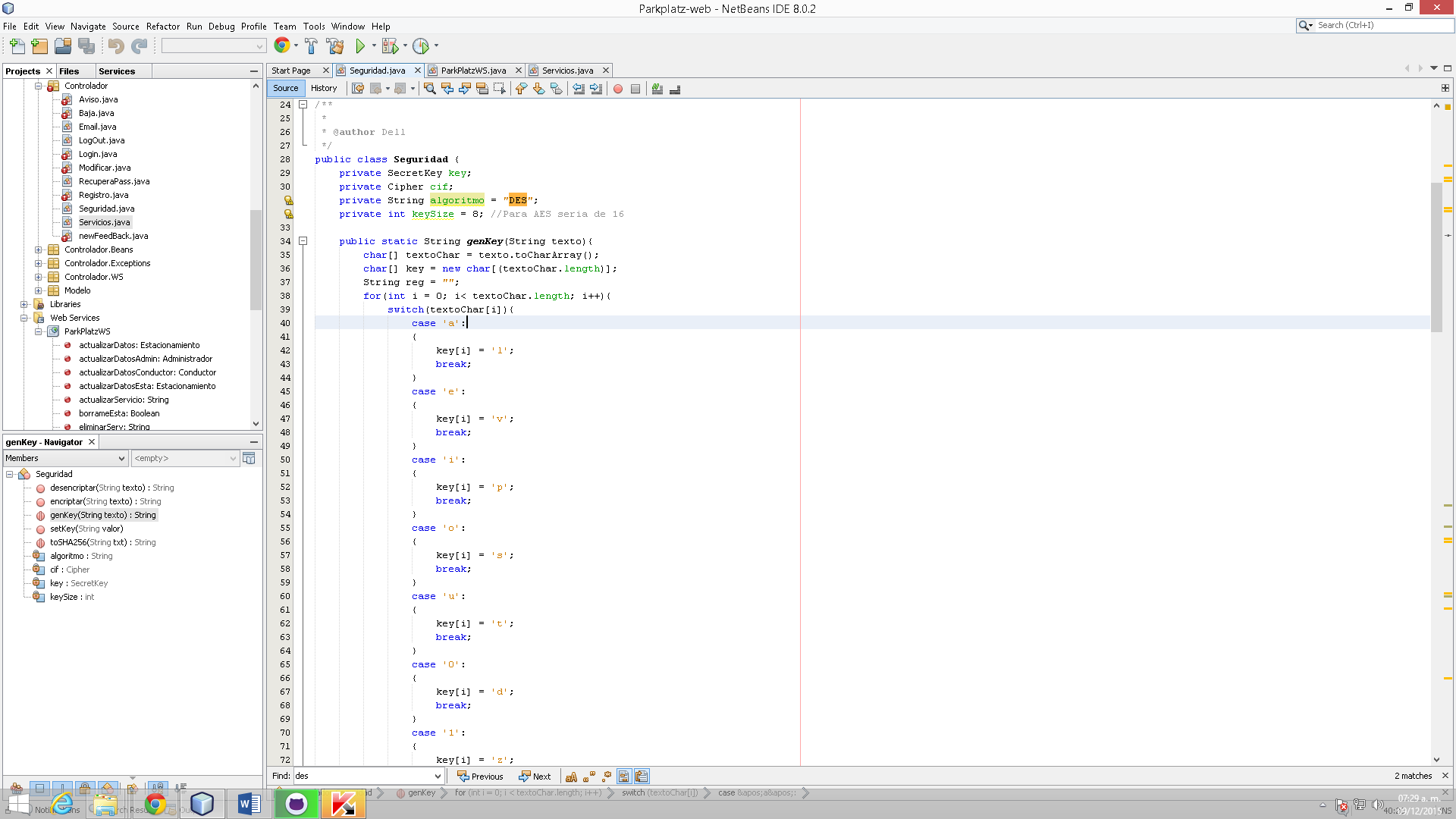
Debido a que internet es parte vital del proyecto, Parkplatz ofrece servicios online, la gestión de riesgos que pueden afectar al sistema es un aspecto muy importante para el buen funcionamiento del sistema. Sin necesidad de usar muchos tecnicismos los ataques están presentes en cualquier sistema informático. La importancia de la seguridad en Parkplatz es básicamente el mantener la privacidad de los datos ingresados de los usuarios para que no caigan en malas manos y puedan realizar actos perjudiciales hacia los usuarios de la plataforma o a la misma. El sistema busca también garantizar la integridad y la navegación segura sin ningún tipo de riesgo

Para nuestro proyecto ocupamos algoritmo de cifrado Des, Sha-256 y un algoritmo propio basado en Cesar.

El cifrado Des trata de un sistema de cifrado simétrico por bloques de 64 bits, de los que [8 bits](http://es.ccm.net/contents/base/binaire.php3) (un byte) se utilizan como control de paridad (para la verificación de la integridad de la clave). Cada uno de los bits de la clave de paridad (1 cada 8 bits) se utiliza para controlar uno de los bytes de la clave por paridad impar, es decir, que cada uno de los bits de paridad se ajusta para que tenga un número impar de "1" dentro del byte al que pertenece. Por lo tanto, la clave tiene una longitud "útil" de 56 bits, es decir, realmente sólo se utilizan 56 bits en el algoritmo.

Las partes principales del algoritmo son las siguientes:

* fraccionamiento del texto en bloques de 64 bits (8 bytes),
* permutación inicial de los bloques,
* partición de los bloques en dos partes: izquierda y derecha, denominadas *I* y *D* respectivamente,
* fases de permutación y de sustitución repetidas 16 veces (denominadas rondas),
* reconexión de las partes izquierda y derecha, seguida de la permutación inicial inversa.



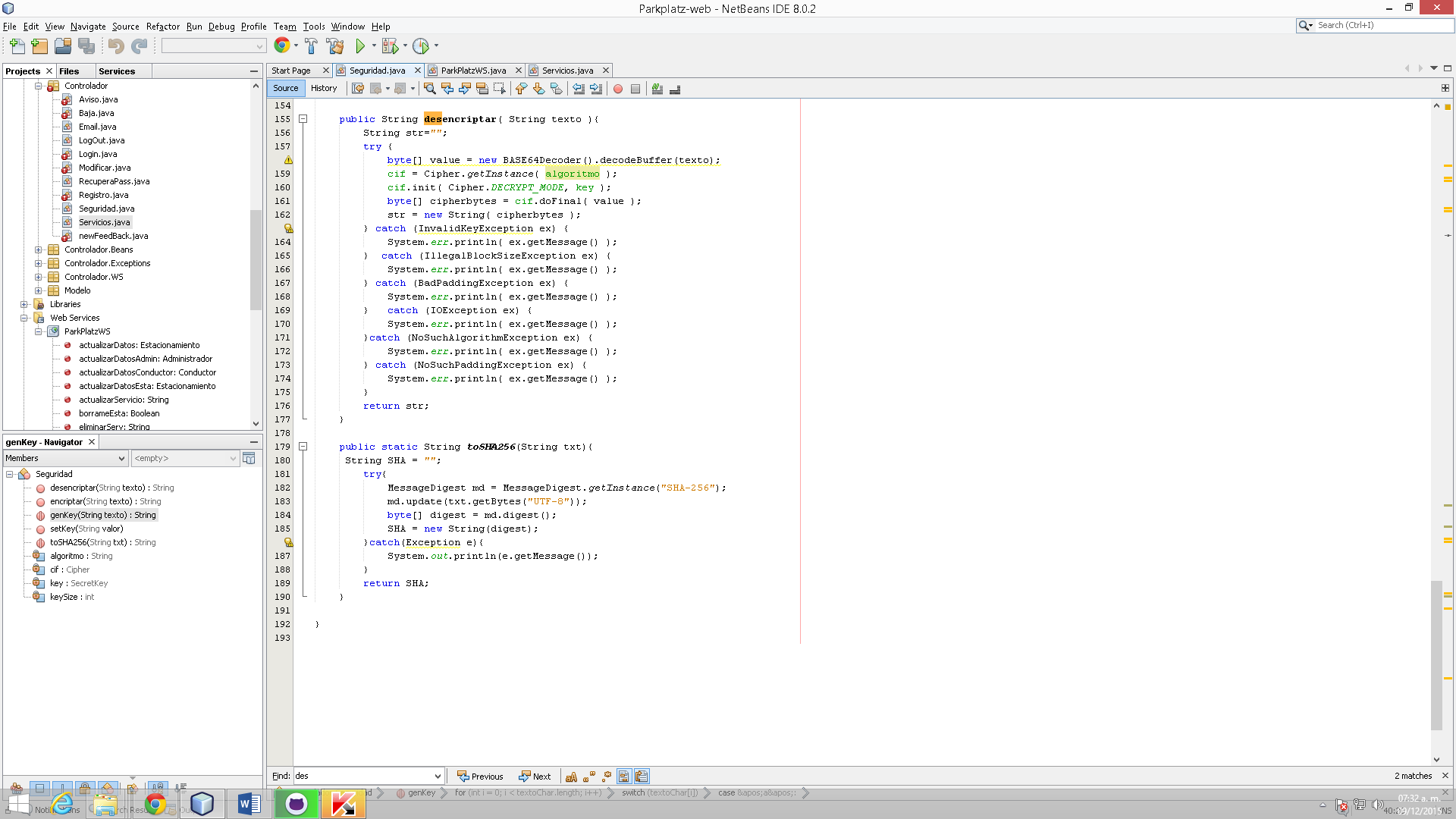
Una función hash es método para generar claves o llaves que representen de manera casi unívoca a un documento o conjunto de datos. Es una operación matemática que se realiza sobre este conjunto de datos de cualquier longitud, y su salida es una huella digital, de tamaño fijo e independiente de la dimensión del documento original. El contenido es ilegible.

Es posible que existan huellas digitales iguales para objetos diferentes, porque una función hash.

A partir de un hash o huella digital, no podemos recuperar el conjunto de datos originales. Cifrar una huella digital se conoce como firma digital.

Requisitos que deben cumplir las funciones hash:

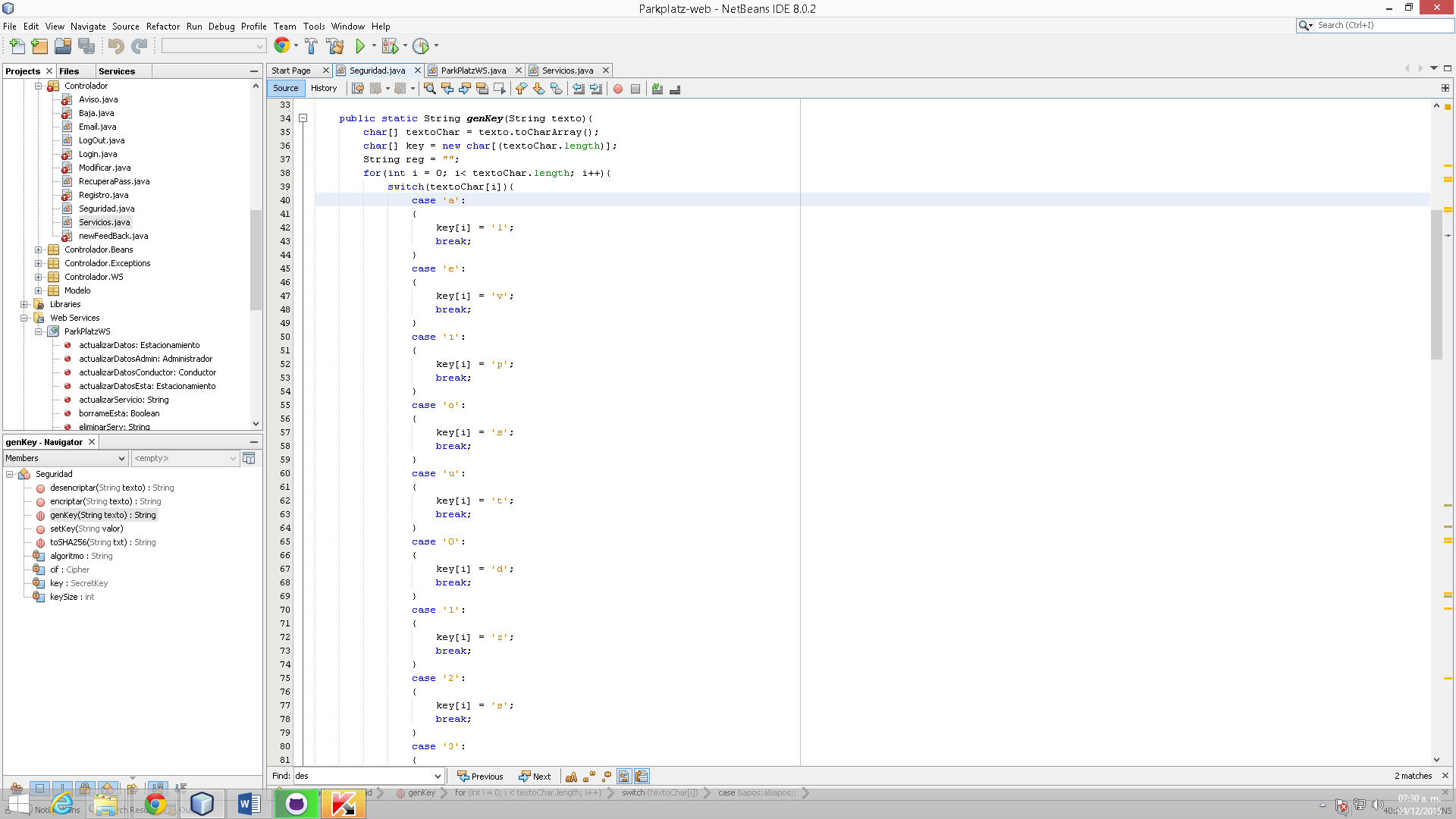
– Imposibilidad de obtener el texto original a partir de la huella digital.  
– Imposibilidad de encontrar un conjunto de datos diferentes que tengan la misma huella digital (aunque como hemos visto anteriormente es posible que este requisito no se cumpla).  
– Poder transformar un texto de longitud variable en una huella de tamaño fijo.  
– Facilidad de empleo e implementación.

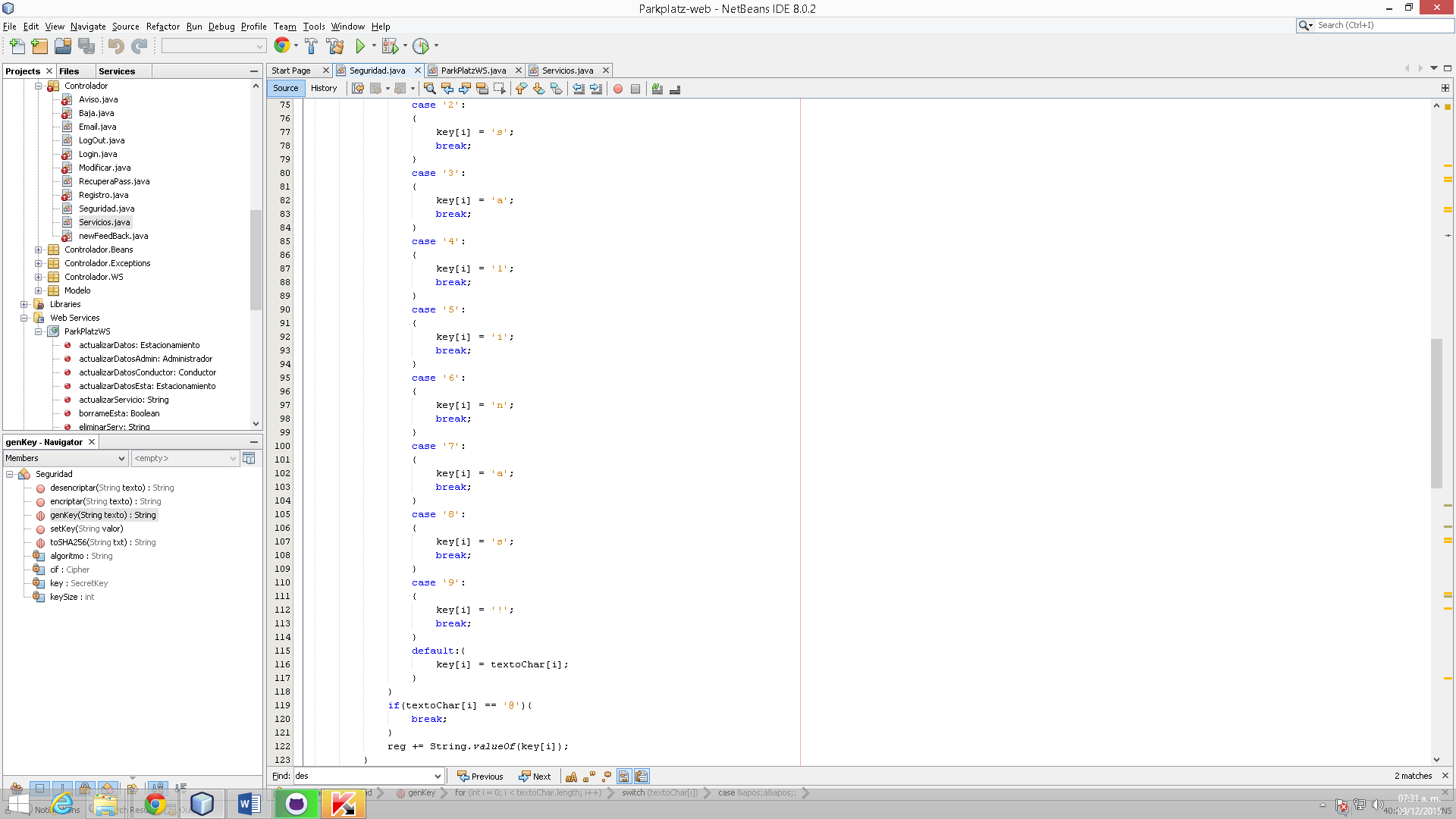


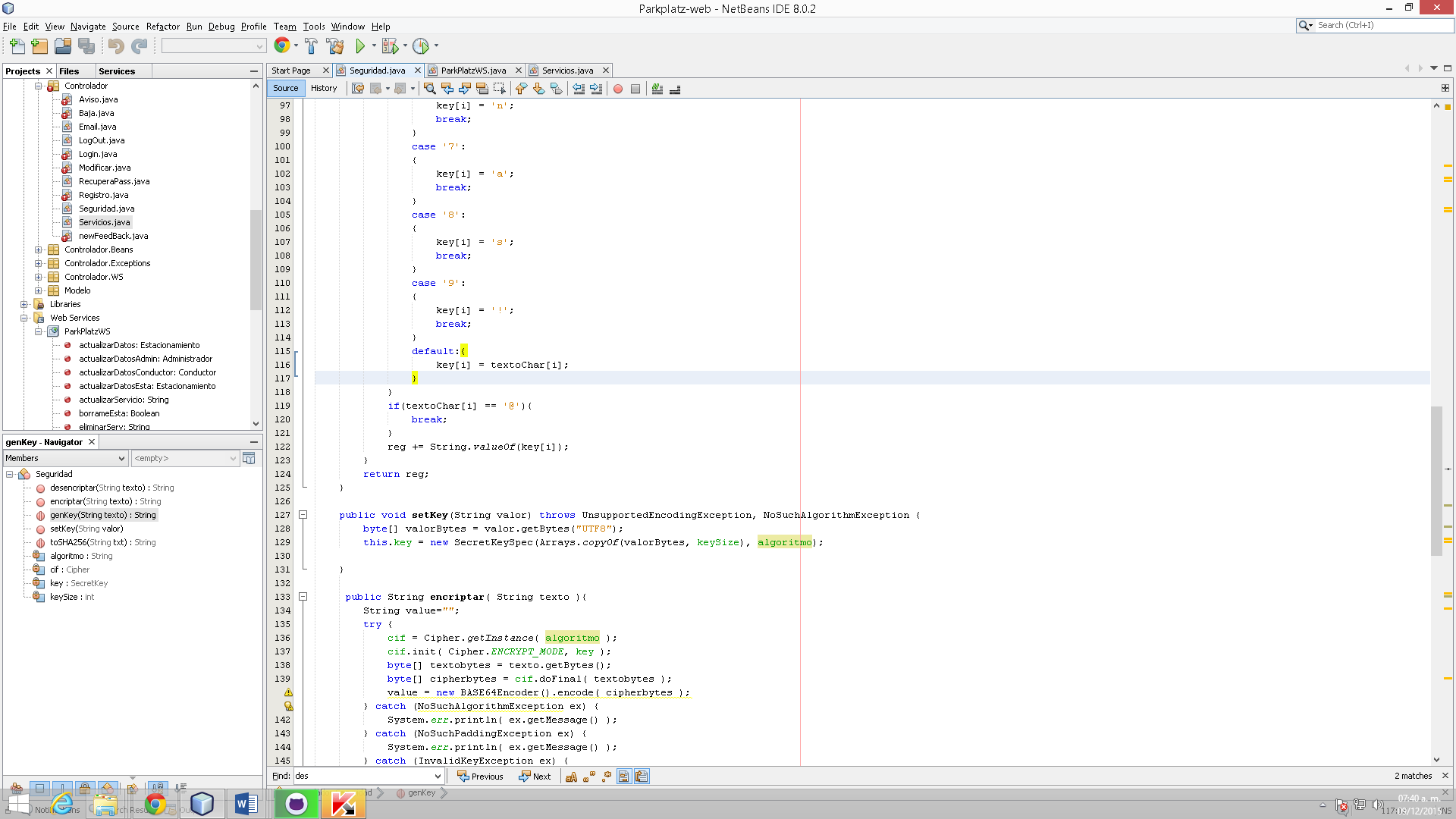
El cifrado César es uno de los primeros métodos de cifrado conocidos históricamente. Julio César lo usó para enviar órdenes a sus generales en los campos de batalla. Consistía en escribir el mensaje con un alfabeto que estaba formado por las letras del alfabeto latino normal desplazadas tres posiciones a la derecha.

El receptor del mensaje conocía la clave secreta de éste (es decir, que estaba escrito con un alfabeto desplazado tres posiciones a la derecha), y podía descifrarlo fácilmente haciendo el desplazamiento inverso con cada letra del mensaje. Pero para el resto de la gente que pudiese accidentalmente llegar a ver el mensaje, el texto carecía de ningún sentido.

Aparentemente es un cifrado muy débil y poco seguro, pero en la época de Julio César no era de conocimiento general la idea de ocultar el significado de un texto mediante cifrado. De hecho, que un mensaje estuviese por escrito ya era un modo de asegurar la confidencialidad frente a la mayoría de la población analfabeta de la época.







En nuestro proyecto el algoritmo de cifrado Des utiliza como llave privada el correo electrónico del usuario y con esa llave cifra la contraseña.

Para la autentificación del URL para la recuperación de la contraseña cifrada guardada en la base de datos y a esa cadena resultante se le aplica un hash y un sha256.

Para generar las llaves nuestro equipo de desarrolladores diseño un algoritmo basado en cifrado cesar y así generar las llaves.

**Glosario**

**Amenaza**  
Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

**Amenazas polimorfas**  
Las amenazas polimorfas son aquellas que tienen la capacidad de mutar y en las cuales cada instancia del malware es ligeramente diferente al anterior a este. Los cambios automatizados en el código realizados a cada instancia no alteran la funcionalidad del malware, sino que prácticamente inutilizan las tecnologías tradicionales de detección antivirus contra estos ataques.

**Aplicaciones engañosas**  
Las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.

**Ataques Web**  
Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

**Blacklisting o Lista Negra**  
La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

**Bot**  
Un bot es una computadora individual infectada con malware, la cual forma parte de una red de bots.

**Encriptación**  
La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.

**Exploits o Programas intrusos**  
Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

**Filtración de datos**  
Una filtración de datos sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados

**Vulnerabilidad**  
Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

* Permitir que un atacante ejecute comandos como otro usuario
* Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
* Permitir a un atacante hacerse pasar por otra entidad
* Permitir a un atacante realizar una negación de servicio

**Encriptación**

 La codificación la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red.

**Referencias**

http://www.seguridad.unam.mx/documento/?id=17

Hacking y seguridad de páginas web

Antonio Ramos Varon, Ra-Ma, 2015

Editorial: RA-MA

**Conclusiones:**

Debido al crecimiento exponencial del Internet en el mundo, es muy importante proteger la información de los usuarios de ataques informáticos, afortunadamente para realizar esta difícil tarea contamos con muchas herramientas para proteger la información como la encriptación la cual es la principal herramienta usada para resguardar la información desde la época de los romanos.

En el curso de Seguridad Web aprendimos cómo funciona la encriptación desde su forma más básica hasta cómo funcionan los algoritmos matemáticos de cifrado más complejos y poder aplicarlos, en nuestro, caso para poder mantener la integridad y confidencialidad de los datos de nuestros usuarios y evitar ataques hacia ellos. Es por esto, que el tomar las medidas de seguridad necesarias para resguardar la integridad de los datos que se manejan en ella, se convierten en un tema primordial de todo usuario.