UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CARRERA DE SISTEMAS INFORMATICOS

"ESTUDIO SOBRE LA IMPLEMENTACIÓN DE ENCRIPTACIÓN MD5 EN SITIOS WEB DURANTE EL FLUJO Y ALMACENAMIENTO DE CONTRASEÑAS"

Estudiante

Juan Gabriel Heredia Torres

Tutor

Ing. Marco Lituma Orellana

Cuenca – Ecuador

Noviembre 2011

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Ing. Marco Lituma Orellana

Director de Tesis

CERTIFICA:

Que el presente trabajo de investigación “Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas”, realizado por el Sr. Juan Gabriel Heredia Torres, egresado de la Facultad de Sistemas Informáticos, se ajusta a los requerimientos técnico-metodológicos y legales establecidos por la Universidad Tecnológica Israel, por lo que se autoriza su presentación.

Cuenca, 7 de Noviembre de 2011

_____

Ing. Marco Lituma Orellana

DIRECTOR DE TESIS

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

ACTA DE CESIÓN DE DERECHOS

Yo, JUAN GABRIEL HEREDIA TORRES, declaro conocer y aceptar la disposición de la Normativa de la Universidad Tecnológica Israel que en su parte pertinente textualmente dice: “Forma parte del Patrimonio de la Universidad la propiedad intelectual de las investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

Cuenca, 7 de Noviembre de 2011

_____

Juan Gabriel Heredia Torres.

C.I: 010533752-1

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE AUTORÍA

Los contenidos, argumentos, exposiciones, conclusiones son de Responsabilidad del autor. El documento de Tesis con título “Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas”, ha sido desarrollado por Juan Heredia Torres, persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de este Trabajo sin previa autorización.

_____

Juan Gabriel Heredia Torres.

C.I: 010533752-1

DEDICATORIA

Este trabajo está dedicado a mi gran Dios que guía e ilumina mi vida, a mi familia en especial a mi madre que con esfuerzo, sacrificio, amor y dedicación, me ha apoyado día a día para que este trabajo llegue a su feliz término. También dedico a mis maestros y compañeros que compartieron todos estos años su gran experiencia de vida.

AGRADECIMIENTO

A Dios, y a todas las personas que en forma desinteresada contribuyeron para que se pueda realizar el análisis, desarrollo y aplicación de este proyecto.

Al docente tutor: el Ing. Marco Lituma, por compartir sus conocimientos y a los Profesores de la Universidad Israel quienes me brindaron sus conocimientos, amistad y apoyo durante mi proceso académico.

RESUMEN

La seguridad en el internet es una constante que se ha dado durante el progreso de los años y la expansión de la misma, esto con el fin de frenar los constantes ataques que sufren los Portales o Sitios Web, por motivos de robo de información o bien por simple diversión de algunos delincuentes informáticos.

En la actualidad se sabe que hay personas con gran talento informático capaces de sobrepasar las más minuciosas seguridades que una página tenga, además de esto aquellas personas no solo usan su talento, sino que también lo compensan con poderosas herramientas informáticas que trabajan a nivel de la Red de Computadoras, por este motivo se debe conocer cuáles son los peligros y por supuesto como remediarlos e incluso evitarlos.

Una página que brinde servicios, debe también brindar seguridades para que nuestros clientes on-line se sientan a gusto y tengan confianza de visitarnos en nuestros sitios web. Por tal motivo hay que conocer y tener una idea real de las seguridades que se pueden dar a un sitio, desde copias de seguridad hasta procesos de Cifrado o Encriptación de información, realizando con esto un complemento ideal para luchar contra los delitos informáticos.

SUMARY

The Internet Safety is a constant that has been given during the years progress and expansion of it, this in order to stop the constant attacks faced by portals or websites, for reasons of data theft or just for fun of some cybercriminals.

Today we know that there are people with great talent computer able to overcome the most minute any assurance that a page has, in addition to this people not only use their talents, but also powerful tools compensated by working at the level of Computer Network, which is why you must know what are the dangers and of course as a remedy or even avoided.

A page that provides services, you must also provide security for our online customers feel comfortable and have confidence to visit us at our websites. For this reason there is to know and have a real idea of the assurances can be given to site from backups to process data encryption or encryption, making it an ideal complement to the fight against cybercrime.

TABLA DE CONTENIDOS

LISTA DE ANEXOS

LISTA DE CUADROS Y GRAFICOS

CAPITULO I

1. INTRODUCCIÓN

1.1 Planteamiento del Problema

1.1.1 Antecedentes

Desde los inicios de la era de la Información y el manejo de datos, siempre se tomaba en cuenta el uso de hardware para manejar las seguridades y conservar la integridad de los mismos, pero con el avance de la tecnología y sobre todo del software de redes, este tipo de seguridades físicas empezaron a convertirse en obsoletas, principalmente por que no garantizaban seguridad en cuanto a los ataques de software a través de internet o incluso dentro de un mismo establecimiento donde resida un sistema de información.

Imagen 1: Informática y Seguridad

Por la poca garantía que brindaba el hardware, también se empezó a desarrollar e ingeniar formas de contrarrestar estos ataques y protegerse de los mismos, una de las maneras de cómo protegerse de intrusos era el uso de Firewalls, pero incluso estos también pueden ser vulnerados, de tal manera las seguridades debían mejorar e ir más allá, e implantarse nuevas formas de prevenir y proteger la seguridad de los datos en un sistema.

Una manera de cuidar datos importantes, fue la implementación de la Encriptación o Cifrado de Datos, que consistía en ocultar el mensaje original con una serie de caracteres para no revelar el verdadero mensaje a un posible intruso. Si bien esto ya se utilizó en sistemas locales de empresas que manejaban información, apareció la gran dificultad con el uso de internet, pero sobre todo en los Sitios Web que manejaban información de Usuarios y demás datos importantes confidenciales que podían ser vistos pues esta red es de libre tráfico para cualquier persona.

Imagen 2: Encriptación y Protección de Datos

Este término de Encriptación está basado dentro de lo que es Criptografía, una ciencia que ya se daba desde épocas muy remotas en las que el hombre usaba símbolos para comunicarse. Desde la época de los 70, las operaciones militares y otras ramas computacionales empezaron a llevarla al término informático para la protección de información. En nuestros días la encriptación se ha dividido en varios tipos como lo son las la Encriptación de claves Simétricas y Asimétricas, destinada principalmente para preservar la Integridad de los datos de un Sistema.

Una de los métodos más usados en lo que es la Encriptación de información, es el MD5, conocido como un algoritmo de reducción criptográficos diseñados por el profesor Ronald Rivest del MIT (*Massachusetts Institute of Technology*, Instituto Tecnológico de Massachusetts). Fue desarrollado en 1991 como reemplazo del algoritmo MD4 después de que Hans Dobbertin descubriese su debilidad.

En la Actualidad para la protección de los datos que pueden ser expuestos y copiados por intrusos en la web, se está usando varios tipos de seguridades como sesiones, Firmas Digitales, Anti-spam, pero sobre todo el uso de encriptación para lo que son las contraseñas y códigos de gran valor que pueden representar pérdida de información.

Muchas Páginas web o Sistemas que funcionen en Internet están usando este tipo de seguridad para cuidar claves y demás datos importantes, debido al poderoso proceso que realiza ocultando la clave original para que no pueda ser usada más que por la misma persona que la creo. Esto representa un incremento a la seguridad y fiabilidad de los procesos que en estos sitios a través del internet se realizan.

Imagen 3: Seguridad en la Red con Encriptación

1.2 Sistematización

1.2.1 Diagnóstico

1.2.1.1 Causas – Efectos

a) Causas

Los procesos de flujo de información en los Sitios Web que al igual que los sistemas locales en empresas, tienen similar funcionamiento, pero la preocupación sobre seguridad se da en mayor grado en Sitios que funcionan a través de internet, debido al robo de información por causa de hackers, y al no estar preparados para proteger los datos, la integridad de los sitios se pone en riesgo.

Entre las causas que ocasionan inseguridad en los Sitios Web tenemos:

- ✓ Robo de Claves de acceso en los Sistemas a través de Loggers.
- ✓ Claves registradas poco seguras por parte de los Usuarios.
- ✓ Debilidades en el uso de Sesiones para la Navegabilidad de los Usuarios.
- ✓ Puertos abiertos en los Servidores de Información del Sistema.
- ✓ Poca protección contra Sniffers.

b) Efectos

- ✓ **Robo de Claves de acceso en los Sistemas a través de Loggers**

  Las Claves o datos Importantes pueden ser grabados y usados para realizar actividades maliciosas, principalmente los causantes de esto son usuarios especializados en hackeo.

- ✓ **Claves registradas poco seguras por parte de los Usuarios**

  Las Claves pueden ser violentadas o burladas con fuerza bruta por usuarios con alto grado de conocimiento informático.

- ✓ **Debilidades en el uso de Sesiones para la Navegabilidad de los Usuarios.**

  La seguridad normal del Sitio puede ser vulnerada por delincuentes informáticos, ocasionando facilidad para la posible destrucción del sitio en casos extremos.

- ✓ **Puertos abiertos en los Servidores de Información del Sistema.**

  Libre acceso al sistema para cualquier usuario con alto conocimiento en redes informáticas.

- ✓ **Poca protección contra Sniffers**

  La Información puede ser monitoreada y robada durante su flujo de almacenamiento en la Red.

1.2.1.2 Pronóstico y Control de Pronóstico

Sabiendo estas dificultades y teniendo una idea de lo que implica esto en la seguridad de los datos, se sabe que si no se corrigen a tiempo, podrían tener consecuencias graves en relación a nuestros datos.

Entre estas consecuencias futuras que se pueden dar podemos mencionar algunas:

- ✓ Robo de Información Importante de Usuarios
- ✓ Suplantación de Identidad
- ✓ Infiltración maliciosa para causar daños en el Sistema (Eliminación de Datos Importantes)

- ✓ Extorción por parte de Usuarios Maliciosos
- ✓ Cuando se trata de Empresas se puede dar el robo de sus Bases de Datos a través de la Entrada Ilegal al Sistema
- ✓ Daños Graves en las Cuentas de los Usuarios

Para estas necesidades se propone usar el método de Cifrado o Encriptación de datos, lo cual ayudaría a salvaguardar el uso ilegal de algunos datos de suma importancia, pero no ayudaría a mejorar toda la seguridad, ya que el proceso de seguridad está basado en un conjunto de métodos relacionados entre sí.

Entre las ventajas que se tienen al usar la Encriptación tenemos:

- ✓ Los Datos encriptados no pueden ser usados si es que son robados de una BD, debido a que la única forma de manipular aquellos datos es usando la clave original.
- ✓ La Encriptación Ofrece seguridad durante el proceso de Flujo de Datos en el Sitio Web
- ✓ Ayuda a que solo el usuario que registro el dato encriptado pueda manipularlo
- ✓ Si el Sistema es vulnerado, los datos encriptados no ofrecen ningún tipo de información ya que solo aparece en caracteres especiales, y esto puede despistar al infiltrado.

1.3 Objetivos

1.3.1 Objetivo General

Estudiar y Presentar la herramienta de Encriptación como una opción válida para que ayude a mejorar la seguridad en un Sitio Web y salvaguarde datos importantes.

1.3.2 Objetivos Específicos

- Estudio del Algoritmo MD5 como Método de Encriptación.
- Estudiar dos Tipos de Encriptación e implementar uno de ellos.
- Desarrollar un cuadro comparativo técnico de los tipos de encriptación estudiados.
- Demostrar prácticamente en un Sitio Web que este método de seguridad es sustentable para el uso en empresas e instituciones en base a los resultados del estudio que se plantea.
- Determinar el Uso correcto de la Encriptación para tomarlo como método de seguridad en los Sitios Web.
- Difundir este Tipo de Seguridad para mejorar el flujo y almacenamiento de datos en un Sitio Web.
- Recomendación para el uso y forma de implementación de la herramienta de Encriptación MD5.

1.4 Justificación

1.4.1 Justificación Teórica

La seguridad ante todo, es lo que se debe tener en cuenta al momento de intentar brindar un servicio a través de internet, por la razón del avance de herramientas de software espía y el hackeo de sistemas simplemente por diversión o por intereses económicos de algunas personas.

La construcción de un Sitio Web implica más que tener un conjunto de páginas asociadas, está derivado en cuál es el servicio que se quiere dar a los usuarios y como se garantizará su satisfacción.

La Seguridad Informática contempla estándares y protocolos a seguir para brindar seguridad e integridad a los datos en un sistema. Estos estándares se aplican de acuerdo al sistema que se quiere desarrollar o mantener.

Los Sitios Web cumplen la función de brindar servicio interactivo a los Usuarios, pero al momento de brindar seguridad usan muchos de estos estándares de Seguridad Informática, como por ejemplo los respaldos de información y métodos de protección de datos. Sin lugar a dudas estos métodos ayudan a que los usuarios tengan mayor confiabilidad sobre los procesos en el sitio y que el sitio cuide mejor de sus datos.

Uno de los Métodos de Seguridad en los Sitios Web que actualmente se aplican es el uso del Cifrado o Encriptación de Datos, generalmente empleado para la protección de contraseñas, Claves de Tarjetas de crédito, etc., esto realizado durante el flujo y almacenamiento de datos.

“Etimológicamente criptografía (…), es la técnica utilizada para transformar un mensaje de texto claro a otro, llamado criptograma, que solo puedan leer las personas autorizadas. El método empleado para realizar los criptogramas se llama algoritmo de encriptación” (Enrique Quero Catalinas, 2007)

De acuerdo a esta cita mencionada anteriormente, este tipo de seguridad de protección de datos y mensajes, se puede complementar con cualquier otra

herramienta de seguridad informática existente en un sitio web. Representando esto un mayor aporte a la protección de la información que se mantenga en flujo y proceso de almacenamiento.

1.4.2 Justificación Metodológica

Para la elaboración de este proyecto se pondrá en uso las herramientas aprendidas para la recolección de datos y análisis de los mismos.

La investigación se fundamentará en:

- La investigación teórica a través de Libros de Seguridades Informáticas, Blogs, Páginas Web de Información Académica y Video Tutoriales.
- La Recolección de Datos a través de la Encuesta, que permitirá conocer de acuerdo al Análisis posterior, cuál es el estado en cuanto a seguridad, que las empresas tienen en sus sitios web.

Además de esto, el trabajo se complementará con los conocimientos durante el proceso educativo sobre seguridades en el área informática, tales como:

- Seguridad Informática
- Sitios Web
- Protección de Bases de Datos
- Redes
- Herramientas de Espionaje en Red
- Métodos de protección de datos en la Red (Encriptación)

Lo que se pretende es dar una solución a grandes dificultades que muchas instituciones desarrolladas o por desarrollarse atraviesan durante las decisiones de cómo proteger la información que estas tienen, ya sean en servidores locales o sitios web que trabajen con servidores contratados.

Está solución está enfocada a la protección de datos importantes y al conocimiento real de lo invaluable que es proteger con varios filtros de seguridad aquellos datos que representan un beneficio para una institución y de igual forma un peligro si estos llegará a caer en manos equivocadas.

1.4.3 Justificación Práctica

El trabajo en su culminación estará enfocado a cumplir con los objetivos planteados, los cuales han sido detallados anteriormente, destacando el entendimiento del uso y la ventaja de incorporarlo como medida de seguridad en los sistemas de información.

Estará aplicado el uso de esta herramienta en los Sitios Web como medida de seguridad para proteger datos de alto riesgo.

En cuanto a la demostración práctica del tema propuesto, se usará un Sitio Web realizado en Visual Studio .NET, ya que de acuerdo a la experiencia obtenida durante el proceso académico en lo que se refiere a desarrollo web, se la ha tomado para realizar un ejemplo demostrativo del uso y la factibilidad de la herramienta de Encriptación.

Además de esta herramienta de desarrollo web, también es viable usar Este tipo de Encriptación en sitios Web hechos en PHP debido a que este tipo de lenguaje ya tiene incorporado en su programación lo que es el Método de cifrado MD5.

1.5 Alcance y Limitaciones

1.5.1 Alcance

El Proyecto que se pretende realizar, permitirá conocer a los Administradores de Sistemas y Desarrolladores de Software, un poco más acerca de la Encriptación y la utilidad que se le puede dar con relación a la Seguridad Informática.

El Trabajo a desarrollar contendrá lo siguiente:

- ✓ Información acerca de la Encriptación de Datos
- ✓ Tipos de Encriptación y su utilidad
- ✓ Función Hash y Algoritmos de Encriptación
- ✓ Ejemplo del Proceso de Encriptación
- ✓ Sugerencias de la Forma de empleo de la Encriptación como medida de seguridad

De acuerdo con esto se informará al usuario acerca de esta herramienta y la utilidad que se puede dar a la misma, quedando abierto su posterior desarrollo y mejora en un Sistema de información.

1.5.2 Limitaciones

El estudio y la realización del Proyecto se limitará a:

- ✓ Solo el Estudio del Algoritmo MD5 como método de Encriptación.
- ✓ Implementar el Algoritmo en un Sitio Web desarrollado para demostrar su funcionamiento.
- ✓ El uso de un módulo de registros de un Sitio Web para el Algoritmo
- ✓ No se desarrollará Software sobre el Algoritmo.

Según estas limitaciones el proyecto se orientará únicamente a dar conocimiento sobre el uso y aplicación de la herramienta de encriptación como medida de seguridad en sitios web y sistemas locales.

1.6 Estudios de Factibilidad

1.6.1 Factibilidad Técnica

Para el Desarrollo del Proyecto, Demostración e Implementación se tomará en cuenta lo siguiente:

- Área de Desarrollo
    - ✓ Software de Programación, que permita desarrollar aplicaciones transaccionales, como por ejemplo Visual Studio, PHP, etc.
    - ✓ Base de Datos, que contendrá los registros de la Aplicación que se desarrolle,
    - ✓ Servidor que contendrá la Aplicación Web o el Sistema de Datos, para esto cada persona de acuerdo al tipo de Aplicación que desee implementar, deberá estudiar las ventajas y desventajas que cada proveedor ofrece desde lo que es el precio hasta las capacidades de software y hardware.

Según estos requerimientos, si se los tiene, el proyecto podrá ser desarrollado e implementado por cualquier persona que quiera hacer uso de la Encriptación como medida de seguridad para la protección de información.

1.6.2 Factibilidad Operativa

En la Factibilidad Operativa se contempla lo siguiente:

- ✓ El Trabajo en su culminación permitirá ayudar a mejorar la Seguridad informática en un Sistema de información, convirtiéndose en un complemento más al conjunto de procesos que la seguridad informática contempla para la protección de los datos.

- ✓ La utilización de la Herramienta no afectará al proceso de trabajo de un sistema ya que el cifrado se lo realizará internamente en las transacciones de datos, por lo tanto no abra resistencia al cambio por parte de los Usuarios.

- ✓ La Culminación del trabajo, permitirá ayudar a conocer al usuario acerca de la herramienta de encriptación, y la aplicabilidad que esta tiene en los Sitios Web que manejen información.

CAPITULO II

2. MARCO DE REFERENCIA

2.1 Marco Teórico

2.1.1 Seguridad Informática

2.1.1.1 Introducción

Imagen 4: Seguridad informática

Cuando hablamos de Seguridad Informática hacemos referencia a la protección de nuestra Información a través de medios Informáticos, divididos entre Hardware y Software que complementados son una excelente defensa contra delitos informáticos.

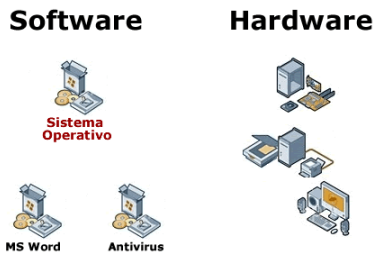


Imagen 5: Seguridad Informática Software – Hardware

“La Seguridad Informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y fiable”. (Asensio, 2006)

A través de estos dos complementos, se centra lo que es la Creación de Seguridad Informática pero para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

La Creación de la Seguridad Informática se basa principalmente en el estudio de los peligros que puedan afectar el desempeño de nuestros sistemas, ya sean Sistemas Locales o Sistemas Web (Sitios Web), según esto siempre se buscará forma de Remediarlos o Prevenirlos con algún tipo de acción planificada.

Las amenazas están estrechamente ligadas a la seguridad debido a que de acuerdo a los estudios de los peligros se implantan la seguridad necesaria para evitar o contrarrestarlas.

2.1.1.2 Las Amenazas

- **Amenazas internas:** Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:
  - ✓ Los usuarios conocen la red y saben cómo es su funcionamiento.
  - ✓ Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.

- ✓ Los IPS y Firewalls son mecanismos no efectivos en amenazas internas.

- **Amenazas externas:** Son aquellas amenazas que se originan de afuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

2.1.1.3 Seguridad Física

Es uno de los aspectos más olvidados a la hora del diseño de un sistema informático.

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

- **Las principales amenazas que se prevén en la seguridad física son:**

- ✓ Desastres naturales, incendios accidentales tormentas e inundaciones.
- ✓ Amenazas ocasionadas por el hombre.
- ✓ Disturbios, sabotajes internos y externos deliberados.

Evaluar y controlar permanentemente la seguridad física del edificio es la base para o comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

- **Tener controlado el ambiente y acceso físico permite:**

✓ Disminuir siniestros

✓ Trabajar mejor manteniendo la sensación de seguridad

✓ Descartar falsas hipótesis si se produjeran incidentes

✓ Tener los medios para luchar contra accidentes

2.1.1.4 Seguridad Lógica

Una vez que se haya planteado la estructura de nuestra Seguridad Física podemos complementar con seguridad Lógica.

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

- **Las recomendaciones que se plantean para crear Seguridad Lógica son:**

✓ Restringir el acceso a los programas y archivos

✓ Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

✓ Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.

✓ Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.

✓ Que la información recibida sea la misma que ha sido transmitida.

✓ Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

- ✓ Que se disponga de pasos alternativos de emergencia para la transmisión de información.

2.1.1.5 Delitos Informáticos

Cuando hablamos de delitos informáticos, hacemos referencia a aquellos delincuentes que sin contar con muchas armas físicas, usan su arma más elemental, su extraordinario conocimiento sobre los métodos Informáticos para extraer información ajena de personas e inclusive Empresas, Organizaciones, Bancos u otros lugares de importancia. El avance de la era informática ha introducido nuevos términos en el vocabulario de cada día. Una de estas palabras, hacker, tiene que ver con los delitos informáticos.

Imagen 6: Delitos Informáticos

A veces escuchamos historias acerca de desapariciones de Información en instituciones de prestigio, dinero desaparecido de Bancos o quizá transacciones financieras de personas que ni siquiera tienen idea de cómo sucedió, pero esto se apega demasiado a la realidad, en especial en el año 1997 en estados Unidos ocasionando pérdidas millonarias y en el 2000 cuando este tipo de delincuencia informática se propago a un nivel más avanzados,

refiriéndonos a las estrategias de manipulación de sistemas e incluso de personas ingenuas que han sido víctimas de este tipo de actividades ilegales.

Una forma de combatir este tipo de delitos, no es tan difícil o inimaginable como parece, es mucho más sencillo, simplemente hay que conocer los procedimientos que este tipo de delincuentes usan, como por ejemplo, saber acerca de seguridades financieras, desconfianza a personas desconocidas, y sobre todo un conocimiento mediano sobre informática. Al estar preparado y prevenido sobre estos delitos, será muy difícil que este tipo de delincuencia nos afecte.

2.1.2 Sitio Web

Es un Sitio localizado en la World Wide Web que contiene documentos denominados “Páginas Web”, organizados jerárquicamente. Los Sitios son gestionados y administrados por personas y son construidos de acuerdo a la necesidad de las personas.

Imagen 7: Sitio Web

Como medio, los Sitios Web son similares a las Películas, Televisión o Periódicos y tienen como objetivo brindar información y guiar a los Usuarios de acuerdo al contenido del sitio y los requerimientos del usuario.

La diferencia del Sitio Web con los otros medios, radica en que está configurado el Sitio para interactuar con el usuario, dándole satisfacción y comodidad.

2.1.2.1 Internet

2.1.2.1.1 Historia

Su origen se remonta a la época de 1960, dentro de ARPA (hoy DARPA), como respuesta a la necesidad de esta organización de buscar mejores maneras de usar los computadores de ese entonces.

En el mes de julio de 1961 Leonard Kleinrock publicó desde el MIT el primer documento sobre la teoría de conmutación de paquetes. Kleinrock convenció a Lawrence Roberts de la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red. El otro paso fundamental fue hacer dialogar a los ordenadores entre sí.

Para explorar este terreno, en 1965, Roberts conectó una computadora TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de computadoras de área amplia jamás construida.

2.1.2.1.2 ¿Qué es el Internet?

Al Internet se lo conoce como el conjunto de Red de Redes interconectadas a través de los protocolos TCP/IP, garantizando que las complejas redes trabajen como redes lógicas únicas.

“Internet es un concepto inseparable de los términos TCP/IP e IP. Se trata del protocolo de transmisión de Internet que regula el intercambio de datos entre ordenadores.” (Lakerbauer, 2001)

Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto.

Imagen 8: Internet

Para un funcionamiento sin problemas de una estructura tan compleja como la del internet es necesaria la identificación de unas directivas muy claras y una clara denominación de los dispositivos que se encuentran en la estructura de internet, a cada recurso de red posee un número unívoco como es la dirección IP.

La Dirección IP tiene forma *aaa.bbb.ccc.ddd* y siempre está compuesto de cuatro números, cada uno de ellos con un máximo de 3 cifras y unos valores entre 0 y 255. Un ejemplo de una dirección IP puede ser 192.198.0.1

Como estos números son difíciles de recordar y las combinaciones son múltiples, los servidores FTP y WWW disponen de un Nombre más Expresivo como por ejemplo www.microsoft.com**.**

El encargado de darle nombres a las direcciones es el Domain Name System (DNS). Los Servidores DNS, que se encuentran en internet, mantienen una constante comunicación entre ellos, con lo que una nueva asignación se hace conocida en todo el mundo al cabo de pocas horas.

Las partes de un nombre están separadas por puntos, a la izquierda se refiere al ordenador o empresa y a la derecha cuando más se avanza, mayor es el nivel de la estructura organizativa del Internet. A la derecha se encuentra lo que Se denomina “Dominio” y describe el tipo de organización o de empresa de ese servidor de red.

Los Dominios usados actualmente son:

Dominios organizativos	Significado
com	Commercial (empresas)
edu	Educational (educativo, académico)
gov	Government (gobierno)
mil	Military (militar)
net	Network (proveedor de servicios de Internet)
org	Organisation (organización sin ánimo de lucro)

Imagen 9: Dominios Organizativos

Dominios geográficos	País
au	Austria
ca	Canadá
ch	Suiza
de	Alemania
es	España
fr	Francia
uk	Reino Unido

Imagen 10: Dominios Geográficos

2.1.2.1.3 Tamaño del Internet y su vinculación a la Sociedad

El tamaño del internet se estima por su cantidad de Páginas Web y la cantidad de Usuarios que crecen continuamente, lo cual es difícil de medir por el continuo crecimiento, pero una de las maneras de hacerlo es a través de los motores de búsqueda, que almacenan en sus bases de datos los Registros de Páginas Web.

Varios estudios realizados apuntan a una cantidad que había ascendido a 63.000 millones de páginas web y para el 2016 se estima un crecimiento de usuarios de 2.000 millones.

El acceso al Internet está extendido por cualquier parte del planeta, lo que permite que la red crezca aún más y que la información sea mucho más compartida por cualquier cultura a nivel mundial. En nuestra sociedad el uso de Internet ha impactado tanto en el ámbito Laboral como en el Investigativo, debido principalmente a la disponibilidad constante que ofrece este servicio.

Si bien el internet es un servicio accesible por cualquier persona, este ya no solo se usa para consultar información, si no que para mejorar la vida del hombre, llegando a un punto en donde ya se puede realizar transacciones bancarias, monetarias y muchos otros servicios que sin duda alguna simplifican las actividades diarias del hombre en su campo laboral.

2.1.2.2 Uso de los Sitios Web

Un sitio web de calidad permite mejorar la imagen profesional, demostrando por encima de todo, el conocimiento y la aceptación de las nuevas tecnologías. Además, cada vez son más los miles de usuarios que acceden a Internet buscando información, un producto o servicio. Por eso, no tener una web supone una gran desventaja competitiva con respecto a otras empresas que sí la tienen.

El uso de un Sitio Web, se nota principalmente por la necesidad que tiene cada usuario y su clasificación va de acuerdo a los requerimientos de quien solicita algún tipo de contenido, como por ejemplo:

- ✓ **Sitios Web Blogs,** usados generalmente para exponer algún tipo de contenido.

- ✓ **Sitios de Comercio Electrónico,** para venta y compra de bienes.
- ✓ **Sitios de Comunidad Virtual,** sitios donde las personas comparten intereses similares, un ejemplo de esto son las redes sociales.
- ✓ **Sitos de Descargas,** para descargar algún tipo de contenido, como software, archivos, imágenes, etc.
- ✓ **Sitios de Juego,** generalmente usados como patio de juegos donde muchas personas usan los recursos de estas páginas para diversión.
- ✓ **Sitios Educativos,** en estas se pueden encontrar una gran cantidad de información académica o de interés educativo.
- ✓ **Sitio Portal,** conocido generalmente, un sitio web que proporciona un punto de inicio, entrada o portal, a otros recursos en Internet o una intranet

2.1.3 Encriptación como medio de Seguridad

2.1.3.1 Introducción a la Criptografía

Desde que el hombre ha necesitado comunicarse con los demás ha tenido la necesidad de que algunos de sus mensajes solo fueran conocidos por las personas a quien estaban destinados. La necesidad de poder enviar mensajes de forma que solo fueran entendidos por los destinatarios hizo que se crearan sistemas de cifrado, de forma que un mensaje después de un proceso de transformación, lo que llamamos cifrado, solo pudiera ser leído siguiendo un proceso de descifrado.

Según el Diccionario de la Real Academia, la palabra Criptografía viene del griego Kryptos, que significa oculto y gráphein, escritura, y su definición es: " Arte de escribir con clave secreta o de un modo enigmático". La Criptografía es

la técnica, bien sea aplicada al arte o la ciencia, que altera las representaciones lingüísticas de un mensaje. Es un término genérico que describe todas las técnicas que permiten cifrar mensajes o hacerlos ilegibles sin recurrir a una acción específica.

“Etimológicamente criptografía (…), es la técnica utilizada para transformar un mensaje de texto claro a otro, llamado criptograma, que solo puedan leer las personas autorizadas. El método empleado para realizar los criptogramas se llama algoritmo de encriptación”. (Enrique Quero Catalinas, 2007)

En la actualidad su utilización se enfoca en la protección de Información cuando esta viaja a través de una determinada Red o un medio de comunicación Electrónico. De acuerdo con esto muchas empresas que poseen Sitios Web o algún sistema que Trabaje a nivel de la Red, han implementado esta seguridad para proteger los datos que viajan a través de las transacciones que en los Sitios web se realizan.

Su funcionamiento básico se basa en que el emisor emite un mensaje en claro, que es tratado mediante un cifrador con la ayuda de una clave, para crear un texto cifrado. Este texto cifrado, por medio del canal de comunicación establecido, llega al descifrador que convierte el texto cifrado, apoyándose en otra clave, para obtener el texto en claro original. Las dos claves implicadas en el proceso de cifrado/descifrado pueden ser o no iguales dependiendo del sistema de cifrado utilizado.

2.1.3.2 Tipos de Encriptación

- ✓ **Encriptación mediante claves simétricas:** Son las funciones más clásicas, es decir, se utiliza una determinada clave en la transformación de la información encriptada para conseguir desencriptarla, el problema reside en la necesidad de que todas las partes conozcan la clave.

- ✓ **Encriptación mediante claves asimétricas o públicas:** Existen también sistemas asimétricos de cifrado o de clave pública, cada usuario dispone de dos claves, una pública, que debe revelar o publicar para que los demás puedan comunicarse con él, y una privada que debe mantener en secreto. Cuando un usuario desea mandar un mensaje protegido, cifra el mensaje con la clave pública del destinatario. De esta manera, sólo el destinatario puede descifrar (con su clave secreta) el mensaje cifrado (Ni si quiera el emisor del mensaje puede descifrar el mensaje cifrado por él).

- ✓ **Encriptación mediante códigos de integridad:** Se utilizan funciones matemáticas que derivan de una huella digital a partir de un cierto volumen de datos (una huella tiene de 128 a 160 bits). Es teóricamente posible encontrar dos mensajes con idéntica huella digital; pero la probabilidad es ínfima.

- ✓ **Encriptación mediante firma digital:** Dado un mensaje, basta calcular su huella digital y cifrarla con la clave secreta del remitente para obtener simultáneamente la seguridad de que el contenido no se manipula (integridad), y de que el firmante es quien dice ser (autenticación). Las firmas digitales suelen ir asociadas a una fecha. La fecha de emisión (y posiblemente la fecha de vencimiento de validez) suelen proporcionarse en texto claro, e incorporarse al cálculo de la huella digital, para ligarlas irrenunciablemente.

2.1.3.3 Funciones Hash

Es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor (un subconjunto de los números naturales por ejemplo). Varían en los conjuntos de partida y de llegada y en cómo afectan a la salida similitudes o patrones de la entrada. Una propiedad fundamental del hashing es que si dos resultados de una misma función son diferentes, entonces las dos entradas que generaron dichos resultados también lo son.

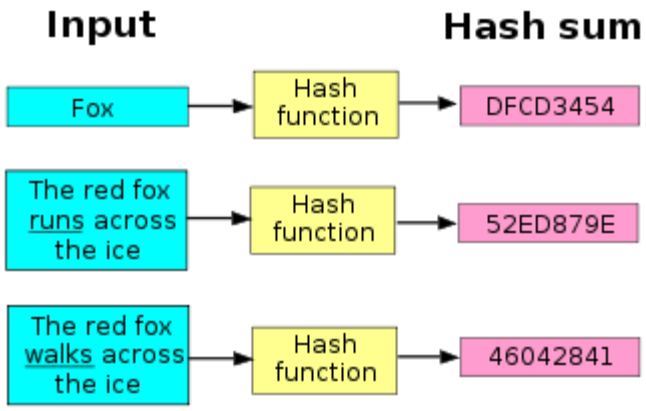


Imagen 11: Función Hash

Son usadas en múltiples aplicaciones, como los arrays asociativos, criptografía, procesamiento de datos y firmas digitales, entre otros. Una buena función de hash es una que experimenta pocas colisiones en el conjunto esperado de entrada; es decir que se podrán identificar unívocamente las entradas.

2.1.3.3.1 Propiedades

- **Unidireccionalidad**

  Conocido un resumen h(M), debe ser computacionalmente imposible encontrar M a partir de dicho Resumen.

- **Compresión**

  A partir de un mensaje de cualquier longitud, el resumen h(M) debe tener una longitud fija (en general menor).

- **Facilidad de Calculo**

  Debe ser fácil calcular h(M) a partir de un mensaje M.

- **Difusión**

  El Resumen h(M) debe ser una función compleja de todos los bits del mensaje M. Si se modifica un solo bit del mensaje M, el hash h(M) debería cambiar la mitad de sus bits.

2.1.3.3.2 Funcionalidades

- Transforma un mensaje de longitud arbitrariamente grande a un número fijo de bits de longitud fija.

- Permiten resolver el problema de la integridad de los mensajes, así como la autenticidad de mensajes y de su origen.

- Una función hash es también ampliamente usada para la firma digital, ya que los documentos a firmar son en general demasiado grandes, la función hash les asocia una cadena de longitud 160 bits que los hace más manejables para el propósito de firma digital.

2.1.3.3.3 Algoritmos HASH más utilizados

- ✓ **MD5 (Message-Digest Algorithm 5 o Algoritmo de Firma de Mensajes 5):** Desarrollado por Ron Rivest, y ha sido hasta los últimos año el algoritmo hash más usado. Procesa mensajes de una longitud arbitraria en bloques de 512 bits generando un compendio de128 bits. Debido a la capacidad de procesamiento actual esos 128 bits son insuficientes, además de que una serie de ataques criptoanalíticos han puesto de manifiesto algunas vulnerabilidades del algoritmo. Puede ser útil para comprobar la integridad de un fichero tras una descarga, por ejemplo, pero ya no es aceptable desde el punto de vista criptoanalítico.

- ✓ **SHA-1 (Secure Hash Algorithm 1 o Algorimo de Hash Seguro 1):** El SHA-1 tomo como entrada un mensaje de longitud máxima 264 bits (más de dos mil millones de Gigabytes) y produce como salida un resumen de 160 bits. Este número es mayor que el que se utilizaba en el algoritmo SHA original, 128 bits. Ya existen nuevas versiones de SHA que trabajan con resúmenes de 224, 256, 384 e incluso 512 bits.

2.2 Marco Conceptual

El Proyecto estará enfocado en el estudio del uso de la Encriptación como método de Seguridad en distintas Empresas, Instituciones, y Entidades que usen Sitios Web en nuestra Ciudad, logrando con esto, segmentar el análisis y tener una apreciación viable para la justificación del Proyecto.

2.3 Marco Espacial

El Trabajo a desarrollarse estará planteado en una duración de 3 meses.

2.4 Marco Legal

La realización del presente trabajo se halla enmarcado en la constitución de la República del Ecuador, reformada por la Asamblea Constituyente en el año 2008, en la “LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS”, bajo los siguientes artículos:

- **Título Preliminar**

Art. 1.- Objeto de la Ley.- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

- **Título I**

DE LOS MENSAJES DE DATOS

Capítulo I

PRINCIPIOS GENERALES

Art. 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

- **Título III**

DE LOS SERVICIOS ELECTRÓNICOS, LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA, LOS DERECHOS DE LOS USUARIOS, E INSTRUMENTOS PÚBLICOS.

Capítulo I

DE LOS SERVICIOS ELECTRÓNICOS

Art. 44.- Cumplimiento de formalidades.- Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley.

- **Título V**

DE LAS INFRACCIONES INFORMÁTICAS

Capítulo I

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

"Art. ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Art. 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"Art. ....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

CAPITULO III

3. METODOLOGÍA

3.1 Metodología de Investigación

3.1.1 Análisis de la Problemática

Para el Análisis del Trabajo propuesto, nos basaremos en el uso de métodos y Técnicas de Investigación para recopilar la mayor cantidad de información y opiniones que ayuden a fundamentar nuestros objetivos. Mediante estas herramientas de investigación se podrá identificar de una manera más certera las dificultades que tiene la empresa, y con esto ayudando a prevenir y corregir las mismas.

3.1.2 Método

a) Cualitativo – Cuantitativo

A través de estos métodos se busca conocer de manera más acertada cuales son las evidencias reales sobre seguridad informática, basándonos en conteos, porcentajes y preferencias sobre algún tipo de seguridad, todo esto con el fin de lograr los objetivos propuestos.

3.1.3 Técnica

a) Encuestas

Esta Técnica es aquella destinada a obtener datos de varias personas, cuyas opiniones impersonales son de gran importancia para el estudio y análisis de algún Tema.

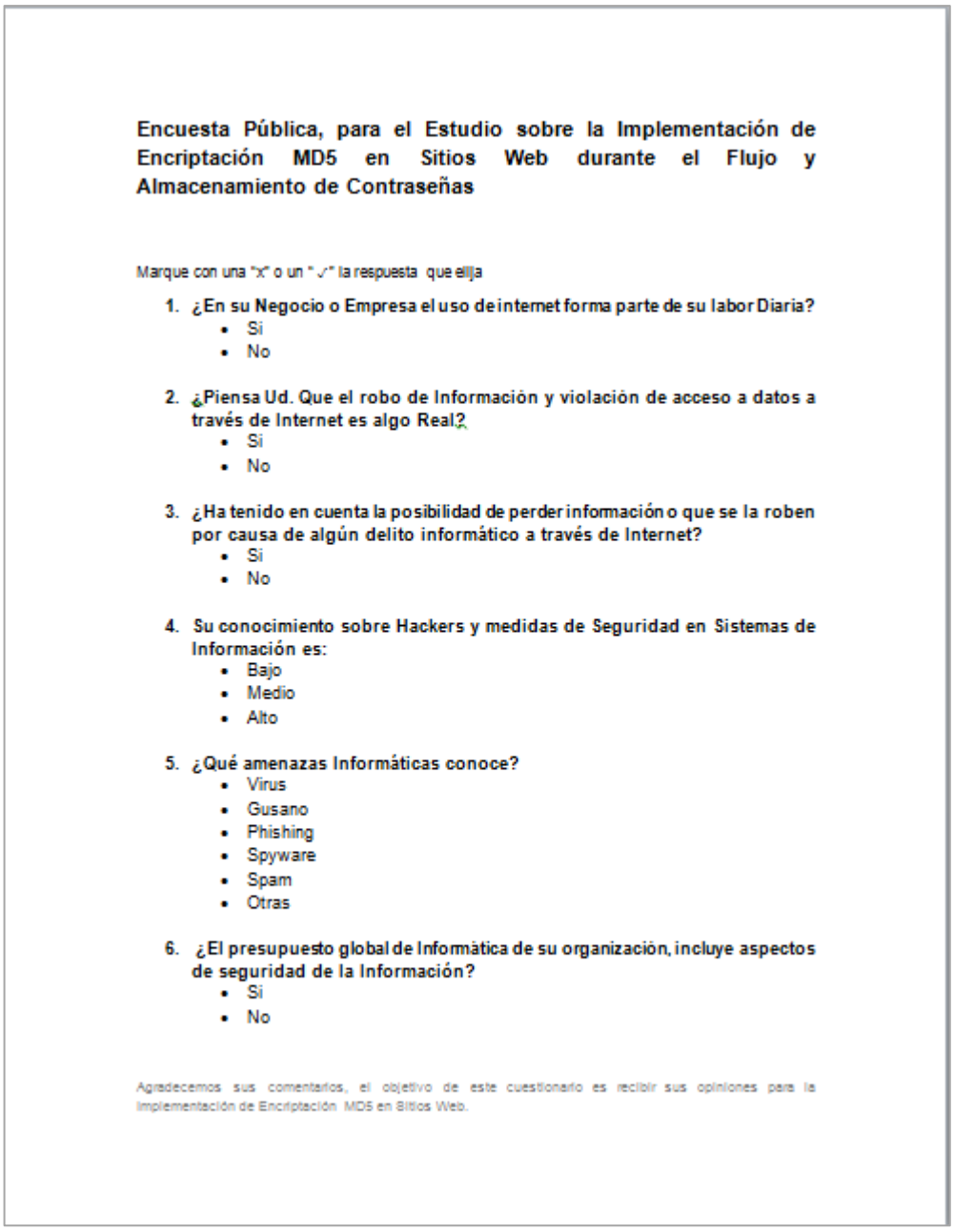
Una vez que se haya recopilado la información de las personas encuestadas se procederá a realizar un Análisis basado en porcentajes para identificar cual es el conocimiento real sobre métodos de seguridad informática y si es que dentro de estos está lo que es la Encriptación como medida de Seguridad.

b) Población Involucrada

Para este proceso de estudio se ha tomado como referencia las opiniones de 20 encuestados, que representan cada uno, a distintas Empresas y Micro – Empresas que poseen Sitios Web o algún servicio similar en los que de por medio esta la integridad de sus datos.

c) Formato de la Encuesta

- **Hoja 1**



Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

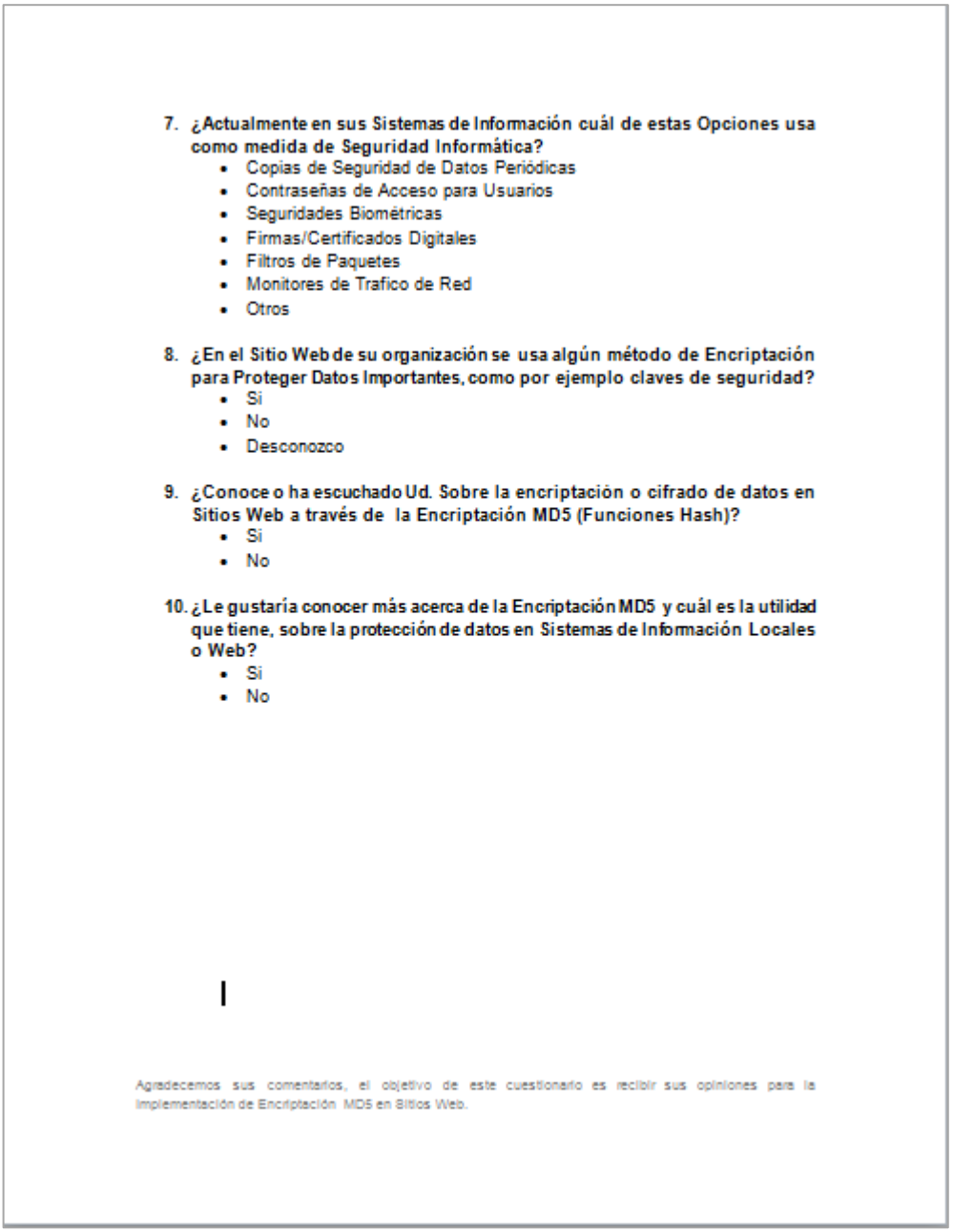
Marque con una "x" o un " ✓" la respuesta que elija

1. ¿En su Negocio o Empresa el uso de internet forma parte de su labor Diaria?
   - Si
   - No
2. ¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?
   - Si
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?
   - Si
   - No
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - Bajo
   - Medio
   - Alto
5. ¿Qué amenazas Informáticas conoce?
   - Virus
   - Gusano
   - Phishing
   - Spyware
   - Spam
   - Otras
6. ¿El presupuesto global de Informàtica de su organización, incluye aspectos de seguridad de la Información?
   - Si
   - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la implementación de Encriptación MD5 en Sitios Web.

Imagen 12: Formato de la Encuesta Parte 1

- **Hoja 2**



7. **¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?**
   - Copias de Seguridad de Datos Periódicas
   - Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros

8. **¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?**
   - Si
   - No
   - Desconozco

9. **¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash)?**
   - Si
   - No

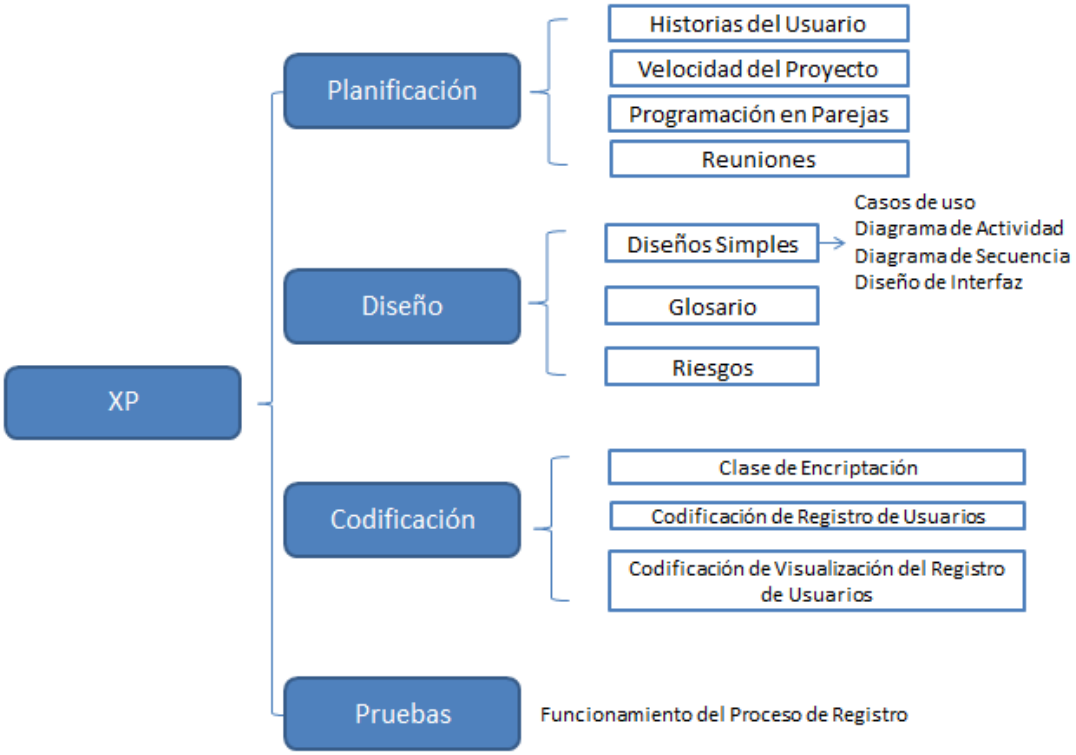
10. **¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?**
    - Si
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la implementación de Encriptación MD5 en Sitios Web.

Imagen 13: Formato de la Encuesta Parte 2

3.2 Metodología Informática

3.2.1 Extreme Programation (XP)



Esquema 1: Metodología XP

A través de esta Metodología se describirá cada uno de los Procesos en los que estará involucrada la parte Practica y Demostrativa de nuestro Proyecto de Tesis, tomando como referencia el "Registro de Clientes con Encriptación de Contraseñas", esto con el fin de dar una idea real de lo que representa la Encriptación como Medida de Seguridad Informática.

Nuestro Diseño de las Actividades del proceso de Registro y Visualización, consistirá en el uso de Diagramas UML, que ayudarán a facilitar al lector la comprensión de la idea Propuesta.

En cuanto a la Demostración práctica se usará como referencia la Herramienta de desarrollo Web “Visual Studio .NET”, la cual es una de las más conocidas en por las enormes ventajas que ofrece al momento de desarrollar una aplicación y por la facilidad de su manejo.

La Codificación y creación de nuestra práctica demostrativa se realizará en la herramienta mencionada anteriormente, pero cabe recalcar que también se puede utilizar en lenguajes como PHP, en donde el Cifrado MD5 ya viene incluido dentro de este lenguaje, por lo que la realización de cifrado de datos no es mayor problema. Cualquiera de estas dos herramientas son totalmente funcionales y brindan ventajas enormes, esto de acuerdo a las características del programador.

3.2.1.1 Planificación

3.2.1.1.1 Historias del Usuario

- **Descripción de Actores**

✓ **Usuario (Cliente)**

“Como usuario al momento de Registrarme en un Sitio Web necesito tener la garantía de que nadie pueda ver o robe mis contraseñas y que únicamente sea yo el que las conozca y pueda manipularlas”

✓ **Administrador (Persona encargada o dueña del Sitio Web)**

“Al tener el Sitio Web, para brindar un servicio, el principal objetivo es hacer que los usuarios tengan la confianza de registrarse sin que haya

inconvenientes por manipulaciones ilícitas de sus cuentas, ya sea por robo de Contraseñas o violaciones de seguridad a las cuentas de nuestros Clientes”

- **Historias**

a) Historia 1: Registro de Usuarios

Historia de Usuario	
Número:1	**Nombre Historia de Usuario:** Registro de Usuarios
Usuario: Cliente	
Prioridad en Negocio: Alta (Alta / Media / Baja)	
Riesgo en Desarrollo: Baja (Alto / Medio / Bajo)	
Descripción: El registro de usuarios se va realizando paulatinamente por personas, es así que el registro de usuarios se da con el llenado del formulario correspondiente, para luego de esto poder extraer los datos de la Base de Datos y realizar Validaciones.	
Observaciones: Se necesita la conformidad de normas de parte del cliente.	

Historia de Usuario 1: Registro de Usuarios

- ✓ **Tareas**

Tarea de Ingeniería	
Número Tarea: 1.1	**Número Historia de Usuario:1**
Nombre Tarea: Diseño estructural de los datos de los Usuarios (Cliente)	
Tipo de Tarea : Desarrollo Desarrollo / Corrección / Mejora / Otra (especificar)	
Fecha Inicio:	**Fecha Fin:**
Programador Responsable: Juan Heredia Torres	
Descripción: Se realiza el diseño de la Tabla de Base de Datos que contendrá los Registros de los clientes.	

Tarea de Usuario 1: Tarea 1.1 – Diseño estructural de los datos de los Usuarios

Tarea de Ingeniería	
Número Tarea: 1.2	**Número Historia de Usuario:1**
Nombre Tarea: Diseño de Interfaz	
Tipo de Tarea : Desarrollo Desarrollo / Corrección / Mejora / Otra (especificar)	
Fecha Inicio:	**Fecha Fin:**
Programador Responsable: Juan Heredia Torres	
Descripción: Se realiza el Diseño de la Interfaz del Formulario que el Cliente usará para Registrar sus Datos.	

Tarea de Usuario 2: Tarea 1.2 - Diseño de Interfaz

Tarea de Ingeniería	
Número Tarea: 1.3	**Número Historia de Usuario:1**
Nombre Tarea: Alertas del Registro	
Tipo de Tarea : Desarrollo Desarrollo / Corrección / Mejora / Otra (especificar)	
Fecha Inicio:	**Fecha Fin:**
Programador Responsable: Juan Heredia Torres	
Descripción: Se usa para alertar al usuario durante el proceso de registro, guiando al usuario cliente con alertas de corrección o de procesos de Activación de la Cuenta a Registrar.	

Tarea de Usuario 3: Tarea 1.3 – Alertas del Registro

Tarea de Ingeniería	
Número Tarea: 1.4	**Número Historia de Usuario:1**
Nombre Tarea: Altas del Registro	
Tipo de Tarea : Desarrollo Desarrollo / Corrección / Mejora / Otra (especificar)	
Fecha Inicio:	**Fecha Fin:**
Programador Responsable: Juan Heredia Torres	
Descripción: Se la usa para realizar el proceso de activación de la Cuenta del Cliente, modificando el Registro de la Base de Datos para que el usuario pueda tener control sobre su Cuenta Registrada.	

Tarea de Usuario 4: Tarea 1.4 – Altas del Registro

b) Historia 2: Visualización de Registro de Usuarios

Historia de Usuario	
Número:2	**Nombre Historia de Usuario:** Visualización de Registro de Usuarios
Usuario: Cliente	
Prioridad en Negocio: Media (Alta / Media / Baja)	
Riesgo en Desarrollo: Baja (Alto / Medio / Bajo)	
Descripción: La visualización se realizará a través de la validación de los datos del usuario, en un formulario de Inicio de Sesión, donde el usuario que desee ver su registro deberá ingresar su Cédula, E-mail y Clave de Acceso. Luego de este ingreso, el Sistema Encriptará la clave y verificará si estos datos existen en la Base de Datos como un Registro Almacenado**.**	
Observaciones: Se necesita la conformidad de normas de parte del cliente.	

Historia de Usuario 2: Visualización de Registro de Usuarios

- ✓ **Tareas**

Tarea de Ingeniería	
Número Tarea: 2.1	**Número Historia de Usuario:2**
Nombre Tarea: Diseño Estructural de los datos de los Usuarios (Cliente)	
Tipo de Tarea : Reutilización	
Fecha Inicio:	**Fecha Fin:**
Programador Responsable: Juan Heredia Torres	
Descripción: Se usará la misma tabla de datos, mencionada en la Tarea 1.1, debido a que los registros se almacenan en dicha tabla, por lo tanto al tener los registros almacenados simplemente se los listara desde la Base de Datos.	

Tarea de Usuario 5: Tarea 2.1 – Diseño Estructural de los datos de los Usuarios

Tarea de Ingeniería	
Número Tarea: 2.2	**Número Historia de Usuario:2**
Nombre Tarea: Diseño Interfaz	
Tipo de Tarea : Desarrollo Desarrollo / Corrección / Mejora / Otra	
Fecha Inicio:	**Fecha Fin:**
Programador Responsable: Juan Heredia Torres	
Descripción: Se realiza el Diseño de la Interfaz de la Bienvenida de Registros y el Formulario de visualización de Datos.	

Tarea de Usuario 6: Tarea 2.2 – Diseño Interfaz

Tarea de Ingeniería	
Número Tarea: 2.3	**Número Historia de Usuario:2**
Nombre Tarea: Alertas de Acceso	
Tipo de Tarea : Desarrollo Desarrollo / Corrección / Mejora / Otra (especificar)	
Fecha Inicio:	**Fecha Fin:**
Programador Responsable: Juan Heredia Torres	
Descripción: Se usa para alertar al usuario, mientras se hacen validaciones de acceso en la Interfaz de Bienvenida, para posteriormente si se valida el ingreso, visualizar los Datos del usuario registrado.	

Tarea de Usuario 7: Tarea 2.3 – Alertas de Acceso

3.2.1.1.2 Velocidad del Proyecto

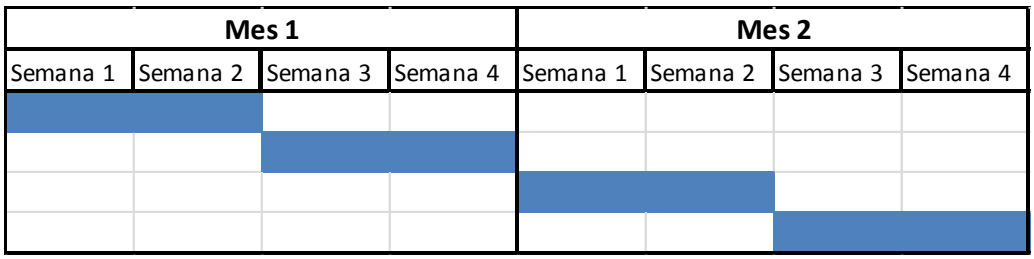


Tabla 1: Tiempo de Desarrollo del Proyecto

Según el Tiempo estimado de Trabajo para la realización del Proyecto, se puede notar que el tiempo es sumamente limitado, por lo que nuestra Prioridad de Esfuerzo y Velocidad en la elaboración del Proyecto la podemos definir como “Alta”.

3.2.1.1.3 Programación en Pareja

El Proceso de Programación se lo realizará de forma individual pero será supervisado por el Docente Tutor quien ayudará a comprobar el perfecto funcionamiento de la codificación que permitirá cifrar las Contraseñas en el Formulario de Registro de los Clientes.

3.2.1.1.4 Reuniones

El proceso de trabajo que se realizará conjuntamente con el Docente Tutor se llevará a cabo en el lapso de dos meses, en el cual se mantendrá reuniones cada viernes durante este período, donde se estudiará y revisará los procedimientos del desarrollo del Proyecto tanto en la Parte Práctica como en la Investigativa.

3.2.1.2 Diseño

3.2.1.2.1 Diseños Simples

3.2.1.2.1.1 Caso de Uso

a) Registro del Usuario

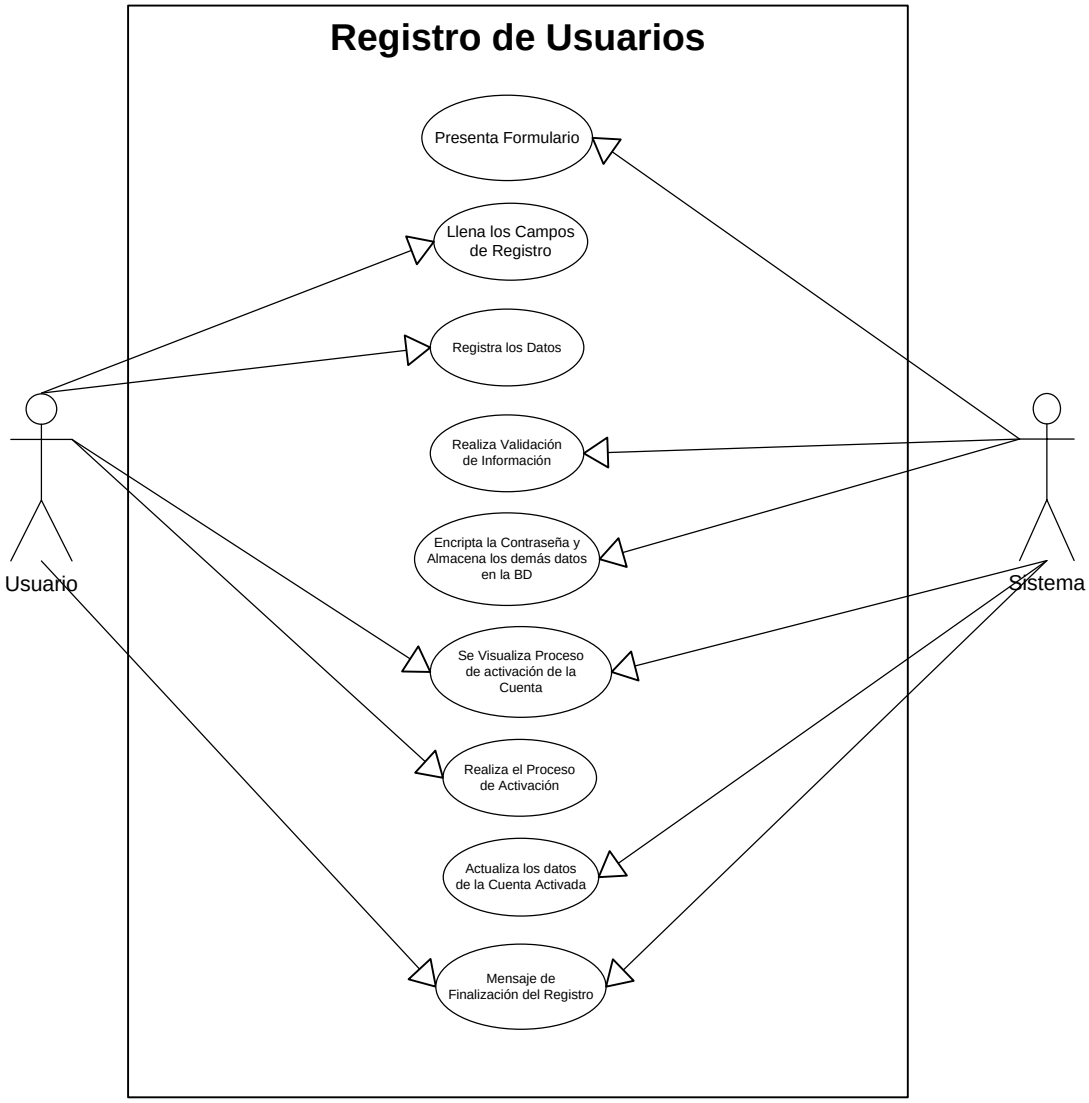


Diagrama Caso de Uso 1: Registro del Usuario

Caso de Uso1: Registro del Usuario

Actor principal: Usuario - Sistema

Personal Involucrado:

- ✓ **Usuario:** El Usuario Ingresa al Formulario de Registro, en donde deberá llenar el Formulario con sus datos originales, y realizar la validación del E-mail, y los demás pasos que conllevan el Proceso de registro y activación de la cuenta.
- ✓ **Sistema:** Es el Encargado de Validar los Datos ingresados por el Usuario, Encriptar la Contraseña, Almacenar datos en la Base de Datos, Realizar el proceso de Validación de la Cuenta y guiar al Usuario a través de los pasos de Registro de Usuario.

Precondiciones: Para que los Usuarios puedan registrarse sin problemas se debe cumplir con lo siguiente:

- ✓ Que el E-mail de registro sea real y no ficticio, debido a que la activación de la Cuenta se realizará, a través de Dicho Correo.
- ✓ Que el Usuario no se haya registrado Previamente.
- ✓ Que ni la Cédula o el E-mail haya sido registrado por el Usuario u otra persona.
- ✓ Que la base de datos esté disponible para almacenar la información.
- ✓ Que el Sistema realice de forma correcta los Pasos de registro sin problemas de codificación.

Garantías del Éxito: Para que el proceso de registro pueda realizarse de forma correcta, el usuario debe cumplir con los requerimientos del Sistema, destacando lo que es:

- ✓ **Que no se haya registrado con Anterioridad**
- ✓ **Que el correo Electrónico sea real**

De acuerdo con esto el Sistema podrá realizar y guiar al Usuario durante todo el Proceso de registro, dándole validación a los datos y almacenándolos en la Base de Datos.

Escenario principal:

- ✓ Los usuarios Ingresan al Formulario de Registro
- ✓ Llenan los datos que el sistema solicita
- ✓ El Usuario debe Validar el E-mail para saber si está disponible en el Sistema
- ✓ El Usuario debe dar Click en la Opción de Registro.
- ✓ El Sistema procede a Validar y almacenar los Datos en la BD.
- ✓ El Sistema muestra las opciones de Activación de la Cuenta.
- ✓ El Usuario Realiza el Proceso de Activación.
- ✓ El Sistema Actualiza los Datos del Usuario.

Excepciones:

- ✓ Que el usuario este registrado.
- ✓ Que el E-mail o Cédula este registrado anteriormente.
- ✓ Que el usuario no realice el proceso de Activación de la Cuenta
- ✓ Que el Sistema tenga errores de Codificación
- ✓ Que la Base de Datos sufra algún desperfecto y realice el procedimiento de Almacenamiento y validación.

b) Visualización del Registro del Usuario

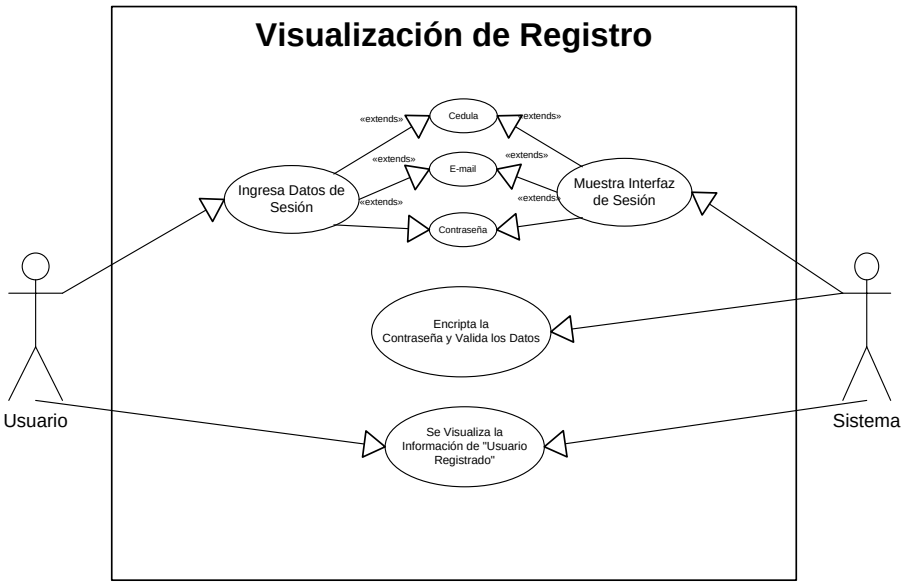


Diagrama Caso de Uso 2: Visualización de Registro

Caso de Uso 2: Visualización del Registro del Usuario
Actor principal: Usuario – Sistema
Personal Involucrado: ✓ **Usuario:** El Usuario Ingresa a la Interfaz de Bienvenida, y tendrá la opción de iniciar Sesión para ver su cuenta Registrada. En esta Opción Deberá Llenar los Datos de ingreso para poder realizar el Proceso. ✓ **Sistema:** Deberá Validar los Datos de Entrada del usuario, luego de haber encriptado la contraseña para poder darle acceso a sus datos registrados.
Precondiciones: Para que este proceso de Inicio de sesión se lleve a cabo, el usuario deberá ingresar sus Datos de Forma correcta para que el sistema pueda comprobar la Existencia del Registro del usuario. Además de esto El Sistema antes de comprobar los datos de ingreso con los ya almacenados, según el usuario, deberá encriptar la contraseña para poder realizar la comprobación
Garantías del Éxito: para que se realice este proceso de forma adecuada deberá cumplirse lo Siguiente: ✓ Que el usuario este Registrado ✓ Que los datos de Inicio de Sesión sean Correctos ✓ Que el Sistema Encripte la Contraseña del Usuario antes de Compararlos con los almacenados de la Base de Datos.
Escenario principal: ✓ El usuario Ingresa los datos de inicio de sesión ✓ El Sistema Encripta la Contraseña, y realiza la consulta de los Datos del usuario con los Almacenados en la Base de Datos. ✓ Si los datos son Validados de forma correcta se le da acceso al Usuario ✓ El Usuario puede ver los Datos Registrados

Excepciones:
- ✓ Que el usuario no este registrado.
- ✓ Que los datos de acceso no concuerden con un registro existente.
- ✓ Que el Sistema no Encripte la Contraseña del Usuario para realizar la consulta.
- ✓ Que la Base de Datos no esté funcionando.

3.2.1.2.1.2 Diagrama de Actividad

a) Registro del Usuario

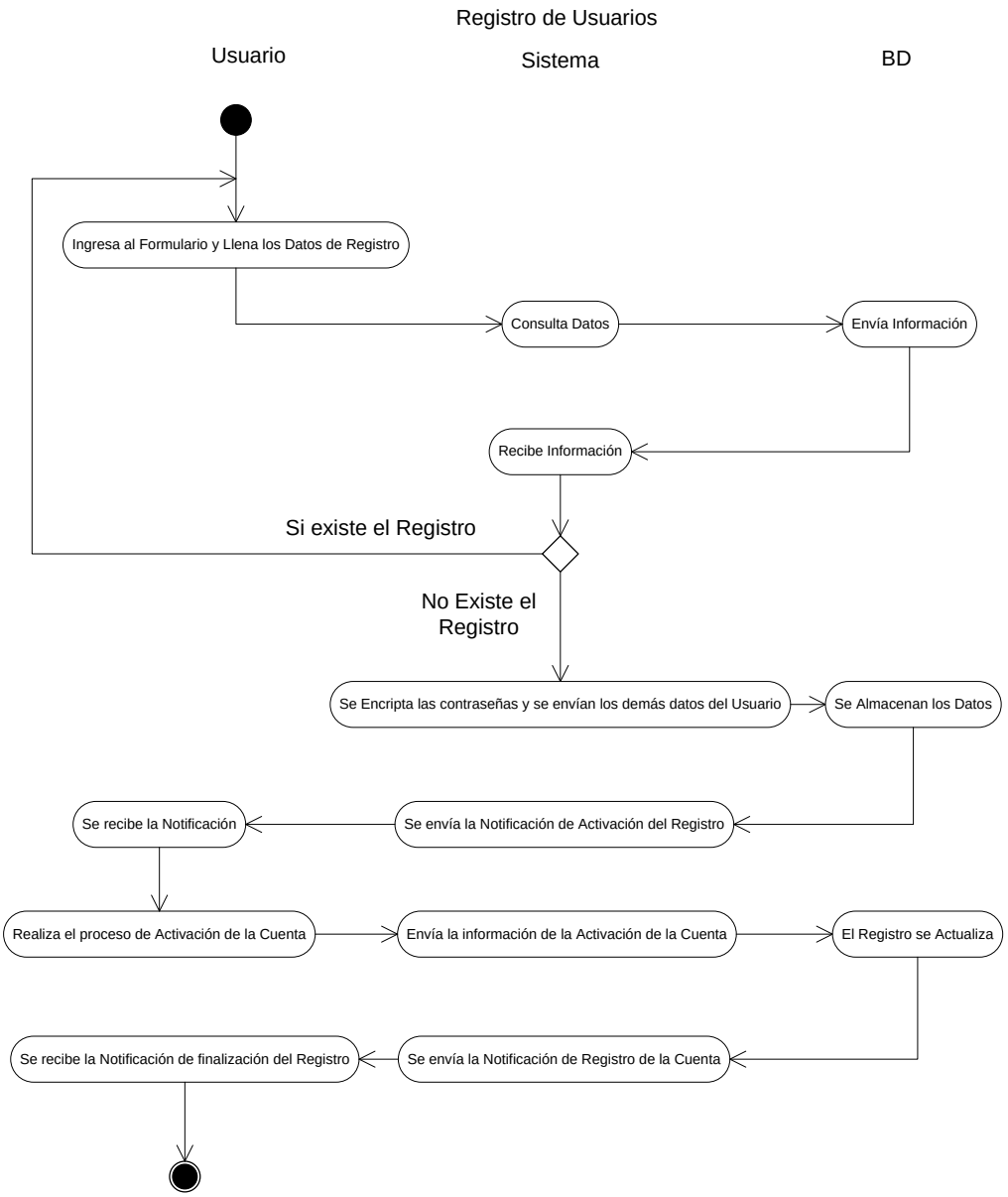


Diagrama de Actividad 1: Registro del Usuario

b) Visualización del Registro del Usuario

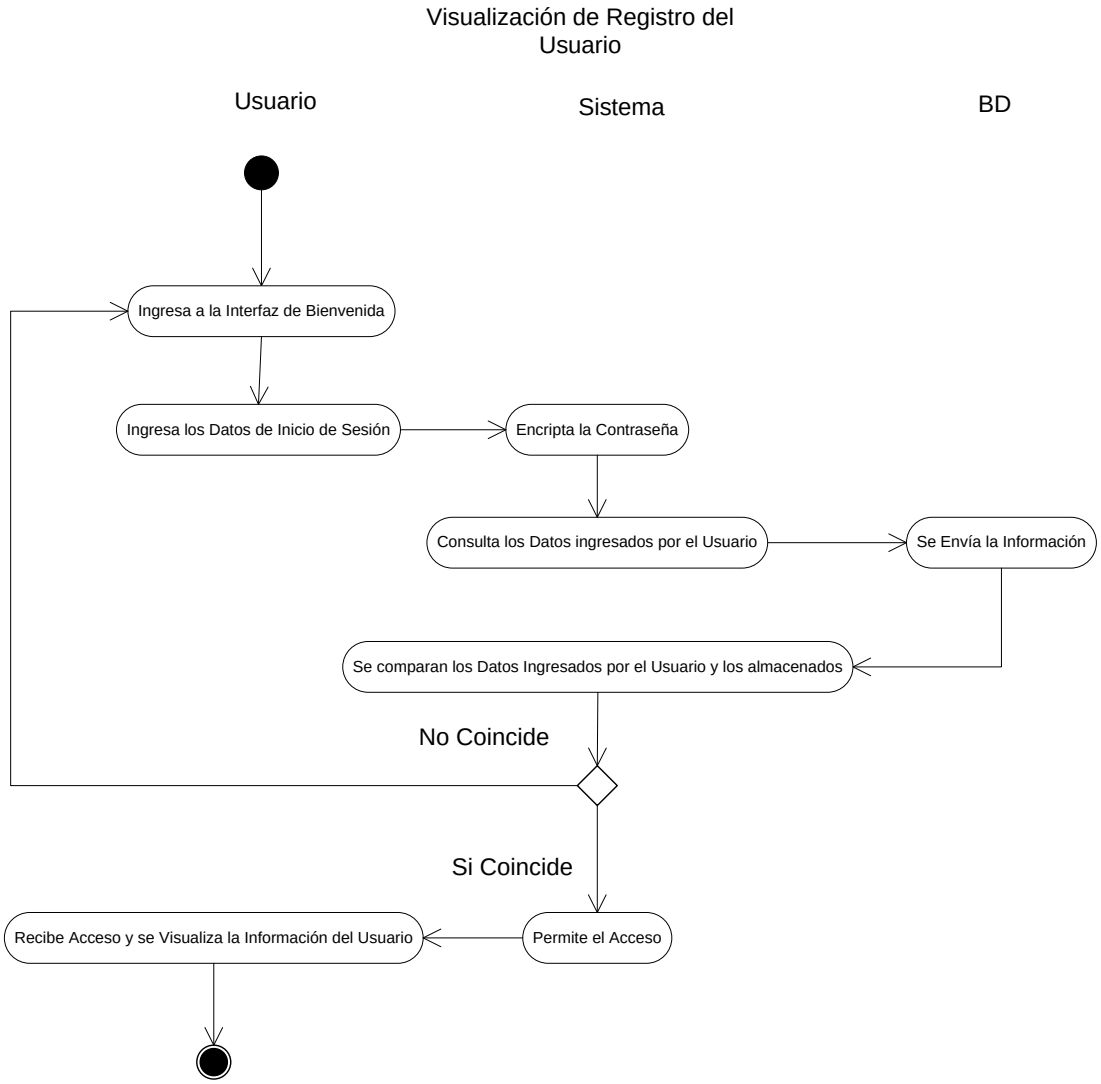


Diagrama de Actividad 2: Visualización de Registro del Usuario

3.2.1.2.1.3 Diagrama de Secuencia

a) Registro del Usuario

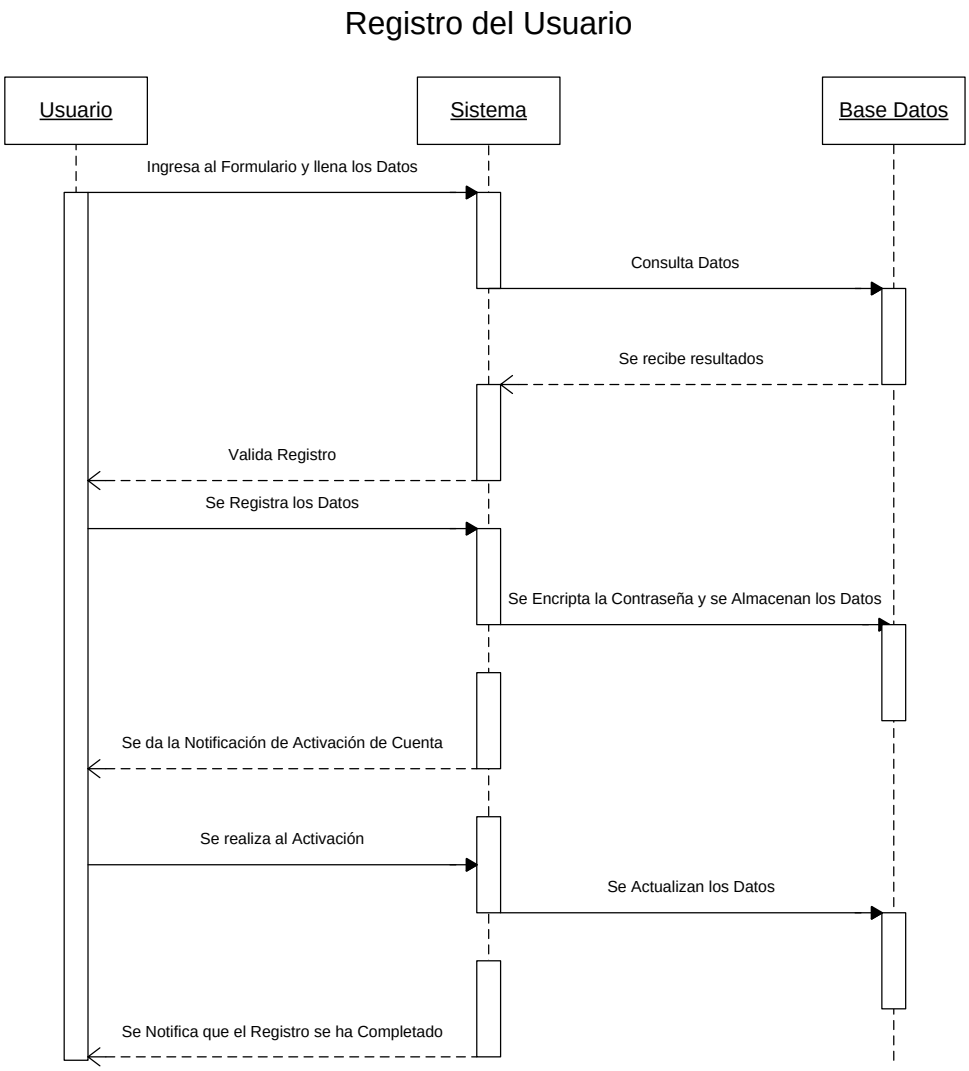


Diagrama de Secuencia 1: Registro del Usuario

b) Visualización de Registro del Usuario

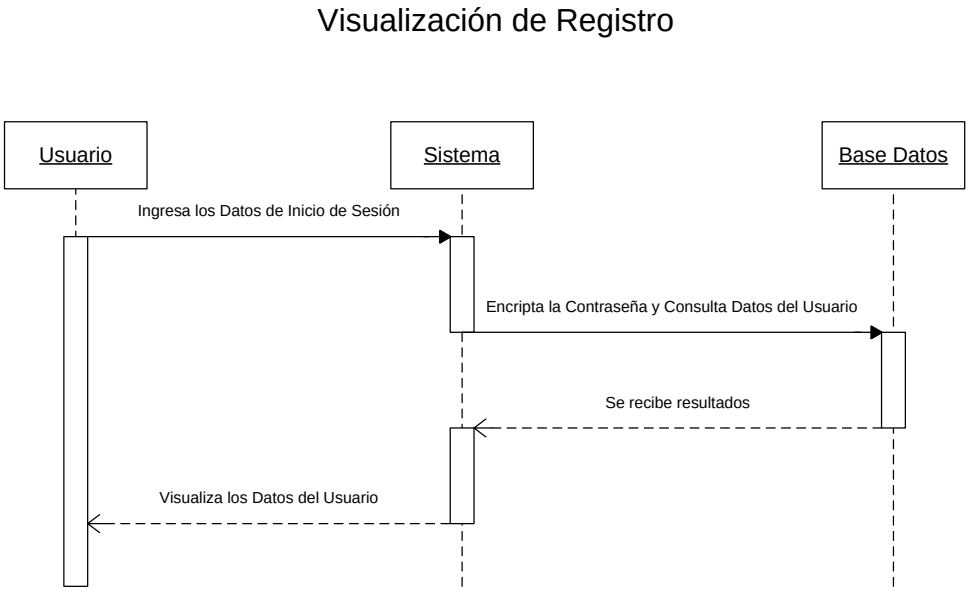


Diagrama de Secuencia 2: Visualización de Registro del Usuario

3.2.1.2.1.4 Diseño de Interfaces

a) Interfaz de Bienvenida

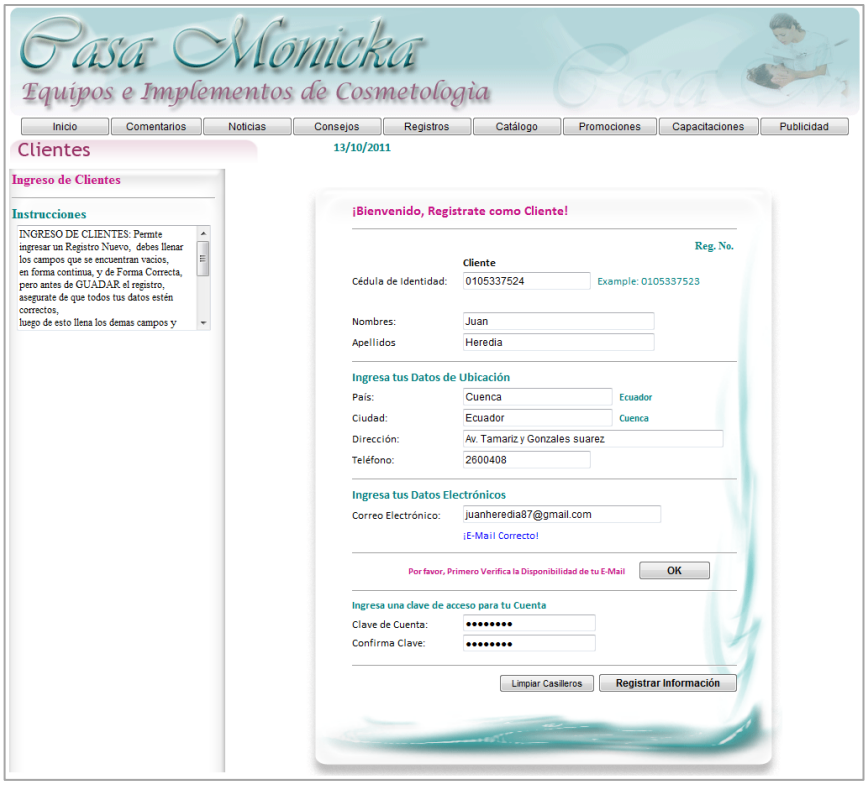
Diseño de Interfaz 1: Bienvenida de Registro

En Esta Interfaz los usuarios pueden Elegir si desean Registrarse o Visualizar su Registro, trabajando estas opciones de la siguiente manera:

- ✓ **Opción de Registro:** Cuando el usuario de Click en esta Opción se le Visualizará un Formulario de Registro, donde el Sistema guiará paso a paso al Usuario hasta cumplir con dicha acción.

- ✓ **Opción de Ingresar:** En esta opción todo usuario que esté registrado podrá visualizar sus Datos de Registro, para esto debe ingresar sus datos de inicio de Sesión (Cédula, E-mail, Contraseña) y una vez que este los ingrese el Sistema Encriptará la Contraseña y Realizará una consulta a la Base de Datos para comprobar si los datos son de un Registro existente y darle acceso al Usuario.

b) Interfaz de Registro del Usuario (Cliente)

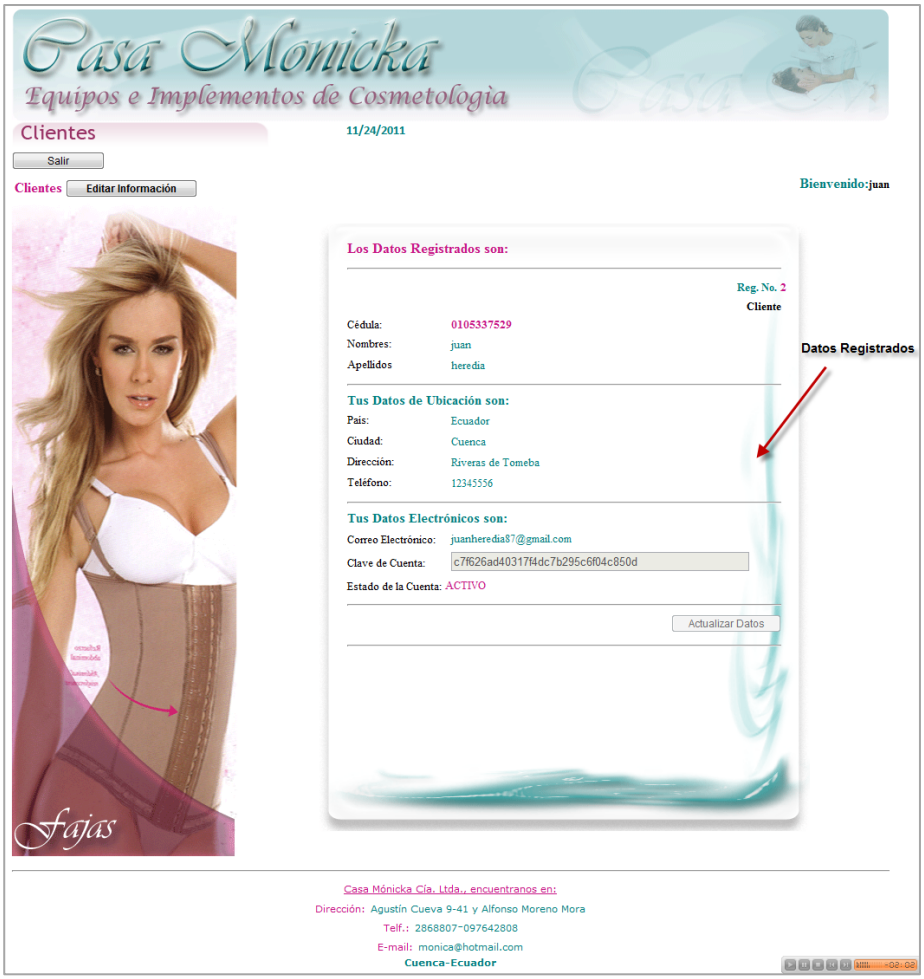


Diseño de Interfaz 2: Formulario de Registro del Usuario

Al momento de registrarse el usuario, el Sistema visualizará el Formulario que vimos anteriormente, que consiste en el ingreso de Cedula, Nombre, Ciudad, E-mail, Contraseña, etc. Este Formulario a través del Sistema Realiza la Validación de los Datos del usuario y la encriptación de la contraseña antes de Mandar a Guardar el Registro.

Si el Registro es validado con normalidad la Información se guardará y el sistema posteriormente guiará al usuario hasta la finalización del Registro.

c) Interfaz de Vista de Registro Almacenado



Diseño de Interfaz 3: Formulario de Visualización de Registro

Esta Interfaz se visualizará luego de que el Usuario haya iniciado sesión, y el contenido del Formulario será el Registro que el Usuario haya tenido almacenado en la Base de Datos con anterioridad por causa de su registro en el Sistema.

3.2.1.2.2 Glosario de Términos

- ✓ **Caso de Uso:** Un caso de uso es una descripción de los pasos o las actividades que deberán realizarse para llevar a cabo algún proceso.
- ✓ **Diagrama de Actividad:** Un diagrama de actividades representa los flujos de trabajo paso a paso de negocio y operacionales de los componentes en un sistema. Un Diagrama de Actividades muestra el flujo de control general.
- ✓ **Diagrama de Secuencia:** Muestra la interacción de un conjunto de objetos en una aplicación a través del tiempo y se modela para cada caso de uso.
- ✓ **Interfaz:** Es parte de un programa que permite el flujo de información entre usuario y la aplicación, o entre la aplicación y otros programas o periféricos.
- ✓ **Algoritmo:** Es un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad.
- ✓ **Codificación:** Es el Proceso por el cual la información de una fuente es convertida en símbolos para ser comunicada.
- ✓ **Metodología:** Hace referencia al conjunto de procedimientos basados en principios lógicos, utilizados para alcanzar una gama de objetivos que rigen en una investigación científica
- ✓ **Encriptación:** Acción de proteger la información mediante técnicas criptográficas ante modificaciones o utilización no autorizada.

3.2.1.2.3 Riesgos

Durante la Elaboración del Proyecto y la Demostración Práctica se pueden encontrar los Siguientes Riegos:

- ✓ **Errores de Codificación,** por lo que se propone la continua Revisión del Código fuente en las reuniones con el Docente Tutor.
- ✓ **Fallas de Conexión con la Base de Datos o mal Funcionamiento de la misma,** para este caso lo más recomendable es tener otro computador en donde probar fallas de Conexión o errores en el software de Base de Datos.
- ✓ **Falla del Cifrado de Contraseñas al Registrarse,** si se diera un problema de estos, hay que revisar si la Clase de Encriptación ha sido creada o llamada en los formularios del Sitio Web como lo vamos a ver más adelante.

Para estos casos los planes de contingencia son ideales, y estos se crean de acuerdo a nuestros posibles riesgos.

3.2.1.3 Codificación

Como ya se mencionó anteriormente, la Codificación se realizará en la Herramienta de Desarrollo Web “Visual Studio .NET”, en la cual realizaremos lo Siguiente:

- ✓ Creación de una Clase de Cifrado MD5
- ✓ Codificación del Formulario de Registro
- ✓ Codificación de Visualización de Datos Registrados

Para la Realización de lo anterior necesitamos contar previamente con lo siguiente:

- ✓ El Sitio Web Creado y configurado.
- ✓ Una base de Datos Creada y con Conexión a nuestro Sitio Web para realizar transacciones.
- ✓ Formularios vinculados a los que nosotros vamos a manipular (Inicio, Ayuda, Envío de E-mails, etc.).
- ✓ Creación del Formulario Web de Bienvenida de Registro de Usuarios.
- ✓ Creación del Formulario Web de Registro de Usuario.
- ✓ Creación del Formulario Web para visualizar Registros existentes de Usuarios.

a) Creación de una Clase de Cifrado MD5

Lo primero que haremos es Crear una Clase que contendrá nuestro proceso de Cifrado, una vez realizada podremos llamarla en cualquier parte del Sitio Web que tengamos y que deseemos usarla para crear seguridad en algún proceso.

Este paso es uno de los más importantes en lo que es la implementación de la Encriptación, ya que de la creación de la clase depende que funcione nuestro cifrado de datos, además de que al crearla puede funcionar en cualquier parte de nuestro Sitio, evitando volver a escribir código en cada página que tengamos que programar.

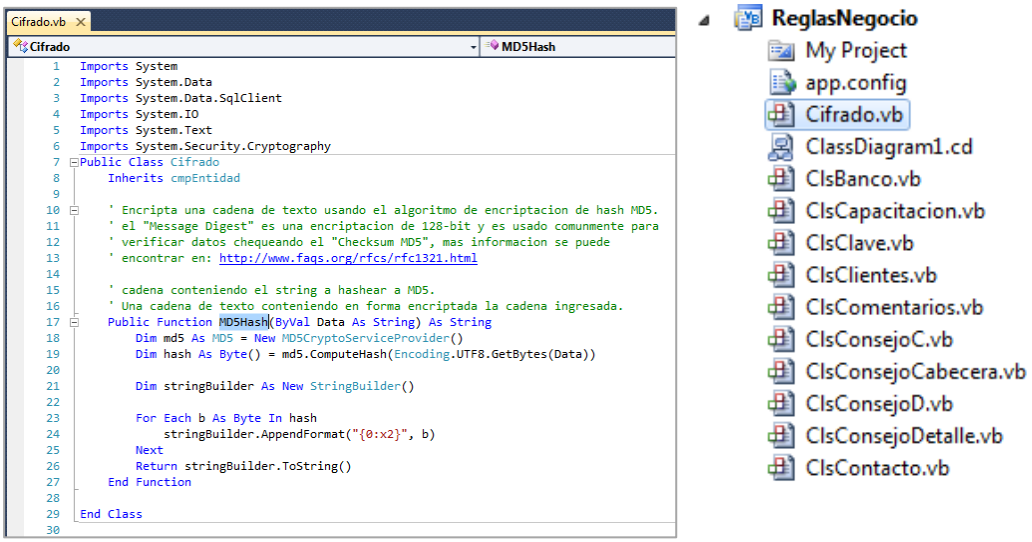


Imagen 14: Codificación del Cifrado MD5

b) Codificación del Formulario de Registro

Lo que se realizará en este caso, es codificar el Formulario para que permita registrar un Usuario en nuestra Base de Datos, pero antes de hacer esto, debemos crear un Formulario como el que se mostró anteriormente en el diseño, para nuestro Código vaya relacionado con la Interfaz.

Una vez que tengamos el Formulario Creado y con la Codificación Básica de Registro, procederemos a realizar la Inserción de Encriptación desde nuestra clase creada, para que nuestras Claves de los Registros tengan seguridad.

```
Dim cifrado As New ReglasNegocio.Cifrado
Dim objClientes As New ReglasNegocio.ClsClientes

Me.TxtPasword.Text = (cifrado.MD5Hash(Me.TxtPasword.Text))

objClientes.Agregar_Clientes(Me.LblNo_Registro.Text, Me.TxtCedula.Text, _
            Me.TxtCodUsuario.Text, Me.TxtNombre.Text, _
            Me.txtApellido.Text, Me.TxtTelefono.Text, Me.TxtPais.Text, Me.txtCiudad.Text, _
             Me.TxtDireccion.Text, Me.TxtEmail.Text, Me.TxtPasword.Text, _
             Me.lblFecha.Text, Me.TxtCod_Activacion.Text, Me.LblEstado.Text)
Response.Write("<script> alert ('¡Tu Información ha sido Registrada con exito!') </script>")
```

Imagen 15: Inserción de Encriptación antes de realizar un Registro

Luego de haber procedido a realizar lo anterior ya podremos poner en funcionamiento el proceso de cifrado de Datos, para que cada vez que se registre un usuario su clave se Encripte y sea enviada a la Base de Datos para ser almacenada.

c) Codificación de Visualización de Datos Registrados

Como parte final en el proceso de Registro de usuarios con Encriptación, se procederá a realizar la codificación de la Visualización del Registro para esto necesitaremos dos Formularios:

- ✓ **Formulario de Inicio de Sesión,** en este Formulario lo que se hará es una validación de los Datos del usuario registrado para poder darle acceso. El usuario tendrá que ingresar sus datos y el sistema Encriptará su contraseña nuevamente para comprarla con el registro de la Base de Datos y así saber si la petición de Sesión coincide con datos Registrados.

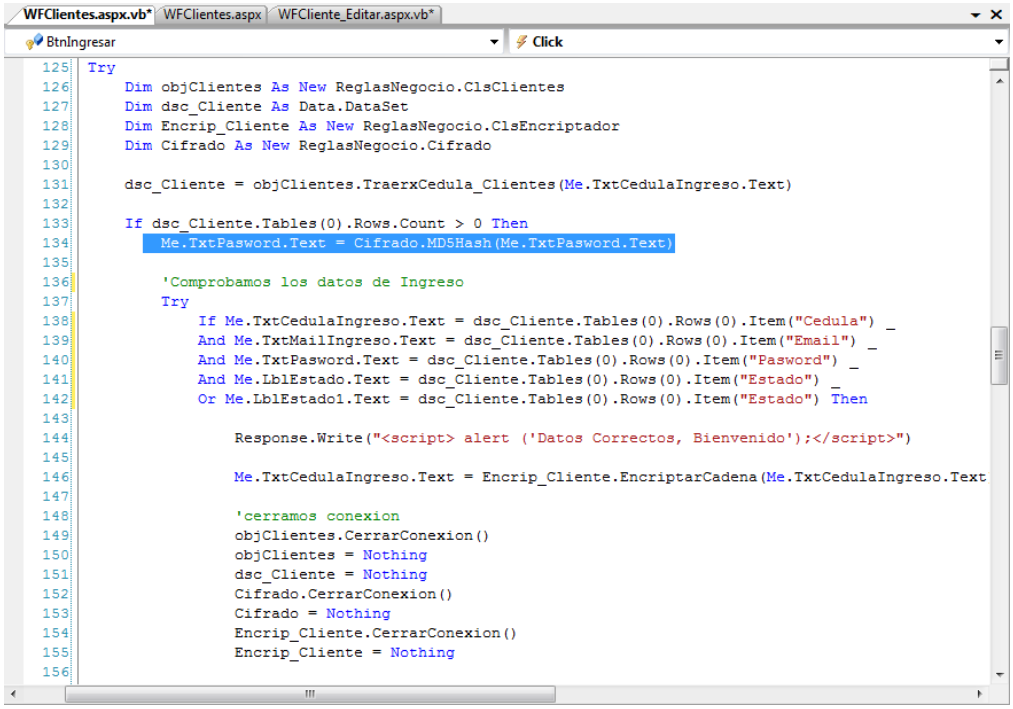


Imagen 16: Vista de Código de Inicio de Sesión

- ✓ **Formulario de Visualización de Datos Registrados,** una vez que el proceso de sesión haya validado al Usuario de la Cuenta, le permitirá a este acceder al siguiente formulario para que pueda ver sus datos registrados y su contraseña encriptada.

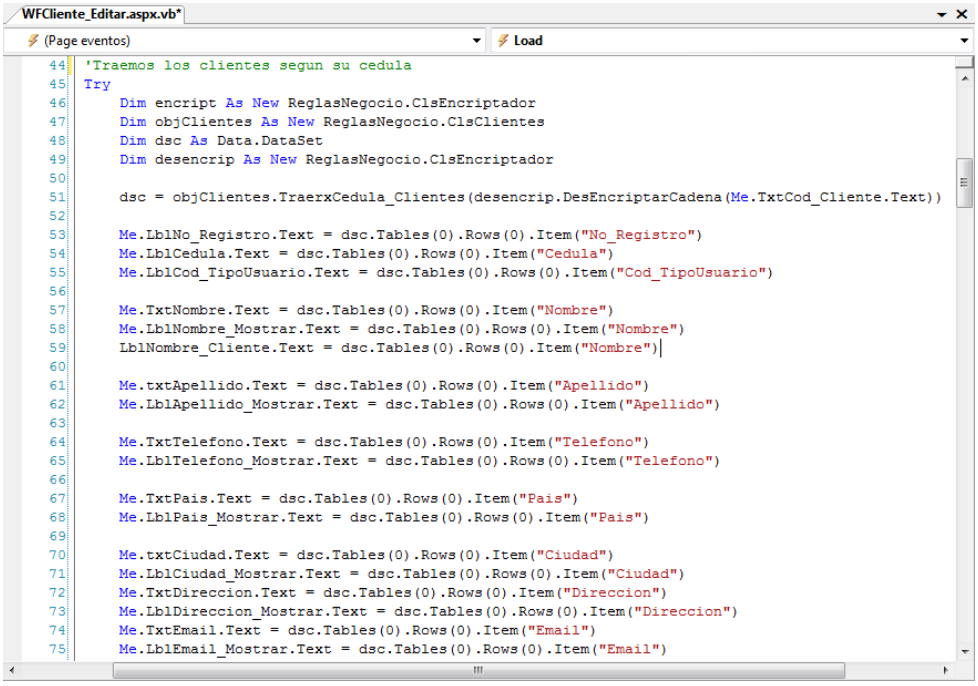


Imagen 17: Vista de Código de Visualización de Registros

3.2.1.4 Pruebas

Para probar el Funcionamiento de nuestro proceso de Codificación y Desarrollo de nuestros tres Formularios, realizaremos los Siguientes pasos:

Paso 1: Registro del Usuario

Imagen 18: Ingreso de Datos al Formulario de Registro

Para esto ingresamos a nuestro Formulario, llenamos los datos y en la sección de Contraseña agregamos una con esta clave “juan1234”, la cual el sistema antes de guardar la Encriptará, luego de esto el sistema validará nuestros datos de ingreso para saber si no hay datos duplicados en la Base de Datos.

Imagen 19: Mensaje de Confirmación de Registro Creado

Paso 2: Ingreso de Datos de Sesión

Imagen 20: Ingreso de Datos de Sesión

Para poder visualizar los Datos debemos Ingresar nuevamente lo datos que usamos en el Formulario de Registro, aquí el Sistema Encriptará nuestra Clave de Acceso y conjuntamente con los otros datos los comparará con los de la Base de Datos.

Paso 3: Visualización del Registro del Usuario

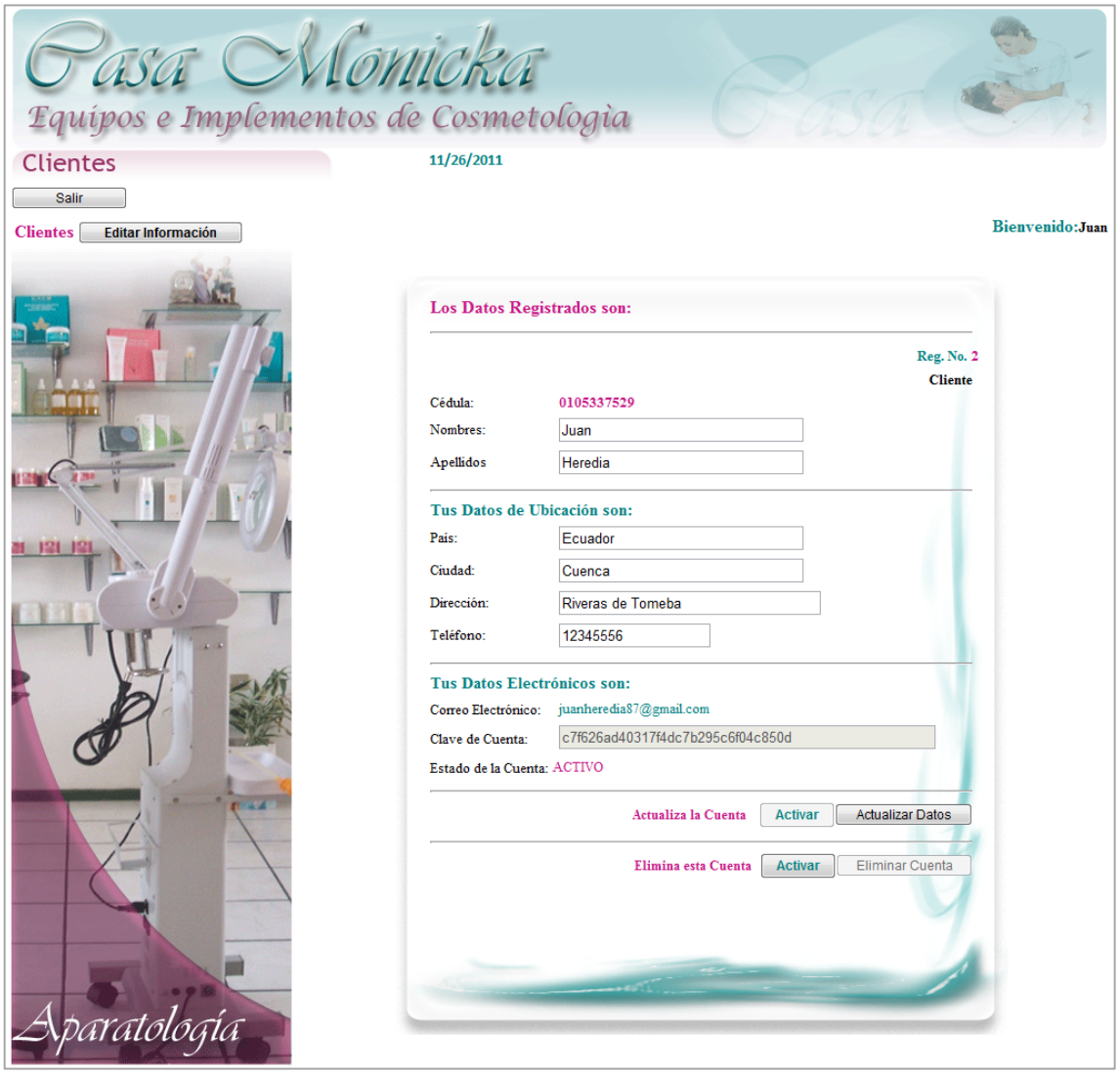


Imagen 21: Visualización de Registro del Usuario

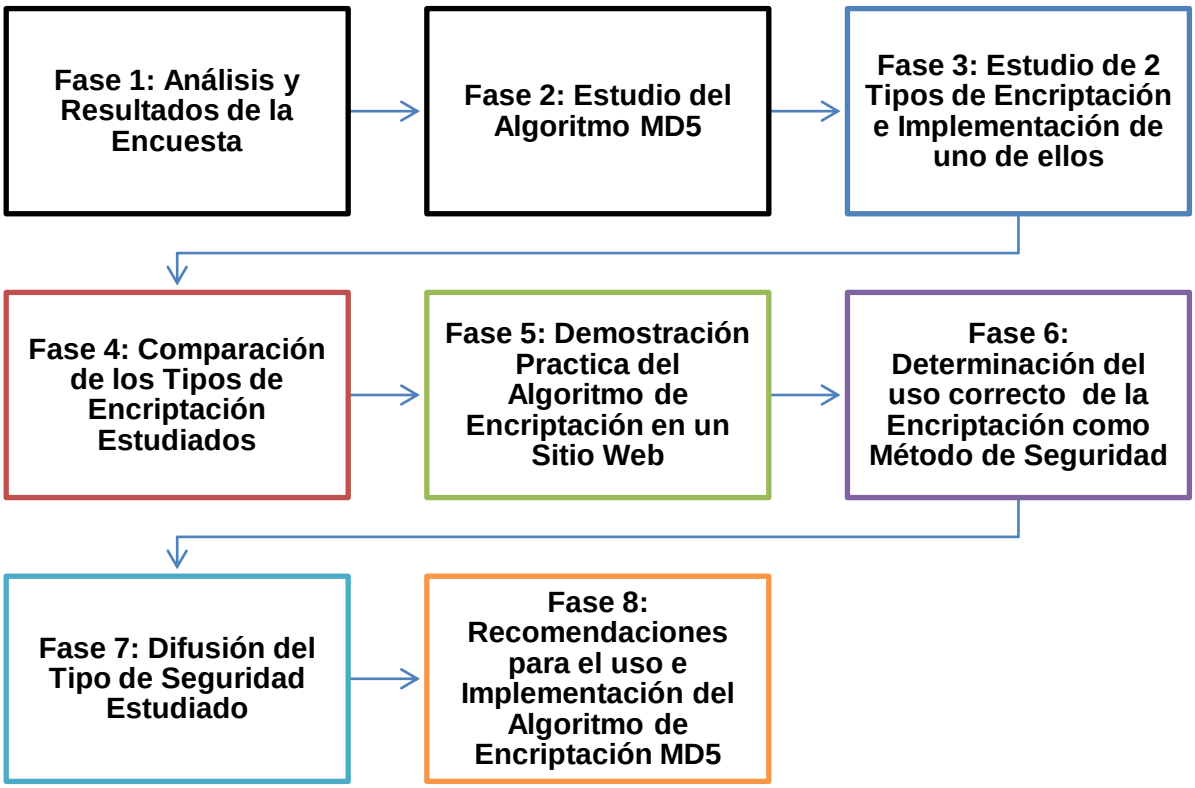
Si los datos de Inicio de sesión son correctos, nuestra información podrá ser visualizada con normalidad, y con esto podremos saber si nuestro proceso de Almacenamiento y Cifrado está funcionando con normalidad, pero sobre todo si es real la manera de brindar seguridad en Nuestros Datos.

En la Imagen podemos Observar el Campo de “Clave de Cuenta”, que esta transformada en muchos caracteres que no se parecen en nada a nuestra

Clave ingresada anteriormente, pero en realidad si es nuestra clave, lo que aparece allí es nuestro proceso de Encriptación, en pocas palabras nuestra clave Encriptada.

3.3 Proceso de Ingeniería

El desarrollo del proyecto se basará en la resolución consecutiva de las siguientes Fases divididas a través del Modelo Cascada.



Esquema 2: Proceso de Ingeniería

a) Análisis y Resultados de la Encuesta

Lo Primero a Realizar, será el estudio de los resultados obtenidos en la Encuesta, para saber si el conocimiento Informático de los encuestados tienen una amplia relación con lo que es seguridad informática y en especial el Algoritmo MD5 como método de cifrado de datos.

b) Fase 1: Estudio del Algoritmo MD5

En esta Fase, como primer paso, se estudiará lo que es el Algoritmo MD5 haciendo referencia a lo que es, en que consiste, las funcionalidades y forma de aplicación como Método de Seguridad.

c) Fase 2: Estudio de 2 Tipos de Encriptación e Implementación de uno de ellos

Según el Estudio Anterior, el siguiente paso será conocer 2 Tipos de Encriptación, estudiarlos y saber en qué consisten los mismos.

d) Fase 3: Comparación de los Tipos de Encriptación Estudiados

Luego del estudio de los Tipos de Encriptación, en esta fase se procederá a compararlos conjuntamente con sus características para saber cuál es el tipo ideal que se acoplará a nuestro Algoritmo de Cifrado.

e) Fase 4: Demostración Práctica del Algoritmo de Encriptación en un Sitio Web

Una vez que sepamos en que consiste nuestro Algoritmo de Encriptación y el Tipo que se complementará, lo siguiente que haremos es mostrar la Funcionalidad Practica que tiene este tipo de Seguridad en un Sitio Web, en cuanto a la protección de datos importantes como por ejemplo contraseñas.

f) Fase 5: Determinación del uso correcto de la Encriptación como Método de Seguridad

De acuerdo al paso anterior, lo que se hace es mostrar la funcionalidad de la Encriptación, pero en este paso se indicará la manera correcta de implementar la encriptación, esto relacionado con el código interno de nuestro sitio web.

g) Fase 6: Difusión del Tipo de Seguridad Estudiado

Al haber realizado el estudio del algoritmo Implementación y Demostración de su real funcionalidad, nuestro siguiente paso será difundir este tipo de seguridad informática, para esto nos basaremos en el uso de herramientas gratuitas como son Video tutoriales, Realización de Papers y Publicaciones en Blogs.

h) Fase 7: Recomendaciones para el uso e Implementación del Algoritmo de Encriptación MD5

Como parte final en este proceso se darán recomendaciones de cómo usar e implementar este Tipo de Seguridad en un Sitio Web, haciendo referencia con esto a los pasos que se deben seguir desde la estructuración del Sitio web hasta la identificación de los lugares Clave en donde se debe realizar el Cifrado de Datos.

CAPITULO IV

4. DESARROLLO

4.1 Fase 1: Análisis y Resultados de la Encuesta

1. **¿En su Negocio o Empresa el uso de internet forma parte de su labor Diaria?**

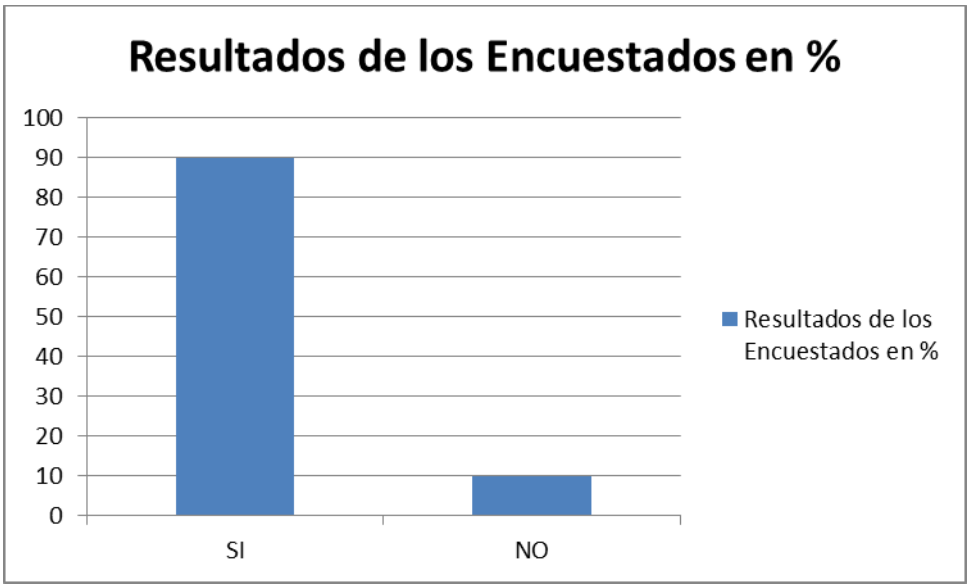


Gráfico 1: Resultados de la Primera Pregunta de la Encuesta

	SI	NO
N° de Encuestados	18	2
Resultados de los Encuestados en %	90	10

Tabla 2: Resultados de la Primera Pregunta de la Encuesta

En esta pregunta, las opiniones apuntaron un 90% por la respuesta “SI”, de esta manera se entiende que la mayoría de Encuestados usan el internet para sus labores diarias, en las que se destacan servicios de publicidad y transacciones diarias a través de la Red.

2. ¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?

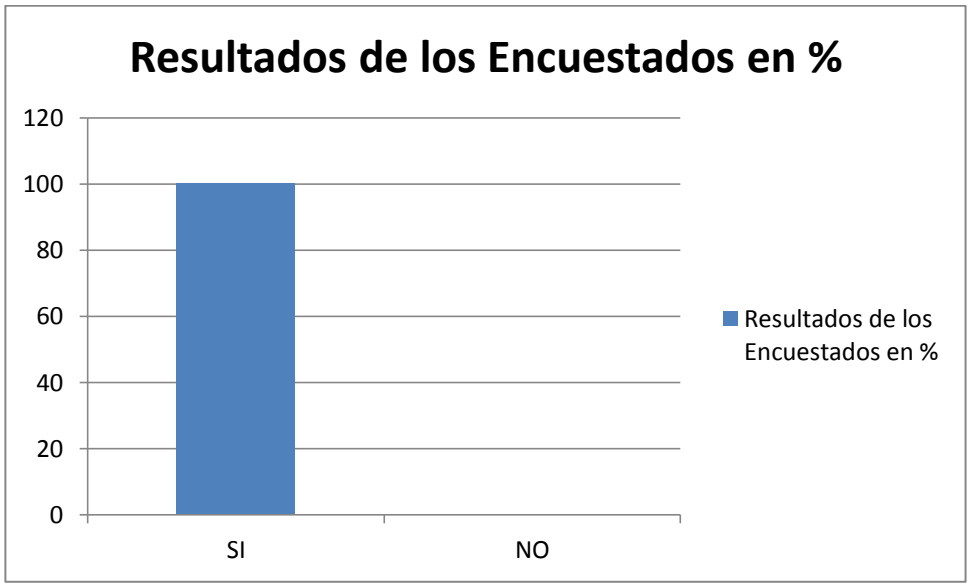


Gráfico 2: Resultados de la Segunda Pregunta de la Encuesta

	SI	NO
N° de Encuestados	20	0
Resultados de los Encuestados en %	100	0

Tabla 3: Resultados de la Segunda Pregunta de la Encuesta

En esta pregunta los resultados que mostro nuestra encuesta apunto claramente un 100% para un “SI”, lo cual nos indica que la gente de hoy en día y aún más aquellas personas que está ligadas al trabajo en Internet consideran que el robo de Información es algo Real, y por supuesto algo que no se debe tomar a la ligera, debido a las constantes evidencias de suplantación de Identidad y robos a través de internet que se han suscitado en la actualidad.

3. **¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?**

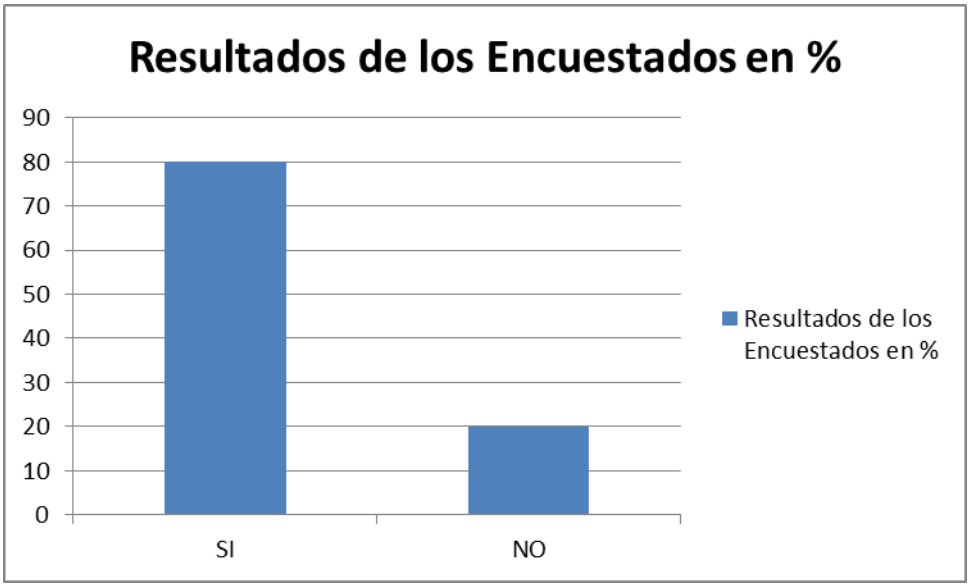


Gráfico 3: Resultados de la Tercera Pregunta de la Encuesta

	SI	NO
N° de Encuestados	16	4
Resultados de los Encuestados en %	80	20

Tabla 4: Resultados de la Tercera Pregunta de la Encuesta

Según la respuesta dada en la pregunta anterior por la gente, se complementa lógicamente con esta debido a que el 80% de encuestados consideran que “SI” han tenido en cuenta perder información, y un “NO” representado por un 20%.

Esto nos demuestra que entre los encuestados si hay una cultura de seguridad informática, y esto lógicamente ayuda a que las personas si opten por mejorar seguridades o simplemente buscar información sobre estas.

4. **Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:**

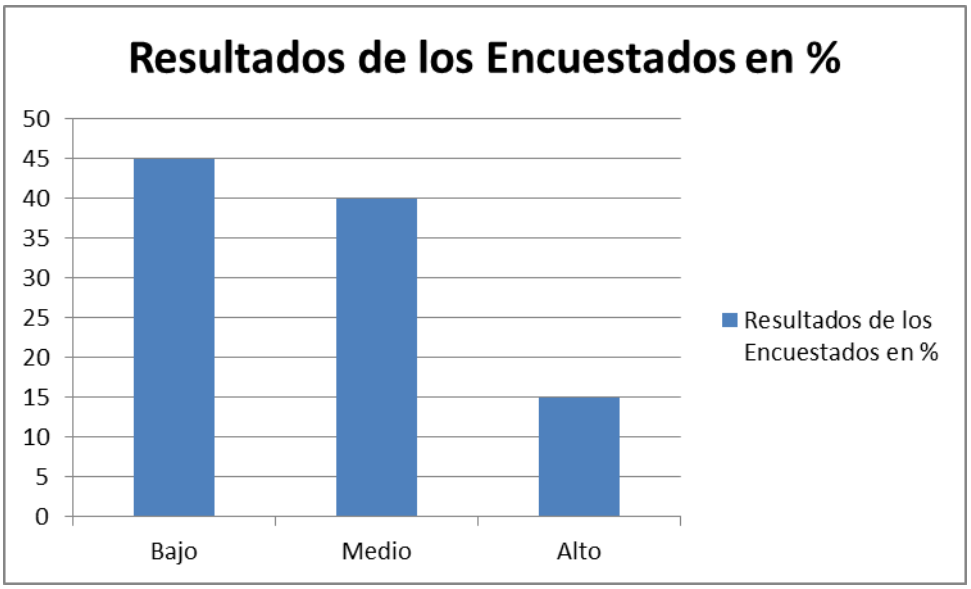


Gráfico 4: Resultados de la Cuarta Pregunta de la Encuesta

	Bajo	Medio	Alto
N° de Encuestados	9	8	3
Resultados de los Encuestados en %	45	40	15

Tabla 5: Resultados de la Cuarta Pregunta de la Encuesta

En la Pregunta 4 sobre conocimientos de Hackers y medidas de Seguridad los resultados de los encuestados reflejaron una opinión dividida, expresada de la siguiente manera:

Bajo 45%, Medio 40% y Alto 15%

De este modo podemos notar que no todas las personas poseen la misma cantidad de conocimiento que otras, y he aquí los resultados que necesitamos saber, pues en el bajo conocimiento es donde apuntaremos el desarrollo de este trabajo.

5. ¿Qué amenazas Informáticas conoce?

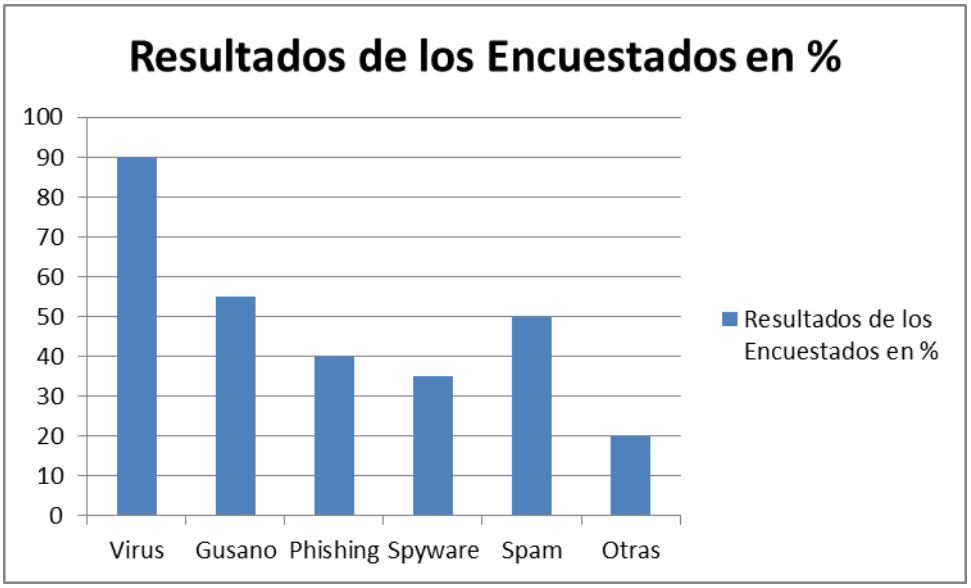


Gráfico 5: Resultados de la Quinta Pregunta de la Encuesta

Aquel conocimiento de amenazas informáticas, que se deseaba saber a través de las opiniones de los Encuestados se mostró de la siguiente manera:

	Virus	Gusano	Phishing	Spyware	Spam	Otras
N° de Encuestados	18	11	8	7	10	4
Resultados de los Encuestados en %	90	55	40	35	50	20

Tabla 6: Resultados de la Quinta Pregunta de la Encuesta

El mayor porcentaje de resultados se expresaron por parte de los “Virus”, aquellos malware tan molestosos e inclusive destructivos, que ya se encuentran en la mente de las personas por causa de su constante desarrollo y ataques a través de las redes informáticas.

6. **¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?**

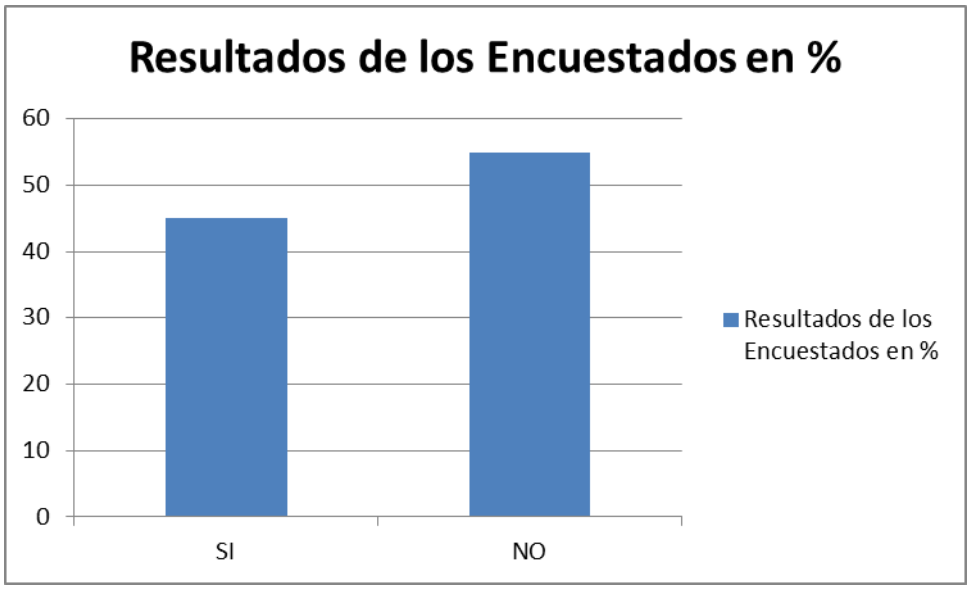


Gráfico 6: Resultados de la Sexta Pregunta de la Encuesta

	SI	NO
N° de Encuestados	9	11
Resultados de los Encuestados en %	45	55

Tabla 7: Resultados de la Sexta Pregunta de la Encuesta

De acuerdo a los presupuestos, las opiniones fueron divididas por la razón de que en muchas empresas no siempre se opta por gastos de seguridad, debido a que en nuestro medio no se conocen muchas herramientas que brinden seguridad o que busquen formas de mejorar y reducir costos de inversión.

7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?

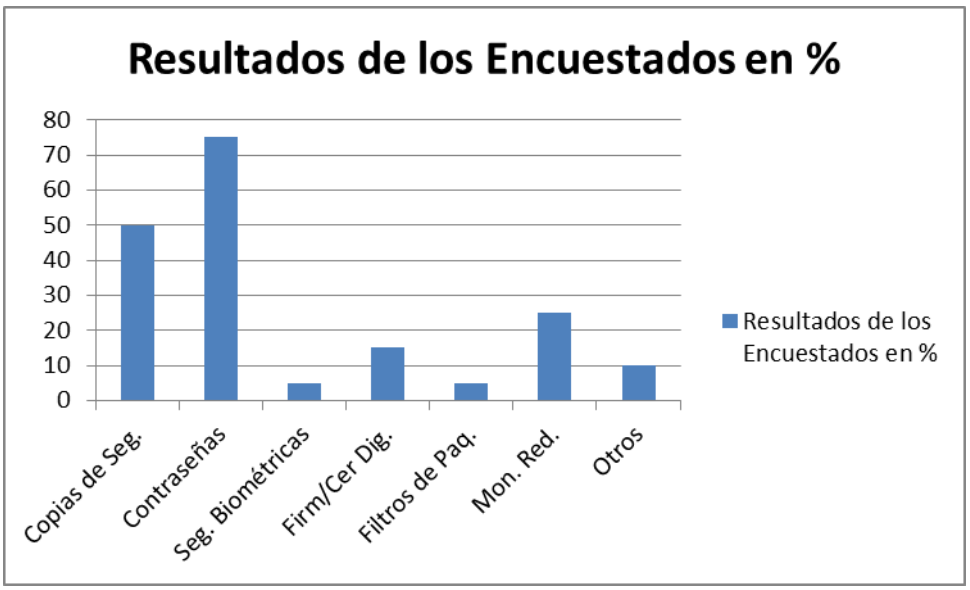


Gráfico 7: Resultados de la Séptima Pregunta de la Encuesta

	Copias de Seg.	Contraseñas	Seg. Biométricas	Firm/Cer Dig.	Filtros de Paq.	Mon. Red.	Otros
N° de Encuestados	10	15	1	3	1	5	2
Resultados de los Encuestados en %	50	75	5	15	5	25	10

Tabla 8: Resultados de la Séptima Pregunta de la Encuesta

Para esta pregunta se planteó varias opciones de respuesta, sobre medidas de seguridad, en las que se optó por dar sugerencias de gran costo como de forma sencilla generalizando de esta manera las respuestas para todo tipo de empresa.

Los Resultados reflejaron que claramente cuál es la respuesta que comúnmente es utilizada como medida de seguridad, las opiniones apuntaron al uso de “Contraseñas”, pues es una forma común de proteger datos y restringir accesos para personas inadecuadas.

8. **¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?**

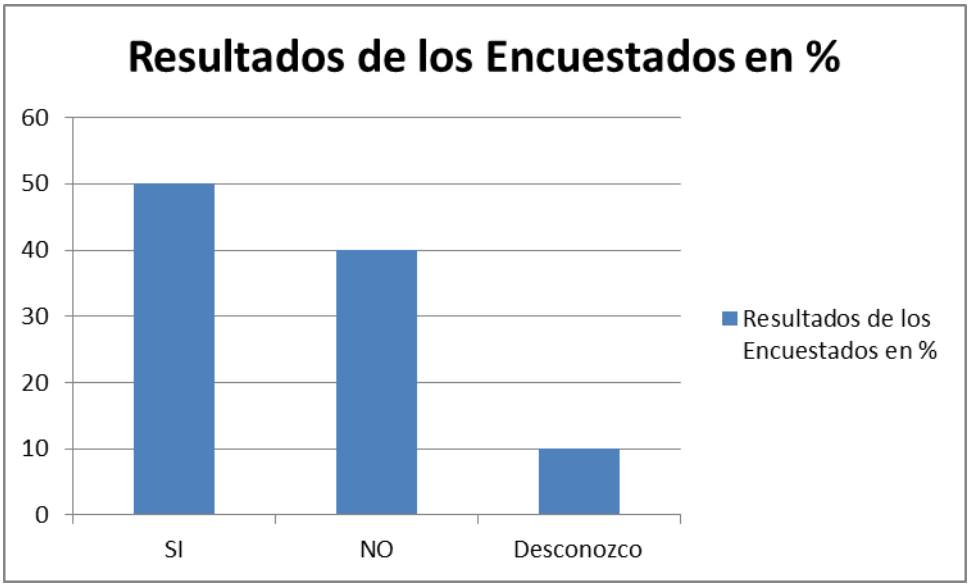


Gráfico 8: Resultados de la Octava pregunta de la Encuesta

Los resultados en esta pregunta se reflejan de la Siguiente manera:

	SI	NO	Desconozco
N° de Encuestados	10	8	2
Resultados de los Encuestados en %	50	40	10

Tabla 9: Resultados de la Octava pregunta de la Encuesta

En este sentido, las opiniones se mostraron un poco divididas, dándole mayor porcentaje a la respuesta de “SI”, lo que significa que los métodos de encriptación como medida de seguridad si son tomados en cuenta para la protección de datos.

9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash)?

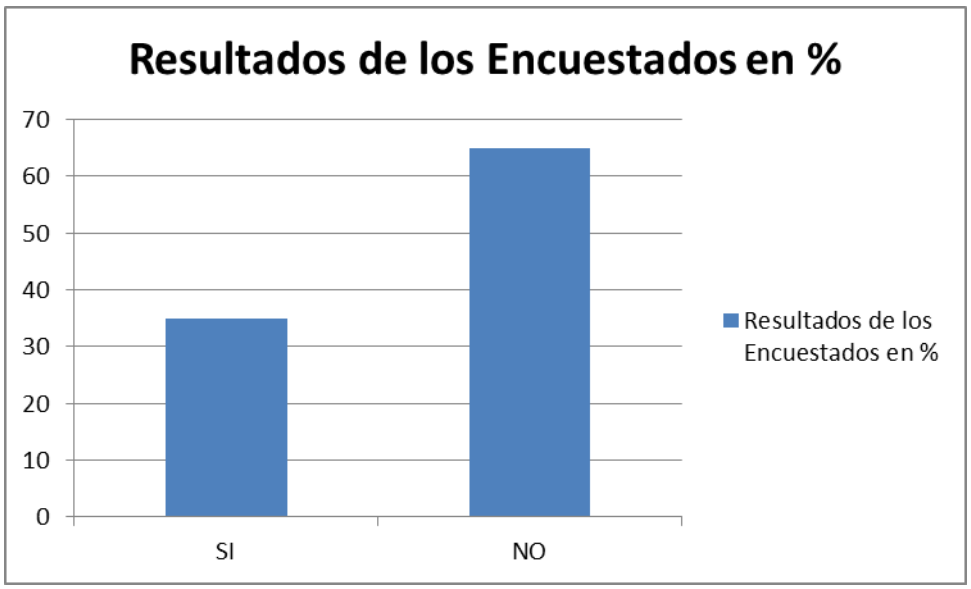


Gráfico 9: Resultados de la Novena Pregunta de la Encuesta

	SI	NO
N° de Encuestados	7	13
Resultados de los Encuestados en %	35	65

Tabla 10: Resultados de la Novena Pregunta de la Encuesta

En la Respuesta anterior se conoció que muchas empresas si optan por usar métodos de Encriptación para proteger datos, pero con relación a esta pregunta muchos de los Encuestados opinaron que no conocen la Encriptación MD5. Esto es razonable debido a que existen muchas formas de Encriptar y algoritmos que ayudan a la consecución de este cifrado.

10. **¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?**

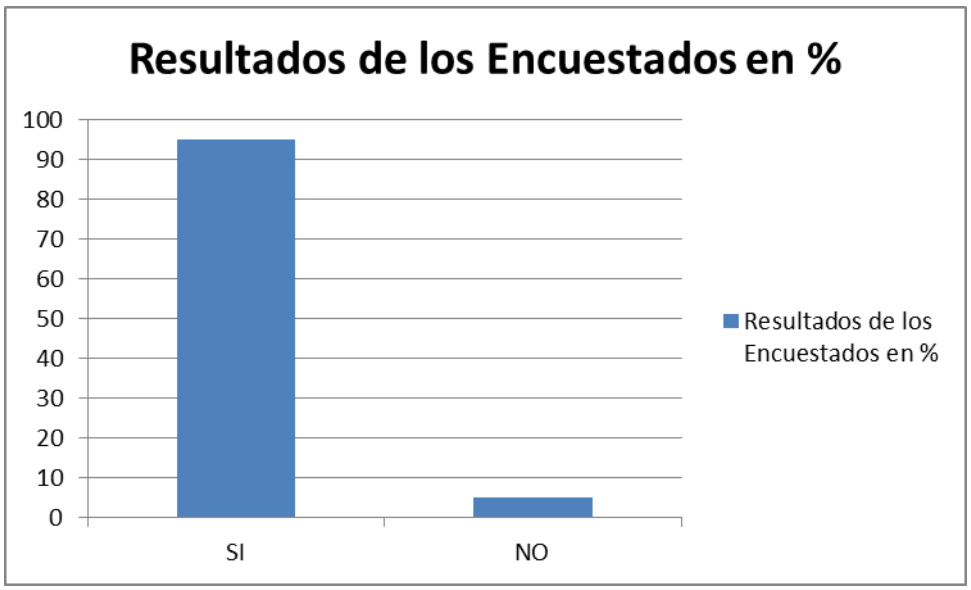


Gráfico 10: Resultados de la Décima Pregunta de la Encuesta

	SI	NO
N° de Encuestados	19	1
Resultados de los Encuestados en %	95	5

Tabla 11: Resultados de la Décima Pregunta de la Encuesta

De forma complementaria con la respuesta anterior que la gente dijo sobre el no conocimiento de Encriptación MD5, en este caso, sobre la pregunta 10 se optó por consultar si se desea conocer acerca de esta Encriptación, lo cual mostro un notable interés con un 95%.

4.2 Fase 2: Estudio del Algoritmo MD5

MD5 se encuentra dentro de lo que son las funciones Hash, conocidas como los métodos para generar claves o llaves que presenten de manera casi unívoca a un documento, registro o archivo. Resume o identifica un dato a través de la probabilidad.

Es uno de los algoritmos de reducción criptográficos diseñados por el profesor Ronald Rivest del MIT (Massachusetts Institute of Technology, Instituto Tecnológico de Massachusetts). Fue desarrollado en 1991 como reemplazo del algoritmo MD4 después de que Hans Dobbertin descubriese su debilidad.

Produce hashes de 128 bits y se lo estudia principalmente por la sencillez del algoritmo.

Ejemplo:

- ✓ MD5("Esto sí es una prueba de MD5") = e99008846853ff3b725c27315e469fbc
- ✓ MD5("Esto no es una prueba de MD5") = dd21d99a468f3bb52a136ef5beef5034
- ✓ MD5("") = d41d8cd98f00b204e9800998ecf8427e

- **Funcionamiento básico**
  - ✓ Un mensaje se convierte en un bloque múltiplo de 512 bits, añadiendo bits al final si es necesario
  - ✓ Con los 128 bits de cuatro vectores iniciales de 32 bits cada uno y el primer bloque del mensaje de 512 bits se realizan diversas operaciones lógicas
  - ✓ La Salida de esta operación (128 bits) se convierte en el nuevo conjunto de 4 vectores y se realiza la misma función con el segundo bloque de 512 bits, y así hasta el último bloque del mensaje
  - ✓ El resumen corresponde a los últimos 128 bits de estas operaciones.

MD5 comienza rellenando el mensaje a una longitud congruente en módulo 448 modulo 512. Es decir la longitud del mensaje es 64 bits menos que un entero múltiplo de 512. El relleno consiste en un bit en 1 seguido por cuantos bits en 0 sean necesarios. La longitud original del mensaje es almacenada en los últimos 64 bits del relleno.

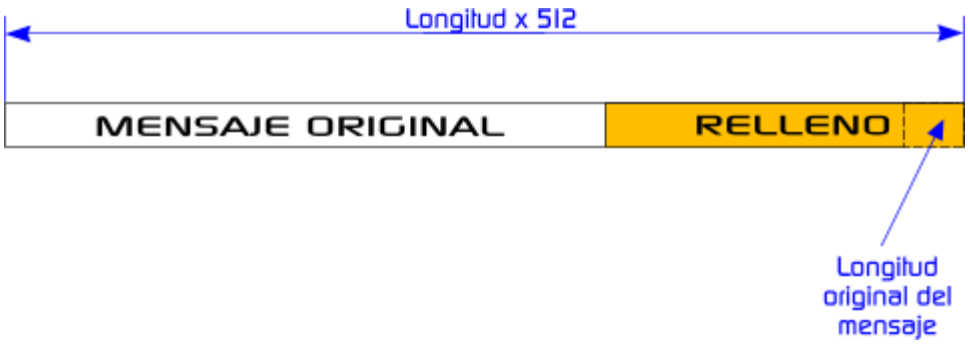


Imagen 22: Funcionamiento Básico del Algoritmo MD5

Adicionalmente se inicializa, con un valor fijo, un buffer de 128 bits. Este buffer puede verse como 4 registros de 32 bits (A,B,C,D) y son inicializados con los siguientes valores hexadecimales:

A=67452301; B=EFCDAB89; C=98BADCFE; D=10325476

Durante varias rondas de procesamiento el algoritmo toma bloques de 512 bits de la entrada y los mezcla con los 128 bits del buffer. Este proceso es repetido hasta que todos los bloques de entrada han sido consumidos. El valor resultante en el buffer es el hash del mensaje.

- **Aplicaciones de MD5**

Los resúmenes MD5 se utilizan extensamente en el mundo del software para proporcionar la seguridad de que un archivo descargado de Internet no se ha alterado.

Este Método de encriptación MD5 por la facilidad de su uso y la sencillez del mismo, se lo usa de forma común en lo que son los sitios web. Gracias a su popularidad y seguridad se lo ha tomado como medida de protección de datos importantes como por ejemplo “claves de seguridad” para usuarios.

- **Seguridad**

Si bien se lo toma como una herramienta de seguridad en sitios web, su seguridad radica en que puede Encriptar datos pero no Desencriptarlos, lo cual garantiza aún más la seguridad de los datos.

La encriptación de este modo consiste en que solo aquel que creo la clave original podrá hacer uso de ella. De este modo la seguridad está enfocada a la manipulación del usuario de forma secreta y confidencial.

En sí, la idea de la Encriptación a través de este algoritmo que genera hash referencia a lo que es el uso en Páginas Web, se lo utiliza para encriptar una clave original y esta sea guardada en otro formato o cadena que represente la clave y esta se utilice para comparación y validación de Usuarios.

4.3 Fase 3: Estudio de 2 Tipos de Encriptación e Implementación de uno de ellos

4.3.1 Encriptación Simétrica

También conocida cono Encriptación de clave secreta, que puede ser un número, una palabra o simplemente una cadena de letras aleatorias, se aplica al texto de un mensaje para cambiar el contenido en un modo determinado. Esto podría ser tan sencillo como desplazando cada letra a un número de posiciones en el alfabeto. Siempre que el remitente y destinatario conocen la clave secreta, puede cifrar y descifrar todos los mensajes que utilizan esta clave.

Imagen 23: Proceso Encriptación Simétrica

Consiste en usar una sola Clave para cifrar el mensaje y la misma Clave para poder descifrarlo, de este modo, el cifrado trabaja en un solo sentido y la garantía de su funcionamiento es que la clave debe ser protegida y usada únicamente por el o los Usuarios de confianza.

El principal problema de seguridad reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Por lo tanto se

tiene que buscar también un canal de comunicación que sea seguro para el intercambio de la clave.

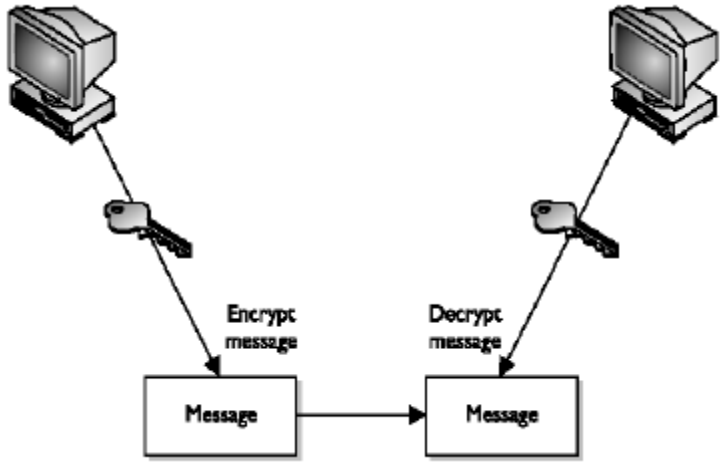


Imagen 24: Encriptación Simétrica

- **Ventajas**

✓ La velocidad de Cifrado es muy alta.

✓ Con Claves pequeñas se obtiene alta seguridad.

✓ La no linealidad del algoritmo hace que el único ataque factible sea fuerza bruta.

- **Desventajas**

✓ **Mala Distribución de claves**, no existe posibilidad de enviar de forma segura una clave a través de un medio inseguro.

✓ **Mala Gestión de Claves**, crece el Número de claves secretas en una proporción igual a n2 para un valor n grande de usuarios lo que imposibilita usarlo.

✓ **No tiene Firma Digital,** es posible autenticar el mensaje mediante una marca, pero no es posible firmar digitalmente el mensaje.

4.3.1.1 Uso de la Encriptación Simétrica

Un ejemplo del uso de este método es la Protección de Contraseñas en Sitios Web que funcionan con Servidores Web y Servidores Locales de Empresas que necesitan proteger datos importantes.

Esta encriptación representa un gran a porte a la velocidad de trabajo en los sitios web, ya que el cifrado de los datos es muy rápido y se obtiene alta seguridad con claves pequeñas.

Su uso en Sitios Web está enfocado en lo que es la protección de Contraseñas de usuarios y transacciones en Comercio Electrónico, en donde muchos datos importantes como claves de seguridades, números de tarjetas de crédito, Cédulas de Identidad, etc., pueden ser robados si es que no son protegidos de forma correcta.

4.3.2 Encriptación Asimétrica

Otro método de encriptación es el que se basa en el uso de dos Claves para el envío de mensajes.

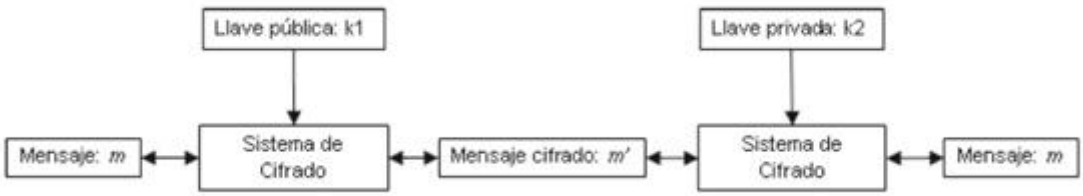


Imagen 25: Proceso Encriptación Asimétrica

Consiste en Cifrar el mensaje con una Clave Pública y Descifrarlo con una clave Privada o viceversa, permitiendo mejorar la seguridad en cuanto a la Autenticidad y Legalidad de quien envía y recibe el mensaje.

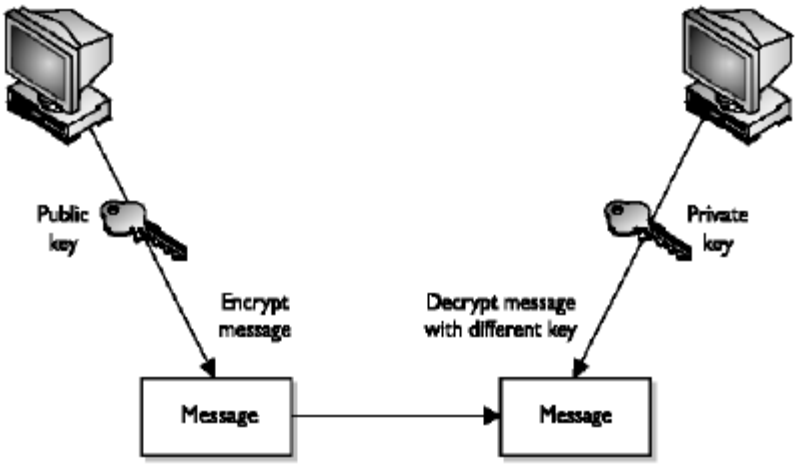


Imagen 26: Encriptación Asimétrica

Cualquier mensaje (texto, archivos binarios o documentos) que están cifrados mediante clave pública sólo puede descifrarse aplicando el mismo algoritmo, pero mediante la clave privada correspondiente. Cualquier mensaje que se cifra mediante la clave privada sólo puede descifrarse mediante la clave pública correspondiente.

Esto significa que no es necesario preocuparse pasando claves públicas a través de Internet (las claves se supone que para ser públicos). Un problema con el cifrado asimétrico, sin embargo, es que es más lento que el cifrado simétrico. Requiere mucha más capacidad de procesamiento para cifrar y descifrar el contenido del mensaje.

- **Ventajas**
  - ✓ **Identidad,** reconoce unívocamente a un emisor como autor del mensaje.
  - ✓ **Integridad,** el documento no puede ser alterado de forma alguna durante la transmisión.
  - ✓ **Confidencialidad**, solo las partes puedan leer el mensaje o documento (si fuera el caso).

- **Desventajas**
  - ✓ Velocidad baja
  - ✓ En ciertos casos es costosa, por causa de entidades certificadoras cuando se quiere tener una Firma Electrónica.

4.3.2.1 Uso de la Encriptación Asimétrica

La Firma Digital, es uno de los ejemplos que representan el funcionamiento del método, ya que este garantiza mayor seguridad con el uso de dos Claves, una para el firmante y otra para quien recibe el mensaje.

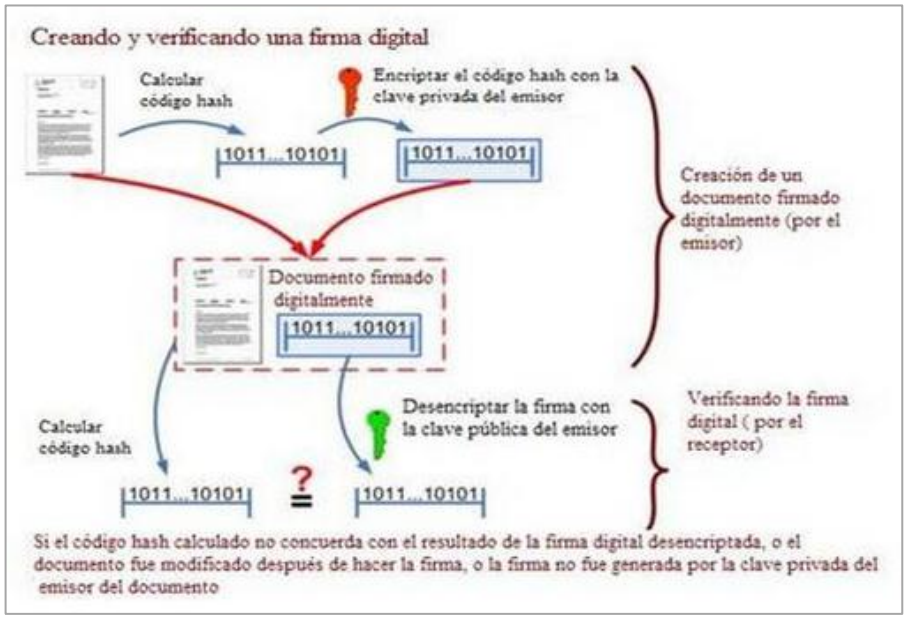


Imagen 27: Creación de Firma Digital

Es la equivalencia digital de la firma manuscrita, tiene la misma validez legal y se encuentra amparada por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Desde el punto de vista técnico, la firma es un conjunto de datos digitales que se añaden a un archivo digital y que se obtienen del cifrado del mismo mediante programas computacionales.

Ayudan a garantizar la Autenticidad del Emisor para posibles tramites online, representando esto Legalidad en el Proceso.

4.3.3 Tipo de Encriptación a Implementar

De acuerdo a las características y la sencillez de su uso para las personas comunes, el tipo a implementar es la “Encriptación Simétrica”, ya que maneja una sola clave.

Al manejar solo una clave, es ideal su uso, para los procesos que se realizan en un Sitio Web, ayudando a dar seguridad y mejorar la velocidad de las transacciones.

Entre los usos más comunes en un sitio Web tenemos:

- ✓ Protección de contraseñas en el registro de Usuarios.
- ✓ Protección de claves de Tarjetas de Crédito cuando se usa para comercio electrónico.

- ✓ Protección de Cédulas o Identificadores de Personas cuando se realizan trámites electrónicos.
- ✓ Protección de datos importantes en una Base de Datos.
- ✓ Seguridad a los datos cuando son procesados durante el flujo de ingreso y almacenamiento de los mismos.

4.4 Fase 4: Comparación de los Tipos de Encriptación Estudiados

Características	Cifrado Simétrico	Cifrado Asimétrico
Seguridad	Representa Confidencialidad	Representa Confidencialidad
Autenticación	Parcial	Total
Firma Digital	Sin Firma Digital	Con Firma Digital
N° de Claves	Una Clave (Emisor – Receptor)	2 Claves (Pública y Privada o viceversa)
Tamaño de Claves	Longitud Pequeña	Longitud Grande
Velocidad	Alta Velocidad	Baja Velocidad
Uso	En cifrado de mucha Información	En Firma e Intercambio de Claves
Ataques por Fuerza bruta	Débil	Resistente a causa del uso de dos claves
Costo	Bajo	Alto por causa de las Entidades Certificadoras

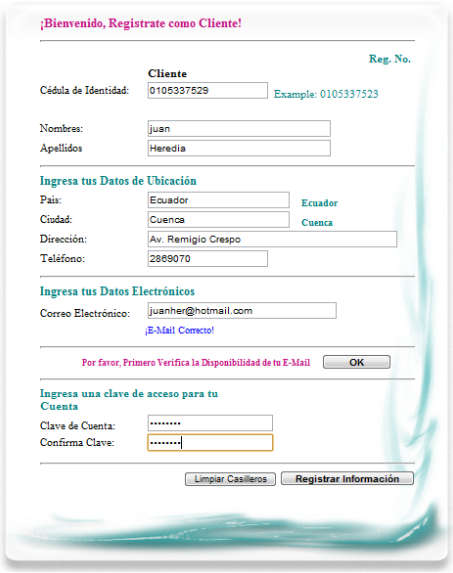
Tabla 12: Cuadro Comparativo de los tipos de Encriptación

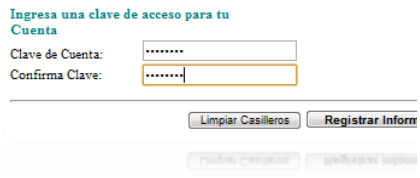
4.5 Fase 5: Demostración Práctica del Algoritmo de Encriptación en un Sitio Web

La Encriptación como método de seguridad es fundamental su uso en nuestra actualidad, por causa de constantes robos de datos y suplantación de identidades en sitios web que se suscitan a diario. Esta seguridad es recomendable para proteger la información de los usuarios cuando naveguen en un sitio web y aún más cuando estos Sitios son Dinámicos.

Para la demostración se procederá a realizar un ejemplo de la Encriptación MD5 con una clave (simétrico), que nos servirá para proteger la contraseña de un Usuario al Registrarse.

a) Ingreso de datos del Usuario para Registrarse





El Usuario llena sus datos en el formulario e ingresa una clave que él conoce “juan1234”, de esta manera solo él sabe cuál es la clave con la que se registró.

Imagen 28: Ingreso de datos a un Formulario de Registro

b) Proceso de Encriptación

Cuando el Usuario da Click en “Registrar”, el proceso de Encriptación, realiza la conversión del dato normal al dato Encriptado.

```
Me.TxtPasword.Text = (cifrado.MD5Hash(Me.TxtPasword.Text))
```

Si el Proceso de Registro es realizado de Forma correcta por el Sistema recibirá el usuario un Mensaje de confirmación.

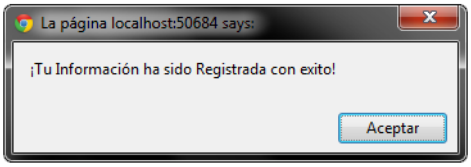


Imagen 29: Finalización de un Registro de Datos

c) Confirmación del Registro en el Sitio Web

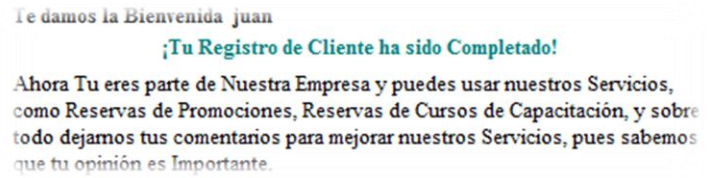


Imagen 30: Mensaje de Registro

El mensaje de Bienvenida da la confirmación de que el registro se ha realizado de forma completa, pero hasta el momento esto no es nada del otro mundo. La seguridad que se ha implementado, se realiza internamente y los usuarios no notan ningún cambio, tan solo ellos saben que su clave es la que ellos ingresaron y ninguna otra.

d) Verificación del Dato en la Base de Datos

Como se puede ver en la imagen siguiente, hay un pasword o contraseña que pertenece al usuario “juan”, esta contraseña es la que ha sido encriptada, para proteger la contraseña original del Usuario “juan”.

Cedula	Nombre	Email	Pasword
0105337529	juan	juanher@hotmail.com	c7f626ad40317f4dc7b295c6f04c850d

Imagen 31: Verificación de la clave Encriptada en la Base de Datos

Ahora bien, quizá se piense que al transformarse la contraseña ya no se podrá usar en el sitio Web pues esta ha cambiado notablemente.

En realidad el Usuario si podrá usar su clave original siempre y cuando no la olvide, ya que cuando se verifica la clave original encriptándola nuevamente,

esta se compara con la ya almacenada en la Base de Datos, si las dos contraseñas coinciden, el usuario es identificado y se le dará acceso a sus datos, si ese fuera el caso.

4.6 Fase 6: Determinación del uso correcto de la Encriptación como Método de Seguridad

La Encriptación MD5 es ideal para la protección de datos pequeños ya que solo se puede encriptar pero no realizar el proceso contrario (desencriptar), esto ayuda a que los datos importantes no puedan ser vulneradas con facilidad y solo usados por el Usuario correcto.

Para poder agregar este complemento de seguridad a nuestro sitio web habrá que tener bien definido la estructura del mismo, como por ejemplo tres partes importantes:

- ✓ Las Páginas en donde voy hacer transacciones dinámicas con usuarios en donde involucre petición de datos personales.
- ✓ Una programación bien probada y lista para la funcionalidad de nuestro Sitio Web.
- ✓ Una Base de datos ya lista para almacenar los datos.

Estos tres requerimientos son de suma importancia pues son la estructura de un sitio con el que se pretende trabajar de forma eficiente.

Cuando se tenga ya la idea de cómo va a trabajar nuestro Sitio Web, también debemos saber donde aplicaremos la Seguridad de Encriptación, para esto

debemos estar al tanto de cuáles podrían ser los peligros que pudiera tener nuestro sitio en cuanto a hackers o delincuentes informáticos, como por ejemplo espionaje o suplantación de identidad, que es lo que está de moda en la actualidad.

Este método de seguridad se debe emplear solo para la protección de datos de suma importancia como claves de tarjetas, cédulas, identificadores personales, etc.

La manera correcta de aplicar la encriptación es la siguiente:

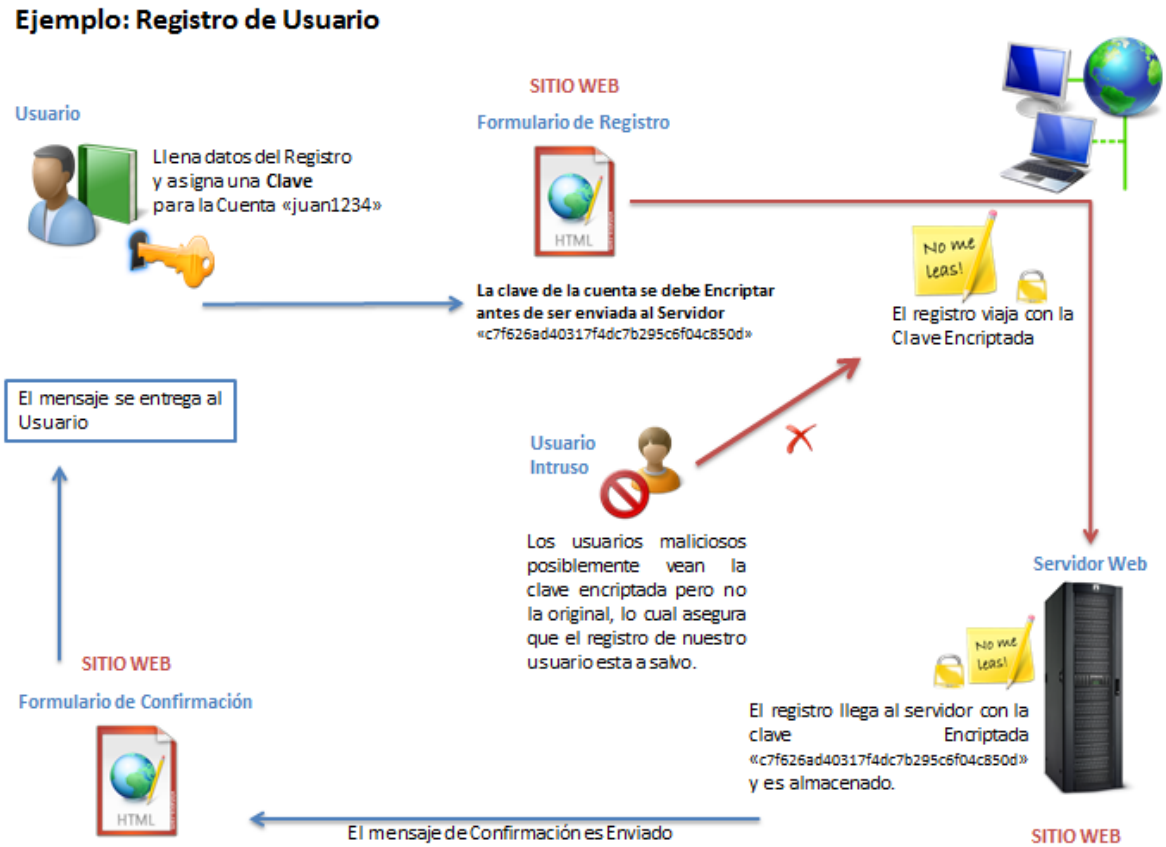


Imagen 32: Proceso de Registro de un Usuario usando la Encriptación

Posteriormente para que el usuario pueda acceder a la cuenta en la que se registró debería realizarlo de esta manera:

Imagen 33: Proceso del uso de la Cuenta Registrada con Encriptación

En este ejemplo se ha mostrado la manera de cómo deben ser tratados los datos antes de su almacenamiento, los datos importantes deben ser Encriptados antes y durante el proceso de almacenamiento, para que no puedan ser robados por usuarios inadecuados.

Si bien este ejemplo muestra la idea de la seguridad de la Encriptación, esta no solo se puede usar en un proceso de registro de usuarios, también es común usarla para propósitos de Comercio Electrónico, en los que generalmente se

usan Números de tarjetas de Crédito, los cuales también deben ser protegidos pues representan un valor importante para nuestros usuarios.

La seguridad ante todo, las maneras de implementar seguridad en un sitio va de acuerdo a las necesidades que se tenga, y si se trata de protección de datos importantes en un proceso transaccional, la Encriptación es la Ideal.

4.7 Fase 7: Difusión del Tipo de Seguridad Estudiado

La seguridad en un Sitio Web es una necesidad que muchas personas tienen, tanto los desarrolladores como las personas que usan estas páginas web están conscientes de que en internet hay peligros que no se deben tomar a la ligera y aún más cuando los sitios web manejan bases de datos de gran importancia ya sea de servicios informativos o Comercio Electrónico.

El proceso de encriptación es más que un complemento de seguridad, es una herramienta que garantiza la autenticidad y confidencialidad de los datos que se registran en un sistema.

Para difundir y dar a conocer al público este tipo de seguridad, se usará el Internet conjuntamente con los medios más populares medios de difusión de información, como lo son; los Blogs, Video Tutoriales en YouTube, y Papers de Información para compartirlos con otros usuarios ya sea en páginas web académicas o vía correo electrónico.

- ✓ **Blogs:** Se los conoce como páginas web en donde uno o más autores desarrollan contenidos para compartirlos. Una de las ventajas que representa usar esta herramienta, es que el autor del artículo puede recibir comentarios y de las misma manera responderlos, creando de esta manera un dialogo entre lector y escritor del tema en cuestión.

- ✓ **Video Tutoriales:** Es uno de los medios más comunes en los que las personas transmiten ejemplos o tutorías sobre algún tema específico, de una manera más completa y real, ya que se realiza en video. Para realizar este tipo de difusión de información, lo único que se necesita es crear una cuenta en YouTube y subir a la cuenta un video que realicemos, todo esto de forma gratuita y sencilla.

- ✓ **Papers:** Son artículos científicos de información sobre algún tema en especial en donde se pone de manifiesto la capacidad del investigador. Se los usa generalmente para exponer ante los lectores un trabajo investigativo basado en recopilación de datos de otras fuentes con la meta de analizarlos y fundamentar su teoría.

Si el propósito es difundir nuestra teoría de sobre Encriptación como medida de Seguridad en sitios web, estas herramientas de difusión son ideales, debido a su popularidad y alto índice de consulta. A través de estas se brindará el conocimiento obtenido sobre seguridades y sitios web, con el fin de aportar al desarrollo académico de las personas.

4.8 Fase 8: Recomendaciones para el uso e Implementación del Algoritmo de Encriptación MD5

Este método de seguridad ya sabemos que se lo usa para proteger los datos importantes, pero es adecuado que sepamos cómo implementarla y en qué lugar de nuestro sitio web.

4.8.1 Recomendaciones

La recomendación más adecuada que se puede hacer para el uso de esta seguridad, es encriptar los datos antes de que sean almacenados en nuestra base de datos, para que durante el proceso de almacenamiento el dato no pueda ser robado y manipulado.

Para poder implementar esta seguridad previamente se recomienda contar con lo siguiente:

- ✓ Nuestro Sitio Web ya creado y programado con su estructura de Páginas y vínculos de comunicación entre las mismas.
- ✓ Base de Datos lista para almacenar datos
- ✓ Software Instalado para el trabajo con este tipo de páginas web ya sea Dreamweaver, Visual .NET u otro Software que permita desarrollar Siitoes Web.

4.8.2 Tarjetas C.R.C. (Clase, Responsabilidad y Colaboración)

a) Registro de Usuario (Cliente)

Historia de Usuario 1: Registro de Usuario

Nombre de Clase: Usuario	
Responsabilidad	**Colaborador**
• Ingresa sus Datos: Cedula, Nombres, Apellidos, Ciudad, País, Teléfono, Correo Electrónico, Clave de Acceso. • Validación del Correo Electrónico • Encriptación de Contraseña	Administrador

Tarjeta C. R. C. 1: Registro de Usuario

b) Visualización de Registro de Usuario (Cliente)

Historia de Usuario 2: Visualización de Registro de Usuario

Nombre de Clase: Usuario	
Responsabilidad	**Colaborador**
• Ingresa sus Datos de Inicio de Sesión: ✓ Cedula ✓ Correo Electrónico ✓ Clave de Acceso • Encriptación de Contraseña • Validación de datos • Comprobación de Registro	Administrador

Tarjeta C. R. C. 2: Visualización de Registro de Usuarios

4.8.3 Implementación de Encriptación MD5 en sitios Web hechos en PHP

PHP es lo que llamamos un lenguaje de programación del lado del servidor, esto significa que el código se interpreta en el servidor y no en el ordenador del

usuario. Es uno de los lenguajes más conocidos y destacados en el mundo de los desarrolladores web, por ser software libre y su rapidez de trabajo.

En PHP el algoritmo MD5 ya viene incorporado por defecto y lo único que hay que hacer antes de almacenar una contraseña es poner la línea de código para Encriptarlo como lo vemos en el siguiente ejemplo:

```
<?
$contrasena = md5($contrasena);
?>
```

Forma rápida y sencilla, que Encripta la clave en un solo sentido, esto quiere decir que la clave se Encripta pero no se puede desencriptar.

4.8.4 Implementación de Encriptación MD5 en Sitios Web hechos en Visual .NET (ASPX)

Para implementar esta medida de seguridad es recomendable tener preparados los siguientes requerimientos:

- ✓ Nuestra Base de Datos ya configurada
- ✓ El Sitio Web ya Estructurado
- ✓ Formularios en donde Realizar la codificación

4.8.4.1 Codificación e Implementación

Lo que se realizará ahora es codificar nuestro proceso de Encriptación, para esto usaremos lo siguiente:

- ✓ Una Clase que Generará la Encriptación MD5
- ✓ Un Formulario de Registro de Usuarios
- ✓ Una Interfaz de Bienvenida para un Inicio de sesión
- ✓ Un Formulario que visualice nuestros Datos Guardados

4.8.4.1.1 Creación de la Clase de Encriptación

Una vez que tenemos ya la idea de donde Implementar nuestra Encriptación lo que debemos hacer es crear una Clase que contendrá nuestro algoritmo de Cifrado, la cual podremos llamar(usar) en cualquier formulario del Sitio Web para realizar procesos de Cifrado.

A la Clase la llamaremos “Cifrado” y le Agregaremos el siguiente Código:

```
Imports System
Imports System.Data
Imports System.Data.SqlClient
Imports System.IO
Imports System.Text
Imports System.Security.Cryptography
Public Class Cifrado
    Inherits cmpEntidad

    ' Encripta una cadena de texto usando el algoritmo de
encriptacion de hash MD5.
    ' el "Message Digest" es una encriptacion de 128-bit y es
usado comunmente para
    ' verificar datos chequeando el "Checksum MD5", mas
informacion se puede
    ' encontrar en: http://www.faqs.org/rfcs/rfc1321.html

    ' cadena conteniendo el string a hashear a MD5.
    ' Una cadena de texto conteniendo en forma encriptada la
cadena ingresada.
    Public Function MD5Hash(ByVal Data As String) As String
        Dim md5 As MD5 = New MD5CryptoServiceProvider()
        Dim hash As Byte() =
md5.ComputeHash(Encoding.UTF8.GetBytes(Data))

        Dim stringBuilder As New StringBuilder()

        For Each b As Byte In hash
            stringBuilder.AppendFormat("{0:x2}", b)
        Next
        Return stringBuilder.ToString()
    End Function

End Class
```

Tabla 13: Código Fuente Clase Cifrado MD5

“Cabe recordar que todos estos algoritmos de encriptado solo obtienen un hash del string original, y no es reversible. Por lo tanto si lo que buscas es luego desencriptar esto debes utilizar otros algoritmos, por ello también hace que éstos sean más seguros al no poder hacer el reverso.” (Snak, 2010)

4.8.4.1.2 Codificación del Registro de Usuarios

Para realizar la Codificación previamente se tendrá que crear el Formulario de Registro, y Adecuarlo similarmente al Diseño de la interfaz que se mostró en el paso de Diseño anteriormente.

```
Inserción de código en el Botón “Registrar”

Try
      Dim objCli_T_Ced As New ReglasNegocio.ClsClientes
      Dim dsc1Ced As Data.DataSet
      dsc1Ced = objCli_T_Ced.TraerxCedula_Clientes(Me.TxtCedula.Text)

        If dsc1Ced.Tables(0).Rows.Count > 0 Then
        Response.Write("<script> alert ('¡Lo Sentimos el Registro no
se puede completar, al parecer esta Cédula de Cliente ya ha sido
Registrada!') </script>")
                Else

       Dim cifrado As New ReglasNegocio.Cifrado
       Dim objClientes As New ReglasNegocio.ClsClientes

       Me.TxtPasword.Text = (cifrado.MD5Hash(Me.TxtPasword.Text))


objClientes.Agregar_Clientes(Me.LblNo_Registro.Text,
Me.TxtCedula.Text, Me.TxtCodUsuario.Text, Me.TxtNombre.Text,
Me.txtApellido.Text, Me.TxtTelefono.Text, Me.TxtPais.Text,
Me.txtCiudad.Text, Me.TxtDireccion.Text, Me.TxtEmail.Text,
Me.TxtPasword.Text, Me.lblFecha.Text, Me.TxtCod_Activacion.Text,
Me.LblEstado_Cliente.Text)
                    Response.Write("<script> alert ('¡Tu Información
ha sido Registrada con exito!') </script>")

                    'Cerramos conexion
                    cifrado.CerrarConexion()
                    cifrado = Nothing

                    objClientes.CerrarConexion()
                    objClientes = Nothing

                    Server.Transfer("WFClientes_Activacion.aspx")
          End If
```

```
    'Cerramos conexion
     objCli_T_Ced.CerrarConexion()
     dsc1Ced = Nothing

 Catch ex As Exception
 Me.LblMsnError.Focus()
 Me.LblMsnError.Text = "ERROR: " & ex.Message.ToString
 End Try
```

Tabla 14: Código Fuente del Registro del Usuario

4.8.4.1.3 Codificación de Visualización de Registro del Usuario

Para esta operación, se trabajará con dos Formularios, el de Bienvenida de Registros y el de Visualización de Registros.

1) Bienvenida de Registros

En esta Codificación lo que se va a realizar es lo siguiente:

- ✓ Receptar los datos de ingreso del usuario para Iniciar Sesión
- ✓ Al receptar los datos el Sistema Encriptará la Contraseña
- ✓ Los Tres Datos de Ingreso se consultarán en la Base de Datos para verificar su Existencia
- ✓ Si los Datos existen el Sistema permitirá el Acceso y visualizará la Información del Usuario.

```
Inserción de código en el Botón "Ingresar"

Try
Dim objClientes As New ReglasNegocio.ClsClientes
Dim dsc_Cliente As Data.DataSet
Dim Encrip_Cliente As New ReglasNegocio.ClsEncriptador
Dim Cifrado As New ReglasNegocio.Cifrado

dsc_Cliente =
objClientes.TraerxCedula_Clientes(Me.TxtCedulaIngreso.Text)

If dsc_Cliente.Tables(0).Rows.Count > 0 Then

Me.TxtPasword.Text = Cifrado.MD5Hash(Me.TxtPasword.Text)

                'Comprobamos los datos de Ingreso
```

```
Try

If Me.TxtCedulaIngreso.Text =
dsc_Cliente.Tables(0).Rows(0).Item("Cedula") And
Me.TxtMailIngreso.Text = dsc_Cliente.Tables(0).Rows(0).Item("Email")
And Me.TxtPasword.Text = dsc_Cliente.Tables(0).Rows(0).Item("Pasword")
And Me.LblEstado.Text = dsc_Cliente.Tables(0).Rows(0).Item("Estado")
Or Me.LblEstado1.Text = dsc_Cliente.Tables(0).Rows(0).Item("Estado")
Then

Response.Write("<script> alert ('Datos Correctos,
Bienvenido');</script>")

Me.TxtCedulaIngreso.Text =
Encrip_Cliente.EncriptarCadena(Me.TxtCedulaIngreso.Text)

  'cerramos conexion
  objClientes.CerrarConexion()
  objClientes = Nothing
  dsc_Cliente = Nothing
  Cifrado.CerrarConexion()
  Cifrado = Nothing
  Encrip_Cliente.CerrarConexion()
  Encrip_Cliente = Nothing


  Server.Transfer("WFCliente_Editar.aspx")

 Else
 LblMsn.Text = "Lo Sentimos, los Datos de Ingreso no Corresponden a un
Registro Existente, si estas Registrado es posible que tu cuenta este
Suspendida"
 Me.LblMsn.Focus()
 End If

 Catch ex As Exception
 Me.LblMsn2.Text = "ERROR: " & ex.Message.ToString()
 End Try

                'cerramos conexion
                objClientes.CerrarConexion()
                objClientes = Nothing
                dsc_Cliente = Nothing
                Cifrado.CerrarConexion()
                Cifrado = Nothing
                Encrip_Cliente.CerrarConexion()
                Encrip_Cliente = Nothing

Else
                LblMsn.Text = "Lo Sentimos, los Datos de Ingreso no
Corresponden a un Registro Existente"
                LblMsn.Focus()
End If

            'cerramos conexion
            objClientes.CerrarConexion()
            objClientes = Nothing
            dsc_Cliente = Nothing
            Encrip_Cliente.CerrarConexion()
```

```
            Encrip_Cliente = Nothing

Catch ex As Exception
            Me.LblMsn2.Text = "ERROR: " & ex.Message.ToString()
End Try
```

Tabla 15: Código Fuente de Interfaz de Bienvenida (Inicio de Sesión)

2) Visualización de Registros

En este caso, si la Opción de bienvenida dio acceso al Usuario de acuerdo a la Validación de Datos, el Formulario de Visualización Cargará la Información del usuario, tal cual este en la base de Datos almacenada.

```
Try
 Dim encript As New ReglasNegocio.ClsEncriptador
 Dim objClientes As New ReglasNegocio.ClsClientes
 Dim dsc As Data.DataSet
 Dim desencrip As New ReglasNegocio.ClsEncriptador

dsc =
objClientes.TraerxCedula_Clientes(desencrip.DesEncriptarCadena(Me.TxtC
od_Cliente.Text))

Me.LblNo_Registro.Text = dsc.Tables(0).Rows(0).Item("No_Registro")
Me.LblCedula.Text = dsc.Tables(0).Rows(0).Item("Cedula")
Me.LblCod_TipoUsuario.Text =
dsc.Tables(0).Rows(0).Item("Cod_TipoUsuario")
Me.TxtNombre.Text = dsc.Tables(0).Rows(0).Item("Nombre")
Me.LblNombre_Mostrar.Text = dsc.Tables(0).Rows(0).Item("Nombre")
LblNombre_Cliente.Text = dsc.Tables(0).Rows(0).Item("Nombre")
Me.txtApellido.Text = dsc.Tables(0).Rows(0).Item("Apellido")
Me.LblApellido_Mostrar.Text = dsc.Tables(0).Rows(0).Item("Apellido")
Me.TxtTelefono.Text = dsc.Tables(0).Rows(0).Item("Telefono")
Me.LblTelefono_Mostrar.Text = dsc.Tables(0).Rows(0).Item("Telefono")
Me.TxtPais.Text = dsc.Tables(0).Rows(0).Item("Pais")
Me.LblPais_Mostrar.Text = dsc.Tables(0).Rows(0).Item("Pais")
Me.txtCiudad.Text = dsc.Tables(0).Rows(0).Item("Ciudad")
Me.LblCiudad_Mostrar.Text = dsc.Tables(0).Rows(0).Item("Ciudad")
Me.TxtDireccion.Text = dsc.Tables(0).Rows(0).Item("Direccion")
Me.LblDireccion_Mostrar.Text = dsc.Tables(0).Rows(0).Item("Direccion")
Me.TxtEmail.Text = dsc.Tables(0).Rows(0).Item("Email")
Me.LblEmail_Mostrar.Text = dsc.Tables(0).Rows(0).Item("Email")
Me.TxtPasword.Text = dsc.Tables(0).Rows(0).Item("Pasword")
Me.LblCod_Activacion.Text =
dsc.Tables(0).Rows(0).Item("Cod_Activacion")
Me.LblEstado.Text = dsc.Tables(0).Rows(0).Item("Estado")

 'Cerramos Conexion
 encript.CerrarConexion()
 encript = Nothing
```

```
 desencrip.CerrarConexion()
 desencrip = Nothing
 objClientes.CerrarConexion()
 objClientes = Nothing
 dsc = Nothing

Catch ex As Exception

End Try
```

Tabla 16: Código Fuente del Formulario de Visualización de Registros

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Durante el desarrollo de este trabajo se pudo conocer a través del análisis cual es el grado de conocimiento sobre la Cultura informática que posee la gente sobre distintos ámbitos que engloba este conocimiento destacando principalmente “La Seguridad” que sin lugar a dudas debe ser tomada como algo primordial en cualquier tipo de Sitio Web o servidor de información. De acuerdo con esto, el trabajo realizado nos dejó las siguientes conclusiones:

- ✓ Cuando se trate de buscar un Algoritmo de Encriptación para implementarlo a nuestros Sitios Web, hay que hacerlo de acuerdo a la necesidad que se tenga, refiriéndonos principalmente a que si solo queremos Cifrar contraseñas o algún Dato parecido deberíamos usar un Algoritmo que sea sencillo de Implementar pero que brinde Seguridad, en este caso se usó el Algoritmo MD5, y de acuerdo a sus características de velocidad de Trabajo, sencillez de implementación y sobre todo seguridad, fue el ideal para protección de datos en un Sitio Web.

- ✓ Según el algoritmo a Estudiar, lo que se hizo posteriormente es identificar qué Tipo de Cifrado se puede Asociar al Algoritmo MD5, por lo cual se comparó dos Tipos, el Simétrico y Asimétrico, quienes mostraron ventajas según su tipo, pero el más adecuado fue el Simétrico debido a su forma de trabajo, que lo hacía usando una sola clave, ideal forma de

trabajo para lo que es el cifrado de Contraseñas, debido a que los Usuarios que se registran en un Sitio siempre lo hacen con una sola Clave de Acceso y no necesitan otra clave, si no únicamente la que ellos imaginan y usan.

- ✓ A través del cuadro Comparativo acerca de los dos Tipos de cifrado, se pudo conocer tanto las Ventajas como las Desventajas, ayudando tanto al desarrollador del Proyecto como al Lector, a saber por qué se eligió el Cifrado Simétrico, el cual se apegaba a lo que es la propuesta del Tema del Proyecto.

- ✓ Una vez elegido el Algoritmo y el Tipo de Encriptación a estudiar e implementar, lo ideal fue realizar una Demostración real de lo que significa el Trabajo de Encriptación en un sitio Web y la Seguridad que representa, con esto el Usuario pudo conocer de una manera más acertada la propuesta del Proyecto y la meta a la cual se quería llegar, “Dar una opción más de Seguridad Informática para la Protección de Datos Importantes”.

- ✓ Gracias a la demostración el usuario conoció lo que es ya la Implementación del Algoritmo, pero lo que faltaba era Determinar cómo se debe Implementar el Algoritmo, para esto se realizó varios pasos en donde se mostró lo que se hizo desde la creación de una “Clase de

Programación” hasta la incorporación de Código en nuestro proceso de grabación de datos, refiriéndonos con esto al Registro de un Usuario.

- ✓ Uno de los Objetivos que se planteó al realizar el proyecto fue difundir el resultado del Estudio planteado, el cuál apuntaba a dar una opción más a lo que es la Seguridad Informática para Proteger Datos, para esto se ha utilizado herramientas gratuitas y famosas en el mundo de la búsqueda de información como lo son los Blogs y Video Tutoriales en YouTube, dando de esta manera un ayuda informativa en lo que se refiere al uso e implementación del algoritmo de Encriptación como medida de Seguridad.

- ✓ Como paso Final luego de todo el proceso de estudio, se procedió a dar Recomendaciones acerca de como Implementar este Tipo de seguridad en Sitios Web, dando ideas desde la conformación del Sitio Web, con su estructura dividida en Formularios, Bases de Datos, Lógica de programación y detalles de Diseño de interfaces. Según estos datos se orienta al usuario a implementar la Encriptación en partes sensibles en donde debe haber seguridad, como por ejemplo Registro de contraseñas, Comercio Electrónico, Inicios de Sesión, etc.

5.2 Recomendaciones

Las seguridades y métodos de protección en un Sistema son muchas pero siempre se opta por la más adecuada, dependiendo del Sistema que se tenga, además de que debe ser estudiada con detenimiento, conociendo las ventajas y desventajas de la utilización de las mismas.

Se debería estudiar todas las opciones que se tengan a la mano sobre seguridades, incluyendo no solo el bajo costo, sino también las ventajas y mejoras que brinde a nuestro Sistema.

Si se piensa en usar Encriptaciones, se debe conocer detalladamente cual es el algoritmo que se va a usar y saber si no tiene debilidades o bien si se piensa en firmas digitales tener la seguridad de que nuestra Entidad Certificadora brinde todas las garantías necesaria para que cada proceso se realice con total seguridad y confiabilidad.

GLOSARIO

- ✓ **Sitio Web:** Traducción del inglés Web Site, conjunto de páginas de una institución o persona.
- ✓ **Delito Informático:** Delito cometido utilizando un PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.
- ✓ **Phishing:** Tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial.
- ✓ **Spam:** Se llama Spam, correo basura o SMS basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.
- ✓ **Spyware:** Software que se instala en una computadora para recopilar información sobre las actividades realizadas en ella.
- ✓ **Integridad:** Garantía de la exactitud de la información frente a la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- ✓ **No repudio:** Propiedad que se consigue por medios criptográficos, que impide a una persona o entidad negar haber realizado una acción en particular relativa a datos.
- ✓ **Firewall:** Elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas.

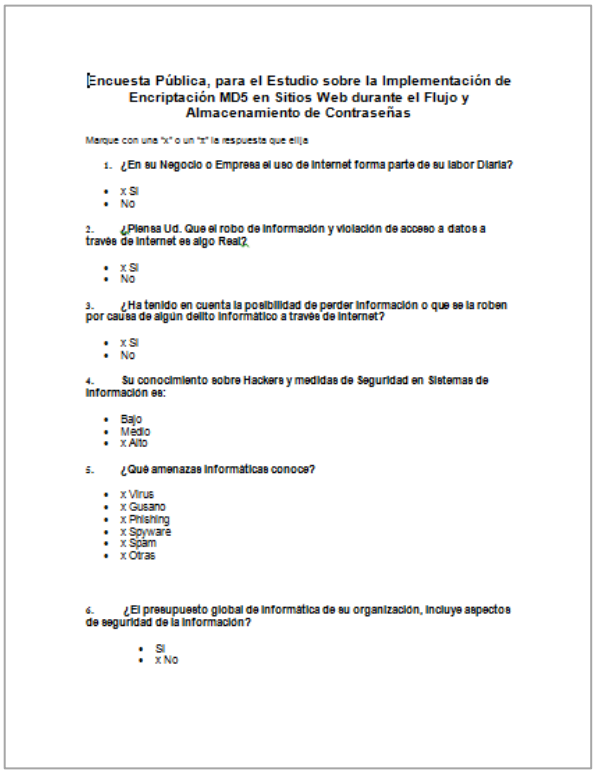
- ✓ **Paquete:** Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.
- ✓ **Criptología:** Ciencia que estudia el arte de crear y utilizar sistemas de encriptación.
- ✓ **Encriptación:** Acción de proteger la información mediante técnicas criptográficas ante modificaciones o utilización no autorizada.
- ✓ **Desencriptación:** Descifrado. Recuperación del contenido real de una información previamente encriptada o cifrada.
- ✓ **Algoritmo de Encriptación:** Codificadores de bloques de bits sobre los que iteran determinadas operaciones tales como sustitución, transposición, suma/producto modular y transformaciones lineales. Cada algoritmo utiliza bloques de distintos tamaños. Ver DES, 3DES y Blowfish.
- ✓ **MD5:** Algoritmo de encriptación de 128-bits del tipo EAP creado en 1991 por el profesor Ronald Rivest para RSA Data Security, Inc. empleado para crear firmas digitales. Emplea funciones hash unidireccionales, es decir, que toma un mensaje y lo convierte en una cadena fija de dígitos.
- ✓ **Firma Digital:** Información añadida o transformación cifrada de los datos que permite al receptor de los mismos comprobar su fuente e integridad y protegerse así de la suplantación o falsificación.

BIBLIOGRAFIA

- ✓ *WebTaller. (22 de Noviembre de 2010). Recuperado el 5 de Nomviembre de 2011, de http://www.webtaller.com/maletin/articulos/seguridad-web.php*
- ✓ *Wikipedia. (2010). Recuperado el 20 de Octubre de 2011, de http://es.wikipedia.org/wiki/Criptograf%C3%ADa*
- ✓ *Cisco. (Agosto de 2011). Recuperado el 20 de Octubre de 2011, de http://www.cisco.com/web/ES/solutions/es/internet_security/index.html*
- ✓ *Herramientas Web. (2011). Recuperado el 4 de Octubre de 2011, de http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/md5.html*
- ✓ *Wikipedia. (2011). Recuperado el Octubre de 2011, de http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica*
- ✓ *Asensio, G. (2006). Seguridad en Internet. Ediciones Nowtilus S.L.*
- ✓ *Enrique Quero Catalinas, A. G. (2007). Mantenimiento de Portales de Información: Explotación de Sistemas Informáticos. Editorial Paraninfo.*
- ✓ *Johns. (12 de Octubre de 2011). Kriptopolis. Recuperado el 17 de Octubre de 2011, de http://www.kriptopolis.org/taxonomy/term/130/all*
- ✓ *Lagranje, E. d. (28 de Octubre de 2004). Maestros del Web. Recuperado el 5 de Octubre de 2011, de http://www.maestrosdelweb.com/editorial/md5/*
- ✓ *Lakerbauer, I. (2001). Internet. Marcombo.*
- ✓ *Merlat, M. (2011). Monografías.com. Recuperado el 5 de Nomviembre de 2011, de http://www.monografias.com/trabajos/hackers/hackers.shtml*
- ✓ *Serrahima, J. (2010). La Amenaza Digital. Profit Editorial I.*
- ✓ *Snak, S. (25 de Junio de 2010). DevTroce. Recuperado el Septiembre de 2011, de http://www.devtroce.com/2010/06/25/diviertete-encriptando-tus-passwords-con-net/*
- ✓ *Vega, J. a. (2010). Información y referencia en entornos digitales: desarrollo de servicios bibliotecarios de consulta. EDITUM.*
- ✓ *XKlibur. (5 de 7 de 2009). CristaLab. Recuperado el 15 de octubre de 2011, de http://www.cristalab.com/blog/consejos-basicos-de-seguridad-en-la-web-c75641l/*

ANEXOS

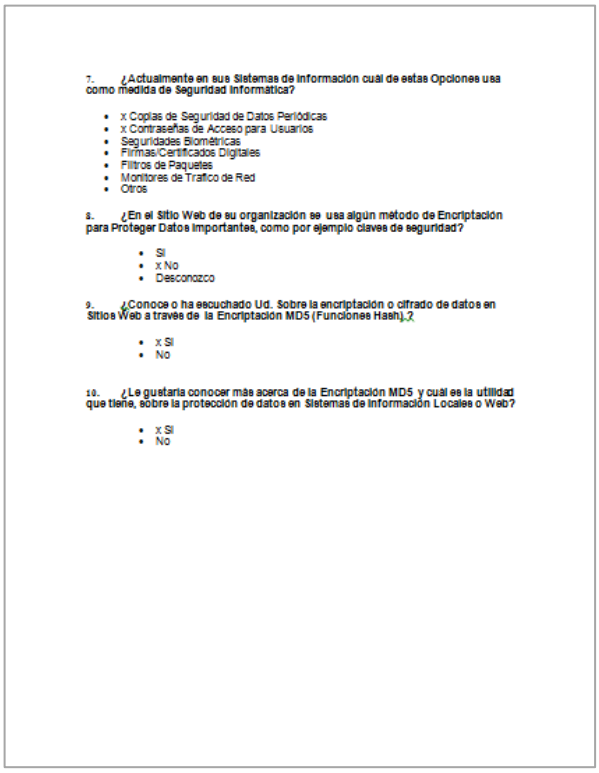
ANEXO 1: Encuestas Realizadas



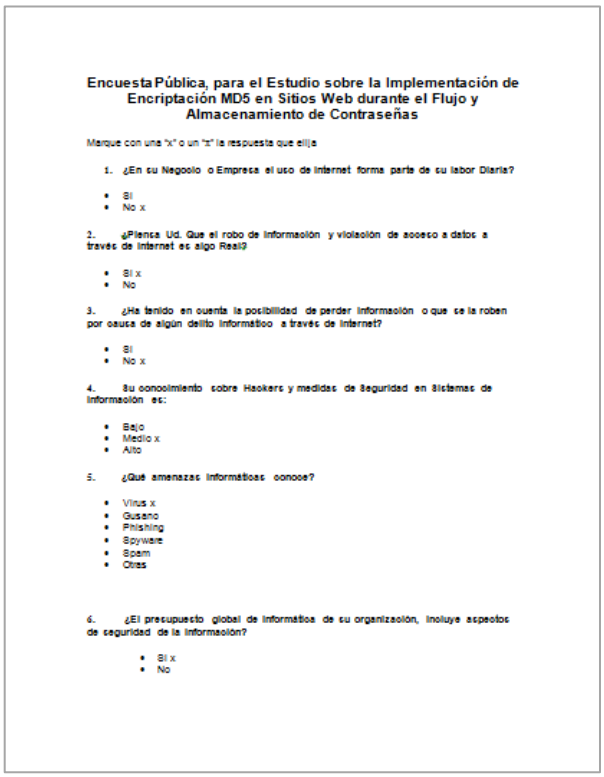
Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "x" la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - x SI
   - No
2. ¿Piensa Ud. Que el robo de información y violación de acceso a datos a través de Internet es algo Real?
   - x SI
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?
   - x SI
   - No
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - Bajo
   - Medio
   - x Alto
5. ¿Qué amenazas Informáticas conoce?
   - x Virus
   - x Gusano
   - x Phishing
   - x Spyware
   - x Spam
   - x Otras
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la información?
   - SI
   - x No



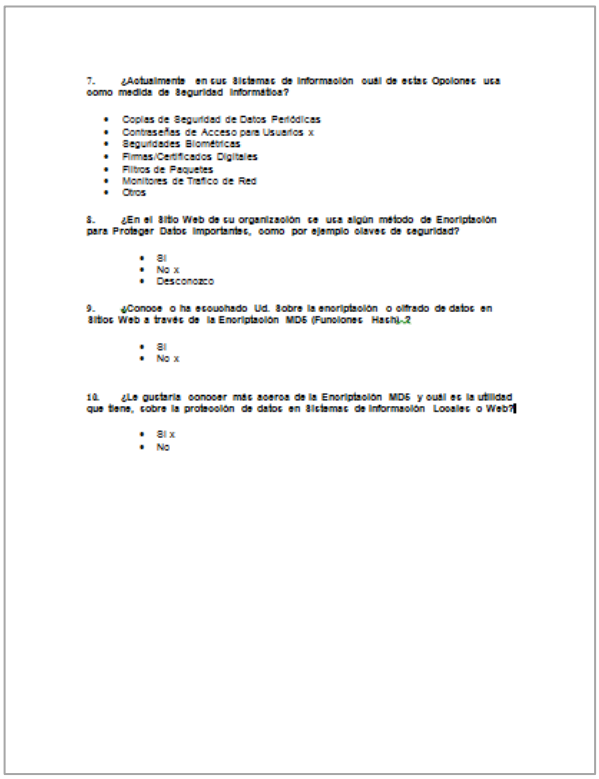
7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - x Copias de Seguridad de Datos Periódicas
   - x Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?
   - SI
   - x No
   - Desconozco
9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash).?
   - x SI
   - No
10. ¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - x SI
    - No



Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "x" la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - SI
   - No x
2. ¿Piensa Ud. Que el robo de información y violación de acceso a datos a través de Internet es algo Real?
   - SI x
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?
   - SI
   - No x
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - Bajo
   - Medio x
   - Alto
5. ¿Qué amenazas Informáticas conoce?
   - Virus x
   - Gusano
   - Phishing
   - Spyware
   - Spam
   - Otras
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la información?
   - SI x
   - No



7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - Copias de Seguridad de Datos Periódicas
   - Contraseñas de Acceso para Usuarios x
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?
   - SI
   - No x
   - Desconozco
9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash).?
   - SI
   - No x
10. ¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - SI x
    - No

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "=" la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - Si x
   - No
2. ¿Piensa Ud. Que el robo de información y violación de acceso a datos a través de Internet es algo Real?
   - Si x
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?
   - Si x
   - No
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - Bajo x
   - Medio
   - Alto
5. ¿Qué amenazas Informáticas conoce?
   - Virus
   - Gusano
   - Phishing x
   - Spyware
   - Spam
   - Otras
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la información?
   - Si x
   - No
7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - Copias de Seguridad de Datos Periódicas
   - Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red x
   - Otros
8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo Claves de seguridad?
   - Si
   - No x
   - Desconozco
9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash)?
   - Si x
   - No
10. ¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - Si x
    - No

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "-/" la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - ~~Si~~
   - No
2. ¿Piensa Ud. Que el robo de información y violación de acceso a datos a través de Internet es algo Real?
   - ~~Si~~
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?
   - ~~Si~~
   - No
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - Bajo
   - ~~Medio~~
   - Alto
5. ¿Qué amenazas Informáticas conoce?
   - ~~Virus~~
   - ~~Gusano~~
   - ~~Phishing~~
   - ~~Spyware~~
   - ~~Spam~~
   - Otras
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la información?
   - ~~Si~~
   - No
7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - ~~Copias de Seguridad de Datos Periódicas~~
   - ~~Contraseñas de Acceso para Usuarios~~
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - ~~Otros~~
8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?
   - ~~Si~~
   - No
   - Desconozco
9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash)?
   - ~~Si~~
   - No
10. ¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - ~~Si~~
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "✓" la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - SI
   - No
2. ¿Piensa Ud. Que el robo de información y violación de acceso a datos a través de Internet es algo Real?
   - SI
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?
   - SI
   - No
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - Bajo
   - Medio
   - Alto
5. ¿Qué amenazas Informáticas conoce?
   - Virus
   - Gusano
   - Phishing
   - Spyware
   - Spam
   - Otras
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la información?
   - SI
   - No
7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - Copias de Seguridad de Datos Periódicas
   - Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?
   - SI
   - No
   - Desconozco
9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash).?
   - SI
   - No
10. ¿Le gustaría conocer mas acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - SI
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "✓" la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - ✓ SI
   - No
2. ¿Piensa Ud. Que el robo de información y violación de acceso a datos a través de Internet es algo Real?
   - ✓ SI
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?
   - SI
   - ✓ No
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - ✓ Bajo
   - Medio
   - Alto
5. ¿Qué amenazas Informáticas conoce?
   - ✓ Virus
   - Gusano
   - Phishing
   - Spyware
   - Spam
   - Otras
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la información?
   - SI
   - ✓ No
7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - Copias de Seguridad de Datos Periódicas
   - ✓ Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?
   - SI
   - No
   - ✓ Desconozco
9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash).?
   - SI
   - ✓ No
10. ¿Le gustaría conocer mas acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - SI
    - ✓ No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "✓" la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - ✓ Si
   - No
2. ¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?
   - ✓ Si
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?
   - ✓ Si
   - No
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - Bajo
   - ✓ Medio
   - Alto
5. ¿Qué amenazas Informáticas conoce?
   - ✓ Virus
   - ✓ Gusano
   - ✓ Phishing
   - Spyware
   - ✓ Spam
   - Otras
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?
   - ✓ Si
   - No
7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - Copias de Seguridad de Datos Periódicas
   - ✓ Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - ✓ Firmas/Certificados Digitales
   - Filtros de Paquetes
   - ✓ Monitores de Trafico de Red
   - Otros
8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?
   - ✓ Si
   - No
   - Desconozco
9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash).?
   - Si
   - ✓ No
10. ¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - ✓ Si
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "✓" la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - Si X
   - No
2. ¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?
   - Si X
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?
   - Si
   - No X
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - Bajo
   - Medio X
   - Alto
5. ¿Qué amenazas Informáticas conoce?
   - Virus X
   - Gusano
   - Phishing
   - Spyware
   - Spam X
   - Otras
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?
   - Si
   - No X
7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - Copias de Seguridad de Datos Periódicas X
   - Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?
   - Si
   - No
   - Desconozco X
9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash).?
   - Si
   - No X
10. ¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - Si X
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un " ✓" la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - SI
   - No
2. ¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?
   - SI
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder Información o que se la roben por causa de algún delito Informático a través de Internet?
   - SI
   - No
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - Bajo
   - Medio
   - Alto
5. ¿Qué amenazas Informáticas conoce?
   - Virus
   - Gusano
   - Phishing
   - Spyware
   - Spam
   - Otras
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?
   - SI
   - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - Copias de Seguridad de Datos Periódicas
   - Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?
   - SI
   - No
   - Desconozco
9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash) ?
   - SI
   - No
10. ¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - SI
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un " ✓" la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - SI X
   - No
2. ¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?
   - SI x
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder Información o que se la roben por causa de algún delito Informático a través de Internet?
   - SI x
   - No
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - Bajo
   - Medio x
   - Alto
5. ¿Qué amenazas Informáticas conoce?
   - Virus x
   - Gusano x
   - Phishing
   - Spyware x
   - Spam x
   - Otras
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?
   - SI
   - No x

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - Copias de Seguridad de Datos Periódicas x
   - Contraseñas de Acceso para Usuarios x
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?
   - SI x
   - No
   - Desconozco
9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash) ?
   - SI
   - No x
10. ¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - SI x
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un " ✓" la respuesta que elija

1. **¿En su Negocio o Empresa el uso de internet forma parte de su labor Diaria?**
   - Si ✓
   - No
2. **¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?**
   - Si ✓
   - No
3. **¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?**
   - Si ✓
   - No
4. **Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:**
   - Bajo
   - Medio
   - Alto ✓
5. **¿Qué amenazas Informáticas conoce?**
   - Virus ✓
   - Gusano ✓
   - Phishing
   - Spyware ✓
   - Spam ✓
   - Otras
6. **¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?**
   - Si ✓
   - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

7. **¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?**
   - Copias de Seguridad de Datos Periódicas ✓
   - Contraseñas de Acceso para Usuarios ✓
   - Seguridades Biométricas ✓
   - Firmas/Certificados Digitales
   - Filtros de Paquetes ✓
   - Monitores de Trafico de Red
   - Otros
8. **¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?**
   - Si
   - No ✗
9. **¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash) ?**
   - Si ✓
   - No
10. **¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?**
    - Si ✓
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un " ✓" la respuesta que elija

1. **¿En su Negocio o Empresa el uso de internet forma parte de su labor Diaria?**
   - (•) Si
   - No
2. **¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?**
   - (•) Si
   - No
3. **¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?**
   - (•) Si
   - No
4. **Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:**
   - Bajo
   - (•) Medio
   - Alto
5. **¿Qué amenazas Informáticas conoce?**
   - (•) Virus
   - Gusano
   - (•) Phishing
   - (•) Spyware
   - Spam
   - Otras
6. **¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?**
   - (•) Si
   - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

7. **¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?**
   - (•) Copias de Seguridad de Datos Periódicas
   - Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. **¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?**
   - (•) Si
   - No
9. **¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash) ?**
   - (•) Si
   - No
10. **¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?**
    - (•) Si
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un " √ " la respuesta que elija

1. **¿En su Negocio o Empresa el uso de internet forma parte de su labor Diaria?**
   - (•) Si
   - • No
2. **¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?**
   - (•) Si
   - • No
3. **¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?**
   - (•) Si
   - • No
4. **Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:**
   - (•) Bajo
   - • Medio
   - • Alto
5. **¿Qué amenazas Informáticas conoce?**
   - (•) Virus
   - (•) Gusano
   - • Phishing
   - • Spyware
   - • Spam
   - • Otras
6. **¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?**
   - • Si
   - (•) No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

7. **¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?**
   - (•) Copias de Seguridad de Datos Periódicas
   - (•) Contraseñas de Acceso para Usuarios
   - • Seguridades Biométricas
   - • Firmas/Certificados Digitales
   - • Filtros de Paquetes
   - • Monitores de Trafico de Red
   - • Otros
8. **¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?**
   - (•) Si
   - • No
9. **¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash) ?**
   - • Si
   - (•) No
10. **¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?**
    - (•) Si
    - • No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un " √ " la respuesta que elija

1. **¿En su Negocio o Empresa el uso de internet forma parte de su labor Diaria?**
   - • Si
   - • No
2. **¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?**
   - • Si
   - • No
3. **¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?**
   - • Si
   - • No
4. **Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:**
   - • Bajo
   - • Medio
   - • Alto
5. **¿Qué amenazas Informáticas conoce?**
   - • Virus
   - • Gusano
   - • Phishing
   - • Spyware
   - • Spam
   - • Otras
6. **¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?**
   - • Si
   - • No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

7. **¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?**
   - • Copias de Seguridad de Datos Periódicas
   - • Contraseñas de Acceso para Usuarios
   - • Seguridades Biométricas
   - • Firmas/Certificados Digitales
   - • Filtros de Paquetes
   - • Monitores de Trafico de Red
   - • Otros
8. **¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?**
   - • Si
   - • No
9. **¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash) ?**
   - • Si
   - • No
10. **¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?**
    - • Si
    - • No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "✓" la respuesta que elija

1. **¿En su Negocio o Empresa el uso de internet forma parte de su labor Diaria?**
   - Si
   - No
2. **¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?**
   - Si
   - No
3. **¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?**
   - Si
   - No
4. **Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:**
   - Bajo
   - Medio
   - Alto
5. **¿Qué amenazas Informáticas conoce?**
   - Virus
   - Gusano
   - Phishing
   - Spyware
   - Spam
   - Otras
6. **¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?**
   - Si
   - No
7. **¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?**
   - Copias de Seguridad de Datos Periódicas
   - Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. **¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?**
   - Si
   - No
9. **¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash) ?**
   - Si
   - No
10. **¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?**
    - Si
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "✓" la respuesta que elija

1. **¿En su Negocio o Empresa el uso de internet forma parte de su labor Diaria?**
   - Si
   - No
2. **¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?**
   - Si
   - No
3. **¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?**
   - Si
   - No
4. **Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:**
   - Bajo
   - Medio
   - Alto
5. **¿Qué amenazas Informáticas conoce?**
   - Virus
   - Gusano
   - Phishing
   - Spyware
   - Spam
   - Otras
6. **¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?**
   - Si
   - No
7. **¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?**
   - Copias de Seguridad de Datos Periódicas
   - Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. **¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?**
   - Si
   - No
9. **¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash) ?**
   - Si
   - No
10. **¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?**
    - Si
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "✓" la respuesta que elija

1. **¿En su Negocio o Empresa el uso de internet forma parte de su labor Diaria?**
   - ✓ Si
   - No
2. **¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?**
   - ✓ Si
   - No
3. **¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?**
   - ✓ Si
   - No
4. **Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:**
   - ✓ Bajo
   - Medio
   - Alto
5. **¿Qué amenazas Informáticas conoce?**
   - ✓ Virus
   - Gusano
   - Phishing
   - Spyware
   - Spam
   - ✓ Otras
6. **¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?**
   - Si
   - ✓ No
7. **¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?**
   - Copias de Seguridad de Datos Periódicas
   - ✓ Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. **¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?**
   - ✓ Si
   - No
9. **¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash) ?**
   - Si
   - ✓ No
10. **¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?**
    - ✓ Si
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un "✓" la respuesta que elija

1. **¿En su Negocio o Empresa el uso de internet forma parte de su labor Diaria?**
   - ✓ Si
   - No
2. **¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?**
   - ✓ Si
   - No
3. **¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?**
   - ✓ Si
   - No
4. **Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:**
   - ✓ Bajo
   - Medio
   - Alto
5. **¿Qué amenazas Informáticas conoce?**
   - ✓ Virus
   - ✓ Gusano
   - Phishing
   - Spyware
   - Spam
   - Otras
6. **¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?**
   - Si
   - ✓ No
7. **¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?**
   - Copias de Seguridad de Datos Periódicas
   - ✓ Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - Otros
8. **¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?**
   - ✓ Si
   - No
9. **¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash) ?**
   - Si
   - ✓ No
10. **¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?**
    - ✓ Si
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - Copias de Seguridad de Datos Periódicas
   - Contraseñas de Acceso para Usuarios X
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red X
   - Otros

8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?
   - Si X
   - No
   - Desconozco

9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash)?
   - Si X
   - No

10. ¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - Si X
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un " ✓ " la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - Si X
   - No
2. ¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?
   - Si X
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?
   - Si X
   - No
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - Bajo
   - Medio
   - Alto X
5. ¿Qué amenazas Informáticas conoce?
   - Virus X
   - Gusano X
   - Phishing X
   - Spyware
   - Spam X
   - Otras X
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?
   - Si X
   - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

Encuesta Pública, para el Estudio sobre la Implementación de Encriptación MD5 en Sitios Web durante el Flujo y Almacenamiento de Contraseñas

Marque con una "x" o un " ✓ " la respuesta que elija

1. ¿En su Negocio o Empresa el uso de Internet forma parte de su labor Diaria?
   - Si X
   - No
2. ¿Piensa Ud. Que el robo de Información y violación de acceso a datos a través de Internet es algo Real?
   - Si X
   - No
3. ¿Ha tenido en cuenta la posibilidad de perder información o que se la roben por causa de algún delito informático a través de Internet?
   - Si X
   - No
4. Su conocimiento sobre Hackers y medidas de Seguridad en Sistemas de Información es:
   - X Bajo
   - Medio
   - Alto
5. ¿Qué amenazas Informáticas conoce?
   - X Virus
   - Gusano
   - Phishing
   - Spyware
   - X Spam
   - X Otras
6. ¿El presupuesto global de Informática de su organización, incluye aspectos de seguridad de la Información?
   - Si
   - X No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

7. ¿Actualmente en sus Sistemas de Información cuál de estas Opciones usa como medida de Seguridad Informática?
   - Copias de Seguridad de Datos Periódicas
   - Contraseñas de Acceso para Usuarios
   - Seguridades Biométricas
   - Firmas/Certificados Digitales
   - Filtros de Paquetes
   - Monitores de Trafico de Red
   - X Otros
8. ¿En el Sitio Web de su organización se usa algún método de Encriptación para Proteger Datos Importantes, como por ejemplo claves de seguridad?
   - Si
   - X No
9. ¿Conoce o ha escuchado Ud. Sobre la encriptación o cifrado de datos en Sitios Web a través de la Encriptación MD5 (Funciones Hash) ?
   - Si
   - X No
10. ¿Le gustaría conocer más acerca de la Encriptación MD5 y cuál es la utilidad que tiene, sobre la protección de datos en Sistemas de Información Locales o Web?
    - X Si
    - No

Agradecemos sus comentarios, el objetivo de este cuestionario es recibir sus opiniones para la Implementación de Encriptación MD5 en Sitios Web.

ANEXO 2: Código Fuente del Algoritmo MD5 en Visual .NET

Cifrado.vb

(General) (Declaraciones)

```vb
Imports System
Imports System.Data
Imports System.Data.SqlClient
Imports System.IO
Imports System.Text
Imports System.Security.Cryptography
Public Class Cifrado
    Inherits cmpEntidad

    ' Encripta una cadena de texto usando el algoritmo de encriptacion de hash MD5.
    ' el "Message Digest" es una encriptacion de 128-bit y es usado comunmente para
    ' verificar datos chequeando el "Checksum MD5", mas informacion se puede
    ' encontrar en: http://www.faqs.org/rfcs/rfc1321.html

    ' cadena conteniendo el string a hashear a MD5.
    ' Una cadena de texto conteniendo en forma encriptada la cadena ingresada.
    Public Function MD5Hash(ByVal Data As String) As String
        Dim md5 As MD5 = New MD5CryptoServiceProvider()
        Dim hash As Byte() = md5.ComputeHash(Encoding.UTF8.GetBytes(Data))

        Dim stringBuilder As New StringBuilder()

        For Each b As Byte In hash
            stringBuilder.AppendFormat("{0:x2}", b)
        Next
        Return stringBuilder.ToString()
    End Function

End Class

```

```vb
Dim cifrado As New ReglasNegocio.Cifrado
Dim objClientes As New ReglasNegocio.ClsClientes

Me.TxtPasword.Text = (cifrado.MD5Hash(Me.TxtPasword.Text))
```

ANEXO 3: Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS
(Ley No. 2002-67)

CONGRESO NACIONAL

Considerando:

Que el uso de sistemas de información y de redes electrónicas, incluida la Internet ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado;

Que es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos;

Que se debe generalizar la utilización de servicios de redes de información e Internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura;

Que a través del servicio de redes electrónicas, incluida la Internet se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una Ley especializada sobre la materia;

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Tannia Mayorga
PARA: Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 30 de Noviembre de 2011

Por medio de la presente certifico que el pregradista Juan Gabriel Heredia Torres con CI No.0105337521 ha realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **ESTUDIO SOBRE LA IMPLEMENTACIÓN DE ENCRIPTACIÓN MD5 EN SITIOS WEB DURANTE EL FLUJO Y ALMACENAMIENTO DE CONTRASEÑAS**, del título de Ingeniero en Sistemas Informáticos.

Atentamente

_____
Ing. Tannia Mayorga

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Pablo Ochoa
PARA: Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 30 de Noviembre de 2011

Por medio de la presente certifico que el pregradista Juan Gabriel Heredia Torres con CI No.0105337521 ha realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **ESTUDIO SOBRE LA IMPLEMENTACIÓN DE ENCRIPTACIÓN MD5 EN SITIOS WEB DURANTE EL FLUJO Y ALMACENAMIENTO DE CONTRASEÑAS**, del título de Ingeniero en Sistemas Informáticos.

Atentamente

_____
Ing. Pablo Ochoa

UNIVERSIDAD TECNOLÓGICA ISRAEL
DIRECCIÓN DE POSGRADOS
AUTORIZACIÓN DE EMPASTADO

DE: Ing. Juan Pérez
PARA: Msc. Luis Andrés Chávez Ing.
DIRECTOR DEL SINED DE LA UNIVERSIDAD ISRAEL
ASUNTO: Autorización de Empastado
FECHA Quito, 30 de Noviembre de 2011

Por medio de la presente certifico que el pregradista Juan Gabriel Heredia Torres con CI No.0105337521 ha realizado las modificaciones solicitadas de acuerdo a la última revisión realizada en mi tutoría, al documento de tesis titulada **ESTUDIO SOBRE LA IMPLEMENTACIÓN DE ENCRIPTACIÓN MD5 EN SITIOS WEB DURANTE EL FLUJO Y ALMACENAMIENTO DE CONTRASEÑAS**, del título de Ingeniero en Sistemas Informáticos.

Atentamente

_____
Ing. Juan Pérez