IMPORTANCIA DE LA APLICACIÓN DEL MECANISMO DE CIFRADO DE INFORMACIÓN EN LAS EMPRESAS PARA LA PREVENCIÓN DE RIESGOS COMO ATAQUES, PLAGIO Y PÉRDIDA DE LA CONFIDENCIALIDAD

YEISON FREDY CHALA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
PROGRAMA DE ESPECIALIZACION EN SEGURIDAD INFORMATICA
NEIVA
2019

IMPORTANCIA DE LA APLICACIÓN DEL MECANISMO DE CIFRADO DE INFORMACIÓN EN LAS EMPRESAS PARA LA PREVENCIÓN DE RIESGOS COMO ATAQUES, PLAGIO Y PÉRDIDA DE LA CONFIDENCIALIDAD

(Autor)
YEISON FREDY CHALA

Monografía Presentada Como Requisito Para Optar Al Título De Especialista En Seguridad Informática

DIRECTOR: EDGAR ALONSO BOJACA GARAVITO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
PROGRAMA DE ESPECIALIZACION EN SEGURIDAD INFORMATICA
NEIVA
2019

TABLA DE CONTENIDO

TABLA DE FIGURAS

GLOSARIO

Amenaza: suceso que tiene la posibilidad de causar daño o perdida, la cual puede presentarse en forma de destrucción, robo o divulgación, modificación de datos.

Algoritmo: secuencia de pasos lógicos que se realizan para realizar una acción o proceso.

Autenticación: proceso de verificación o comprobación de la identidad de algo a alguien.

Ciberseguridad: acción caracterizada por tratar de minimizar las amenazas o riesgos a una infraestructura tecnológica.

Ciberdelito: operación ilícita realizada a través de internet o que tiene como objeto destruir o dañar un ordenador, redes de internet o medios electrónicos.

Cifrado: proceso de ocultar o codificar información importante para evitar que personas no autorizadas puedan acceder a ellas.

Confidencialidad: acción de guardar la privacidad**.**

Encriptación: es un proceso para convertir en secreto información que se considere importante. Luego de encriptarse la información, la idea es que solo pueda ser descriptada por la persona que conozca la clave.

Filtración de datos: es divulgación o escape de datos que puede permitir el acceso a personal no autorizado, lo cual puede permitir la adquisición de información confidencial que puede considerarse robo.

Hardware: palabra que hace descripción a cada uno de los elementos físicos que componen un ordenador como por ejemplo (teclado, mouse, disco duro, pantalla).

Open Source: es un software en base a código abierto, el cual en su mayoría se puede conseguir de forma gratuita.

Protección: conjunto de acciones que pretenden salvaguardar la seguridad de algo a alguien.

Riesgos: es el evento de que una amenaza se pueda manifestar o se produzca.

Robo de datos: es la pérdida de la información importante para la empresa, el cual puede ser causado por un empleado o por un ataque informático.

Software libre: son todos los programas informáticos los cuales su código fuente puede ser estudiado, modificado, y utilizado libremente con cualquier fin.

Vulnerabilidad: son las pequeñas debilidades que se pueden presentar en una infraestructura informática, las cuales pueden ser aprovechadas para causar daños por robo de información.

INTRODUCCION

La Seguridad de la Información es uno de los temas de mayor importancia y preocupación en las diferentes entidades ya sean de carácter público o privado. Para el funcionamiento y desempeño eficaz de una empresa fuere cual fuere su razón social es fundamental el manejo de información confidencial la cual debe ser protegida de la mejor manera para evitar que sea plagiada y utilizada para fines diferentes que ocasionen ataques o desastres en los datos de la organización.

Algunas empresas cuentan en las áreas de sistemas con personal que se encarga de tomar las precauciones correspondientes con el fin de evitar ataques en los datos de la organización. Sin embargo, no todas cuentan con estas herramientas o los mecanismos utilizados no son suficientes o adecuadamente aplicados.

Actualmente, las amenazas a la información corporativa incluyen desde el malware y la explotación de vulnerabilidades, suplantación de identidad, hasta el robo de dispositivos móviles. Además, teniendo en cuenta que el tema de la privacidad de las comunicaciones y la información está en pleno debate internacional, el concepto de cifrado de datos se popularizó como una manera de mantener la información segura, tanto en el ámbito familiar como en el corporativo.[1]

El objetivo de este trabajo es profundizar en el tema de cifrado de la información y de ese modo poder dar a conocer los beneficios que este sistema puede ofrecer a las empresas. Además hacer una reseña de algunas herramientas de muy fácil manejo y bajo costo para su implementación.

---

[1] ESET “Cifrado De La Información: Guía Corporativa” {En línea} {10 de marzo de 2017} disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014.pdf

1. TITULO

IMPORTANCIA DE LA APLICACIÓN DEL MECANISMO DE CIFRADO DE INFORMACIÓN EN LAS EMPRESAS PARA LA PREVENCIÓN DE RIESGOS COMO ATAQUES, PLAGIOS Y PÉRDIDA DE LA CONFIDENCIALIDAD

2. PLANTEAMIENTO DEL PROBLEMA

2.1 Descripción Del Problema

Actualmente en algunas empresas de nuestro país no se cuenta con los mecanismos adecuados para la protección de la información digital, además se tiene poco conocimiento de las herramientas de protección de datos convirtiéndolas en vulnerables a los riesgos existentes como ataques informáticos, plagio de la información y perdida de la confidencialidad, lo que hace necesario la implementación de herramientas para prevenir dichos riesgos.

Según estadísticas de ESET Latinoamérica se conoce que el 40% de las empresas sufrió incidentes maliciosos en el último año; de igual manera en el Informe Global sobre Fraudes y Riesgos de Kroll de 2016 se dice que en el año estudiado el 82% de las empresas sufrió fraude corporativo, lo anterior evidencia que el riesgo existe en cualquier tipo de empresa, no importando su tamaño, lo que la convierte potencialmente vulnerable a ataques específicos[2].

2.2 Formulación Del Problema

La implementación de sistemas de seguridad diseñados para la protección de los entornos digitales de datos a causado la necesidad de la realización de búsquedas de herramientas que ayuden a la salva guarde de estas.
Por ese motivo se recomienda el uso del cifrado de datos, ya que a través de este método se pueden realizar una serie de estrategias que permiten mejorar los niveles

[2] ESET “Cifrado De La Información: Guía Corporativa” {En línea} {10 de marzo de 2017} disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014.pdf

de autenticidad y fiabilidad de los mismos. Además en el mercado se pueden encontrar mecanismos económicos y fáciles de implementar.

¿Cuáles ventajas y beneficios proporcionará la implementación de cifrado de la información en las empresas?

Falta de implementación de mecanismos de protección de información digital por parte de algunas empresas en nuestro país.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Proponer estrategias a las empresas para la protección de los datos ante algunos riesgos como ataques informáticos, plagio de la información y pérdida de la confidencialidad mediante la implementación de cifrado de la información.

3.2 OBJETIVOS ESPECÍFICOS

1. Profundizar en el tema de cifrado de información

2. Describir los beneficios de encriptación de datos

3. Dar a conocer algunas herramientas que pueden ser utilizadas para proteger la información

4. Brindar una herramienta útil para la protección de datos en las empresas

5. Realizar un análisis de los sistemas de cifrado en la actualidad.

4. JUSTIFICACION

En la actualidad cualquier empresa u organización está expuesta a riesgos de ataques informáticos como falsificación, alteración de documentos, destrucción de información, suplantación de identidad, plagio o robo de la información, siendo la información el activo más importante para el correcto funcionamiento de la misma, por lo que se hace indispensable tomar medidas y utilizar estrategias para protegerla ante todos los riesgos existentes.

El presente trabajo trata el tema de mecanismos de cifrado de información y algunas herramientas útiles con los cuales se dará solución a varias problemáticas que se están presentado en algunas empresas como son ataques, fuga y plagio de información.

Con esta monografía se pretende dar a conocer información de gran importancia, realizando un estudio de todos los aspectos de cifrado de información desde su definición hasta su aplicación según las necesidades de protección de información; muestra de manera clara y actualizada las diferentes herramientas, beneficios y la manera como pueden ser implementados estos mecanismos en cualquier empresa que requiera proteger sus datos.

Con lo anterior se pueden aportar las soluciones para la confidencialidad y protección de la información, manejada en cualquier organización por los diferentes medios de difusión como correos electrónicos, navegación en los diferentes sitios web, datos locales y dispositivos móviles. De manera que se permita garantizar la integridad, confidencialidad y disponibilidad, de sus datos.

5. ALCANCE Y DELIMITACION DEL PROYECTO

Dar a conocer información de gran importancia realizando un estudio de todos los aspectos de cifrado de información desde su definición hasta su aplicación según las necesidades de protección de información; mostrar de manera clara y actualizada los beneficios y la manera como pueden ser implementadas herramientas criptográficas con la ayuda de los mecanismos de cifrado en cualquier empresa que requiera proteger sus datos e información.

Esta monografía aplica a las empresas colombianas que busquen proteger sus datos o cualquier entidad que maneje información de vital importancia que requiera de confidencialidad, autenticidad de su información e integridad y disponibilidad de la misma, se dará a conocer la metodología de cifrado de datos, algunas herramientas existentes y la manera como se pueden implementar con el fin de salvaguardar la información.

El cifrado de información es un método muy fácil de implementar, sólo se deben conocer las herramientas correctas, para ello mediante esta monografía se dará a conocer algunas, las cuales se podrían considerar como las mejores herramientas de cifrado de información disponibles de manera gratuita o de Open Source, con las cuales se pretenderá garantizar la integridad y seguridad de la información cifrando correos electrónicos, dispositivos de almacenamiento como USB y discos duros, estas son compatibles con Windows y Linux lo que permitirá que cualquier persona pueda realizar la implementación en cualquier empresa u organización según sea su necesidad y presupuesto.

6. METODOLOGIA

6.1 Metodología documental

La técnica utilizada para la recolección de datos en el presente proyecto es la recopilación documental y bibliográfica. “Esta modalidad o técnica en la recopilación de datos parte del capítulo de las fuentes secundarias de datos, o sea aquella información obtenida indirectamente a través de documentos, libros o investigaciones adelantadas por personas ajenas al investigador. Aquí el "documento" no es otra cosa que un testimonio escrito de un hecho pasado o histórico, el cual se diferencia del estudio de campo en que éste se refiere a una fuente de datos directa, y que se obtiene de las personas o del medio donde se generan y se desarrollan los hechos y los fenómenos estudiados” [3]

El tipo de investigación en que se apoya el trabajo es documental, ya que ésta se desarrolló usando fuentes documentales bibliográficas, puesto que la monografía se realizó en forma investigativa y pretende dar a conocer la importancia del cifrado de la información ya que en estos tiempos es un pilar fundamental y un activo vital para todo tipo de organización.

“La investigación documental es aquella que se realiza a través de la consulta de documentos (libros, revistas, periódicos, memorias, anuarios, registros, códices, constituciones, etc.). La de campo o investigación directa es la que se efectúa en el lugar y tiempo en que ocurren los fenómenos objeto de estudio. La investigación mixta es aquella que participa de la naturaleza de la investigación documental y de la investigación de campo. (Zorrilla ,1993:43)”

---

[3] CERDA, H. “Capítulo 7: Medios, Instrumentos, Técnicas y Métodos en la Recolección de Datos e Información” disponible en:http://postgrado.una.edu.ve/metodologia2/paginas/cerda7.pdf

7. MARCO REFERENCIAL

El intercambio de información ha sido un aspecto fundamental en la sociedad, el cual ha cobrado mayor importancia en los últimos tiempos dentro o fuera de cualquier organización, gracias a los adelantos tecnológicos, lo que ha obligado a que estas implanten constantes controles de seguridad que ofrezcan y garanticen la protección de la información con la que se cuente o vaya a ser intercambiada.

Para garantizar esta protección es necesario establecer políticas y medidas preventivas en los procesos de intercambio de información que la organización emplee. Para ello se hace necesario que se conozca a fondo algunos mecanismos entre ellos el cifrado de datos del cual se ampliará información en el desarrollo de la presente monografía.

Algunas medidas que pueden ser implementadas son:

- Programaciones de un correcto uso de los medios informáticos y de comunicación.

- Controles para evitar la modificación, la manipulación, el copiado o la destrucción de la información.

- Utilización de Antivirus actualizados.

- Uso de cifrado en datos que se consideren necesarios.

Según los estudios realizados actualmente el robo de información es un negocio en crecimiento y muy rentable, lo que lleva a que las empresas empiecen a buscar medios para salvaguardar su valiosa información.

Una herramienta en crecimiento es el cifrado de datos o encriptación. "Las tecnologías de la encriptación constituyen el avance tecnológico más importante de los últimos mil años. Ningún otro descubrimiento tecnológico desde las armas nucleares (espero) hasta Internet tendrá un impacto más significativo en la vida social y política de la humanidad. La criptografía va a cambiar absolutamente todo". Lawrence Lessig.[4]

Existen herramientas que pueden ser adoptadas por las empresas para la protección de los datos como lo es la implementación de norma ISO 27001, entre otras.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados que constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

• Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

---

[4] La criptografía y la protección a la información digital. Disponible en: https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI (Sistema de Gestión de la Seguridad de la Información). [5]

7.1 MARCO TEÓRICO

La acumulación de enormes cantidades de datos de carácter personal por entidades públicas y privadas, incorporada a la capacidad de los sistemas informáticos para combinar y procesar las informaciones viene generando claras amenazas a la privacidad de los individuos. La comprobación de estas amenazas por parte de la mayoría de países ha llevado a la elaboración de leyes y normas que limitan el tratamiento de los datos de carácter personal. [6]

Además de leyes se hace necesario la implementación de herramientas que permitan la protección de los datos y una de ellas es el cifrado de datos o encriptación. Y para ello se hace necesario que existan manuales que facilitan la implementación de estas.

La criptografía es la técnica utilizada para cifrar mensajes que contienen información, palabra que proviene del griego Kryptos y Graphein, que significan “escondido” y “escritura”, respectivamente[7]

---

[5] Sistema de Gestión de la Seguridad de la Información. disponible en:http://www.iso27000.es/download/doc_sgsi_all.pdf

[6] Que es la seguridad informática disponible en : https://www.monografias.com/trabajos94/que-seguridad-informatica/que-seguridad-informatica

[7]El objeto la criptografía no es ocultar la existencia de un mensaje, sino más bien ocultar su significado, un proceso que se conoce como codificación” (Sgarro, 1990: 20).

El Cifrar datos de forma correcta es una de las obligaciones que impone la normativa española para una inmensa cantidad de empresas. Muchas de ellas no cifran por miedo o desconocimiento. Cifrar no es complicado, el coste es asequible y los beneficios se muestran desde el inicio. [8]

En Colombia y en el mundo no se han establecido normas claras en el tema del cifrado de datos, sin embargo es fundamental que todas las empresas u organizaciones adopten dicho mecanismo.

La implementación de sistemas de gestión, de normas ISO, será un pilar fundamental en la seguridad de la información de cualquier organización, siendo esto confidencialidad, integridad y disponibilidad. Estos 3 aspectos importantes a la hora de verificar el grado de importancia de nuestros datos.

7.1.1 Que Es El Cifrado De Datos

El cifrado de los datos es una práctica que consiste en codificar los datos para modificar su formato original y que no sea posible leerlos. La información solo podrá leerse cuando se dispone de la contraseña o el código de cifrado y se aplica la clave previamente acordada. Además, es posible cifrar todo un dispositivo (por ejemplo, un disco duro), haciendo ilegible todo su contenido, o cifrar solamente determinadas carpetas o archivos con información confidencial.[9]

---

[8] ABANLEX “Informe Sobre La Necesidad Legal De Cifrar Información Y Datos Personales” disponible en: https://www.abanlex.com/wp-content/Sophos/Informe_II.pdf

[9] GDX GROUP DIGITAL TRANSFORMATION “Cuándo es necesario cifrar los datos” disponible en: https://gdx-group.com/cuando-es-necesario-cifrado-de-datos/

7.1.2 Tipos De Algoritmos

Hay dos tipos básicos de algoritmos de encriptación:

Los algoritmos de cifrado simétrico más comúnmente usados son los cifradores de bloques. Un cifrado de bloques procesa la entrada de texto claro en bloques de tamaño fijo y genera un bloque de texto cifrado del mismo tamaño para cada texto claro

- ***Clave secreta (o clave simétrica)****:* utiliza la misma clave para cifrar y descifrar un mensaje. Estos métodos de cifrado se usan principalmente para proteger información que se almacena en un disco duro o para transmisión de datos entre ordenadores. El algoritmo de encriptación más usado de este tipo es el DES (Data Encryption Standard) que usa una clave de 56-bits. Un mensaje cifrado con este algoritmo es bastante seguro aunque ya puede ser descifrado con máquinas muy potentes en menos de un día, por lo que su uso está restringido a ámbitos civiles. Otros algoritmos comúnmente usados son el RC2, RC4, RC5 e IDEA. La mayoría de estos algoritmos tienen patente, aunque su uso público está permitido[7]

- ***Clave pública (o clave asimétrica)*****:** que utiliza una clave pública para cifrar el mensaje y una clave privada para descifrarlo De esta forma cualquiera puede cifrar un mensaje pero solo quien tenga la clave privada puede descifrarlo. Esto sirve para poder enviar un mensaje a un determinado destino sin que otro pueda descifrarlo. El objeto de estos métodos es la de asegurar la integridad y la autentificación del origen de los datos (por ejemplo, usando firmas digitales). RSA es el algoritmo de encriptación más conocido de clave pública. RSA utiliza una clave pública que es usada para cifrar el mensaje y una clave privada que es usada para descifrar el mensaje. [7]

Cuadro Comparativo Algoritmo Simétrico y Asimétrico

	VENTAJAS	DESVENTAJAS	SEGURIDAD	UTILIDADES	ALGORITMOS	LONGITUD DE LA CLAVE
SIMETRICA	Este sistema es eficiente en un grupo muy pequeño de usuario, ya que solo se requiere de una clave. Se puede utilizar por muchos años Su uso es sencillo Su velocidad es superior	Es necesario compartir la clave por medios que no necesariamente puede ser no seguros	Integridad Confidencialidad Autenticidad	El cifrado de mensaje es una de sus principales usos Además del cifrado de grandes volúmenes de datos	DES su tamaño de clave de 56 bits TRIPLE DES su tamaño de clave de 128 bits a 256 bits BLOWFISH el cual cuenta con un tamaño de clave de 128 a 256 bits AES con un tamaño de clave de 192 a 256 bits	54 bits (vulnerable) 256 bit (seguro)
ASIMETRICA	Se requiere de un número reducido de claves Además no se requiere trasmitir la clave privada entre el emisor y receptor Permite autenticar quien está utilizando la clave privada	Es más lenta en su proceso Se requiere de un procesos computacional para la generación de las clave La clave pública se debe de compartir con todas las personas.	Confidencialidad Integridad Autenticidad , no repudio	Cifrado de mensajería Uso en firmas digitales Intercambio de claves	**RSA** su tamaño de clave debe de ser mayor o igual a 1024 bits **DSA** su tamaño de clave debe estar entre 512 bits y 1024 bits **ElGamal** su tamaño de clave debe de estar entre los 1024 bit y los 2048 bits	1024 bits mínimos

Fuente: Fundamentos de Seguridad en Redes Aplicacione y Estandares-William Stallings. Disponible en: https://infosegur.wordpress.com/unidad-4/criptografia-simetrica-y-asimetrica/

7.1.3 Firma Digital

La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación.

La firma digital se basa en la propiedad ya comentada sobre que un mensaje cifrado utilizando la clave privada de un usuario sólo puede ser descifrado utilizando la clave

pública asociada. De tal manera, se tiene la seguridad de que el mensaje que ha podido descifrarse utilizando la clave pública sólo pudo cifrarse utilizando la privada. La firma digital, por tanto, es un cifrado del mensaje que se está firmando pero utilizando la clave privada en lugar de la pública. [10]

7.1.3.1 Características de Una Firma Digital

Requisitos de la firma digital:

a) Debe ser fácil de generar. [8]
b) Será irrevocable, no rechazable por su propietario. [8]
c) Será única, sólo posible de generar por su propietario. [8]
d) Será fácil de autenticar o reconocer por su propietario y los usuarios receptores.
e) Debe depender del mensaje y del autor. [8]

7.1.4 Protocolos Criptográficos

Protocolo Criptográfico es un protocolo (es decir un conjunto bien definido de etapas, implicando a dos o más partes y acordado por ellas, designado para realizar una tarea específica) que utiliza como herramienta algún algoritmo criptográfico. Existe una amplia variedad de protocolos criptográficos, que dan respuesta a diferentes objetivos.[11]

---

[10] Ramió Aguirre Jorge, "Libro Electrónico de seguridad informática y criptografía" versión 4.1, 6ª edición, Marzo 2006, Madrid España.

[11] TENA AYUSO, Juan "Protocolos Criptográficos" {En línea} {11 de marzo de 2017} disponible en: http://www.criptored.upm.es/guiateoria/gt_m023c.htm

Algunos de los protocolos de uso general más utilizados son:

- ***SSL (Security Sockets Layer):*** Es el protocolo dominante para encriptar la comunicación en general entre los navegadores y servidores. Es un sistema de encriptamiento de flexible de propósito general, tu probablemente lo has usado aún que no te has dado cuenta, puesto que está construido dentro de los navegadores (Browser) de Netscape Navigator .y Microsoft La habilidad del navegador para encriptar las comunicaciones fue un punto importante de venta para Nestcape, un característica enfatizada por frecuentes advertencias desplegadas por el navegador cuando la criptografía no estaba siendo usada. [12]

- ***SET (Secure Electronic Transaction)*** es un protocolo especializado para salvaguardar transacciones basadas en tarjetas de crédito. [10]

- ***IP SEC*****:** Es uno de los más empleado es un grupo de extensiones de la familia del protocolo IP pensado para proveer servicios de seguridad a nivel de red,(GRE 47) el protocolo de Encapsulación de Enrutamiento Genérico. Se emplea en combinación con otros protocolos de túnel para crear redes de internet virtuales. Conjunto de protocolos definido como parte de IPv6 (nueva versión), permite cifrar y/o autentificar todo el tráfico a nivel IP. [13]

- **FUNCIONES HASH:** También conocidas como huellas digitales (finger-prints), son funciones de una vía que se basan en operaciones matemáticas

---

[12] GOMEZ CARDENAS, Roberto “Protocolos Criptograficos” {En línea} {11 de marzo de 2017} disponible en: http://www.cryptomex.org/SlidesSeguridad/ProtoCripto.pdf

[13] UNIVERSIDAD DE LA RIOJA “Cifrado de comunicaciones” {En línea} {11 de marzo de 2017} disponible en: http://www.unirioja.es/servicios/si/seguridad/difusion/cifrado.shtml

para tomar a la entrada un conjunto de datos de longitud variable; y, convertirlos en información de longitud fija a la salida. La función hash debe cumplir los siguientes requisitos: imposibilidad de obtener el texto original a partir de la huella digital, imposibilidad de encontrar un conjunto de datos diferentes que tengan la misma huella digital, transformar un texto de longitud variable en una huella de tamaño fijo, facilidad de empleo e implementación. A continuación se muestra algunos ejemplos de funciones de una vía:

1) **Algoritmo MD5**.- Es una función hash de 128 bits. Este algoritmo se usa para firmas digitales, más no para encriptar mensajes. La información original no se puede recuperar ya que hay pérdida de datos.

2) **SHA-1**.- En una función de 160bits, la compresión es más compleja que la función de MD5, por lo que es más lento que MD5; sin embargo el contar con una mayor longitud (160bits contra 128bits), hace que SHA-1 sea más robusto y seguro.

3) **SHA-2**.- En esta función los rangos de salida han sido incrementados: SHA-224, SHA256, SHA-384, y SHA-512. Convirtiéndose en el más seguro SHA-512, pues cuenta con mayor número de bits a la salida.

7.1.5 Beneficios Del Cifrado De Datos

- ***Proteger la información confidencial de una organización*****:** si la información sensible de una compañía llegara a caer en las manos equivocadas, pueden producirse perjuicios económicos, pérdidas de ventaja competitiva, o incluso significar el cierre de la empresa. En este sentido, la encriptación ayuda a proteger Información delicada, como los datos

financieros, de los colaboradores, procedimientos o políticas internas, entre otros. [14]

- ***Proteger la imagen y el prestigio de una organización*:** existe cierta información que si es robada, puede dañar la imagen corporativa. Un ejemplo notable, son los datos que se almacenan de los clientes; el robo de los mismos puede afectar considerablemente a la empresa, llevándola a pérdidas irrecuperables. [12]

- ***Proteger las comunicaciones de una organización:*** el cifrado es comúnmente asociado con las transmisiones de datos, dado que los mensajes enviados por una empresa suelen viajar por canales o infraestructura externa, como Internet, y son susceptibles a ser interceptados. El ejemplo más significativo, es el cifrado de los mensajes enviados por correo electrónico. [12]

- ***Proteger dispositivos móviles e inalámbricos***: todos aquellos dispositivos que salen de la empresa, como teléfonos celulares, tablets o computadoras portátiles, pueden ser extraviados y/o robados. Ante estas situaciones, es importante asegurarse de que ningún tercero esté autorizado pueda acceder a la información. [12]

7.1.6 Algunas Herramientas De Cifrado De Open Source

El cifrado de información se puede implementar de forma fácil y económica ya que sólo debemos contar con las herramientas correctas.

---

[14] ESET “Cifrado De La Información: Guía Corporativa” {En línea} {10 de marzo de 2017} disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014.pdf

Además existen mecanismos de seguridad que puede implantar como herramientas técnicas y métodos técnicos que se utilizan para implementación de los servicios de seguridad. Un mecanismo puede funcionar por sí solo, o con otros, para proporcionar un servicio determinado.

En el mercado se cuenta con herramientas de cifrado disponibles de manera gratuita que garantiza que el algoritmo de cifrado implementado este solo con la persona que lo implemente garantizando la integridad y seguridad del programa. Algunas de estas herramientas son:

Figura 1. Logo Aplicación DiskCryptor

Fuente: https://diskcryptor.net/

DiskCryptor es una solución Open Source para el cifrado de particiones y discos duros completos. Al igual que TrueCrypt podemos cifrar archivos, particiones o dispositivos de almacenamiento externo USB. Trabaja con los siguientes algoritmos: Twofish, AES y Serpent –es un algoritmo de cifrado simétrico de

bloques, utiliza un tamaño de bloque de 128 bits, tamaños de llave de 128, 192 y 256 bits y consta de 32 rondas–, y las posibles combinaciones entre ellos. [15]

Los algoritmos de cifrado simétrico que soporta son AES con 256 bits, Twofish y también Serpent, incluyendo las combinaciones de todos ellos para dotar al sistema de una mayor seguridad. De hecho, la propia herramienta nos da la posibilidad de lanzar un benchmark y comprobar el rendimiento que seremos capaces de tener dependiendo del algoritmo que elijamos:

Figura 2. Logo Aplicación VeraCrypt

Fuente: https://www.veracrypt.fr/en/Downloads.html

VeraCrypt es una solución de cifrado Open Source basada en TrueCrypt. Utiliza la misma interfaz y características con la diferencia que incluye un número mayor de iteraciones para el cifrado de la información. La desventaja del aumento significativo de iteraciones es que VeraCrypt es más lento al momento de implementar lectura y escritura de información en el disco. Al igual que TrueCrypt, VeraCrypt incluye algoritmos de cifrado tales como AES, Twofish y Serpent. [16]

---

[15] DiskCryptor"Solución de cifrado de partición de código abierto". Disponible en: https://diskcryptor.net/

[16] VeraCrypt. Disponible en: https://www.veracrypt.fr/en/Downloads.html

Figura 3. Logo Aplicación OpenStego

Fuente: https://www.openstego.com

OpenStego es una herramienta Open Source que permite utilizar la técnica de Estenografía para guardar información de manera segura a través de imágenes, música y/o videos. En términos simples, con OpenStego podemos enviar mensajes ocultos dentro de una imagen o cualquier archivo multimedia. La Estenografía es una rama de la criptografía.[17]

- OpenStego está escrito en Java puro y debería ejecutarse en todas las plataformas compatibles con Java. Se ha probado en MS Windows y Linux, pero tampoco debería tener ningún problema en otras plataformas. Por favor, informe de errores si encuentra alguno.
- Admite cifrado de datos basado en contraseña para una capa adicional de seguridad. Se admiten los algoritmos AES 128 y AES 256.
- Utiliza una arquitectura basada en complementos, donde se pueden crear varios complementos para diferentes tipos de algoritmos esteganográficos / de marca de agua. Actualmente, admite dos complementos: RandomLSB (Randomized LSB) para ocultar datos y el algoritmo de Dugad para la marca de agua, pero se pueden crear fácilmente nuevos complementos para otros algoritmos. Los complementos también se pueden agregar fácilmente para otro tipo de archivos de portada como archivos de audio.[17]

[17] Samir Vaidya “OpenStego” {En línea} {11 de marzo de 2017} disponible en: https://www.openstego.com/index-es.html

Figura 4. Logo Aplicación OpenPuff

Fuente: https://embeddedsw.net/OpenPuff_Steganography_Home.html

OpenPuff es una herramienta Open Source para Windows de Estenografía. Fue una de las primeras herramientas de estenografía. Soporta imágenes en formato BMP y JPG, archivos de audio MP3 y WAV, archivos de video MPG4, entre otros. [18]

- Criptografía de clave simétrica de 256 bits + 256 bits (con extensión de contraseña KDF4) [18]
- Codificación de datos de clave simétrica de 256 bits (barajado basado en CSPRNG) [18]
- Blanqueamiento de datos de clave simétrica de 256 bits (mezcla de ruido basada en CSPRNG) [18]
- Codificación de bits de portadora no lineal adaptativa [18]

[18] OpenPuff. Disponible en: https://embeddedsw.net/OpenPuff_Steganography_Home.html

Figura 5. Logo Aplicación GNUGPG

Fuente: https://www.gnupg.org/

GNUGPG es una implementación libre de PGP (Pretty Good Privacy). GNUGPG permite el cifrado y firma de datos y de las comunicaciones. GNUPGP es una de las herramientas de cifrado utilizadas por Edward Snowden ex-contratista de la NSA.[19]

Soporte protocolos Criptograficos como SHA-256 y SHA-512 pertenecen a un grupo de hashes conocidos colectivamente como "SHA-2". PGP llama a SHA-256 y SHA-512 con los nombres no estándar "SHA-2-256" y "SHA-2-512", [19]

Figura 6. Logo Aplicación OpenSSH

Fuente. https://www.openssh.com/

OpenSSH es una herramienta Open Source de acceso remoto a través del protocolo IP. OpenSSH es la alternativa perfecta al protocolo Telnet. Con OpenSSH podemos conectarnos de manera segura a un dispositivo en la red, ya que la

---

[19] GNUPG "El Guardia de privacidad de GNU" {En línea} {11 de marzo de 2017} disponible en: https://gnupg.org/

información que viaja entre ambos nodos va cifrada utilizando algoritmos de cifrado simétricos. OpenSSH también incluye capacidad de Tunneling y autenticación.[20]

Además gestiona claves RSA y proporciona seguridad para FTP (File Transfer Protocol)

OpenSSH implementa todos los algoritmos criptográficos necesarios para la compatibilidad con las implementaciones SSH que cumplen con los estándares [20]

Figura 7. Logo Aplicación SSL

Fuente: https://www.openssl.org/

OpenSSL es un la implementación Open Source del protocolo SSL (Secure Socket Layer). Este protocolo permite el cifrado de información a través de la red. Su gran adopción es gracias a que no es necesaria la instalación de un software cliente para cifrar la información entre dos dispositivos, ya que SSL viene instalado en prácticamente el 99% de todos los navegadores web. Este SSL protocolo es utilizado para realizar de manera segura la mayoría de transacciones financieras en línea. OpenSSL es también utilizado como solución de VPN (Virtual Private Network) como alternativa al protocolo IPSEC, principalmente en la conectividad de usuarios remotos.[21]

---

[20] OpenSSH 7.6 “Open SSH keeping your comuniques secret” {En línea} {11 de marzo de 2017} disponible en: https://www.openssh.com/

[21] Abrir SSL Kit de herramientas de criptografía y SSL / TLS disponible en:https://www.openssl.org/

Los algoritmos criptofiguras que implementa son: AES, Blowfish, Camellia, SEED, CAST-128, DES,IDEA, RC2, RC4, RC5, TDES, GOST 28147-89, RSA y DSA.

Figura 8. Logo Aplicación Tor

Fuente: https://www.torproject.org/

TOR es una aplicación de código abierto que nos ayuda a mantener nuestra privacidad mientras navegamos por Internet. Cuando descargamos e instalamos TOR en nuestro ordenador, nos conectamos a una red P2P (Peer to Peer) totalmente cifrada utilizando el algoritmo de encriptación AES, donde el tráfico que sale de nuestra computadora es ilegible para cualquiera que trate de ver el contenido de nuestras comunicaciones. [22]

[22] Navega con Privacidad.Explora libremente.Defiéndete de la vigilancia de red y el análisis de tráfico. Elude la censura.disponible en:https://www.torproject.org/

Figura 9. Descripción aplicación USB Safe Guard

Fuente: usbsafeguard.altervista.org/download.html

En la actualidad uno de los recursos a la hora de llevar o almacenar información son los dispositivos o memoria USB (de Universal Serial Bus) y una forma de cuidar la información podría ser el cifrado. Debido a la importancia para cualquier persona o empresa y más si los archivos son secretos; el cifrar las memorias USB facilitará la movilización de información fuera del contexto de red e internet, a continuación se describirán algunos programas que podrán ser de utilidad:

USB Safe Guard: esta Aplicación que se ejecuta sobre la memoria USB, el único problema es que la versión gratuita tiene un límite de 2GB para cifrar información.[23]

El software funciona cifrando sus datos utilizando el algoritmo de cifrado AES de 256 bits [23]

[23] pen drive de forma segura disponible en: usbsafeguard.altervista.org/download.html

Figura 10. Logo de aplicación Bitlocker

Fuente: https://www.muycomputerpro.com/movilidad-profesional/2017/09/19/bitlocker-guia/

Bitlocker: Aplicación que viene incorporada en los sistemas Windows en las versiones Profesional y Enterprise, puede ser de mucha ayuda.

Está diseñado para proteger los datos al proporcionar cifrado para volúmenes enteros. Por defecto se utiliza el algoritmo de cifrado estándar AES en modo CBC con una clave de 128 bits

Figura 11. Logo Aplicación Rohos mini drive

Rohos Mini Drive – Rohos

Fuente: https://www.rohos.com/products/rohos-disk.../rohos-mini-drive/

Rohos mini drive: Es una aplicación libre y puede cifrar archivos hasta 8GB en su versión portable. [24]

Rohos Mini Drive usa los más fuertes algoritmos para codificar los datos AES (256 bits). Se utiliza el estándar de algorítmico de cifrado aprobado por NIST

Además la partición cifrada está protegida por la contraseña.

[24] Rohos Mini Drive disponible en https://www.rohos.com/products/rohos-disk.../rohos-mini-drive/

7.1.7 Análisis De La Utilización Del Cifrado En Colombia

Según Microsoft, Colombia es el tercer país en Latinoamérica con mayor índice de cibercrimen. De acuerdo con cifras avaladas por el IDC Colombia (empresa dedicada al análisis del mercado de Tecnología Informática y telecomunicaciones), los ciberataques han aumentado entre el 30% y el 40% en América Latina, una de las zonas con mayor actividad en el mundo. Durante 2015, se registraron más de 20 violaciones a la seguridad por segundo en la región, lo cual equivale a 400 mil vulneraciones a causa de virus. Por su parte, en el mismo año, Colombia ha sido el tercer país más afectado por el cibercrimen con 5 millones de ataques informáticos, seguido de Brasil y México con 27 millones y 16 millones de incidentes de este tipo respectivamente.

Según la compañía de ciber seguridad Digiware, Colombia participó con el 8,05% del total de los delitos informáticos de América Latina, lo que equivale a pérdidas por más de US$6.179 millones. Con estas cifras, Colombia es quinto en la clasificación latinoamericana en materia de ataques informáticos[25].

En la actualidad en muy pocas empresas colombianas dentro de sus planes de seguridad de sus datos se encuentra la implementación de cifrado de información, por desconocimiento o por que en Colombia no existen normas claras sobre cifrado de información.

---

[25] Ontological Model of Cybercrimes: Case study Colombia. Marin, Jhon; Nieto, Yuri; Huertas, Freddy; Montenegro, Carlos. Disponible en: https://search.proquest.com/openview/ef48269d2b309b4657581d7bc7b8172a/1?pq-origsite=gscholar&cbl=1006393

Con respecto a las empresas de telecomunicaciones, existe la ley de inteligencia y contrainteligencia (Ley No. 1621 de 2013) establece que los operadores de servicios de telecomunicaciones deberán ofrecer el servicio de llamadas de voz cifradas a personal del alto gobierno y de inteligencia (Ley 1621 de 2013. Parágrafo 2 del artículo 44). Lo que limita la prestación de este servicio a cierta parte del estado.[26]

En algunas empresas del país está implementada la herramienta token o firma digital, provista por empresas como certicamara o GSE (Gestión De Seguridad Electrónica), la cuales son líderes en certificados digitales y seguridad informática.

7.1.8 Sistemas De Cifrado En La Actualidad

En los últimos años el sistema de cifrado mejora de forma significativa, en la actualidad cifrar datos se ha convertido en una herramienta de gran ayuda para la seguridad de la información.

Es cierto que el cifrado de datos, existe hace varios años, lo mismo ocurre con los múltiples algoritmos que han contribuido al mejoramiento del internet actual.

No es de ocultar que en la actualidad existen infinidad de delitos informáticos como fugas de información, suplantación de identidad, espionaje corporativo y es por esta razón que la criptografía vuelve a tomar fuerza.

---

[26] LEY 1621 DE 2013 (Abril 17)por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones en ".http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1685400

Edward Snowde en una de sus entrevistas, comenta que el cifrado de datos debe ser una cultura de todo tipo de profesionales, y sobre todo en aquellas que manejen información sensible. Se ha vuelto tan importante el cifrado que empresas como Apple y Google, en sus últimos sistemas operativos han incorporado el cifrado de datos.

Desde la aparición del IOS8 en el año 2015 que utiliza un sistema de cifrado que impide a Apple leer la información del usuario, aunque a unos gobiernos no ha caído muy bien esta implementación, lo que ha generado múltiples críticas, y lo que argumentan es que con este cifrado va ser más complicado perseguir delincuentes informáticos.

Así mismo, Whatsapp anunció que está implementando el cifrado de datos “end to end”, esto significa que el mensaje de chat se cifra de forma segura y solo podrá leerlo el que lo genera y el destinatario.

Es tan atrayente lo que está pasando con las nuevas aplicaciones tecnológicas y el cifrado, que algunas plataformas como Telegram están ofreciendo premios de hasta 300.000 dólares y BITCOIN para la personas que logren resolver el algoritmo que las fundamenta, los participantes se encontrarán con un ambiente simulado donde tendrán la libertad de monitorear el tráfico de mensajes, además de tomar el supuesto control del servidor.

En el mercado tecnológico actual se pueden conseguir aplicaciones que ofrecen cifrado de datos, como servicios en la nube, correo electrónico, chat, plataformas de comunicación, dispositivos, los cuales están construidos sobre bases criptográficas

Uno de los actuales sistemas de cifrado es el de extremo a extremo este utiliza una combinación de algoritmos (llaves) para identificar a un usuario y otros algoritmos que identifican a una conversación para cifrar mensajes.

Este sistema de cifrado se ha venido utilizando en muchas aplicaciones de mensajería instantánea, el cual es una medida de seguridad que se encarga de encriptar los contenidos transmitidos para que solo puedan ser vistos por el emisor y el receptor. En la actualidad, el WhatsApp es una de las aplicaciones que está utilizando este tipo de cifrado por su alta eficiencia.

Pero el cifrado de extremo a extremo como cualquier otro sistema tiene su falla, por ejemplo, si alguno de los dispositivos está infectado por malware o controlado por un atacante, a pesar del sistema de encriptado, el intruso puede acceder a los mensajes e información sin que los integrantes de la conversación se percaten de ello.

"Existen excelentes servicios de cifrado de extremo a extremo, pero por definición dependen de que el dispositivo permanezca seguro", explica el Dr. Jiangshan Yu, de la Universidad de Luxemburgo. "Una vez que se ha comprometido un dispositivo, poco podemos hacer. Ese es el problema que queríamos resolver".

La solución que han hallado estos investigadores es un protocolo que hace que los atacantes dejen evidencias de su acceso, poniendo a los usuarios en alerta. Se llama DECIM (Detecting Endpoint Compromise in Messaging) y obliga al dispositivo del destinatario a certificar de manera automática los nuevos pares de claves que

se solicitan en el encriptado, guardando los certificados en un libro público a prueba de manipulaciones. [27]

Los sistemas de cifrado utilizan pares de claves criptográficas para que el remitente y el destinatario las desencripten. En caso de que el teléfono móvil haya sido hackeado, los atacantes pueden robar las claves para acceder a los mensajes sin ser descubiertos. Sin embargo, con el nuevo protocolo DECIM esta acción deja un rastro en el libro público de certificados, poniendo alerta a los implicados en la conversación. [26]

Otra de Las tecnologías es la biometría, esta utiliza la criptografía, lo mismo pasa con el uso de firmas digitales y electrónicas. El mayor ejemplo de la criptografía, es cuando da click en el candado de un sitio web, en él se puede ver algoritmos como el SHA1, RSA, los cuales integran muchos certificados digitales de sitios web.

7.1.9 Costos

La implantación de cifrado en la empresa dependerá de la capacidad de adquisición que tenga ésta. En este proyecto se pretende que sean utilizados software libre o sistemas operativos como Linux, ya que este sistema operativo es uno de los mejores en cuanto a seguridad informática y los costos son muy bajos, de manera que se reduzcan gastos y se gane seguridad, permitiendo la implementación y creación de bancos de trabajo en las empresas lo que permite que en las organizaciones se puedan aplicar las herramientas como experimento previo a su aplicación real, según las necesidades y además al no pagar licencias se podrán experimentar y ajustar a las necesidades con un costo muy bajo.

---

[27] Vivo HD Online “Nuevo protocolo mejora la seguridad en el cifrado de mensajes” {En línea} {12 de marzo de 2018} disponible en: https://vivofullperiodicos.blogspot.com.co/2017_09_24_archive.html

8. MARCO LEGAL

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

1. Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

2. Capitulo Segundo: De los atentados informáticos y otras infracciones.

8.1 Capitulo Primero

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de

100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien “sustraiga” e “intercepte” dichos datos a pedir autorización al titular de los mismos.

Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

8.2 Capítulo Segundo:

Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. [28]

[28] LEY 1273 DE 2009 (Enero 05) {En línea} {12 de marzo de 2018} disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

9. HERRAMIENTAS UTILES PARA LA PROTECCIÓN DE DATOS EN LAS EMPRESAS

En la actualidad existen infinidad de herramientas que se utilizan para la protección de la información de las empresas así como planes de seguridad que se pueden implementar de forma económica y muy eficaces, pero aquí se realizara una corta descripción de algunas aplicaciones de software libre, (donde se debe tener en cuenta que no todas son gratuitas).

Lo primero que hay que aclarar es que las herramientas de software libre siempre han sido discriminadas por la creencia de que no tienen la misma estabilidad y soporte que tienen los sistemas pagos.

Lo anterior ha venido siendo desmentido, ya que en estos momentos existen organizaciones que brindan un excelente soporte y además cuentan con un gran prestigio, otro punto a favor de la herramientas de software libre es que ya está disponible en todo el mundo y en casi todos los idiomas, lo que nos permite que cualquier fallo que se presente pueda ser compartido y mejorado.

Todas las empresas buscan economizar en sus gastos y una manera de hacerlo puede ser la implementación de software gratuito, de los cuales algunos están diseñados para que cualquier persona pueda manejarlo sin tener amplios conocimientos en programación. Además se tiene la ventaja de que estos sistemas son más confiables en lo que respecta a la seguridad.

Dentro de las empresas el intercambio de información viene jugando un papel de gran importancia, por esta razón se dará a conocer algunas herramientas de gran utilidad y de fácil instalación y manejo.

La primera es mailvelope, esta herramienta básicamente permite cifrar el envío de correos electrónicos, se puede utilizar de forma personal o empresarial ya que como se pueda analizar en la actualidad, la mayoría de las personas y algunas empresas se comunican mediante correo electrónico y según noticias recientes, la información se ha convertido en pública, ocasionando la perdida de privacidad y desinformación puesto que cualquier persona puede modificar o cambiar el contenido de la información (MAILVELOPE o Gpg4win) pueden ser una pequeña ayuda para mantener la confidencialidad e integridad de la información.

Descripción de esta herramienta:

MAILVELOPE - ENCRIPTACIÓN OPENPGP PARA WEBMAIL

MailVelope es una extensión para los navegadores Google Chrome y Mozilla Firefox completamente gratuita y muy fácil de usar, tuvo sus inicios en el año 2012 y desde entonces esta extensión permite enviar y recibir mensajes de correo electrónico cifrados desde los servidores de correo electrónico conocidos como son Gmail, Google App, GMX, Outlook.com, Yahoo! Mail, Posteo, WEB.DE. Tiene como característica especial que sigue el estándar Open PGP (Pretty Good Privacy), para el cifrado, utilizando una combinación de clave pública y cifrada simétrica (o clave privada). [MailVelope es de código abierto y está basado en la librería OpnePGP.js, una librería OpenPGP para Java Script La última versión disponible actualizada día el 6 de marzo de 2018 es la 2.2.0 tiene una capacidad de 1.64 Mbit y disponible en 15 idiomas. [29]

[29] MAILVELOPE - ENCRIPTACIÓN OPENPGP PARA WEBMAIL disponiblen en https://securityinabox.org/en/guide/mailvelope/web/

Algunas características

- Ofrece cifrado de extremo a extremo lo que garantiza confidencialidad de la información
- Se integra directamente a las interfaces de usuario de los servicios de correo como Gmail, Google App, GMX, no se requiere copiar y pegar porque mailvelope agrega los controles para cifra y descifrar en el servicio de correo favorito.
- Se pude configurar para que funcione con la mayoría de proveedores de correo electrónico.
- Asegura las comunicaciones personales y profesionales por correo electrónico.
- Mailvelope depende una forma de criptografía de clave pública *que requiere que todo usuario genere su propio par de* claves.

Modo de uso

MailVelope se instala en los navegadores Firefox y/o Chrome, cuando esta extensión ha sido instalada podemos empezar a utilizarla, generando nuestras propias claves PGP, la pública y la privada para garantizar privacidad en las comunicaciones telemáticas. De esta forma cuando se redacta un correo aparecerá un candado el cual podremos pulsar para cifrar el mensaje. Si recibimos un mensaje cifrado el proceso es inverso, inicialmente aparecerá el mensaje con un candado sobre impreso en el mensaje. Para poder leer el mensaje damos click en el candado para introducir la clave.

La segunda herramienta que se puede recomendar es GPG4WIN la cual posiblemente es la más completa puesto que permite la utilización de firma digital y cifrado, lo que genera una mayor seguridad a la hora de enviar información a través de correo electrónico.

¿Qué es Gpg4win?

Es una herramienta que les permite a los usuarios transportar correos electrónicos y archivos de forma segura con la utilización de encriptación y firmas digitales. La encriptación protege el contenido contra una parte no deseada que lo lee. Las firmas digitales se aseguran de que no se haya modificado y provenga de un remitente específico.

Gpg4win es compatible con los estándares de criptografía relevantes, OpenPGP y S / MIME (X.509) y es la distribución oficial de GnuPG para Windows. Lo mantienen los desarrolladores de GnuPG. Gpg4win y el software incluido con Gpg4win son Software Libre (Código Abierto, entre otros, de forma gratuita para fines comerciales y no comerciales).

La creación de Gpg4win fue respaldada por la Oficina Federal Alemana de Seguridad de la Información (BSI) [30]

- utiliza una longitud de clave de 2048 bits de forma predeterminada [30]
- El algoritmo predeterminado para firmar y cifrar es RSA. [30]

Otras herramientas son las de cifrado de USB

Dentro de las herramientas de dispositivos de almacenamientos tenemos:

BitLocker: Esta aplicación viene incluida dentro del sistema operativo Windows es una herramienta muy sencilla de utilizar y de una seguridad muy efectiva. Esta

[30] Acerca de Gpg4win {En línea} {13 de junio de 2018} https://www.gpg4win.org/about.html

genera una clave de recuperación por si el usuario olvida la contraseña y ofrece guardarla en tu cuenta Microsoft.

Cryptainer LE encriptar dispositivos USB, también hace lo mismo con discos rígidos y CD Roms. Su nivel de encriptación utiliza llave de 448 bits. Cree y envíe adjuntos encriptados de correos electrónicos para que sean desencriptados utilizando una clave de acceso y el DecypherIT (GRATUITO)[31]

GPG4USB - CIFRADO DE ARCHIVOS Y TEXTOS DE CORREO ELECTRÓNICO
Es un programa simple, ligero y portátil que te permite cifrar y descifrar mensajes de texto y archivos. gpg4usb está basado en la criptografía de las claves públicas. Bajo este método cada individuo debe crear su propio par de claves personal. La primera clave se conoce como la clave privada. Esta clave está protegida por una contraseña o frase de acceso, que se guarda y nunca se comparte con nadie[32]

COMO INSTALAR GPG4USB

gpg4usb es una herramienta portátil que no requiere ser instalada en la computadora. El programa se encuentra como archivo comprimido Zip y debe ser extraído directamente a un disco USB o a una carpeta en la computadora. Para comenzar realiza los pasos siguientes:

1 primero nos dirigimos al link de descarga

https://www.gpg4usb.org/download.html

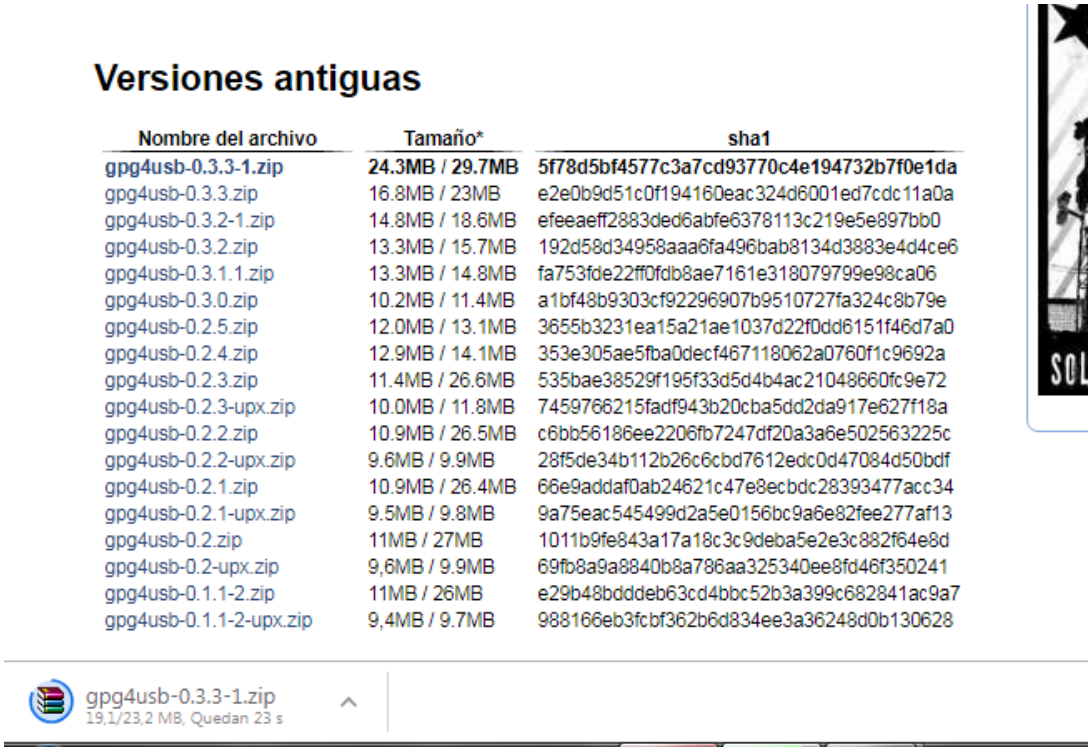
---

[31] CRYPTAINER LE {En línea} {13 de junio de 2018} http://www.cypherix.es/downloads.htm

[32] GPG4USB - CIFRADO DE ARCHIVOS Y TEXTOS DE CORREO ELECTRÓNICO https://securityinabox.org/es/guide/gpg4usb/windows/

Allí seleccionamos la versión a descargar-

Figura 12. Descarga de paquete



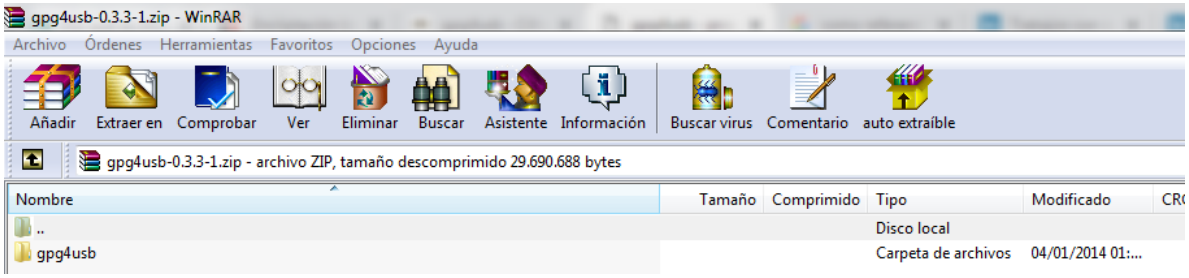
Versiones antiguas

Nombre del archivo	Tamaño*	sha1
gpg4usb-0.3.3-1.zip	**24.3MB / 29.7MB**	**5f78d5bf4577c3a7cd93770c4e194732b7f0e1da**
gpg4usb-0.3.3.zip	16.8MB / 23MB	e2e0b9d51c0f194160eac324d6001ed7cdc11a0a
gpg4usb-0.3.2-1.zip	14.8MB / 18.6MB	efeeaeff2883ded6abfe6378113c219e5e897bb0
gpg4usb-0.3.2.zip	13.3MB / 15.7MB	192d58d34958aaa6fa496bab8134d3883e4d4ce6
gpg4usb-0.3.1.1.zip	13.3MB / 14.8MB	fa753fde22ff0fdb8ae7161e318079799e98ca06
gpg4usb-0.3.0.zip	10.2MB / 11.4MB	a1bf48b9303cf92296907b9510727fa324c8b79e
gpg4usb-0.2.5.zip	12.0MB / 13.1MB	3655b3231ea15a21ae1037d22f0dd6151f46d7a0
gpg4usb-0.2.4.zip	12.9MB / 14.1MB	353e305ae5fba0decf467118062a0760f1c9692a
gpg4usb-0.2.3.zip	11.4MB / 26.6MB	535bae38529f195f33d5d4b4ac21048660fc9e72
gpg4usb-0.2.3-upx.zip	10.0MB / 11.8MB	7459766215fadf943b20cba5dd2da917e627f18a
gpg4usb-0.2.2.zip	10.9MB / 26.5MB	c6bb56186ee2206fb7247df20a3a6e502563225c
gpg4usb-0.2.2-upx.zip	9.6MB / 9.9MB	28f5de34b112b26c6cbd7612edc0d47084d50bdf
gpg4usb-0.2.1.zip	10.9MB / 26.4MB	66e9addaf0ab24621c47e8ecbdc28393477acc34
gpg4usb-0.2.1-upx.zip	9.5MB / 9.8MB	9a75eac545499d2a5e0156bc9a6e82fee277af13
gpg4usb-0.2.zip	11MB / 27MB	1011b9fe843a17a18c3c9deba5e2e3c882f64e8d
gpg4usb-0.2-upx.zip	9,6MB / 9.9MB	69fb8a9a8840b8a786aa325340ee8fd46f350241
gpg4usb-0.1.1-2.zip	11MB / 26MB	e29b48bdddeb63cd4bbc52b3a399c682841ac9a7
gpg4usb-0.1.1-2-upx.zip	9,4MB / 9.7MB	988166eb3fcbf362b6d834ee3a36248d0b130628

Fuente: https://www.gpg4usb.org/download.html

Luego de la descarga descomprime el archivo

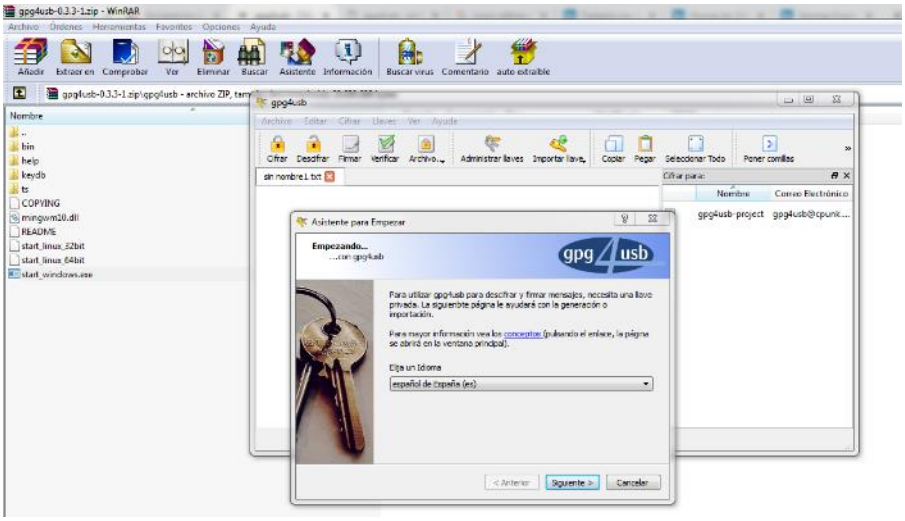
Figura 13. Procesos de descomprimir archivo



Fuente: autor

Se ejecuta el archivo start_windows.exe

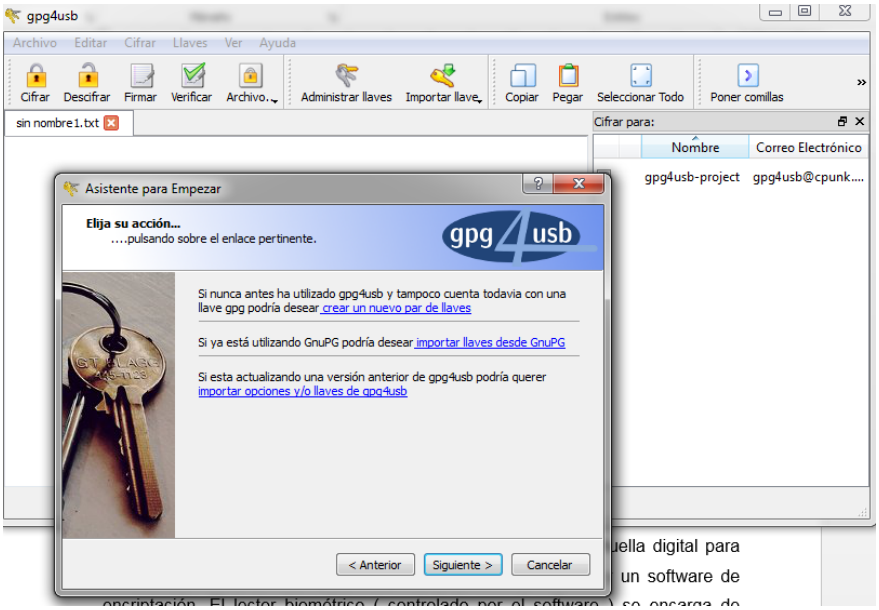
Figura 14: ejecución de punto exe



Fuente. Autor

En la ventana Asistente para empezar, pulsa Crear un nuevo par de claves.

Figura 15 ventana asistente



Fuente: Autor

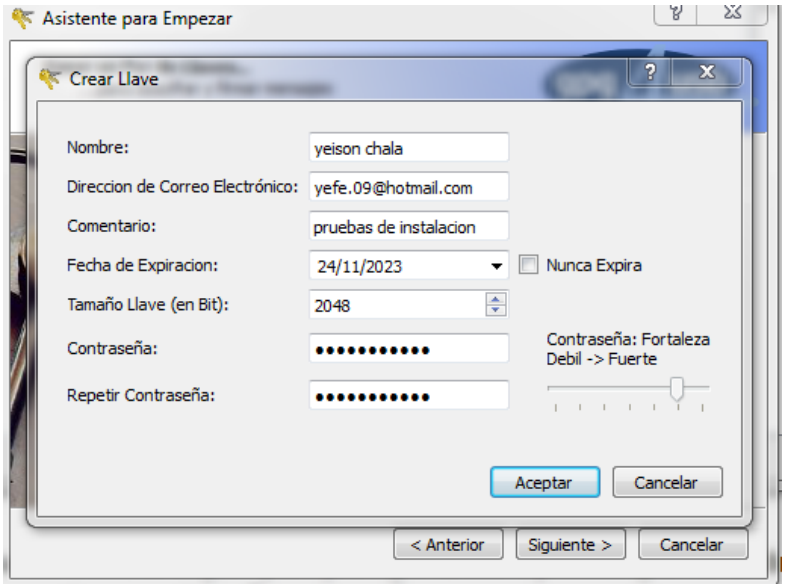
Seleccionamos Crear un par de llaves

Figura 16. Creación de las llaves

Fuente: Autor

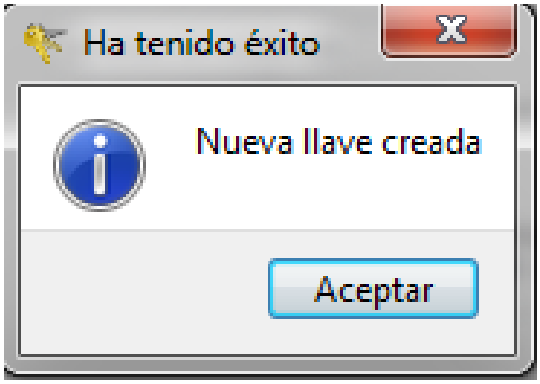
Se debe de llenar los datos correspondientes

Figura 17 cuentas y claves



Fuente: Autor

Figura 18. Llave creada



Fuente: Autor

Ya fueron creadas las llaves y queda instalado el programa

Figura 19. Final del proceso

Fuente: Autor

Token de seguridad

Es un dispositivo portátil electrónico (USB o aplicación móvil) que genera una clave de 6 dígitos de forma aleatoria de manera irreemplazable dicha clave se actualiza periódicamente cada 60 segundos.

Con un dispositivo token de seguridad las posibilidades de fraudes disminuyen en gran manera, además que permite tener una clave que lo puede identificar como titular de cierto servicio financiero, además tendrá una clave adicional por transacción. Inicialmente, el token fue una estrategia de seguridad dirigida solo a empresas, hoy en día está autorizado para cualquier persona

En Google Play se pueden encontrar aplicaciones para poder utilizar estos token en los distintos dispositivos móvil sin problema y así poder garantizar un poco de tranquilidad cuando se realice operaciones en internet a través del celular o cualquier dispositivo móvil.

Token USB Criptográfico

Figura 20: Token USB criptográfico

Fuente. http://salmoncorp.com/producto/token-usb-criptografico-2/

Cifrado Biométrico

De los distintos sistemas de biometría, el de mayor reconocimiento es el de biométrico de huella digital siendo este el que tiene más aceptación, tanto por su nivel de seguridad como el desarrollo de su tecnología y la comodidad para el usuario.

Los sistemas biométricos de huella digital, permiten a los usuarios mantener la privacidad de la información electrónica de sus archivos. Las huellas dactilares de la persona son usadas como clave de encriptación. Una vez encriptados los datos, éstos no pueden ser desencriptados a no ser que se use como clave una de las huellas dactilares que tiene permiso para hacerlo.

Los sistemas de encriptación y desencriptación biométrica de huella digital para entornos de PC están compuestos por un escáner biométrico y un software de encriptación. El lector biométrico (controlado por el software) se encarga de capturar la huella digital y el mismo software realiza el proceso de encriptación desencriptación de la información electrónica.

10. IMPORTANCIA DE LA APLICACIÓN DE MECANISMOS DE CIFRADO DE INFORMACIÓN DE LAS EMPRESAS PARA LA PREVENCIÓN DE RIESGOS COMO ATAQUES Y PÉRDIDA DE LA CONFIDENCIALIDAD

La seguridad informática se ha convertido en un factor importante en la actualidad, en un mundo interconectado donde las empresas actuales buscan expandir sus horizontes, aumentar sus ganancias y tener la capacidad de competir.

Lo anterior hace que las empresas busquen mecanismos que permitan garantizar la confidencialidad, integridad y disponibilidad de su información, en este campo es donde juega un papel importante el cifrado o encriptado de la misma.

Este es uno de los métodos más confiables y seguros a la hora de la protección de información junto a una buena planeación lo cual permitirá garantizar los pilares básicos de la seguridad informática, Integridad, Confidencialidad y Disponibilidad.

¿Para qué cifrar la información?

Con el cifrado de datos se busca que mediante el uso de una clave o contraseña la información permanezca segura y que solo las personas que la conozcan puedan tener acceso a ella.

Proteger la privacidad de los datos y la información sensible, disminuir el riesgo de alteración de datos.

En la actualidad la pérdida de confidencialidad y el abuso informático se ha incrementado en una forma abrumadora, por ello se hace necesario el establecimiento de normas de seguridad aplicables, las cuales deben ser prioridad

tanto en las organizaciones como también a nivel personal con el fin tener segura su información.

A continuación se describen algunos tips básicos que pueden ayudar:

- Cambio de contraseñas cada 3 meses.
- Implantación de claves seguras
- implantación de cláusulas de confidencialidad.
- Implementación de SGSI (Sistema De Gestión De Seguridad De La Información)

10.1 Uso de técnicas de cifrado de datos para la protección de datos

Una de las estrategias más eficientes que se pueden encontrar en el mercado son las herramientas que permiten ocultar la información o datos.

Toda empresa debe estar especialmente protegida tanto en tránsito como cuando está almacenada su información. Por esta razón debe de aplicar estrategias que permitan garantizar su seguridad.

10.1.1 Estrategias que se puede aplicar a las empresas para la protección de los datos.

A la hora de la aplicación de cualquier medida de seguridad primero deberá realizar una planificación para garantizar la protección

Clasificación de la Información susceptible de ser cifrada: La clasificación de la información debe de servir para saber qué información debe ser cifrada para garantizar su confidencialidad e integridad. Dentro de los cuales se puede tener:

- información de carácter personal o confidencial
- registros con credenciales de autenticación.
- información almacenada en dispositivos personales o de terceros
- información transferida a través de redes de telecomunicación no confiables o en soportes de almacenamiento físicos no protegidos adecuadamente.

Implementación de firma electrónica. Uso de la firma electrónica en los casos que sea necesario garantizar la autenticidad y el no repudio de la información, para realizar trámites con las administraciones Públicas o emisión de facturas.

Tipo de certificado de representación legal

- certificado de representante
- certificado de pertenencia a empresa
- certificado de persona jurídica
- certificado de factura electrónica

Certificados web otra forma para garantizar la seguridad de la información en los sitio web de las empresas, en especial si se trata de una tienda online es la adquisición de un certificados web (SSL/TLS)

- validación de dominio, de la organización y validación extendida (para tiendas online)
- para un dominio, múltiples dominios y subdominios, wildcard.

Cifrado de datos sensibles cuando se contratan servicios externos. Si se requiere de contratar servicios externos que traten datos confidenciales o sensibles, se deberá realizar la verificación de que se estén utilizando canales seguros o cifrando los datos antes de transferirlos.

- Al realizar backup en la nube de ficheros que contengan datos confidenciales o datos personales de empleados o clientes, se realizara cifrado de estos.
- si se tiene un servicio de gestión que incluya el tratamiento de datos personales (por ejemplo: nóminas, seguridad social,…) o confidenciales se debe asegurar que las transferencias de datos se realizan con canales cifrados (como por ejemplo vía VPN o cifrando los datos antes de enviarlos)

Algoritmos de cifrado autorizados. Evitar el uso de sistemas de cifrado antiguos, Se aconseja el uso de sistemas de cifrado asimétrico en pérdida de los sistemas de cifrado simétrico

Cifrado de la wifi de la empresa. La Configuración de la wifi de la empresa debe de contar con estándar de cifrado más seguro, actualmente WPA2.

Uso de protocolos seguros de comunicación se debe de realizar capacitación en las herramientas de comunicación que utilicen protocolos criptográficos actualizados

- SFTP/FTPS para la transferencia segura de ficheros
- HTTPS para la transferencia segura de datos en servicios web críticos (pagos online, descarga de información sensible, etc.)
- SSH para el acceso seguro remoto a la administración de equipos (no utilizar Telnet que no va cifrado)

Aplicaciones autorizadas para usos criptográficos se contara con una lista de las aplicaciones autorizadas para fines criptográficos.

- cifrado del disco de arranque
- cifrado de discos internos y extraíbles
- cifrado de correo; ν cifrado de backups

- cifrado de ficheros y directorios
- cifrado de dispositivos móviles

Encuesta mundial de productos de cifrado

El criptógrafo Bruce Schneier, en su blog publicó, los resultados de una encuesta que realizó, donde logro identificar 619 entidades que venden productos de cifrado de las cuales 412 están fuera de los EE. UU. Lo que cuestiona la eficacia de los mandatos estadounidenses que obliga a la creación de puertas traseras para acceder a la aplicación según la ley. También logro mostrar que cualquiera que quiera evitar la vigilancia de EE. UU. Tiene más de 567 productos para elegir. Estos productos ofrecen una amplia variedad de aplicaciones seguras como: cifrado de voz, cifrado de mensajes de texto, cifrado de archivos, cifrado de tráfico de red y moneda anónima, brindando los mismos niveles de seguridad que los productos de EE. UU. Hoy en día. [33]

Detalles de la investigación:

Hay al menos 865 productos de hardware o software que incorporan cifrado de 55 países diferentes. Esto incluye 546 productos de cifrado de fuera de EE. UU., Que representan dos tercios del total. [31]

El país no estadounidense más abundante para productos de encriptación es Alemania, con 112 productos. Esto es seguido por el Reino Unido, Canadá, Francia y Suecia, en ese orden. [31]

---

[33] Encuesta mundial de productos de cifrado {En línea} {16 de julio de 2018} https://www.schneier.com/blog/archives/2016/02/worldwide_encry.html

Los cinco países más comunes para productos de cifrado, incluido EE. UU., Representan dos tercios del total. Pero los países más pequeños como Argelia, Argentina, Belice, las Islas Vírgenes Británicas, Chile, Chipre, Estonia, Irak, Malasia, San Cristóbal y Nieves, Tanzania y Tailandia producen cada uno al menos un producto de cifrado. [31]

De los 546 productos de encriptación extranjeros que encontramos, el 56% están disponibles para la venta y el 44% son gratuitos. El 66% son propietarios y el 34% son de código abierto. Algunos productos de venta también tienen una versión gratuita. [31]

Al menos 587 entidades, principalmente empresas, venden o regalan productos de cifrado. De ellos, 374, o aproximadamente dos tercios, están fuera de los EE. UU. De los 546 productos de cifrado externos, 47 son productos de cifrado de archivos, 68 productos de cifrado de correo electrónico, 104 productos de cifrado de mensajes, 35 productos de cifrado de voz y 61 productos de redes privadas virtuales. [31]

Confidencialidad De La Información De La Empresa

La confidencialidad es garantizar que la información personal o de la organización sea protegida de tal forma que no sea divulgada sin aprobación. Dicha garantía se debe llevar a cabo por medio de un grupo de reglas o programas que permitan limitar el acceso a ésta información.

La información junto con las tecnologías y medios utilizados para su procesamiento, debe de constituirse en uno más de los activos de Información de la Entidad, los cuales se deben proteger, salvaguardar, administrar y gestionar de manera segura frente a los riesgos internos o externos, deliberados o accidéntales.

Por lo anterior las organizaciones deben de estar comprometidas con la protección, preservación y fortalecimiento de la confidencialidad, integridad, disponibilidad, accesibilidad, legalidad, confiabilidad de la información, mediante la Gestión del Riesgo y mejora continua.

Por eso muchas empresas deben de clasificar su información según su grado de importancia, el valor que este tiene para su funcionamiento y como ésta afectará su rendimiento.

11. ALGUNOS MENCANISMOS DE CIFRADO PARA EVITAR EL PLAGIO DE LA INFORMACION

Un método de cifrado se forma principalmente de dos elementos, un algoritmo criptográfico y de una o más claves secretas (clave pública, clave privada). Mientras que el algoritmo se encarga de describir el método de encriptado a utilizar. Lo que define al cifrado como un procedimiento por el cual se entrega un texto en claro y una clave al algoritmo criptográfico y se obtiene un texto cifrado.

Dentro de los mecanismos básicos del cifrado tenemos la implementación de claves a base de datos o archivos que no quiera que sean alterados.

La protección de los datos que se puedan encontrar en servidores y centros de datos, controlar el acceso a carpetas y archivos confidenciales que se guardan en unidades de disco duro de servidores locales y remotos, en unidades de red y en servidores de archivos.

La seguridad debe ser algo primordial a la hora de asignar los recursos en una empresa. La ofimática es una de las herramientas de más utilidad y a la cual no se le da gran importancia. Estos programas son muy utilizados no solo a nivel empresarial, sino también a nivel personal por parte de usuarios comunes.

11.1 Cifrar documentos

El paquete ofimático cuenta con una opción que nos permite poner contraseña a los archivos que se crean de gran importancia. Esto nos permite proteger la información frente a otros usuarios. Cifrar documentos es de gran ayuda para quienes deben

compartir su equipo con otras personas o también puede ser de gran ayuda cuando se deban de compartir documentos de Excel o Word [34]

Se puede cifrar los archivos para que nadie pueda abrirlos sin saber la contraseña. Otra forma es hacer que los documentos sean de sólo de lectura, restringir la edición u otorgar permisos sólo a ciertos usuarios.

Contraseña para archivo, los siguientes pasos:

- Lo primero es abrir el archivo en el cual se le va a insertar contraseña
- Se dirige a la opción, Archivo. En la opción Información y selecciona Proteger documento, Cifrar contraseña.
- En este paso se debe de introducir una contraseña en dos ocasiones, aceptemos.

De esta forma se tendrá un poco de privacidad de la información básica de las empresas.

Cifrado de dispositivos de almacenamiento

La implantación de mecanismos de cifrado en los dispositivos de almacenamiento como disco duro o USB puede ser un medio de seguridad básica que también puede mejorar la seguridad de los datos puesto que el trasporte de información en muchas partes se está realizando mediante estos dispositivos de almacenamientos. En lo cual el cifrado de datos puede ser de gran utilidad.

---

[34] Protección y seguridad en Excel disponible en https://support.office.com/es-es/article/protecci%C3%B3n-y-seguridad-en-excel-be0b34db-8cb6-44dd-a673-0b3e3475ac2d

A continuación se sugiere o recomienda una herramienta de gran utilidad:

1.**OpenSSL**.-Es una implementación de los protocolos SSL (Seccure Sockets Layer) y TLS (Transport Layer Security), utiliza lenguaje de programación C. Tiene versiones disponibles para los sistemas operativos Linux y Microsoft Windows, y los algoritmos criptoFiguras que implementa son: AES, Blowfish, Camellia, SEED, CAST-128, DES, IDEA, RC2, RC4, RC5, TDES, GOST 28147-89, RSA y DSA.

2. TrueCrypt.-Es una aplicación disponible para los sistemas operativos Linux y Windows. Permite crear archivos encriptados a los que se puede acceder si se conoce la contraseña y/o clave que se utilizó para su creación. Trabaja con los siguientes algoritmos: Twofish, AES y Serpent –es un algoritmo de cifrado simétrico de bloques, utiliza un tamaño de bloque de 128 bits, tamaños de llave de 128, 192 y 256 bits y consta de 32 rondas–, y las posibles combinaciones entre ellos.

3.DiskCryptor.-Soporta algoritmos de encriptación AES, Twofish, Serpent, y las combinaciones entre ellos. Realiza unbenchmarking de la velocidad de encriptación de los algoritmos. Disponible para los sistemas operativos Windows

4.VeraCrypt

Es una herramienta de cifrado de código abierto, por lo cual no se tendrá que pagar ninguna licencia para poder utilizarla y además es multiplataforma, lo que permite que se pueda utilizar en cualquier sistema operativo. Para su instalación se dirigirán a la página oficial [35]

[35] VeraCrypt {En línea} {10 de Abril de 2019} https://www.veracrypt.fr/en/Downloads.html

Principales características de VeraCrypt:

- Crea un disco virtual encriptado dentro de un archivo y lo monta como un disco real.

- Cifra una partición completa o un dispositivo de almacenamiento como una unidad flash USB o un disco duro.

- Cifra una partición o unidad donde está instalado Windows (autenticación previa al arranque).

- El cifrado es automático, en tiempo real (sobre la marcha) y transparente.

- La paralización y la canalización permiten que los datos se lean y escriban tan rápido como si la unidad no estuviera encriptada.

- El cifrado puede ser acelerado por hardware en los procesadores modernos.

- Proporciona una negación plausible, en caso de que un adversario te obligue a revelar la contraseña: volumen oculto (esteganografía) y sistema operativo oculto.[36]

[36]VeraCrypt {En línea} {10 de Abril de 2019} https://www.veracrypt.fr/en/Home.html

Infraestructura de clave pública

Figura 21. Resumen Infraestructura de clave pública

Fuente http://leoecommerce.blogspot.com/p/infraestructura-de-clave-publica.html

Una infraestructura de clave pública (en inglés: Public Key Infrastructure –PKI–) es una combinación de hardware, software, y políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital, y el no repudio de transacciones electrónicas.[37]

[37] El Manual Práctico de Supervivencia En La Administración disponible en:

https://books.google.com.co/books?isbn=8461434137

Las buenas prácticas de PKI, lograra que los usuarios eliminen posibles riesgos de fugas de datos.

El sistema PKI, es capaz de proteger correctamente objetos que poseen un identificador único (claves) y tienen la capacidad de comunicar información a través de la red, brindando integridad y no repudio al intercambio de datos que realicen. Además sirve para gestionar de forma segura la comunicación de información, también implementan mecanismos de autenticación, para certificar la identidad de quienes realizan el intercambio[38]

Donde se puede utilizar PKI

- Firmas digitales
- Firmas electrónicas
- Cifrado y descifrado de datos
- Transacciones por internet
- Autenticación de usuario
- Intercambio de correo electrónicos

Otros usos de los sistemas de PKI, de distintos tipos y proveedores, tienen muchos usos, incluyendo la asociación de una llave pública con una identidad para:

- Cifrado y/o autenticación de mensajes de correo electrónico

[38]Infraestructura de clave pública en una universidad del Paraguay disponible en : http://repositorio.uigv.edu.pe/handle/20.500.11818/692

- Cifrado y/o autenticación de documentos (ej., la firma XML o el cifrado XML si los documentos son codificados como XML).
- Autenticación de usuarios o aplicaciones (ej., logo por tarjeta inteligente, autenticación de cliente por SSL). [38]
- Bootstrapping de protocolos seguros de comunicación, como IKE y SSL.
- Garantía de no repudio (negar que cierta transacción tuvo lugar)

Módulos de seguridad de hardware (HSM)

HSM son las siglas de "Hardware Security Module" (Módulo de Seguridad Hardware)

¿Qué es un módulo de seguridad de hardware?

Es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas. El cual fue diseñado específicamente para proteger el ciclo de vida de la clave criptográfica.[39]

Los algoritmos más comunes en HSM son:

- RSA, que funciona para facturación electrónica.
- TDES, usado por el sector financiero para proteger PINS.
- Curva elíptica, es la variante asimétrica y usa claves más cortas.
- AES, es la variante simétrica y se usa para cifrar información.

---

[39] HSM {En línea} {10 de Abril de 2019} https://es.wikipedia.org/wiki/HSM

11.2 Evolución Del Cifrado

Durante décadas la necesidad de comunicación ha generado que el ser humano cree elementos para ello.

La necesidad de garantizar que las comunicaciones que se quieran trasmitir lleguen de manera segura y de forma eficiente ha obligado a la búsqueda de mecanismos que permitan la autenticidad, confidencialidad, integridad y disponibilidad de ellos.

Uno de estos mecanismos es el cifrado el cual a lo largo de la historia han venido evolucionado, con aparición de las computadoras la complejidad de cifrar datos ha cambiado ya que ha permitido la implementación de medidas más eficientes y eficaces facilitando así su implantación a continuación se hará una breve recuento de la evolución de cifrado.

Escitala

Figura 22. Imagen Escitala

Fuente: http://ojoscuriosos.com/la-escitala/

Este mecanismo de cifrado fue utilizado por los espartanos. Este sistema consistía en dos varas del mismo grosor que se entregaban una al emisor y otro receptor. Para enviar el mensaje se enrollaba una cinta de forma espiral a uno de los varas y se escribía el mensaje longitudinalmente, de forma que en cada vuelta de cinta

apareciera una letra cada vez. Una vez escrito el mensaje, se desenrollaba la cinta y se enviaba al receptor, el cual sólo tenía que enrollarla a la vara gemela para leer el mensaje original.

Por tal razón solo la persona que tuviera la otra vara podía entender el mensaje enviado. [40]

Cifrado César

Figura 23. Ejemplo cifrado cesar

Fuente: https://justcodeit.io/tutorial-cifrado-cesar-en-python/

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

---

[40] Una **escítala** (griego: *skytálē*) es un sistema de criptografía utilizado por los éforos espartanos para el envío de mensajes secretos. Está formada por dos varas de grosor variable (pero ambas de grosor similar) y una tira de cuero o papiro, a las que ambas se puede denominar escítala
https://es.wikipedia.org/wiki/Esc%C3%ADtala

Es otro método de cifrado que también fue utilizó en la edad antigua. Consistió en la sustituir determinadas letras del texto por otras letras o números. Dé tal manera que el texto sea ininteligible para aquellos que no conozcan la regla de sustitución. Por ejemplo, el texto “casa” se convertiría en “ECUC” al reemplazar cada letra por la que le sigue en el alfabeto.

Este tipo de cifrado se puede complicar tanto como se quiera, pero al final siempre existe una vulnerabilidad ante lo que se denomina un análisis de frecuencias, que consiste en estudiar con qué frecuencia aparecen los caracteres codificados en el texto y compararlo con la repetición de cada una de las letras en el lenguaje natural.[41]

Cifrado Vigenère

Figura 24: ejemplo cifrado de vigenere

Fuente: http://blog.andresed.me/2015/07/cifrado-de-vigenere.html

[41] El cifrado César y otros cifrados de sustitución monoalfabeto disponible en: http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/cesar.html

El cifrado Vigenère se basa en la sustitución de caracteres pero no mediante la aplicación de una regla predefinida, sino con una clave externa la cual debe estar en manos del emisor y del receptor para cifrar y descifrar mutuamente el mensaje. Este tipo de cifrados es virtualmente invulnerable si la clave utilizada es compleja y no se repite.

Pero en la práctica no es viable disponer de una clave distinta para cada mensaje enviado por tal razón en ocasiones se pasa a utilizar una misma clave para cifrar todos los mensajes. En el momento en que se reutiliza las claves, cualquier atacante será capaz de recopilar varios mensajes cifrados con ella, por lo que así descifrar dichos mensajes utilizando el cálculo de frecuencias.

Este cifrado soluciona la debilidad del cifrado del César en que una letra se cifra siempre igual. Se usa una clave K de longitud L y se cifra carácter a carácter sumando módulo n el texto en claro con los elementos de esta clave.[42]

[42] El cifrado de comunicaciones, uno de los inventos que ha cambiado el mundo disponible en: https://aunclicdelastic.blogthinkbig.com/cifrado-de-comunicaciones-un-invento-que-ha-cambiado-el-mundo/

Rotores

Figura 25.Maquina enigma de cuatro rotores

Fuente: https://www.u-historia.com/uhistoria/tecnico/articulos/enigma/enigma.htm

El siguiente paso en la evolución de los métodos de cifrado vino con el uso de máquinas codificadoras. Básicamente se trataba de un mecanismo en el que las sustituciones de caracteres se hacían utilizando al menos tres rotores que iban girando y modificando, así, la tabla de asignaciones en cada pulsación.

Al tratarse de una asignación dinámica, la máquina debía estar calibrada en una posición inicial determinada, ya que ese estado inicial determinaba el descifrado del mensaje. Estos estados iniciales se copiaban en un libro denominado “Libro de códigos” que se entregaba a los capitanes de los navíos para que pudieran descifrar los mensajes que recibiesen. Las páginas del libro estaban cortadas en tiras que se iban arrancando y destruyendo, de manera que si el buque era capturado no se pudiesen recuperar las claves utilizadas previamente.

La máquina codificadora más famosa fue Enigma, que se utilizó durante la segunda guerra mundial por parte del bando alemán. Finalmente sus códigos pudieron ser descifrados con la ayuda de uno de los primeros ordenadores construidos, que se utilizó para realizar un ataque de fuerza sobre los mensajes interceptados.

Con la utilización de un ordenador, se logró realizar una gran cantidad de operaciones en un tiempo corto, lo que determino la muerte de los métodos tradicionales de cifrado y el nacimiento de los métodos modernos.[43]

Cifrado de mensajes digitales

Figura 26: firma y autentificación de usuario: firma digital

Fuente. http://convista.es/encriptacion-firma-digital-sap-bcm/

Desde que los ordenadores en la actualidad son capaces de probar un gran número de combinaciones rápidamente, las técnicas de cifrado modernas han sido obligadas aumentar la complejidad de los códigos para evitar que estos puedan encontrados de forma más rápida. Por tal razón se han redoblado los esfuerzos por

[43] El cifrado de comunicaciones, uno de los inventos que ha cambiado el mundo disponible en: https://aunclicdelastic.blogthinkbig.com/cifrado-de-comunicaciones-un-invento-que-ha-cambiado-el-mundo/

construir sistemas más seguros los cuales se han concentran en el mundo digital. [44]

Un mensaje digital independientemente de su formato, se puede expresar como una cadena binaria de ceros y unos. Por eso para codificarlo es necesario generar una clave, también binaria de la misma longitud que el mensaje, y aplicarle una transformación denominada XOR, los cuales son la base de todos los cifrados que se utilizan hoy en día. Siendo resultante una tercera cadena binaria que se denomina mensaje cifrado bajo clave. Para descifrar el mensaje es preciso volver a aplicar la operación XOR sobre la cadena cifrada y la clave.

Uno de los inconvenientes de esta técnica es que, si se utiliza la misma clave para cifrar diferentes mensajes, lo que puede resultar sencillo para que un atacante la obtenga para descifrar todos los mensajes que se envié en el futuro.41

Generadores

La necesidad de que no se repita la clave de cifrado y, a la vez, cifrar mensajes arbitrariamente largos ha llevado a la creación de unos algoritmos denominados generadores, los cuales son capaces de construir claves de longitud arbitraria y una distribución estadística poco más o menos aleatoria.

Cuanto más cerca esté de una distribución aleatoria pura, más seguro será el cifrado, ya que no se podrán apreciar repeticiones. Esta técnica se utiliza en

---

[44] El cifrado de comunicaciones, uno de los inventos que ha cambiado el mundo disponible en : https://aunclicdelastic.blogthinkbig.com/cifrado-de-comunicaciones-un-invento-que-ha-cambiado-el-mundo/

situaciones en las que es necesario contar con un cifrado sencillo y rápido como en las redes wifi, comunicaciones telefónicas, de radio, etc.[45]

10 generadores online de contraseñas:

PasswordLive: este servicio es relativamente novedoso, nos permite usar una palabra clave secreta que tomará como base para generar una contraseña entre 8 y 64 caracteres. Nosotros podemos personalizar la cantidad de caracteres, y si tendrá o no números, mayúsculas, y caracteres especiales, entre otros.[46]

Strong Password Generator: con este generador podemos también crear claves con caracteres especiales, seleccionando en una drop down box la cantidad de caracteres que queremos que tenga. El resultado es una contraseña muy segura, aunque un tanto difícil de recordar.[47]

Random Generator: desde Random.org nos llega este generador de contraseñas, que permite que generemos varias contraseñas para diferentes servicios al mismo tiempo –un máximo de 100 por cada generación-. Nada más tenemos que seleccionar la cantidad de caracteres –mínimo 6, máximo 24- pero no podemos elegir si incluirá o no un carácter especial, esto viene por default.[48]

---

[45] El cifrado de comunicaciones, uno de los inventos que ha cambiado el mundo disponible en : https://aunclicdelastic.blogthinkbig.com/cifrado-de-comunicaciones-un-invento-que-ha-cambiado-el-mundo/

[46] **PasswordLive**: ¡No más contraseñas olvidadas! disponible en : http://passwordlive.github.io/

[47] Strong Password Generator: Generador de contraseña segura disponible en: https://passwordsgenerator.net/

[48] **Random Generator**: Servicio de números aleatorios verdaderos https://www.random.org/

Generate Password: con este generador nos metemos en el mundo de las llamadas “contraseñas pronunciables” que son igualmente seguras pero más fáciles de recordar. En este caso, este servicio nos genera dos contraseñas: una fuerte, completamente aleatoria, y otra pronunciable, que nos servirá para acordarnos de la contraseña sin comprometer la seguridad.

Clave Segura: este es un generador de contraseñas Fuertes muy simple de usar: básicamente no tenemos que seleccionar nada y el generador se encargará de hacer todo el trabajo. Podemos elegir dos cosas: el tipo –letras y números, sólo números, caracteres especiales- y la longitud –de 4 a 20 caracteres-.[49]

What’s My IP: este servicio sirve para averiguar nuestra dirección IP de forma fácil, pero además tienen una herramienta de generación de contraseñas que nos permite generar claves aleatorias de 8 y 12 caracteres. Tenemos bastantes opciones de personalización, como por ejemplo, evitar que en la contraseña se ingresen caracteres con formas similares como I, l, 1.[50]

New Password Generator: en el mismo estilo de las claves pronunciables, este servicio nos permite crear dos tipos de contraseña, lo que ellos llaman “una fácil de recordar”, y otra segura. En la parte izquierda vamos a ver la contraseña fácil, una combinación entre letras y números que igualmente es completamente aleatoria, y por el otro una contraseña segura que es aún más aleatoria.[51]

---

[49] **Generate Password**: generador de números y contraseñas disponible en https://www.pwdgen.org/

[50]**What’s My IP**: Generador de contraseñas aleatorias disponible en: https://www.whatsmyip.org/random-password-generator/

[51] **New Password Generator** disponible en: https://www.lastpass.com/es/password-generator

Online Password Generator: los muchachos de este servicio tienen una filosofía, y es, ¿para qué tener contraseñas megas seguras que después no podemos recordar? Por eso, proponen un servicio más simple que nos permite crear claves con muchas opciones de personalización. Es bueno si no queremos tener que guardar una enorme cantidad de claves.[52]

Norton Identity Safe: los creadores del antivirus también nos proponen un generador de contraseñas con muchas opciones de personalización, desde cantidad y tipo de caracteres hasta la cantidad de letras y números que queremos que incluya.[53]

Phonetic Password Generator: cerramos con este servicio que se basa en la fonética para crear contraseñas más fáciles de recordar pero igualmente seguras. Ingresamos una palabra y supuestamente nos generará de forma fonética una alternativa. He ingresado varias y los resultados no tienen nada que ver con la palabra original. Lo que quizás lo vuelve hasta más seguro.[54]

---

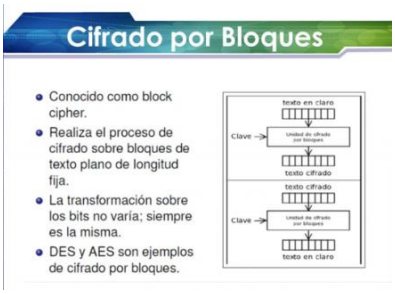
[52] **Online Password Generator:** generador de contraseña disponible en: https://codebeautify.org/password-generator

[53] Norton Identity Safe:disponible en: https://my.norton.com/extspa/idsafe

[54] **Phonetic Password Generator** disponible en: https://tools.arantius.com/password

Cifrado de bloques

Figura 27 ejemplo de cifrado de bloques



Fuente http://seginfdianaescarcega.blogspot.es/1489384943/cifrado-en-bloque/

Se emplea para cifrar grandes cantidades de información en las que es necesario un grado de seguridad alto. Para ello, se rompen las cadenas binarias en bloques más pequeños de tamaño fijo y se someten a un proceso iterativo. El tamaño del bloque y de la clave y el número de iteraciones (o rondas) dependerá del tipo de cifrado.

Así, por ejemplo, el cifrado basado en AES-128 utiliza bloques y claves de 128 bits y 4 iteraciones, mientras que el cifrado basado en AES-256 utiliza bloques de 128 bits, claves de 256 bits y 14 iteraciones. Como es lógico, a medida que aumenta el número de iteraciones y el tamaño de las claves se obtienen cifrados más seguros, aunque el resultado también es más lento

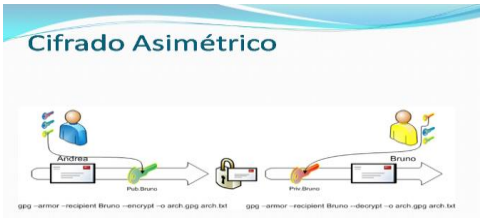
.

Los cifrados de claves largas, 256, 512, etc. son de alta seguridad, ya que generan un nivel de entropía muy elevado. Por ejemplo, para romper por la fuerza un mensaje cifrado con una clave de 256 bits, sería necesario calcular todas las

posibles combinaciones de 2256 y 1,6·1077 es un número monstruosamente grande, no asequible para los métodos de computación actual.[55]

Cifrado asimétrico

Figura 28 cifrado asimétrico



Fuente https://pablo.sarubbi.com.ar/instalaciones/herramientas-de-cifrado-y-firma-digital-multiplataforma

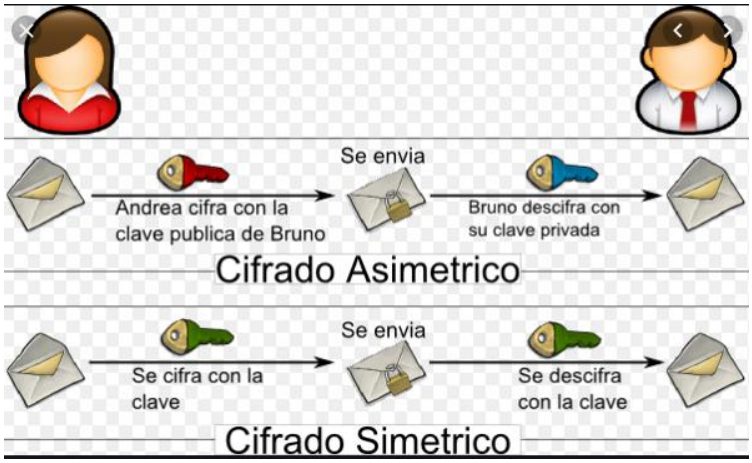
Es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que recibirá el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.[56]

---

[55] El cifrado de comunicaciones, uno de los inventos que ha cambiado el mundo disponible en:https://aunclicdelastic.blogthinkbig.com/cifrado-de-comunicaciones-un-invento-que-ha-cambiado-el-mundo/

[56] Criptografía asimétrica {En línea} {10 de Abril de 2019} https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

Figura 29: Clave pública y clave privada

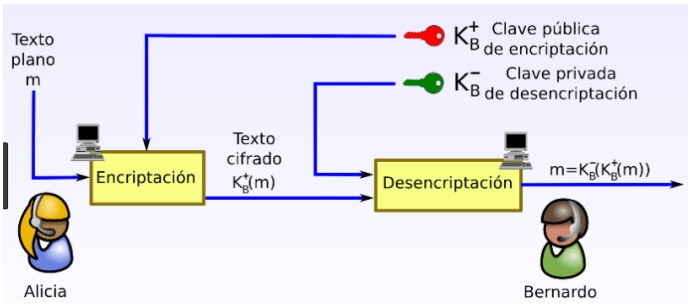


Fuente https://hackxcrack.net/foro/criptografia-y-esteneografia/funcion-clave-privada-en-csr/

Son los dos elementos (claves) utilizadas en el cifrado asimétrico. Las dos claves deben de pertenecer a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. El usuario que quiere enviar un mensaje utiliza la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar ese mensaje

Cifrado RSA

Figura 30: Algoritmo de Cifrado RSA



Fuente: http://www.elembrion.com/2017/06/algoritmo-de-cifrado-rsa.html

El algoritmo de cifrado asimétrico RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977.por Ron Rivest, Adi Shamir y Leonard Adleman, del Instituto Tecnológico de Massachusetts (MIT)

Su fundamento matemático es bastante complejo y se apoya en la capacidad de análisis que tienen los sistemas computacionales en la actualidad lo que permite factorizar números primos de muchos dígitos. Si se cifra un mensaje en forma de factores primos, para descifrarlo será necesario factorizar dicho número.

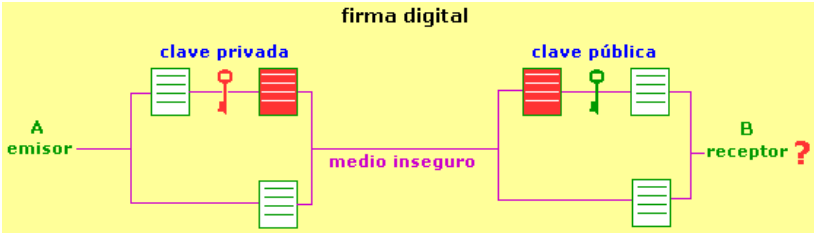
Si es tan complicado factorizar este número, ¿cómo puede descifrar el mensaje su legítimo receptor? Para descifrar el mensaje enviado por el servidor y cifrado con la clave pública, el receptor utilizará su clave privada, la cual cumple una propiedad definida por el teorema de Fermat-Euler que establece que, al aplicar la clave privada sobre el mensaje cifrado, se obtendrán todos los factores y, por tanto, el

mensaje decodificado. El cifrado RSA es el más amplio hoy en día en los casos en los que es necesario utilizar cifrado asimétrico.[57]

El cifrado RSA utiliza un algoritmo fundamentado en la multiplicación de grandes números primos. Mientras que, en general, no representa ningún problema multiplicar dos números primos elevados a 100, a 200 o a 300, no existe hasta hoy ningún algoritmo suficientemente eficaz que sea capaz de descomponer el producto en sus factores primos. Este es el problema de la factorización de números enteros

La Firma

Figura 31 firma digital



Fuente: http://usuaris.tinet.cat/acl/html_web/seguridad/cripto/cripto_5.html

Uno de los usos más importantes del cifrado digital es la generación de firmas, las cuales permiten identificar de forma segura el remitente de documento. En el mundo físico, la firma de documentos se basa en la capacidad de las personas de realizar una firma única que nos identifica y, en teoría, no puede ser copiada.

En el mundo digital esta forma de firmar ya no es útil, ya que se puede crear un duplicado mediante una imagen de la firma de una persona lo que facilita su

---

[57] Criptosistemas de clave pública. El cifrado RSA disponible en:http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/rsa.html

reproducción de forma sencilla. Entonces, ¿cómo firmar un documento para asegurar que proviene de una persona concreta?

La firma digital se basa en la posesión de una clave privada de esta manera, cuando un usuario dispone de un archivo de firma proporcionado por un organismo público certificado, puede firmar documentos realizando una operación de cifrado sobre el fichero. Tras esta operación de cifrado, el fichero se modifica internamente para incluir la firma cifrada del usuario. Y es importante que la firma esté cifrada para que no pueda ser copiada por cualquier curioso que acceda al documento.

El organismo emisor de la firma dispone de una clave pública que le permite descifrar la firma y comprobar que es auténtica. Asimismo, la seguridad de los métodos de cifrado se basa en fundamentos matemáticos que arrancan en el S. XVIII y llegan hasta nuestros días lo que nos puede aseguran que los métodos de cifrado que usan actualmente son robustos y confiables.[58]

[58] El cifrado de comunicaciones, uno de los inventos que ha cambiado el mundo disponible en:https://aunclicdelastic.blogthinkbig.com/cifrado-de-comunicaciones-un-invento-que-ha-cambiado-el-mundo/

12. RESULTADOS ESPERADOS

Aportar soluciones para la confidencialidad y protección de la información manejada en cualquier organización por los diferentes medios de difusión como correos electrónicos, navegación en los diferentes sitios web, datos locales y dispositivos móviles.

Dar a conocer los medios y las políticas con que se cuenta actualmente para la implantación de cifrado en una organización

Mostrar los beneficios de tener normas de seguridad con base al cifrado de datos permitiéndole a las empresas poder tener competitividad, garantizar la exclusividad de sus productos y mantener la confidencialidad de sus bases de datos, etc.
Proporcionar información de los sistemas de cifrado de datos en la actualidad y su mecanismo de acción.

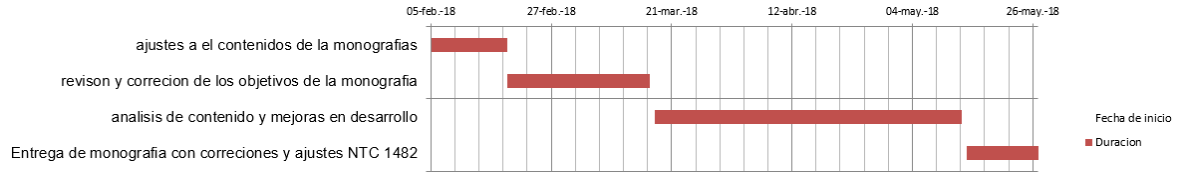
Mostrar herramientas de bajo precio pero con características similares a las de software pago o licenciado

13. PLANIFICACION DEL ANTEPROYECTO

13.1 Cronograma De Actividades

Tabla 1 cronograma de actividades

CRONOGRAMA DE MONOGRAFIA CIFRADO DE DATOS			
Actividad	Fecha de inicio	Duracion	Fecha de terminacion
ajustes a el contenidos de la monografias	05-feb-18	14	19-feb-18
revison y correcion de los objetivos de la monografia	19-feb-18	26	17-mar-18
analisis de contenido y mejoras en desarrollo	18-mar-18	56	13-may-18
Entrega de monografia con correciones y ajustes NTC 1482	14-may-18	13	27-may-18



	Entrega de monografia con correciones y ajustes NTC 1482	analisis de contenido y mejoras en desarrollo	revison y correcion de los objetivos de la monografia	ajustes a el contenidos de la monografias
Fecha de inicio	14-may.-18	18-mar.-18	19-feb.-18	05-feb.-18
Duracion	13	56	26	14

Fuente Autor

14. CONCLUSIONES

La seguridad en una organización es de vital importancia y requiere de estar en constante actualización lo que demanda inversiones e implementación de mecanismos de protección ante algún tipo de ataque informático o pérdida de la información basados en la importancia de la información a proteger.

1. Con esta monografía se puso en contexto algunos aspectos de importancia y relevancia en cuanto a cifrado de datos lo cual sirve como herramienta para ampliar conocimientos en el tema y proporciona orientación sobre la implementación de este mecanismo en las empresas.

2. La encriptación de datos es fundamental para un correcto funcionamiento de las empresas y genera grandes beneficios en cuanto a la protección de información.

3. Existen múltiples herramientas las cuales pueden ser usadas para proteger la información y no generan costos muy altos respecto al beneficio recibido como son los software libre

4. Las empresas pueden escoger la opción de protección que más se ajuste a sus necesidades y presupuesto teniendo en cuenta las múltiples opciones a las que se puede acoger para no dejar su información desprotegida.

5. Continuamente aparecen sistemas y herramientas que permiten la protección de la información basados en cifrado de datos en la actualidad se han perfeccionado dichos mecanismos para proporcionar mejores resultados y el día a día hace que aparezcan y se creen o evoluciones dichas herramientas en busca de una mayor efectividad.

6. Permite la identificación de aplicaciones seguras en sistemas informáticos y sus métodos criptográficos, según las necesidades de cada usuario o empresa

7. proporciona los controles necesarios para que los sistemas de cifrado sugeridos sean confiables y cuenten con un buen nivel de seguridad.

8. Se evidencio como ha mejorado la eficacia del cifrado de datos a través de los años desde sus inicios hasta el día de hoy

9. se puede entender que para cifrar información ya no es necesario ser un ingeniero ni un matemático, sino entender lo que se quiere proteger y tomar la herramienta que más se ajuste a la necesidad del usuario

10. se da a entender que los mecanismo de cifrado de datos cumplen con los principales pilares de la seguridad informática como son confidencialidad, integridad y disponibilidad

REFERENCIAS BIBLIOGRÁFICAS

[1] ESET “Cifrado De La Información: Guía Corporativa” {En línea} {10 de marzo de 2017} disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014.pdf

[2] CERDA, H. “Capítulo 7: Medios, Instrumentos, Técnicas y Métodos en la Recolección de Datos e Información” {En línea} {10 de marzo de 2017} disponible en:http://postgrado.una.edu.ve/metodologia2/paginas/cerda7.pdf

[3] “Sistema de Gestión de la Seguridad de la Información” {En línea} {10 de marzo de 2017} disponible en:http://www.iso27000.es/download/doc_sgsi_all.pdf

[4] Que es la seguridad informática disponible en : https://www.monografias.com/trabajos94/que-seguridad-informatica/que-seguridad-informatica

[5] Jhonny Antonio Pabón Cadavid*¨La criptografía y la protección a la información digital¨ disponible en https://revistas.uexternado.edu.co/index.php/propin/article/download/2476/3636?inline=1

[6] ABANLEX “Informe Sobre La Necesidad Legal De Cifrar Información Y Datos Personales” {En línea} {11 de marzo de 2017} disponible en: https://www.abanlex.com/wp-content/Sophos/Informe_II.pdf

[7] FERNANDEZ GALLEGO, José Armando “Encriptación y Desencriptacion de Datos Usando Técnicas Caóticas” {En línea} {11 de marzo de 2017} disponible en: http://www.bdigital.unal.edu.co/3373/1/josearmandofernandezgallego.2007.pdf

[8] Ramió Aguirre Jorge, “Libro Electrónico de seguridad informática y criptografía” versión 4.1, 6ª edición, Marzo 2006, Madrid España.

[9] TENA AYUSO, Juan “Protocolos Criptográficos” {En línea} {11 de marzo de 2017} disponible en: http://www.criptored.upm.es/guiateoria/gt_m023c.htm

[10] GOMEZ CARDENAS, Roberto “Protocolos Criptograficos” {En línea} {11 de marzo de 2017} disponible en: http://www.cryptomex.org/SlidesSeguridad/ProtoCripto.pdf

[11] UNIVERSIDAD DE LA RIOJA “Cifrado de comunicaciones” {En línea} {11 de marzo de 2017} disponible en: http://www.unirioja.es/servicios/si/seguridad/difusion/cifrado.shtml

[12] ESET “Cifrado De La Información: Guía Corporativa” {En línea} {10 de marzo de 2017} disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014.pdf

[13] DiskCryptor ”Solución de cifrado de partición de código abierto”. Disponible en: https://diskcryptor.net/

[14] veracrypt disponible en https://www.veracrypt.fr/en/Downloads.html

HORMINKA “Estado de Privacidad Colombia” {En línea} {11 de marzo de 2017} disponible en: http://www.horminka.org/privacidad/2017/03/16/estado-de-privacidad-colombia.html

[15] Samir Vaidya “OpenStego” {En línea} {11 de marzo de 2017} disponible en: https://www.openstego.com/index-es.html

[16] OpenPuff disponible en https://embeddedsw.net/OpenPuff_Steganography_Home.html

[17] GNUPG “El Guardia de privacidad de GNU” {En línea} {11 de marzo de 2017} disponible en: https://gnupg.org/

[18] OpenSSH 7.6 “Open SSH keeping your comuniques secret” {En línea} {11 de marzo de 2017} disponible en: https://www.openssh.com/

[19] https://www.openssl.org/

[20] USB-Memorias.com, “Protege Los Datos De Tus Memorias USB” {En línea} {16 de marzo de 2018} disponible en: https://www.usb-memorias.com/noticias/protege-los-datos-de-tus-memorias-usb/

[21] “usbsafeguard” {En línea} {16 de marzo de 2018} disponible en: http://www.usbsafeguard.com/index.html[

[22] GUILLOT, Fernando “Cómo usar Bitlocker en máquinas que no tienen TPM” {En línea} {16 de marzo de 2018} disponible en: https://blogs.technet.microsoft.com/guillot/2011/01/10/cmo-usar-bitlocker-en-mquinas-que-no-tienen-tpm/

[23] Rohos mini drive, tomado de: https://www.rohos.com/products/rohosdisk-encryption/rohos-mini-drive/

[24] LEY 1621 DE 2013 - SUIN-Juriscol http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1685400

[25] Vivo HD Online “Nuevo protocolo mejora la seguridad en el cifrado de mensajes” {En línea} {12 de marzo de 2018} disponible en: https://vivofullperiodicos.blogspot.com.co/2017_09_24_archive.html

[26] LEY 1273 DE 2009 (Enero 05) {En línea} {12 de marzo de 2018} disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[27] MAILVELOPE - ENCRIPTACIÓN OPENPGP PARA WEBMAIL disponiblen en https://securityinabox.org/en/guide/mailvelope/web/

[28] GPG4WIN, tomado de: https://www.gpg4win.org/

[29] CRYPTAINER LE {En línea} {13 de junio de 2018} http://www.cypherix.es/downloads.htm

[30] GPG4USB - CIFRADO DE ARCHIVOS Y TEXTOS DE CORREO ELECTRÓNICO
https://securityinabox.org/es/guide/gpg4usb/windows/

[31] Encuesta mundial de productos de cifrado {En línea} {16 de julio de 2018} https://www.schneier.com/blog/archives/2016/02/worldwide_encry.html

TELINFORMATICA “El cifrado de datos comienza a hacerse un hueco en la Pyme” {En línea} {11 de marzo de 2017} disponible en: http://tii.es/?q=articles/el-cifrado-de-datos-comienza-hacerse-un-hueco-en-la-pyme

UNIVERSIDAD DE ZARAGOZA “Procedimiento Para Cifrado De Datos Utilizando La Herramienta TRUECRYPT” {En línea} {11 de marzo de 2017} disponible en: http://moncayo.unizar.es/sicuz/docutec.nsf/2e52318decb4e752c1256fda004289a3/aed4725c45395912c12571fc003251b3/$FILE/dt120.pdf

PABON CADAVID, Jhonny Antonio “La criptografía y la protección a la información digital” {En línea} {12 de marzo de 2017} disponible en: http://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636#nu63

RODRIGUEZ, Katitza “Anonimato y cifrado” {En línea} {12 de marzo de 2017} disponible en: https://www.eff.org/files/2015/03/18/anonimatoycifrado-eff-11.pdf

ZULETA PULGARÍN, Sandra Liliana “Protección De Datos Personales En Colombia” {En línea} {12 de marzo de 2017} disponible en: http://repository.unimilitar.edu.co/bitstream/10654/13571/2/PROTECCION%20DE%20DATOS%20PERSONALES%20EN%20COLOMBIA.pdf

CASTAÑEDA GOMEZ, Juan Diego “La peligrosa ambigüedad de las normas sobre cifrado de comunicaciones en Colombia” {En línea} {12 de marzo de 2017} disponible en: https://www.digitalrightslac.net/es/la-peligrosa-ambiguedad-de-las-normas-sobre-cifrado-de-comunicaciones-en-colombia/

CRYPTAINER LE {En línea} {13 de junio de 2018} http://www.cypherix.es/downloads.htm

EMPRESAS QUE REQUIEREN CIFRADO DE INFORMACIÓN EN COLOMBIA https://www.informatica.com/co/products/data-security/data-masking.html

SU EMPRESA PUEDE ESTAR EXPUESTA AL FRAUDE, IMPLEMENTE UN PROCESO DE SEGURO DE PAGO
http://securefile.co/es/

SEGURIDAD DE LA INFORMACION EN LATINOAMERICA TENDENCIAS 2009 http://52.0.140.184/typo43/fileadmin/Revista_110/05investigacion1.pdf

PROTECCIÓN DE DATOS PERSONALES EN COLOMBIAhttp://unimilitar-dspace.metabiblioteca.org/handle/10654/13571https://repository.javeriana.edu.co/bitstream/handle/10554/7485/Tesis211.pdf?sequence=1

[PDF] A ADOPTAR EN MATERIA DE CIBERSEGURIDAD EN LAS EMPRESAS COLOMBIANAS, A PARTIR DEL ESTUDIO DE CASO: BBVA COLOMBIA http://repository.unimilitar.edu.co/bitstream/10654/15765/3/MedinaRomeroJuanDiego2016.pdf

RIESGO Y SEGURIDAD. UN CONTINUO DE CONFIANZA IMPERFECTA https://www.researchgate.net/profile/Jeimy_Cano_M/publication/321197873_Riesgo_y_seguridad_Un_continuo_de_confianza_imperfecta/links/5a148a68458515005213055e/Riesgo-y-seguridad-Un-continuo-de-confianza-imperfecta.pdf

DISEÑO DE POLÍTICAS Y CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN EN PEQUEÑAS EMPRESAS CON REDES SOHO EN EL SECTOR TRANSPORTE DE BOGOTÁ http://bibliotecadigital.usbcali.edu.co:8080/handle/10819/2952

ELECTRÓNICAS EN LÍNEA Y LA CRIPTOGRAFÍA COMO MODELO DE SEGURIDAD INFORMÁTICA http://publicaciones.usm.edu.ec/index.php/GS/article/view/44

Implementación de una infraestructura de clave pública con herramientas de software libre http://42jaiio.sadio.org.ar/proceedings/simposios/Trabajos/JSL/10.pdf

https://securityinabox.org/en/guide/secure-communication/

Desarrollo de una interface web para la administración de infraestructura de llaves

públicas (PKI) basada en OPENSSL http://www.miunespace.une.edu.ve/jspui/bitstream/123456789/1147/1/TG3433%20resumen.pdf

Seguridad digital y privacidad para los defensores de los derechos humanos www.frontlinedefenders.org/manual/en/esecman.

La criptografía y la protección a la información digital https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

TDM desempeña un papel vital en la privacidad de datos. https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/tdm-desempena-un-apel-vital-en-la-privacidad-de-datos

Encuesta mundial de productos de cifrado. https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf

B-SECURE “Cifrado De Equipos, Carpetas, Recursos Compartidos Y Medios Extraíbles” {En línea} {11 de marzo de 2017} disponible en:https://www.b-secure.co/tecnologias/proteccion-de-datos

El cifrado de comunicaciones, uno de los inventos que ha cambiado el mundo https://aunclicdelastic.blogthinkbig.com/cifrado-de-comunicaciones-un-invento-que-ha-cambiado-el-mundo/

Delitos informáticos: disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Uso técnicas criptograficas.pdf

https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf

EL CIFRADO DE DATOS UNA NECESIDAD disponible en https://www.cloudseguro.co/cifrado-de-datos/

Anexo

RESUMEN ANALITICO ESPECIALIZADO

RAE

1. Información General	
Tema	SEGURIDAD DE LA INFORMACION
Titulo	IMPORTANCIA DE LA APLICACIÓN DEL MECANISMO DE CIFRADO DE INFORMACIÓN EN LAS EMPRESAS PARA LA PREVENCIÓN DE RIESGOS COMO ATAQUES, PLAGIO Y PÉRDIDA DE LA CONFIDENCIALIDAD
Tipo de proyecto	MONOGRAFIA
Autor (es)	YEISON FREDY CHALA
Director	EDGAR ALONSO BOJACA
Fuente Bibliográfica	[1] ESET "Cifrado De La Información: Guía Corporativa" {En línea} {10 de marzo de 2017} disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014.pdf [2] CERDA, H. "Capítulo 7: Medios, Instrumentos, Técnicas y Métodos en la Recolección de Datos e Información" {En línea} {10 de marzo de 2017} disponible en:http://postgrado.una.edu.ve/metodologia2/paginas/cerda7.pdf [3] "Sistema de Gestión de la Seguridad de la Información" {En línea} {10 de marzo de 2017} disponible en:http://www.iso27000.es/download/doc_sgsi_all.pdf 4] B-SECURE "Cifrado De Equipos, Carpetas, Recursos Compartidos Y Medios Extraíbles" {En línea} {11 de marzo de 2017} disponible en:https://www.b-secure.co/tecnologias/proteccion-de-datos [5] ABANLEX "Informe Sobre La Necesidad Legal De Cifrar Información Y Datos Personales" {En línea} {11 de marzo de 2017} disponible en: https://www.abanlex.com/wp-content/Sophos/Informe_II.pdf [6]FERNANDEZ GALLEGO, José Armando "Encriptación y Des encriptación de Datos Usando Técnicas Caóticas" {En línea} {11 de marzo de 2017} disponible en: http://www.bdigital.unal.edu.co/3373/1/josearmandofernandezgallego.2007.pdf [7] Corporación Colombia Digital "Cifrar o no los datos, esa es la cuestión" {En línea} {11 de marzo de 2017} disponible en: https://colombiadigital.net/actualidad/noticias/item/5363-cifrar-o-no-los-datos-esa-es-la-cuestion.html

[8] Ramió Aguirre Jorge, “Libro Electrónico de seguridad informática y criptografía” versión 4.1, 6ª edición, Marzo 2006, Madrid España.

[9] TENA AYUSO, Juan “Protocolos Criptográficos” {En línea} {11 de marzo de 2017} disponible en: http://www.criptored.upm.es/guiateoria/gt_m023c.htm

[10] GOMEZ CARDENAS, Roberto “Protocolos Criptograficos” {En línea} {11 de marzo de 2017} disponible en: http://www.cryptomex.org/SlidesSeguridad/ProtoCripto.pdf

[11] UNIVERSIDAD DE LA RIOJA “Cifrado de comunicaciones” {En línea} {11 de marzo de 2017} disponible en: http://www.unirioja.es/servicios/si/seguridad/difusion/cifrado.shtml

[12] HORMINKA “Estado de Privacidad Colombia” {En línea} {11 de marzo de 2017} disponible en: http://www.horminka.org/privacidad/2017/03/16/estado-de-privacidad-colombia.html

[13] Samir Vaidya “OpenStego” {En línea} {11 de marzo de 2017} disponible en: https://www.openstego.com/index-es.html

[14] GNUPG “El Guardia de privacidad de GNU” {En línea} {11 de marzo de 2017} disponible en: https://gnupg.org/

[15] OpenSSH 7.6 “Open SSH keeping your comuniques secret” {En línea} {11 de marzo de 2017} disponible en: https://www.openssh.com/

[16] TELINFORMATICA “El cifrado de datos comienza a hacerse un hueco en la Pyme” {En línea} {11 de marzo de 2017} disponible en: http://tii.es/?q=articles/el-cifrado-de-datos-comienza-hacerse-un-hueco-en-la-pyme

[17] UNIVERSIDAD DE ZARAGOZA “Procedimiento Para Cifrado De Datos Utilizando La Herramienta TRUECRYPT” {En línea} {11 de marzo de 2017}disponible en: http://moncayo.unizar.es/sicuz/docutec.nsf/2e52318decb4e752c1256fda004289a3/aed4725c45395912c12571fc003251b3/$FILE/dt120.pdf

[18] PABON CADAVID, Jhonny Antonio “La criptografía y la protección a la información digital” {En línea} {12 de marzo de 2017}

	disponible en: http://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636#nu63 [19] RODRIGUEZ, Katitza “Anonimato y cifrado” {En línea} {12 de marzo de 2017} disponible en: https://www.eff.org/files/2015/03/18/anonimatoycifrado-eff-11.pdf [20] “usbsafeguard” {En línea} {16 de marzo de 2018} disponible en: http://www.usbsafeguard.com/index.htm [21] GUILLOT, Fernando “Cómo usar Bitlocker en máquinas que no tienen TPM” {En línea} {16 de marzo de 2018} disponible en: https://blogs.technet.microsoft.com/guillot/2011/01/10/cmo-usar-bitlocker-en-mquinas-que-no-tienen-tpm/ [22] USB-Memorias.com, “Protege Los Datos De Tus Memorias USB” {En línea} {16 de marzo de 2018} disponible en: https://www.usb-memorias.com/noticias/protege-los-datos-de-tus-memorias-usb/ [23] Vivo HD Online “Nuevo protocolo mejora la seguridad en el cifrado de mensajes” {En línea} {12 de marzo de 2018} disponible en: https://vivofullperiodicos.blogspot.com.co/2017_09_24_archive.html [24] ZULETA PULGARÍN, Sandra Liliana “Protección De Datos Personales En Colombia” {En línea} {12 de marzo de 2017} disponible en: http://repository.unimilitar.edu.co/bitstream/10654/13571/2/PROTECCION%20DE%20DATOS%20PERSONALES%20EN%20COLOMBIA.pdf [25] CASTAÑEDA GOMEZ, Juan Diego “La peligrosa ambigüedad de las normas sobre cifrado de comunicaciones en Colombia” {En línea} {12 de marzo de 2017} disponible en: https://www.digitalrightslac.net/es/la-peligrosa-ambiguedad-de-las-normas-sobre-cifrado-de-comunicaciones-en-colombia/
Año	2019
Resumen	En la actualidad cualquier empresa u organización está expuesta a riesgos de ataques informáticos y plagio de información la cual es su recurso más importante para el funcionamiento de la misma, lo

	que hace indispensable tomar medidas y utilizar estrategias para protegerla ante todos los riesgos existentes. El presente trabajo trata el tema de cifrado de información porque permite dar solución a la problemática presentada en algunas empresas de ataques, fuga y plagio de información. En esta monografía pretendo dar a conocer información de gran importancia ya que da a conocer un estudio de todos los aspectos de cifrado de información desde su definición hasta su aplicación según las necesidades de protección de información; muestra de manera clara y actualizada los diferentes beneficios y la manera como puede ser implementado este beneficio en cualquier empresa que requiera proteger sus datos. Con lo anterior se pueden aportar soluciones para la confidencialidad y protección de la información manejada en cualquier organización por los diferentes medios de difusión como correos electrónicos, navegación en los diferentes sitios web, datos locales y dispositivos móviles.
Palabras Claves	Seguridad de la información, Cifrado De La Información, ataques informáticos, Mecanismos De Protección De Información.
Contenidos	TABLA DE CONTENIDO

2. Descripción del Problema de Investigación

3. PLANTEAMIENTO DEL PROBLEMA

2.1 Descripción Del Problema

Actualmente en algunas empresas de nuestro país no se cuenta con los mecanismos adecuados para la protección de la información digital, además se tiene poco conocimiento de las herramientas de protección de datos convirtiéndolas en vulnerables a los riesgos existentes como ataques informáticos, plagio de la información y perdida de la confidencialidad, lo que hace necesario la implementación de herramientas para prevenir dichos riesgos.

Según estadísticas de ESET Latinoamérica se conoce que el 40% de las empresas sufrió incidentes maliciosos en el último año; de igual manera en el Informe Global sobre Fraudes y Riesgos de Kroll de 2016 se dice que en el año estudiado el 82% de las empresas sufrió fraude corporativo, lo anterior evidencia que el riesgo existe en cualquier tipo de empresa, no importando su tamaño, lo que la convierte potencialmente vulnerable a ataques específicos[59].

2.2 Formulación Del Problema

La implementación de sistemas de seguridad diseñados para la protección de los entornos digitales de datos a causado la necesidad de la realización de búsquedas de herramientas que ayuden a la salva guarde de estas.

Por ese motivo se recomienda el uso del cifrado de datos, ya que a través de este método se pueden realizar una serie de estrategias que permiten mejorar los niveles de autenticidad y fiabilidad de los mismos. Además en el mercado se pueden encontrar mecanismos económicos y fáciles de implementar.

¿Cuáles ventajas y beneficios proporcionará la implementación de cifrado de la información en las empresas?

Falta de implementación de mecanismos de protección de información digital por parte de algunas empresas en nuestro país.

3. Objetivos

3. OBJETIVOS

3.1 OBJETIVO GENERAL

[59] ESET “Cifrado De La Información: Guía Corporativa” {En línea} {10 de marzo de 2017} disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014.pdf

Proponer estrategias a las empresas para la protección de los datos ante algunos riesgos como ataques informáticos, plagio de la información y pérdida de la confidencialidad mediante la implementación de cifrado de la información.

3.2 OBJETIVOS ESPECÍFICOS

1. Profundizar en el tema de cifrado de información
2. Describir los beneficios de encriptación de datos
3. Dar a conocer algunas herramientas que pueden ser utilizadas para proteger la información
4. Brindar una herramienta útil para la protección de datos en las empresas
5. Realizar un análisis de los sistemas de cifrado en la actualidad.

4. Referentes Teóricos

7. MARCO REFERENCIAL

El intercambio de información ha sido un aspecto fundamental en la sociedad, el cual ha cobrado mayor importancia en los últimos tiempos dentro o fuera de cualquier organización, gracias a los adelantos tecnológicos, lo que ha obligado a que estas implanten constantes controles de seguridad que ofrezcan y garanticen la protección de la información con la que se cuente o vaya a ser intercambiada.

Para garantizar esta protección es necesario establecer políticas y medidas preventivas en los procesos de intercambio de información que la organización emplee. Para ello se hace necesario que se conozca a fondo algunos mecanismos entre ellos el cifrado de datos del cual se ampliará información en el desarrollo de la presente monografía.

Algunas medidas que pueden ser implementadas son:

- Programaciones de un correcto uso de los medios informáticos y de comunicación.
- Controles para evitar la modificación, la manipulación, el copiado o la destrucción de la información.
- Utilización de Antivirus actualizados.
- Uso de cifrado en datos que se consideren necesarios.

Según los estudios realizados actualmente el robo de información es un negocio en crecimiento y muy rentable, lo que lleva a que las empresas empiecen a buscar medios para salvaguardar su valiosa información.

Una herramienta en crecimiento es el cifrado de datos o encriptación. "Las tecnologías de la encriptación constituyen el avance tecnológico más importante de los últimos mil años. Ningún otro descubrimiento tecnológico desde las armas nucleares (espero) hasta Internet tendrá un impacto más significativo en la vida social y política de la humanidad. La criptografía va a cambiar absolutamente todo". Lawrence Lessig.[60]

Existen herramientas que pueden ser adoptadas por las empresas para la protección de los datos como lo es la implementación de norma ISO 27001, entre otras.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados que constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:
• Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI (Sistema de Gestión de la Seguridad de la Información). [61]

5. Referentes Teóricos y Conceptuales

7.1 MARCO TEÓRICO

La acumulación de enormes cantidades de datos de carácter personal por entidades públicas y privadas, incorporada a la capacidad de los sistemas informáticos para combinar y procesar las informaciones viene generando claras

[60] La criptografía y la protección a la información digital. Disponible en: https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

[61] Sistema de Gestión de la Seguridad de la Información. disponible en:http://www.iso27000.es/download/doc_sgsi_all.pdf

amenazas a la privacidad de los individuos. La comprobación de estas amenazas por parte de la mayoría de países ha llevado a la elaboración de leyes y normas que limitan el tratamiento de los datos de carácter personal. [62]

Además de leyes se hace necesario la implementación de herramientas que permitan la protección de los datos y una de ellas es el cifrado de datos o encriptación. Y para ello se hace necesario que existan manuales que facilitan la implementación de estas.

La criptografía es la técnica utilizada para cifrar mensajes que contienen información, palabra que proviene del griego Kryptos y Graphein, que significan "escondido" y "escritura", respectivamente[63]
El Cifrar datos de forma correcta es una de las obligaciones que impone la normativa española para una inmensa cantidad de empresas. Muchas de ellas no cifran por miedo o desconocimiento. Cifrar no es complicado, el coste es asequible y los beneficios se muestran desde el inicio. [64]

En Colombia y en el mundo no se han establecido normas claras en el tema del cifrado de datos, sin embargo es fundamental que todas las empresas u organizaciones adopten dicho mecanismo.

La implementación de sistemas de gestión, de normas ISO, será un pilar fundamental en la seguridad de la información de cualquier organización, siendo esto confidencialidad, integridad y disponibilidad. Estos 3 aspectos importantes a la hora de verificar el grado de importancia de nuestros datos.

7.1.1 Que Es El Cifrado De Datos

El cifrado de los datos es una práctica que consiste en codificar los datos para modificar su formato original y que no sea posible leerlos. La información solo podrá leerse cuando se dispone de la contraseña o el código de cifrado y se aplica la clave previamente acordada. Además, es posible cifrar todo un dispositivo (por ejemplo, un disco duro), haciendo ilegible todo su contenido, o cifrar solamente

[62] Que es la seguridad informática disponible en : https://www.monografias.com/trabajos94/que-seguridad-informatica/que-seguridad-informatica

[63]El objeto la criptografía no es ocultar la existencia de un mensaje, sino más bien ocultar su significado, un proceso que se conoce como codificación" (Sgarro, 1990: 20).

[64] ABANLEX "Informe Sobre La Necesidad Legal De Cifrar Información Y Datos Personales" disponible en: https://www.abanlex.com/wp-content/Sophos/Informe_II.pdf

determinadas carpetas o archivos con información confidencial.[65]

7.1.2 Tipos De Algoritmos

Hay dos tipos básicos de algoritmos de encriptación:

Los algoritmos de cifrado simétrico más comúnmente usados son los cifradores de bloques. Un cifrado de bloques procesa la entrada de texto claro en bloques de tamaño fijo y genera un bloque de texto cifrado del mismo tamaño para cada texto claro

- ***Clave secreta (o clave simétrica)****:* utiliza la misma clave para cifrar y descifrar un mensaje. Estos métodos de cifrado se usan principalmente para proteger información que se almacena en un disco duro o para transmisión de datos entre ordenadores. El algoritmo de encriptación más usado de este tipo es el DES (Data Encryption Standard) que usa una clave de 56-bits. Un mensaje cifrado con este algoritmo es bastante seguro aunque ya puede ser descifrado con máquinas muy potentes en menos de un día, por lo que su uso está restringido a ámbitos civiles. Otros algoritmos comúnmente usados son el RC2, RC4, RC5 e IDEA. La mayoría de estos algoritmos tienen patente, aunque su uso público está permitido[7]

- ***Clave pública (o clave asimétrica)*****:** que utiliza una clave pública para cifrar el mensaje y una clave privada para descifrarlo De esta forma cualquiera puede cifrar un mensaje pero solo quien tenga la clave privada puede descifrarlo. Esto sirve para poder enviar un mensaje a un determinado destino sin que otro pueda descifrarlo. El objeto de estos métodos es la de asegurar la integridad y la autentificación del origen de los datos (por ejemplo, usando firmas digitales). RSA es el algoritmo de encriptación más conocido de clave pública. RSA utiliza una clave pública que es usada para cifrar el mensaje y una clave privada que es usada para descifrar el mensaje. [7]

7.1.3 Firma Digital

La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación.
La firma digital se basa en la propiedad ya comentada sobre que un mensaje cifrado utilizando la clave privada de un usuario sólo puede ser descifrado

[65] GDX GROUP DIGITAL TRANSFORMATION "Cuándo es necesario cifrar los datos" disponible en: https://gdx-group.com/cuando-es-necesario-cifrado-de-datos/

utilizando la clave pública asociada. De tal manera, se tiene la seguridad de que el mensaje que ha podido descifrarse utilizando la clave pública sólo pudo cifrarse utilizando la privada. La firma digital, por tanto, es un cifrado del mensaje que se está firmando pero utilizando la clave privada en lugar de la pública. [66]

7.1.3.1 Características de Una Firma Digital

Requisitos de la firma digital:

a) Debe ser fácil de generar. [8]
b) Será irrevocable, no rechazable por su propietario. [8]
c) Será única, sólo posible de generar por su propietario. [8]
d) Será fácil de autenticar o reconocer por su propietario y los usuarios receptores.
e) Debe depender del mensaje y del autor. [8]

7.1.4 Protocolos Criptográficos

Protocolo Criptográfico es un protocolo (es decir un conjunto bien definido de etapas, implicando a dos o más partes y acordado por ellas, designado para realizar una tarea específica) que utiliza como herramienta algún algoritmo criptográfico. Existe una amplia variedad de protocolos criptográficos, que dan respuesta a diferentes objetivos.[67]
Algunos de los protocolos de uso general más utilizados son:

- ***SSL (Security Sockets Layer):*** Es el protocolo dominante para encriptar la comunicación en general entre los navegadores y servidores. Es un sistema de encriptamiento de flexible de propósito general, tu probablemente lo has usado aún que no te has dado cuenta, puesto que está construido dentro de los navegadores (Browser) de Netscape Navigator .y Microsoft La habilidad del navegador para encriptar las comunicaciones fue un punto importante de venta para Nestcape, un característica enfatizada por frecuentes advertencias desplegadas por el navegador cuando la criptografía no estaba siendo usada. [68]

[66] Ramió Aguirre Jorge, "Libro Electrónico de seguridad informática y criptografía" versión 4.1, 6ª edición, Marzo 2006, Madrid España.

[67] TENA AYUSO, Juan "Protocolos Criptográficos" {En línea} {11 de marzo de 2017} disponible en: http://www.criptored.upm.es/guiateoria/gt_m023c.htm

[68] GOMEZ CARDENAS, Roberto "Protocolos Criptograficos" {En línea} {11 de marzo de 2017} disponible en: http://www.cryptomex.org/SlidesSeguridad/ProtoCripto.pdf

- ***SET (Secure Electronic Transaction)*** es un protocolo especializado para salvaguardar transacciones basadas en tarjetas de crédito. [10]

- ***IP SEC*****:** Es uno de los más empleado es un grupo de extensiones de la familia del protocolo IP pensado para proveer servicios de seguridad a nivel de red,(GRE 47) el protocolo de Encapsulación de Enrutamiento Genérico. Se emplea en combinación con otros protocolos de túnel para crear redes de internet virtuales. Conjunto de protocolos definido como parte de IPv6 (nueva versión), permite cifrar y/o autentificar todo el tráfico a nivel IP. [69]

- **FUNCIONES HASH:** También conocidas como huellas digitales (finger-prints), son funciones de una vía que se basan en operaciones matemáticas para tomar a la entrada un conjunto de datos de longitud variable; y, convertirlos en información de longitud fija a la salida. La función hash debe cumplir los siguientes requisitos: imposibilidad de obtener el texto original a partir de la huella digital, imposibilidad de encontrar un conjunto de datos diferentes que tengan la misma huella digital, transformar un texto de longitud variable en una huella de tamaño fijo, facilidad de empleo e implementación. A continuación se muestra algunos ejemplos de funciones de una vía:

    4) **Algoritmo MD5**.- Es una función hash de 128 bits. Este algoritmo se usa para firmas digitales, más no para encriptar mensajes. La información original no se puede recuperar ya que hay pérdida de datos.

    5) **SHA-1**.- En una función de 160bits, la compresión es más compleja que la función de MD5, por lo que es más lento que MD5; sin embargo el contar con una mayor longitud (160bits contra 128bits), hace que SHA-1 sea más robusto y seguro.

    6) **SHA-2**.- En esta función los rangos de salida han sido incrementados: SHA-224, SHA256, SHA-384, y SHA-512. Convirtiéndose en el más seguro SHA-512, pues cuenta con mayor número de bits a la salida.

7.1.5 Beneficios Del Cifrado De Datos

- ***Proteger la información confidencial de una organización*****:** si la información sensible de una compañía llegara a caer en las manos

[69] UNIVERSIDAD DE LA RIOJA "Cifrado de comunicaciones" {En línea} {11 de marzo de 2017} disponible en: http://www.unirioja.es/servicios/si/seguridad/difusion/cifrado.shtml

equivocadas, pueden producirse perjuicios económicos, pérdidas de ventaja competitiva, o incluso significar el cierre de la empresa. En este sentido, la encriptación ayuda a proteger Información delicada, como los datos financieros, de los colaboradores, procedimientos o políticas internas, entre otros. [70]

- ***Proteger la imagen y el prestigio de una organización*:** existe cierta información que si es robada, puede dañar la imagen corporativa. Un ejemplo notable, son los datos que se almacenan de los clientes; el robo de los mismos puede afectar considerablemente a la empresa, llevándola a pérdidas irrecuperables. [12]

- ***Proteger las comunicaciones de una organización:*** el cifrado es comúnmente asociado con las transmisiones de datos, dado que los mensajes enviados por una empresa suelen viajar por canales o infraestructura externa, como Internet, y son susceptibles a ser interceptados. El ejemplo más significativo, es el cifrado de los mensajes enviados por correo electrónico. [12]

- ***Proteger dispositivos móviles e inalámbricos***: todos aquellos dispositivos que salen de la empresa, como teléfonos celulares, tablets o computadoras portátiles, pueden ser extraviados y/o robados. Ante estas situaciones, es importante asegurarse de que ningún tercero esté autorizado pueda acceder a la información. [12]

6. Resultados y Conclusiones

RESULTADOS ESPERADOS

Aportar soluciones para la confidencialidad y protección de la información manejada en cualquier organización por los diferentes medios de difusión como correos electrónicos, navegación en los diferentes sitios web, datos locales y dispositivos móviles.

Dar a conocer los medios y las políticas con que se cuenta actualmente para la implantación de cifrado en una organización

Mostrar los beneficios de tener normas de seguridad con base al cifrado de datos permitiéndole a las empresas poder tener competitividad, garantizar la

[70] ESET “Cifrado De La Información: Guía Corporativa” {En línea} {10 de marzo de 2017} disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014.pdf

exclusividad de sus productos y mantener la confidencialidad de sus bases de datos, etc.
Proporcionar información de los sistemas de cifrado de datos en la actualidad y su mecanismo de acción.

Mostrar herramientas de bajo precio pero con características similares a las de software pago o licenciado.

14. CONCLUSIONES

La seguridad en una organización es de vital importancia y requiere de estar en constante actualización lo que demanda inversiones e implementación de mecanismos de protección ante algún tipo de ataque informático o pérdida de la información basados en la importancia de la información a proteger.

1. Con esta monografía se puso en contexto algunos aspectos de importancia y relevancia en cuanto a cifrado de datos lo cual sirve como herramienta para ampliar conocimientos en el tema y proporciona orientación sobre la implementación de este mecanismo en las empresas.

2. La encriptación de datos es fundamental para un correcto funcionamiento de las empresas y genera grandes beneficios en cuanto a la protección de información.

3. Existen múltiples herramientas las cuales pueden ser usadas para proteger la información y no generan costos muy altos respecto al beneficio recibido como son los software libre

4. Las empresas pueden escoger la opción de protección que más se ajuste a sus necesidades y presupuesto teniendo en cuenta las múltiples opciones a las que se puede acoger para no dejar su información desprotegida.

5. Continuamente aparecen sistemas y herramientas que permiten la protección de la información basados en cifrado de datos en la actualidad se han perfeccionado dichos mecanismos para proporcionar mejores resultados y el día a día hace que aparezcan y se creen o evoluciones dichas herramientas en busca de una mayor efectividad.

6. Permite la identificación de aplicaciones seguras en sistemas informáticos y sus métodos criptográficos, según las necesidades de cada usuario o empresa

7. proporciona los controles necesarios para que los sistemas de cifrado sugeridos sean confiables y cuenten con un buen nivel de seguridad.

8. Se evidencio como ha mejorado la eficacia del cifrado de datos a través de los años desde sus inicios hasta el día de hoy

9. se puede entender que para cifrar información ya no es necesario ser un ingeniero ni un matemático, sino entender lo que se quiere proteger y tomar la herramienta que más se ajuste a la necesidad del usuario

10. se da a entender que los mecanismo de cifrado de datos cumplen con los principales pilares de la seguridad informática como son confidencialidad, integridad y disponibilidad