**TITULO**

**Pamela Isabel Gonzales Maldonado**

**METODOS DE ENCRIPTACION PARA REDES PRIVADAS VIRTUALES**

***Universidad Mayor de San Andrés – Postgrado en Informática***
***Diplomado en Auditoría de Sistemas y Seguridad de los Activos de la Información***
***ycha_g@hotmail.com***

## 1. ABSTRACT

A VPN is a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed though some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis. But the VPN result will been aviable, outwith a encriptacion method.

## 2. RESUMEN

La conexión remota a la red corporativa se ha convertido en una necesidad para las empresas de hoy en día. El aumento del teletrabajo o los desplazamientos de personal, obligan a establecer sistemas de conexión con la red corporativa para, de esa manera, poder acceder a sus recursos. Uno de los sistemas más extendidos para comunicarse de forma remota con una red es a través de conexiones VPN. Sin embargo, una conexión VPN es también un punto crítico de entrada de todo tipo de ataque. A través de una VPN cualquier tipo de ataque puede entrar directamente en los servidores de la empresa. El problema radica en verificar la seguridad del equipo que se está conectando de forma remota y las políticas de seguridad adecuadas para que la información no quede expuesta a posibles ataques y para esto la implementación de métodos de encriptación es esencial.

## 3. INTRODUCCIÓN

### 3.1 VPN (RED PRIVADA VIRTUAL)

Una Red Privada Virtual (VPN) es una red de información privada que hace uso de una infraestructura pública de telecomunicaciones, que conecta diferentes segmentos de red o usuarios a una red principal, manteniendo la privacidad a través del uso de un protocolo de

túnel o aislamiento así como de otras tecnologías que proveen seguridad. La función principal de una VPN es la de brindar conectividad a una red, a través de una red pública, brindando la integridad de la información.

Para la implementación de una VPN, existen aspectos fundamentales que deben considerarse: costo, desempeño, confianza y seguridad. De estas características, la seguridad es la más primordial, sin la existencia de esta característica las otras resultan ser improductivos; puesto que no importa qué tan barata, rápida y confiable sea una red, sin la seguridad adecuada, los riesgos causaran la inestabilidad de la red.
En adición a los riesgos de seguridad, hay aspectos de Calidad en el Servicio (QoS) concernientes a al Internet que se deben de tratar. La calidad en el servicio se refiere al acuerdo de servicio ofrecido por un Proveedor de Servicios de Internet (ISP) a un cliente, que garantiza cierto nivel de desempeño.

### 3.1.1 VENTAJAS Y DESVENTAJAS

**VENTAJAS**

- Ahorro en costos.
- No se compromete la seguridad de la red empresarial.
- El cliente remoto adquiere la condición de miembro de la LAN con permisos, directivas de seguridad.
- El cliente tiene acceso a todos los recursos ofrecidos en la LAN como impresoras, correo electrónico, base de datos.
- Acceso desde cualquier punto del mundo, siempre y cuando se tenga acceso a internet.

**DESVENTAJAS**

- No se garantiza disponibilidad la conectividad Internet --> VPN.
- No se garantiza el caudal.
- Gestión de claves de acceso y autenticación delicada y laboriosa.
- La fiabilidad es menor que en una línea dedicada

- Mayor carga de encapsulación y encriptación en el cliente VPN.
- Mayor complejidad en la configuración del cliente, proxy, servidor de correo.
- Una VPN se considera segura pero al viajar por Internet no seguro y expuestos a ataques.

### 3.1.2 Funcionamiento de una VPN

Una red privada virtual se basa en un protocolo denominado **protocolo de túnel**, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro.

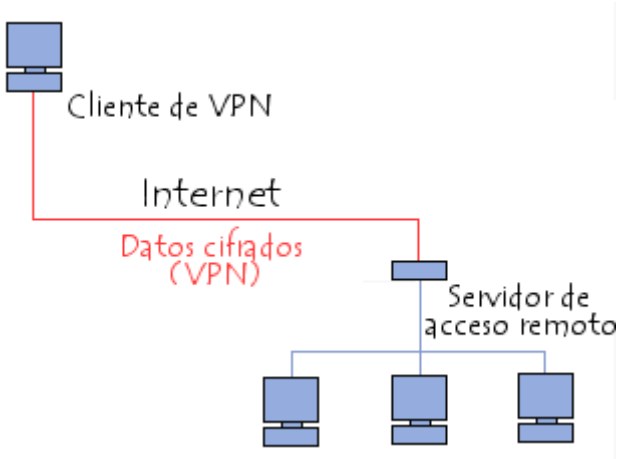



Fig 1. Funcionamiento del VPN
Fuente: www.argo.es

La palabra "túnel" se usa para simbolizar el hecho que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella y, por lo tanto, son incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN, como si los datos viajaran a través de un túnel. En una VPN de dos equipos, el cliente de VPN es la parte que cifra y descifra los datos del lado del usuario y el servidor VPN (comúnmente llamado servidor de acceso remoto) es el elemento que descifra los datos del lado de la organización.

De esta manera, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite sin cifrar al sistema de pasarela, que se conecta con la red remota mediante la infraestructura de red pública como intermediaria; luego transmite la solicitud de manera cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y éste envía la

respuesta cifrada. Cuando el cliente de VPN del usuario recibe los datos, los descifra y finalmente los envía al usuario.

### 3.1.3 Tunel

El túnel es una técnica de que usa una infraestructura entre redes para transferir datos de una red a otra. Los datos o la carga pueden ser transferidos como tramas de otro protocolo. El protocolo de tuneling encapsula las tramas con una cabecera adicional, en vez de enviarla como se produjo en el nodo original. La cabecera adicional proporciona información al routing para hacer capaz a la carga de atravesar la red intermedia. Las tramas encapsuladas son encaminadas a través de un túnel que tiene como puntos finales, los dos puntos entre la red intermedia. El túnel en un camino lógico a través del cual se encapsulan paquetes viajando entre la red intermedia. Cuando una trama encapsulada llega a su destino en la red intermedia, se desencapsula y se envía a su destino final dentro de la red. Tunneling incluye todo el proceso de encapsulado, desencapsulado transmisión de las tramas.

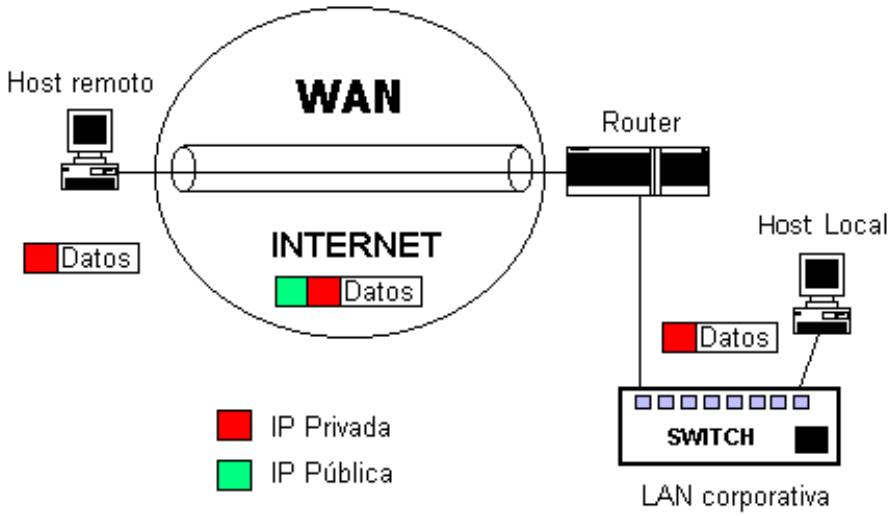



Fig 2. Funcionamiento del TUNEL
Fuente: www.argo.es

### 3.1.4 Protocolos de túneles

Los protocolos PPTP, L2F y L2TP se enfocan principalmente a las VPN de acceso remoto, mientras que IPSec se enfoca mayormente en las soluciones VPN de sitio – sitio.

Los principales protocolos de túnel son:

- PPTP (Protocolo de túnel punto a punto) o (Point-to-Point Tunneling Protocol) permite extenderse a una red privada a través de una red pública como Internet a través de túneles. Es un estándar propuesto por Microsoft, entre otras compañías, y junto con L2TP, propuesto por Cisco Systems, son los candidatos más sólidos para sentar las bases de un nuevo estándar de la IETF. Con PPTP, que es una extensión del protocolo PPP (Point-to-Point Protocol), cualquier usuario/a de un PC con soporte de cliente PPP, puede usar un ISP (Internet Service Provider) independiente para conectar con un servidor cualquiera dentro de la red privada a la que esté accediendo, de forma segura.

- L2F (Reenvío de capa dos) es un protocolo de capa 2 desarrollado por Cisco, Northern Telecom y Shiva. Actualmente es casi obsoleto. Precursor del L2TP. Ofrece métodos de autentificación de usuarios remotos y carece de cifrado de datos

- L2TP (Protocolo de túnel de capa dos) o (Layer Two Tunneling Protocol) es una extensión del protocolo PPTP, usado por un ISP para conseguir crear una red privada virtual o VPN (Virtual Private Network) a través de Internet. L2TP surge de la confluencia de las mejores características de otros dos protocolos de entunelamiento: PPTP de Microsoft, y L2F (Layer-2 Forwarding) de Cisco Systems. Además de las diferencias en el sistema de autentificación, L2TP ha adquirido una popularidad particular por el uso de IPsec (IP Security) para garantizar la privacidad. Los dos principales componentes que conforman L2TP son el LAC (L2TP Access Concentrator), que es el dispositivo que canaliza físicamente la llamada, y el LNS (L2TP Network Server), que es el que canaliza y autentifica el stream PPP. Se define en el RFC 2661.

- **IPSec** es un protocolo de capa 3 creado por el IETF que puede enviar datos cifrados para redes IP.

  IPSec es un protocolo definido por el IETF que se usa para transferir datos de manera segura en la capa de red. En realidad es un protocolo que mejora la seguridad del protocolo IP para garantizar la privacidad, control de acceso, integridad, confidencialidad y autentificación del origen de los datos.

IPSec se basa en tres módulos:

- *Encabezado de autenticación IP* (**AH**), que incluye integridad, autenticación y protección contra ataques de REPLAY a los paquetes.


- *Carga útil de seguridad encapsulada* (**ESP**), que define el cifrado del paquete. ESP brinda privacidad, integridad, autenticación y protección contra ataques de REPLAY.


- *Asociación de seguridad* (**SA**) que define configuraciones de seguridad e intercambio clave. Las SA incluyen toda la información acerca de cómo procesar paquetes IP (los protocolos AH y/o ESP, el modo de transporte o túnel, los algoritmos de seguridad utilizados por los protocolos, las claves utilizadas). El intercambio clave se realiza manualmente o con el protocolo de intercambio IKE, lo que permite que ambas partes se escuchen entre sí.

### 3.1.5 Encriptación de VPN

Una vez dentro de la VPN, cada uno de los gateways envían su clave pública a todos los demás gateways pertenecientes al sistema. Con el uso de sistemas de encriptación simétricos, de clave pública y clave privada, la información se encripta matemáticamente de tal forma que es extremadamente complejo desencriptar la información sin poseer las claves. Existe un proceso de gestión de dichas claves (Key management) que se encarga de su distribución, su refresco cada cierto tiempo, y revocarlas cuando sea necesario hacerlo. Se ha de conseguir un balance entre los intervalos de intercambio de las claves y la cantidad de información que se transfiere: Un intervalo demasiado corto sobrecargaría los servidores de la VPN con la generación de claves, mientras que uno excesivamente largo podría comprometer la clave y la información que esta protege.

### 3.1.5.1 Algoritmos de encriptación

Una manera segura de la transmisión de datos o información en una red virtual privada (VPN) es implementar uno o más algoritmos de encriptación, en la configuración del VPN, ya que como medio de comunicación se usa el internet o similares, data que puede ser vulnerable por este medio y puede ser fácilmente capturada por personas ajenas, pero con los medios de encriptación, esta data esta cifrada y no puede ser entendible por personas ajenas.

- **DES** Data Encryption Standard, es un algoritmo de cifrado en bloque simétrico, de longitud fija, el cual consiste de dos permutaciones, 16 vueltas en donde el mensaje de 64 bits es dividido en dos bloques de 32 bits, después de usar la primer permutación llamada P1, es cifrado 16 veces utilizando cada vez una subclave, la cual se genera 16 veces en un proceso paralelo. En el proceso para descifrar se utiliza el mismo algoritmo con las subclaves en orden inverso, dando como consecuencia, la simetría del algoritmo.

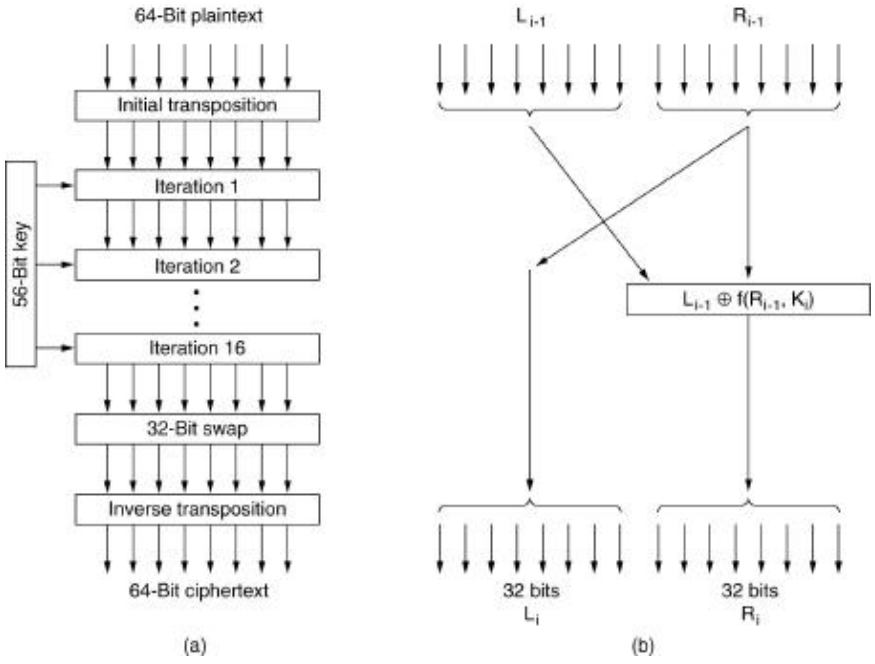



Fig.: DES [Data Encryption Standard]
Fuente: www.jalercom.com/cms/upload/articles/art-pwrline.pdf

**Funcionamiento:**

DES, es un algoritmo de cifrado en bloques simétrico, el tamaño del bloque es de longitud fija de 64 bits, el algoritmo consta de dos permutaciones, una al inicio conocida como *P1*, la cual se muestra a continuación:

| Tabla antes la Permutación | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |

| Permutación Inicial (P1) | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |

Tabla 1: algoritmo DES permutación Inicial
Fuente: ccia.ei.uvigo.es/docencia/SSI/Tema3.p2.pdf

Después de recibir un bloque de entrada de 64 bits, el *primer paso* consiste en aplicar al bloque de entrada la permutación P1, teniendo como resultado un orden de salida que se identifica leyendo la tabla de izquierda a derecha y de arriba abajo. Significa que el bit del lugar 58 en el mensaje de entrada, después de la permutación, ocupara la posición 1 y así sucesivamente.

Se muestra el resultado de haber realizado la permutación *P1*, la parte superior se encuentra marcada con el fin de indicar cuales son los bits que forman el sub-bloque $L_0$, los bits restantes forman el sub-bloque $R_0$, dando como resultado:

**$L_0$ = 11111111 00011000 11010111 11101010**

**$R_0$ = 00000000 11111110 11001100 10000100**

*Sub-bloques iníciales*

**Permutación E:** La salida de $R_0$ es de 32 bits, se utiliza la permutación E, con el propósito de expandir a 48 bits y así poder realizar la suma OR exclusiva con la clave $K_i$. A continuación se muestra la tabla para realizar la permutación E.

| 32 Bits | | | |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 |

Tabla 2: algoritmo DES – 32 bits
Fuente: ccia.ei.uvigo.es/docencia/SSI/Tema3.p2.pdf

Al tener la secuencia de $R_0$ de 32 bits, es necesario aplicar la permutación E, la cual se muestra a continuación.

**$R_0$ = 0000 0000 1111 1110 1100 1100 1000 0100**

| Permutación E | | | | | |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 |

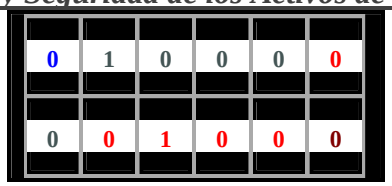



Tabla 3: algoritmo DES permutación E
Fuente: ccia.ei.uvigo.es/docencia/SSI/Tema3.p2.pdf

El resultado de la permutación E(R0) es:

**E(R0) = 000000 000001 011111 111101 011001 011001 010000 001000**

- **RSA** (Rivest-Shamir-Adleman) es el algoritmo de encriptación y autentificación más comúnmente usado. Fue desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman, y se incluye como parte de los navegadores de Netscape y Microsoft, así como aplicaciones como Lotus Notes y muchos otros productos. El sistema de encriptación era propiedad de RSA Security hasta que en septiembre de 2000 caducó la patente que había sobre este algoritmo. Basado en la dificultad de la factorización en factores primos de números enteros bastante grandes y ampliamente utilizado en nuestros tiempos.

  El funcionamiento de este algoritmo se basa en multiplicar dos números primos extremadamente grandes, y a través de operaciones adicionales obtener un par de números que constituyen la clave pública y otro número que constituye la clave privada. Una vez que se han obtenido las claves, los números primos originales ya no son necesarios para nada, y se descartan. Se necesitan tanto las claves públicas como las privadas para encriptar y desencriptar, pero solamente el dueño de la clave privada lo necesitará. Usando el sistema RSA, la clave privada nunca necesitará ser enviada. La clave privada se usa para desencriptar el código que ha sido encriptado con la clave pública. Por tanto, para enviar un mensaje a alguien, hay que conocer su clave pública, pero no su clave privada. Al recibir el mensaje, se necesitará la clave privada para desencriptarlo. También se puede usar para autentificar un mensaje, firmando con la clave privada un certificado digital. Su longitud típica de llaves es 512 y 1024 bits.

  En el algoritmo RSA si:

  - A genera dos enteros primos bastante grandes **p** y **q**.

- A calcula **n=pq** y **Ø(n)=(p-1)(q-1)**.
- A escoge aleatoriamente un **b** tal que **1<b<Ø(n)** y **mcd(b, Ø(n))=1**.
- A calcula **a=b-1mod Ø(n)**.
- A guarda su llave privada **(a,n)**.
- A publica su llave pública **(b,n)**

RSA en la encriptación de mensaje de un elemento B:

- B compone el mensaje **x** (un entero).
- B recupera la llave publica de A **(b,n)**.
- B encripta el mensaje **y=xbmod n**.
- B envía el mensaje codificado **y** a A.

RSA para la Decriptación de un mensaje el elemento A:

- A recibe el mensaje codificado **y**.
- A decripta el mensaje **x=yamod n** con su llave privada **(a,n)**.

RSA contra intento de Ataque de un elemento C:

- C recupera la llave pública de A **(b,n)**.
- C recupera el mensaje codificado **y** enviado a A yB
- C necesita conocer **a** para poder descodificar el mensaje. Factorizando **n** en **p** y **q**, se puede calcular **Ø(n)=(p-1)(q-1)**, y con **b** se puede calcular **a=b-1mod Ø(n)**.
- Pero la FACTORIZACIÓN es un problema MUY DIFICIL.

❖ **AES** (Advanced Encryption Standard) es un algoritmo de encriptación para proteger información delicada, aunque no clasificada, por las agencias gubernamentales de USA y, como consecuencia, puede transformarse en el estándar de facto para las transacciones comerciales en el sector privado. La criptografía para las comunicaciones clasificadas, incluyendo las militares, es gestionada por algoritmos secretos. En enero de 1997, El NIST (Nacional Institute of Standards and Technology) inició un proceso para encontrar un algoritmo más robusto que reemplazara a DES y en menor medida a triple DES (3DES). La especificación solicitaba un algoritmo simétrico usando encriptación por bloques de 128 bits de tamaño, que soportara como mínimo claves de 128, 192 y 256 bits. Debía ser royalty-free para su uso en todo el mundo, y ofrecer un nivel de seguridad suficiente para los próximos 20 ó 30 años.

- **IDEA** (International Data Encryption Algorithm) es un algoritmo de encriptación desarrollado en el ETH de Zurich (Suiza) por James Massey y Xuejia Lai. Usa criptografía de bloque con una clave de 128 bits, y se suele considerar como muy seguro. Está considerado como uno de los algoritmos más conocidos. Durante los años que lleva siendo usado, no ha sido publicado ningún método práctico para reventarlo, a pesar de los numerosos intentos que han habido de encontrar uno. IDEA está patentada en USA y en la mayor parte de los países europeos, y la patente está en manos de Ascom-Tech AG. El uso no comercial de IDEA es gratuito.

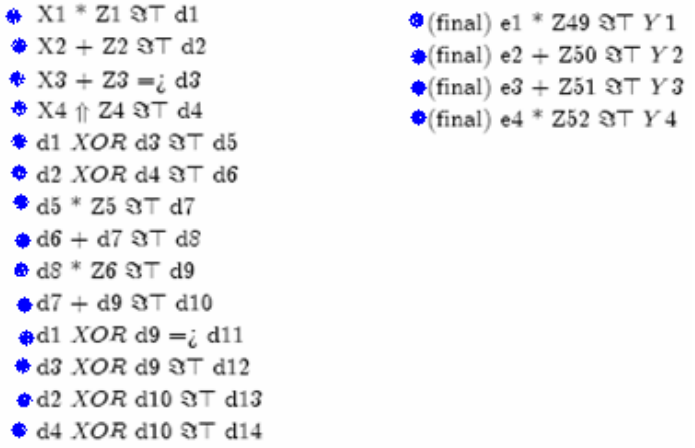
**Funcionamiento**

IDEA – Generación de las sub-llaves

1. La llave de 128 bits divididos en 8 sub-llaves de 16 bits.
2. Los bits de la llave de 128 bits sufren una rotación circular de 25 bits a la izquierda. Con esta nueva llave se continúa en el paso 1.
3. Los pasos anteriores se repiten hasta obtener las 52 sub-llaves de 16 bits, llamadas: Z1, Z2,...,Z52.

IDEA en la Encriptación:

1. El mensaje se divide en bloques de 64 bits, los cuales son codificados uno por uno.
2. Cada bloque de 64 bits se divide en 4 subbloques de 16 bits, llamados: X1, X2, X3 y X4.
3. A estos cuatro bloques se aplica 8 veces los pasos 1 a 14 de la transparencia consecutiva.
4. Finalmente, a los cuatro bloques resultantes se les aplica los pasos 15 a 18 de la transparencia consecutiva.
5. Estos últimos cuatro bloques resultantes forman el bloque de 64 bits codificado.




IDEA en la Decriptación

La decriptación de un bloque de 64 bits se realiza de la misma manera que la encriptación, salvo que las sub-llaves son las sgtes.:

- 1ra vuelta Z49*,Z50',Z51',Z52*,Z47,Z48
- 2da vuelta Z43*,Z44',Z45',Z46*,Z41,Z42
- 3ra vuelta Z37*,Z38',Z39',Z40*,Z35,Z36
- 4ta vuelta Z31*,Z32',Z33',Z34*,Z29,Z30
- 5ta vuelta Z25*,Z26',Z27',Z28*,Z23,Z24
- 6ta vuelta Z19*,Z20',Z21',Z22*,Z17,Z18
- 7ma vuelta Z13*,Z14',Z15',Z16*,Z11,Z12
- 8va vuelta Z7*,Z8',Z9',Z10*,Z5,Z6
- Transformación final Z1*,Z2',Z3',Z4*
- ZXX* = inverso multiplicativo de ZXX modulo $2^{16}+1$
- ZXX' = inverso aditivo de ZXX modulo $2^{16}$

### 3.1.5.2 Controles y riesgos asociados a la tecnología VPN

Cuando se desea implantar una VPN se debe estar consciente de las ventajas que va a aportar a la organización, sin embargo, es importante considerar los riesgos que estas facilidades implican en caso de no adoptarse las medidas necesarias al implantar una VPN segura. Los estándares utilizados para la implementación de VPNs, garantizan la privacidad e integridad de los datos y permiten la autenticación de los extremos de la comunicación, pero esto no es suficiente: el uso erróneo de las VPN puede ser catastrófico para el negocio. Las medidas para implantar una VPN "segura" incluyen el uso de certificados digitales para la autenticación de equipos VPN, token cards o tarjetas inteligentes para la autenticación "fuerte" de usuarios remotos, y para el control de acceso es importante contar con un Firewall y sistemas de autorización.

**3.1.5.3 Certificados digitales:**

Con el uso de certificados digitales, se garantiza la autenticación de los elementos remotos que generan el túnel y elimina el problema de la distribución de claves. Implantar un sistema PKI (Infraestructura de Clave Pública) para emitir los certificados digitales, permite tener el control absoluto de la emisión, renovación y revocación de los certificados digitales usados en la VPN. El uso de PKI no se limita sólo a las VPNs sino que puede utilizarse para aplicaciones como firmas digitales, cifrado de correo electrónico, entre otras.

**3.1.5.4 Autenticación fuerte:**

En la implantación de una VPN se debe verificar que se estén realmente autenticando los usuarios. Esto dependerá de dónde se almacene el certificado digital y la clave privada. Si el certificado digital y la clave privada se almacenan, protegidos por un PIN, en una tarjeta inteligente que el usuario lleva consigo, se está autenticando al usuario. Desafortunadamente, aun no existe un estándar definido que permita la implantación a gran escala de lectores de tarjetas en los PCs. Por lo que esta opción en algunos casos no es factible. Si, por el contrario, el certificado digital y la clave privada se almacenan en el propio PC, no se está autenticando al usuario sino al PC. Para autenticar al usuario, algunos fabricantes de sistemas VPN han añadido un segundo nivel de autenticación.

El uso de contraseñas es un nivel adicional de seguridad, pero no es el más adecuado, ya que carecen de los niveles de seguridad necesarios debido a que son fácilmente reproducibles, pueden ser capturadas y realmente no autentican a la persona.

El método más adecuado es autenticar a los usuarios remotos mediante un la utilización de sistemas de autenticación fuerte. Estos sistemas se basan en la combinación de dos factores: el token y el PIN. De esta forma se asegura que sólo los usuarios autorizados acceden a la VPN de la organización.

**Métodos de autentificación recomendables**

- MS-CHAP v2
  - Versión mejorada de MS-CHAP
  - Usada frecuentemente

  - Desde el punto de vista del cifrado es mas fuerte que PAP, CHAP, MS-CHAP
  - Recomendada cuando no es posible implementar EAP-TLS

- EAP
  - Extensible Authentication Protocol
  - Soporta varios tipos de Autenticación
    - EAP-MD5: Desafió/Respuesta. No muy seguro.
    - EAP-TLS: Basado en cerificados; requiere pertenencia a un dominio; diseñado para ser utilizado con Smart Cards
    - EAP-RADIUS: Mecanismo proxy de reenvió de datos en un formato EAP especifico a un servidor RADIUS
  - El tipo a utilizar se puede especificar en el servidor o mediante políticas a un grupo especifico de usuarios.
- PEAP: Protected EAP
  - Protege las negociaciones EAP envolviéndolas con TLS
  - Se usa solo para conexiones wireless 802.11
    - Soporta reconexiones rápidas para entornos grandes con roaming
  - Puede usar PEAP plus
    - EAP-MS-CHAPv2: añade autenticación mutua; requiere que el cliente confié en los certificados del servidor; fácil de implementar.
    - EAP-TLS: Muy seguro; requiere una infraestructura PKI
  - Hay documentación completa de como implementarlo en la Web de TechNet

**Métodos de autentificación no recomendables**

- Password Authentication Protocol (PAP)
  - Envía la password en texto claro.
- Shiva Password Authentication Protocol (SPAP)
  - Utiliza cifrado reversible
- Challenge Handshake Authentication Protocol (CHAP)
  - Utiliza MD5 para proporcionar autenticación mediante desafío-respuesta

  - Requiere almacenar las contraseñas con cifrado reversible en el servidor

- MS-CHAP
  - Existen debilidades conocidas

### 3.1.5.5 Firewall y Sistemas de Autorización:

El control de acceso se puede realizar utilizando Firewalls y sistemas de autorización; de esta manera se aplican políticas de acceso a determinados sistemas y aplicaciones de acuerdo al tipo de usuarios o grupos de usuarios que los acceden.

## 4. CONCLUSIONES

- Las VPNs representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha convertido en un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro.

- Las VPNs sin embargo, tienen inconvenientes y para ello primeramente se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no está bien definido pueden existir consecuencias serias.

- Para permitir la comunicación entre dos personas sin que una tercera persona pueda comprender el mensaje transmitido se puede optar por algún tipo de algoritmos de encriptación.
- Para elaboración de políticas de seguridad de VPNs, estas deben estar construidas de acuerdo al tipo de empresa, donde están implementadas.

- La seguridad es uno de los factores fundamentales y de éxito de la utilización de algoritmos de encriptación, garantiza en todo momento que las comunicaciones sean fiables.
- El uso de métodos de autentificación en implementación de VPNs asegura que sólo los usuarios autorizados acceden a la VPN de la organización, puedan tener acceso a esta.
- La resistencia de la criptografía a los ataques está basada en la dificultad calculatoria de ciertos problemas matemáticos, o en la extrema confusión y dispersión aplicada a la información.

- En un entorno distribuido y abierto como es Internet, la criptografía tiene un papel muy importante.
- Con el uso de protocolos de encriptación, la información que atraviesa Internet lo hace de forma cifrada, de modo que sólo el destinatario seleccionado será capaz de leer la misma. Incluso en el caso de escuchas no permitidas, no será posible la recuperación de la información original de forma legible sin conocer las claves que sólo los interlocutores legítimos poseen.

## 6. DATOS PERSONALES

Pamela Isabel Gonzales Maldonado nació un 3 de noviembre de 1982,en la ciudad de La Paz - Bolivia, estudio en el Colegio Santa Ana de esta misma ciudad, egresando el año 2000, posteriormente ingreso a estudiar a la Universidad Católica Boliviana “San Pablo” donde obtuvo el grado de Licenciada en Ingeniería de Sistemas. Actualmente se encuentra cursando la Maestría de telecomunicaciones Y Telemática en Universidad Católica Boliviana “San Pablo”, y el Diplomado en Auditoría de Sistemas y Seguridad de los Activos de la Información en la Universidad Mayor de San Andres.

## 6. INFOGRAFIA


- http://www.acis.org.co/memorias/JornadasSeguridad/IVJNSI/MauricioMunoz-IVJNSI.pdf
- http://www.idg.es/computerworld/articulo.asp?id=153363
- http://www.computing.es/Informes/200802210018/Control-de-acceso-la-solucion-de-seguridad-para-redes-de-altas-prestaciones.aspx
- http://www.microsoft.com/spain/technet/recursos/articulos/ipsecch5.mspx
- www.idg.es/comunicaciones/articulo.asp?id=133140
- http://www.canalsw.com/ayudas/glosario/glosario2.asp?id=805&ic=4
- http://www.uv.es/ciuv/cas/vpn/index.html
- www.publispain.com/supertutoriales/matematica/criptografia/cursos/3/crypto.pdf -
- eia.udg.es/~cmantill/admonxarxes/clase12.pdf -
- ccia.ei.uvigo.es/docencia/SSI/practicas/cifrado-jce.pdf -
- cia.ei.uvigo.es/docencia/SSI/Tema3.p2.pdf
- www.caserveis.net/aplication/cms/documentos/doc1_14122005013629.pdf
- www.jalercom.com/cms/upload/articles/art-pwrline.pdf
- www.gemelostorage.com/Contenidos/Manuales/Personal/GBO_Personal_Inscripción.pdf
- geneura.ugr.es/~jmerelo/DyEC/Tema4/DyEC-Tema4.pdf
- www.cesip.org/es/enlaces-bdd/trabajos/bolivia/2003/villalba_criptografia.pdf