2

ESCENARIO DE RED WAN SEGURA

Objetivo

- Describir el escenario de seguridad que necesitan las redes WAN para funcionar sobre la Internet pública.

Manual de clases

Última modificación:
24 de febrero de 2023

Tema 2 de:
REDES WAN
Edison Coimbra G

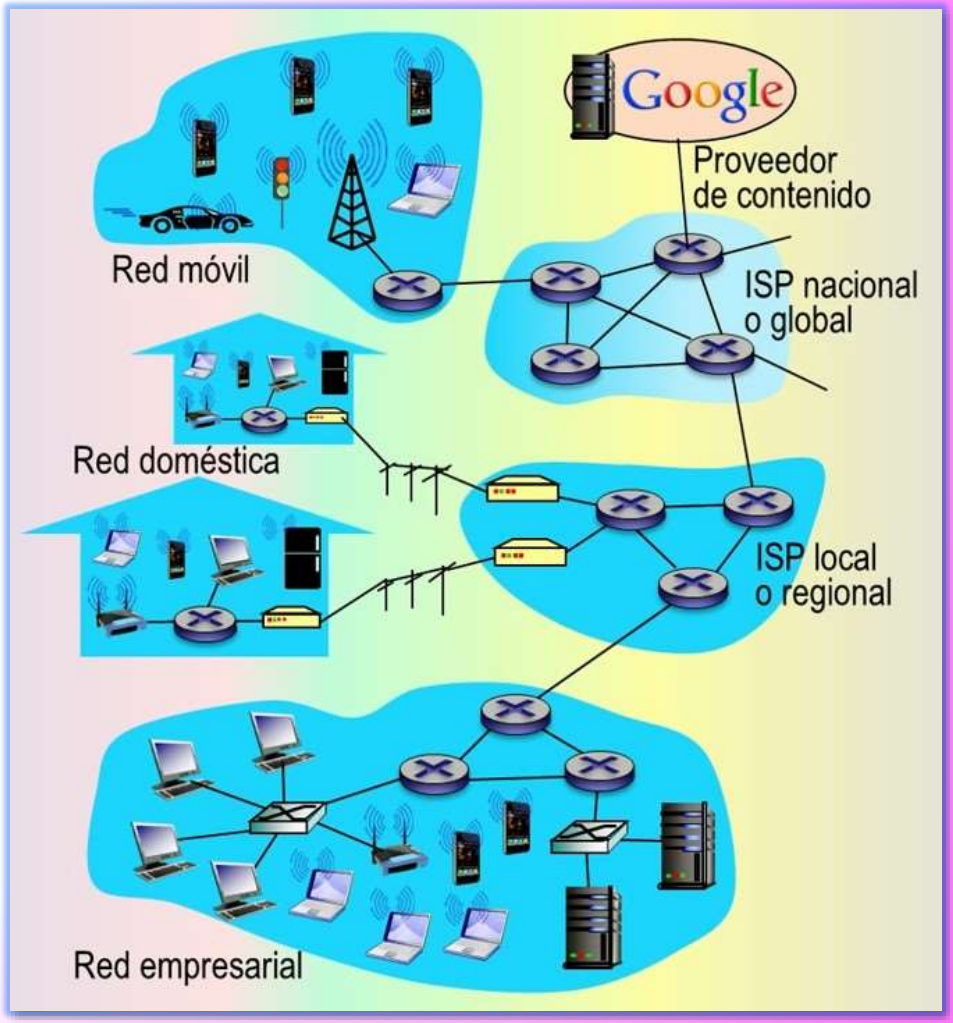
1. LA SEGURIDAD EN REDES

ESCENARIO DE RED WAN SEGURA

¿A qué hace referencia la seguridad en las redes?

(Kurose, 2017)

- **Internet** se ha convertido en una herramienta crítica para muchas instituciones, incluyendo empresas pequeñas y medianas, universidades y organismos gubernamentales.
- **Muchas personas** confían en Internet para llevar a cabo sus actividades profesionales, sociales y personales. Miles de millones de "cosas" se conectan hoy en día a Internet.
- **Detrás** de todas estas utilidades y toda esta excitación, hay un lado oscuro: desde el punto de vista de un administrador de red, el mundo se divide de forma bastante nítida en dos bandos:
  - ▶Los buenos, aquellos que pertenecen a la red de la organización y que deben poder acceder a los recursos internos de la misma de una forma relativamente poco restringida y….
  - ▶Los malos, todos los demás, aquellos que deben ser cuidadosamente escrutados a la hora de acceder a los recursos de la red.
- **El campo de la seguridad de red** se ocupa de ver cómo "los malos" pueden atacar a las redes de computadoras y cómo se las puede defender de esos ataques, o mejor todavía, de cómo diseñar nuevas arquitecturas que sean inmunes a tales ataques.



ESCENARIO DE RED WAN SEGURA

¿Por qué Internet se ha convertido en un lugar inseguro? (Kurose, 2017)

- **Básicamente**, la respuesta es que Internet fue diseñada originalmente de esa manera, ya que se basaba en el modelo de un "grupo de usuarios que confiaban entre sí, conectados a una red transparente", un modelo en el que, por definición, no había necesidad de pensar en la seguridad.
- **Muchos aspectos** de la arquitectura de Internet original reflejan profundamente esta idea de confianza mutua, pero la comunicación entre usuarios de mutua confianza es la excepción, mas que la regla. Este es el mundo de las redes modernas de comunicaciones.
- **Se ha dicho que** "los malos" atacan a las redes de computadoras, por ello, dada la frecuencia y variedad de ataques existentes, así como la amenaza de nuevos y mas destructivos ataques futuros, la seguridad de red se ha convertido en un tema crucial en el campo de las redes de computadoras.
- **Para defender** a las redes de computadoras de esos ataques, o mejor todavía, para diseñar nuevas arquitecturas que sean inmunes a tales ataques, es preciso hacer una clasificación de los ataques más habituales actualmente en Internet.

Principales ataques a las redes modernas			
1. Introducción de software malicioso	**2. Ataque a los servidores y a la infraestructura de red**	**3. Examen y análisis de paquetes**	**4. Suplantación IP**
Virus	Ataque de vulnerabilidad	Programas sniffers	Inyección de paquetes
Gusano	Inundación del ancho de banda		
Troyano	Inundación de conexiones		

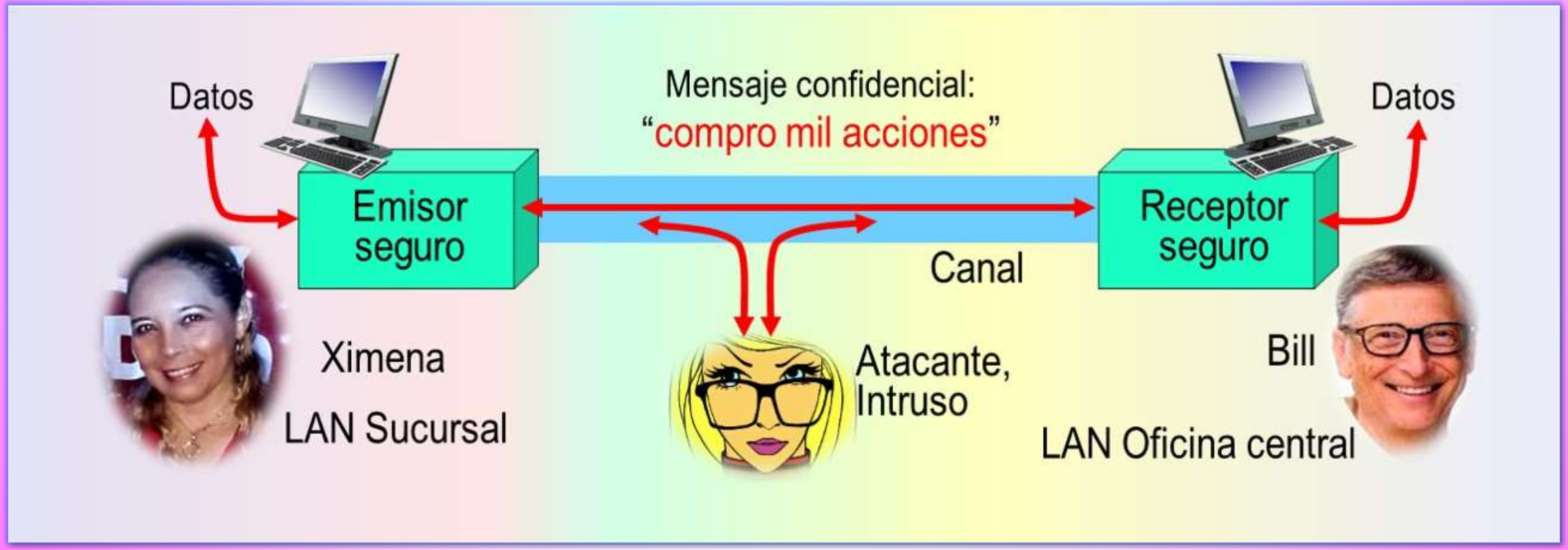
- **Se identifican** cuatro clases de ataques.

ESCENARIO DE RED WAN SEGURA

¿Cómo garantizar una comunicación segura?

(Kurose, 2017)

- **Considere la conexión WAN** de dos redes LAN empresariales en la que dos ejecutivos se comunican confidencialmente. ¿Qué acciones tomaría para garantizar que el atacante no comprenda el contenido del mensaje, aún cuando pueda leerlo? Justifique y demuestre su respuesta.



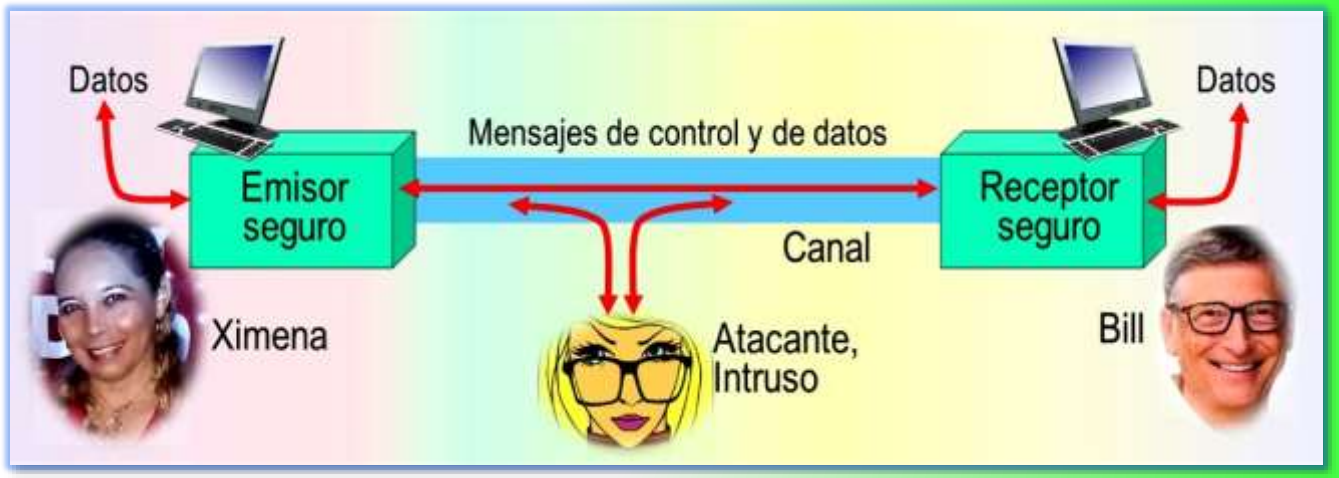
2.- ESCENARIO DE UNA COMUNICACIÓN SEGURA

ESCENARIO DE RED WAN SEGURA

¿Qué quiere decir comunicación segura?

(Kurose, 2017)

- **Para tener un visión panorámica** del escenario de la seguridad, se presenta a Ximena y a Bill que desean comunicarse y desean hacerlo "de manera segura", resaltando que estas dos personas podrían ser:
  - ⊠Dos routers que desean intercambiar sus tablas de routing en forma segura.
  - ⊠Un cliente y un servidor que desean establecer una conexión de transporte segura.
  - ⊠Dos aplicaciones de correo electrónico que quieren intercambiar mensajes de correo seguros.
- **Pero,** ¿qué quiere decir exactamente comunicarse de manera segura? En realidad:



- ▶**Ximena** quiere que solo Bill sea capaz de comprender los mensajes que ella envía, incluso aunque estén comunicándose a través de un medio no seguro en el que un intruso pueda interceptar lo que Ximena transmite.
- ▶**Bill** también quiere estar seguro de que el mensaje que él recibe de Ximena fue realmente enviado por Ximena.
- ▶**Ximena** quiere estar segura de que la persona que se está comunicando con ella es realmente Bill.
- ▶**Ambos** también quieren estar seguros que el contenido de sus mensajes no ha sido alterado en el camino.
- ▶**Además**, quieren estar seguros de que siempre podrán comunicarse, es decir, que nadie les puede denegar el acceso a los recursos necesarios para comunicarse.

Escenario de una comunicación segura

ESCENARIO DE RED WAN SEGURA

Propiedades de una comunicación segura

- **Se identifican** cuatro propiedades deseables en una comunicación segura.
- ▶**1. Confidencialidad**. Solo el emisor y el receptor deberán comprender el contenido de los mensajes transmitidos. Es necesario que los mensajes sean cifrados de alguna manera, de modo que un mensaje interceptado no pueda ser comprendido por algún curioso que lo ha interceptado.

(Kurose, 2017)

Propiedades de una comunicación segura			
1. Confidencialidad	**2. Integridad de los mensajes**	**3. Autenticación del punto terminal**	**4. Seguridad operacional**
Cifrado PGP para correo	Cifrado PGP para correo	Cifrado PGP para correo	Firewalls (Filtros de paquetes. Filtros con memoria del estado. Gateways de aplicación)
Protocolo TCP-SSL	Protocolo TCP-SSL	Protocolos de autenticación (Contraseñas y números distintivos)	Sistemas de Detección y de Prevención de Intrusiones
Protocolo IPsec (ESP)	Protocolo IPsec (AH, ESP)	Protocolo TCP-SSL Protocolo IPsec (AH, ESP)	Zonas de seguridad y zonas desmilitarizadas

- ▶**2. Integridad de los mensajes**. Las personas que se comunican quieren estar seguras de que el contenido de sus comunicaciones no se vea alterado durante la transmisión, ni maliciosamente ni por accidente.
- ▶**3. Autenticación del punto terminal**. Tanto el emisor como el receptor deberán poder confirmar la identidad del otro en el proceso de comunicación (confirmar que el otro es de hecho quien dice ser). La comunicación humana frente a frente resuelve este problema fácilmente gracias al reconocimiento visual. Cuando las entidades se comunican a través de un medio en el que no es posible ver al otro, la autenticación no es tan sencilla.
- ▶**4. Seguridad operacional**. Todas las organizaciones (empresas, universidades, etc.) disponen de redes conectadas a Internet. Estas redes pueden, potencialmente, verse comprometidas. Los atacantes pueden intentar depositar gusanos en los hosts de la red, conseguir secretos corporativos, realizar un mapa de las configuraciones internas de la red y ejecutar ataques DoS. Para responder a estos ataques, se emplean dispositivos operacionales como los firewalls y los sistemas de detección de intrusiones.

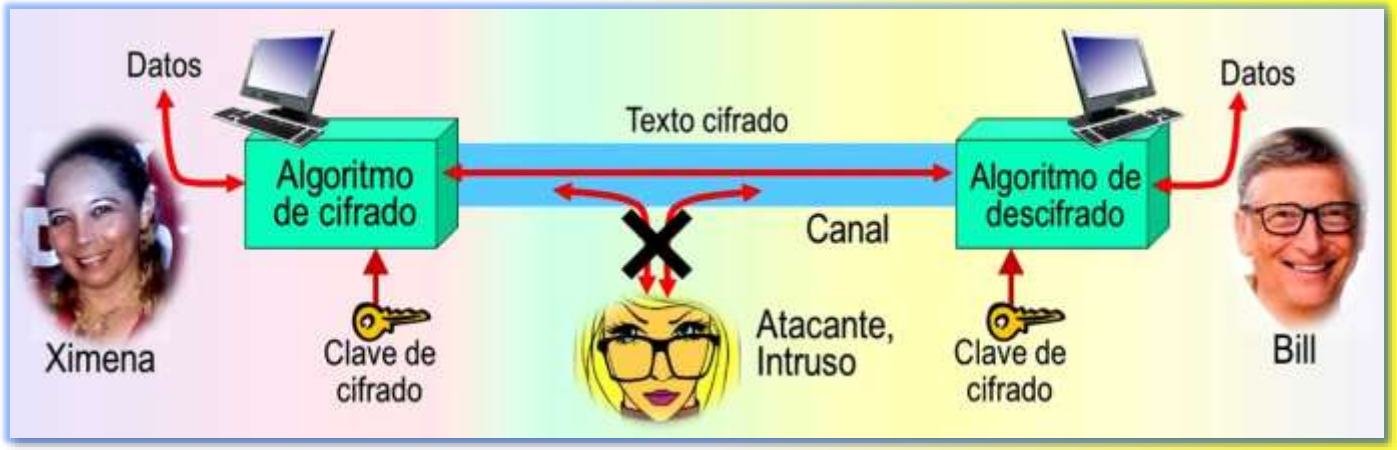
3. TÉCNICAS CRIPTOGRÁFICAS – CLAVE SIMÉTRICA

ESCENARIO DE RED WAN SEGURA

¿En qué consisten las técnicas criptográficas?

(Kurose, 2017)

- **Todos los algoritmos** criptográficos implican sustituir alguna cosa por otra, es decir cifrar.
  - ⊠ La palabra cifrado se emplea a menudo para designar a un método que permite encriptar los datos.



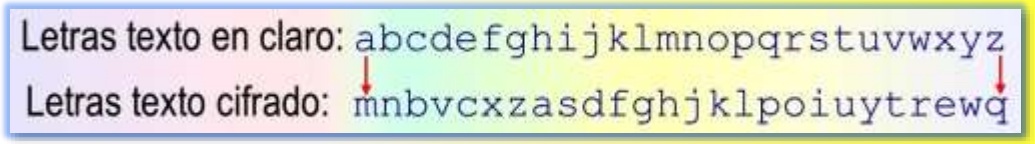
- ▶**El emisor** toma el texto en claro, calcula y lo sustituye por el texto cifrado, ininteligible para cualquier intruso. Para cifrar el mensaje, el emisor utiliza un algoritmo de cifrado y una clave de cifrado.
  - ⊠La clave de cifrado es una secuencia de números o caracteres secretos como entrada para el algoritmo de cifrado.
- ▶**El receptor**, por supuesto, debe ser capaz de recuperar el texto en claro a partir del texto cifrado. Para descifrar el mensaje utiliza un algoritmo de descifrado y una clave de descifrado.
- **Este sistema básico** es un sistema de clave simétrica, las claves de Ximena y de Bill son idénticas y deben mantenerse en secreto.
- **Aunque el uso** de la criptografía para conseguir confidencialidad es el principal tema a resolver, se ha visto que la criptografía está también muy relacionada a la integridad de los mensajes, a la autenticación, al no repudio y a otras muchas cuestiones.

ESCENARIO DE RED WAN SEGURA

Tipos de cifrado clave simétrica

(Kurose, 2017)

- ▶**1.Cifrado simple: Cifrado de César.** Un algoritmo de clave simétrica muy simple y muy antiguo es el atribuido a Julio Cesar y que se conoce con el nombre de cifrado de César.
  - ▶**Ejemplo 1**. Para un texto en español, el Cifrado de César funcionaría tomando una letra del mensaje en claro y sustituyéndola por la letra que es *K* posiciones por detrás del alfabeto (volviendo al principio una vez que se llega al final). Ejemplo texto cifrado con *k*=3 (la clave de cifrado). El mensaje de texto en claro "Hola Ximenita" se transforma en "krod alphqlwd" en el texto cifrado.
- ▶**2.Cifrado monoalfabético.** Sustituye una letra del alfabeto por otra. Sin embargo esas sustituciones no siguen un patrón regular, cualquier letra puede sustituirse por cualquier otra, siempre que cada una tenga una única letra y viceversa. La regla de sustitución de la figura (la clave) muestra la codificación para el texto en claro.



- ▶**3.Cifrado polialfabético.** Utiliza varios cifrados monoalfabéticos, los cuales codifican cada letra en una posición especifica dentro del mensaje de texto en claro.

  - ▶**Ejemplo 2**. En la figura se muestra un esquema de cifrado polialfabético compuesto por dos cifrados de César (*k* = 5 y *k* = 19). Se podría decidir utilizar estos dos cifrados de César, C_1 y C_2, según el patrón repetitivo C_1, C_1, C_2, C_1, C_2. Así, el mensaje de texto en claro "Hola Ximenita", tendría el equivalente de texto cifrado "mtef qnrxsbyf".

ESCENARIO DE RED WAN SEGURA

Tipos de cifrado clave simétrica (cont.)

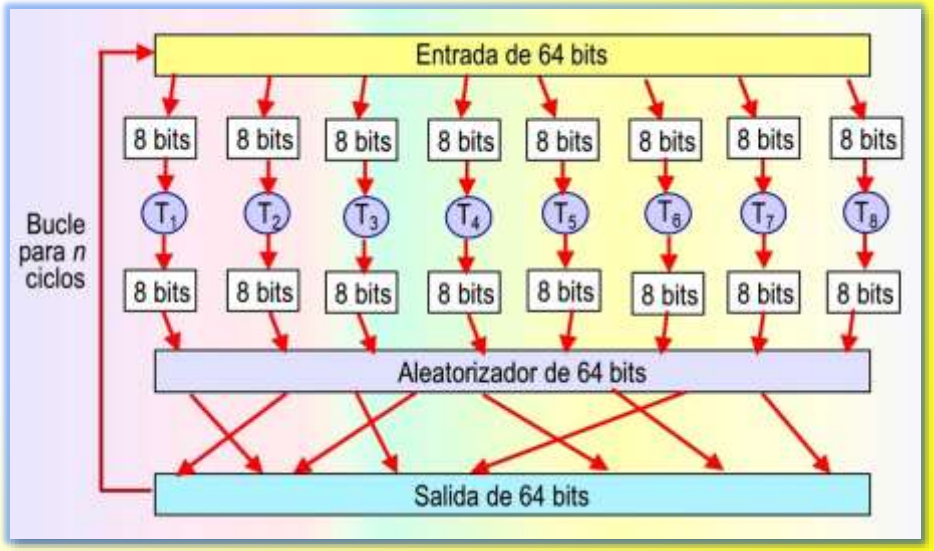
(Kurose, 2017)

- ▶**4. Cifrado de bloque de tabla completa.** El mensaje a cifrar se procesa en bloques de *k* bits. Por ejemplo si *k* = 64, entonces el mensaje se descompone en bloques de 64 bits y cada bloque se cifra de forma independiente. Para codificar un bloque, el sistema de cifrado asigna una correspondencia uno-a-uno, con el fin de asignar el bloque de *k* de bits de texto en claro a un bloque de *k* bits de texto cifrado.

- ▶**Ejemplo 3**. Suponga que *k* = 3, de modo que el cifrado de bloque asigna a cada entrada de 3 bits (texto en claro) una salida de 3 bits (texto cifrado). En la tabla se proporciona una posible correspondencia.

Cifrado en bloque específico de 3 bits			
Entrada	**Salida**	**Entrada**	
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

- ▶**5. Cifrado de bloque con funciones.** El mensaje a cifrar se procesa en bloques de *k* bits. Por ejemplo si *k* = 64, entonces el mensaje se descompone en bloques de 64 bits y estos en bloques de 8 bits y cada bloque se cifra de forma independiente mediante las 8 tablas T_i. Para codificar un bloque, el sistema de cifrado asigna una correspondencia uno-a-uno, con el fin de asignar el bloque de *k* de bits de texto en claro a un bloque de *k* bits de texto cifrado.



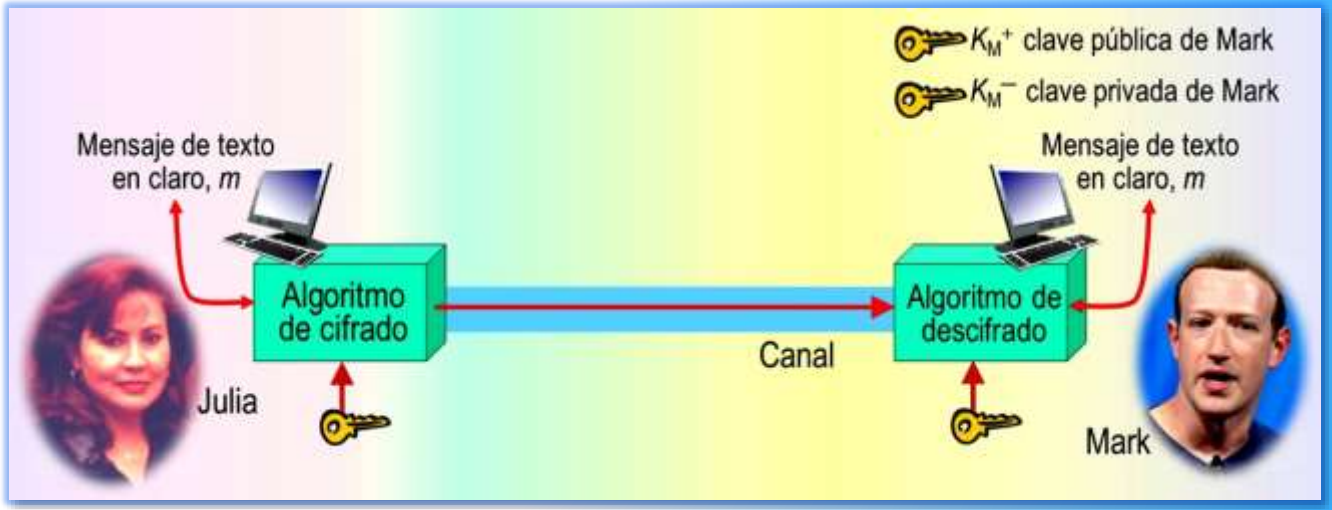
- **Los sistemas** de cifrados de bloque suelen utilizar una técnica denominada encadenamiento de bloques cifrados (*CBC, Cipher Block Chaining*) que proporciona una mayor seguridad.

4.- CIFRADO DE CLAVE PÚBLICA

ESCENARIO DE RED WAN SEGURA

Del cifrado de clave simétrica al cifrado de clave pública (Kurose, 2017)

- **En los sistemas de clave simétrica**, la comunicación cifrada requiere que los dos interlocutores compartan una clave secreta: la clave simétrica utilizada para el cifrado y el descifrado.
  - ✉ Una dificultad con esta técnica es que ambas partes deben acordar de alguna manera cuál es esa clave compartida, pero el hacer eso requiere que se comuniquen de forma segura.
  - ✉ Quizás ambas partes podrían primero reunirse y acordar en persona cuál es esa clave y en lo sucesivo comunicarse mediante un método de cifrado.
- **Sin embargo**, en un mundo conectado en red, los que se están comunicando pueden no llegar a encontrarse nunca de forma física, y puede que incluso no lleguen a conversar excepto a través de la red. ¿Es posible que dos partes se comuniquen de forma cifrada sin conocer de antemano una clave secreta compartida?



- **En 1976. Diffie y Hellman** inventaron un algoritmo (el algoritmo de intercambio de claves de Diffie-Hellman) para hacer precisamente eso; se trata de un enfoque radicalmente distinto y elegante para las comunicaciones seguras y que ha conducido al desarrollo de los sistemas del cifrado actuales de clave pública.
- **En los sistemas de clave pública**, se emplea una pareja de claves. Una de las claves es conocida tanto por Julia como por Mark (de hecho es conocida por todo el mundo). La otra clave solo es conocida por Julia o por Mark, pero no por ambos .

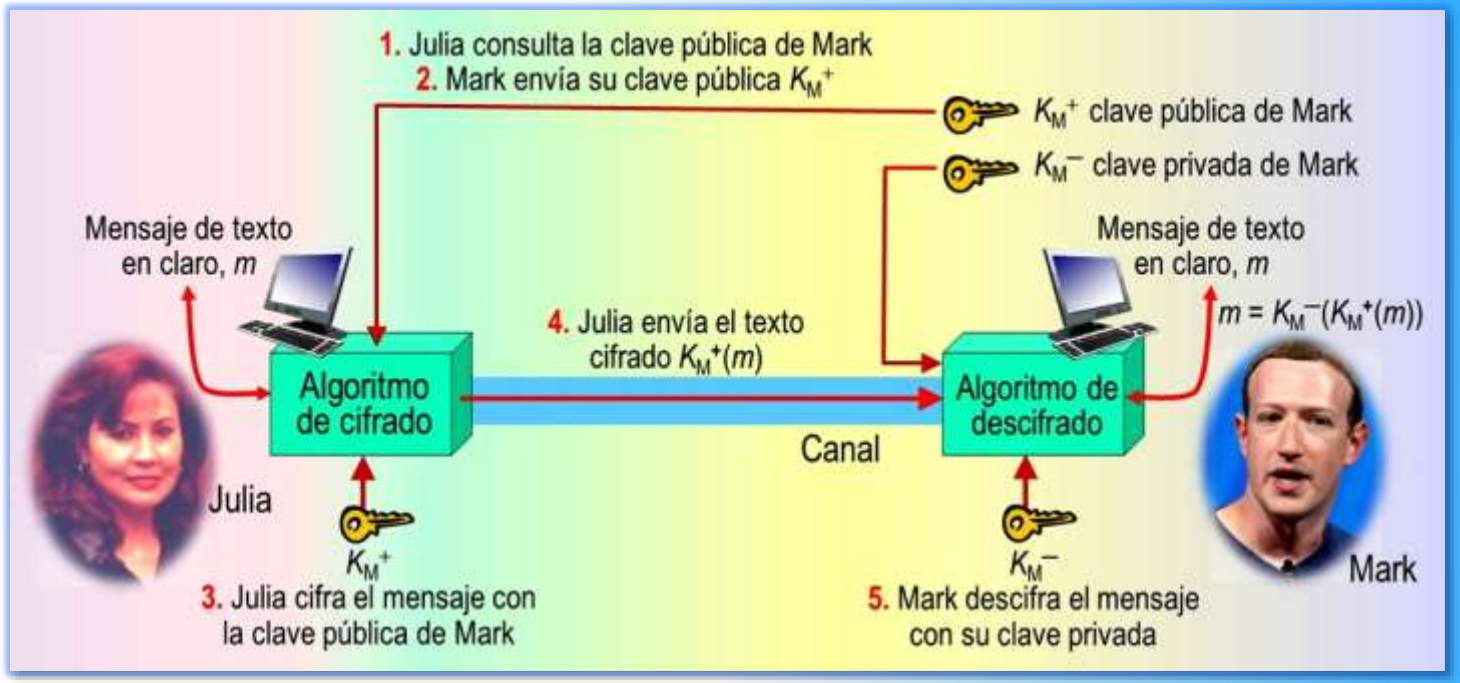
Cifrado de clave pública

ESCENARIO DE RED WAN SEGURA

Cifrado de clave pública

(Kurose, 2017)

- **Conceptualmente**, la utilización de un sistema de criptografía de clave pública es muy simple. Suponga que Julia quiere comunicarse con Mark.
- **En lugar** de que Julia y Mark compartan una única clave secreta, Mark dispone de dos claves:
  - ▶Una clave publica que está disponible para todo el mundo. Se utilizará la notación K_M^+ para hacer referencia a esta clave.
  - ▶Una clave privada que solo Mark conoce. Se utilizará la notación K_M^- para hacer referencia a esta clave.



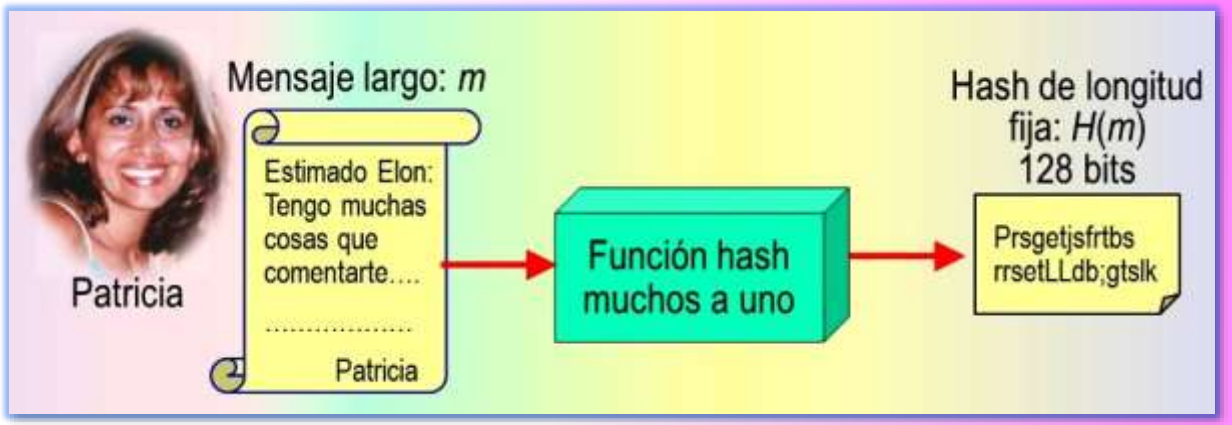
- **La figura** describe el procedimiento para el cifrado – descifrado.
- **Aunque pueden** existir algunos algoritmos que se correspondan con la descripción realizada, el algoritmo RSA (llamado así por sus inventores, R. Rivest, A. Shamir y L. Adjeman) se ha convertido casi en sinónimo de la criptografía de clave pública.
- **De hecho**, la mayor parte de los sitios web hoy integran seguridad SSL/TLS, y permiten la autenticación mediante RSA.

5.- FUNCIONES HASH CRIPTOGRÁFICAS

ESCENARIO DE RED WAN SEGURA

¿Qué hace una función hash criptográfica

(Kurose, 2017)



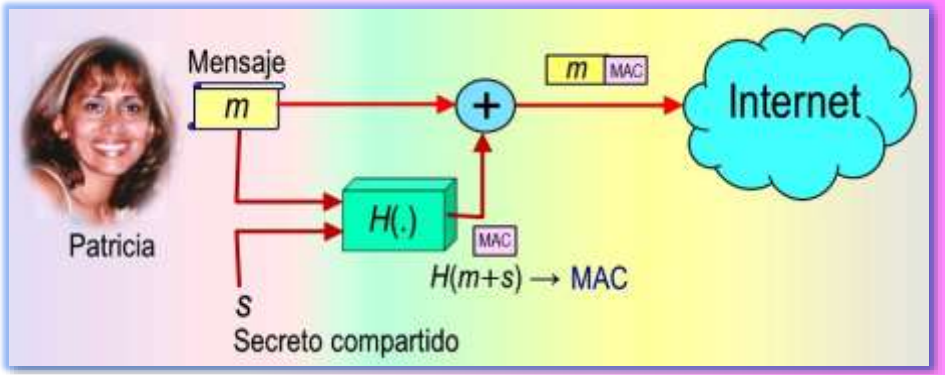
- **Una función hash** toma una entrada, *m*, y calcula una cadena de tamaño fijo *H*(*m*) conocida con el nombre de hash.
- **Cumplen** con esta definición, las técnicas utilizadas para la detección de errores, es decir, para determinar si los bits contenidos en un mensaje enviado han sido alterados según se desplazaban desde el origen hasta el destino.
- ▶**Ejemplo 4.** La suma de comprobación de Internet es un ejemplo de una función hash criptográfica. La idea de cómo funciona: suponga que los datos son una lista de cinco números de 4 bits cada uno que se quieren enviar a destino: (7, 11, 12, 0, 6).
  - ✉El emisor calcula la suma de todos los datos y envía (7, 11, 12, 0 , 6, -36), donde -36 es el valor negativo de la suma de los números originales (el complemento).
  - ✉El receptor suma todos los números recibidos (incluyendo la suma de comprobación); si el resultado es 0, asume que no hay error, acepta los cinco números y descarta la suma.
- **Una función hash** comúnmente usada toma una entrada, *m*, y calcula una cadena de tamaño fijo *H*(*m*) conocida con el nombre de hash, de 128 bits. Esta función hash criptográfica necesita exhibir la siguiente propiedad adicional:
  - ▶Es computacionalmente impracticable encontrar dos mensaje distintos *x* e *y* tales que *H*(*x*)= *H*(*y*).
- **De manera informal**, se podría decir que esta propiedad significa que es computacionalmente impracticable que un intruso sustituya un mensaje protegido mediante la función hash por otro mensaje diferente.

Funciones hash criptográficas

ESCENARIO DE RED WAN SEGURA

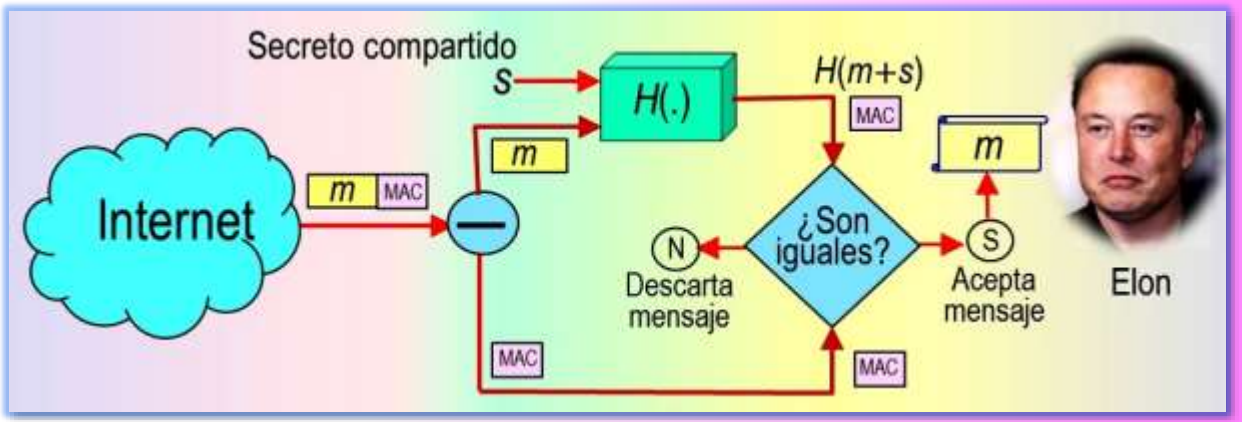
Integridad de los mensajes con funciones hash (Kurose, 2017)

- **Para garantizar** la integridad de los mensajes, además de utilizar funciones hash criptográficas Patricia y Elon necesitan un secreto compartido *s*, el cual es una cadena de bits que se denomina clave de autenticación. La figura se muestra cómo esta clave garantiza la integridad de los mensajes.



- ▶**En el emisor**, el mensaje creado por Patricia es enviado junto con el Código de Autenticación de Mensajes MAC, calculado mediante la función hash.

- ▶**En el receptor**, se separan el mensaje y el código MAC. Con el mensaje, se vuelve a crear un nuevo código MAC, el cual se compara con el recibido. Si son iguales, Elon concluye que el mensaje es íntegro y lo acepta.



- **Utilizando un Codigo MAC**, las entidades pueden autenticar los mensajes que se intercambian sin tener que incluir complejos algoritmos de cifrado en el proceso de garantía de la integridad.

- ▶**El algoritmo hash MD5** (Algoritmo de Resumen del Mensaje) de Ron Rivest (RFC 1321) se utiliza ampliamente hoy en día. Este algoritmo calcula un valor hash de 128 bits.

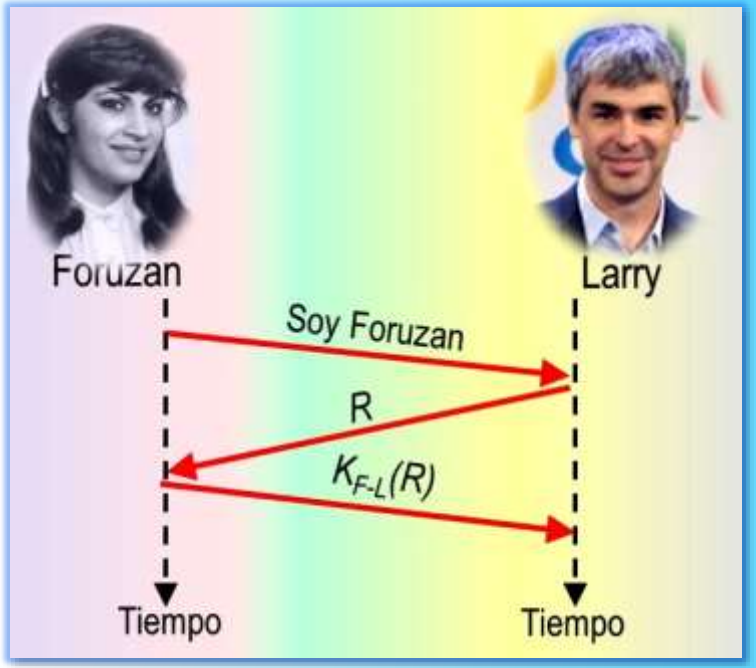
6. AUTENTICACIÓN DEL PUNTO TERMINAL

ESCENARIO DE RED WAN SEGURA

¿Qué es la autenticación del punto terminal?

(Kurose, 2017)

- **Es el proceso** de demostrar a alguien la propia identidad a través de una red. Por ejemplo, un usuario demostrando su identidad a un servidor de correo electrónico.
- **La autenticación** se realiza con base en los mensajes y datos intercambiados como parte de un protocolo de autenticación, el cual, normalmente, se ejecuta antes de que los dos interlocutores ejecuten algún otro protocolo.
- ▶**Ejemplo 5.** El uso de un número distintivo y de la criptografía de clave simétrica forma la base de un protocolo de autenticación, cuyo proceso es el siguiente;
  - ▶ **1.** Foruzan envía a Harry el mensaje "Soy Foruzan"
  - ▶**2.** Harry selecciona un número distintivo *R*, y se lo envía a Foruzan.
  - ▶**3.** Foruzan cifra el número distintivo mediante la clave secreta simétrica que comparten Foruzan y Harry, $K_{F\text{-}L}$, y devuelve el número distintivo cifrado $K_{F\text{-}L}(R)$ a Harry.
  - ▶**4.** Harry descifra el mensaje recibido. Si el número distintivo descifrado coincide con el que envió a Foruzan. Foruzan quedará autenticada.



- **El hecho** de que Foruzan conozca $K_{F\text{-}L}$ y la use para cifrar un valor, permite a Harry saber que el mensaje recibido ha sido generado por Foruzan. El número distintivo se utiliza para cerciorarse que Foruzan se está comunicando en vivo.

7.- CONEXIONES TCP SEGURAS

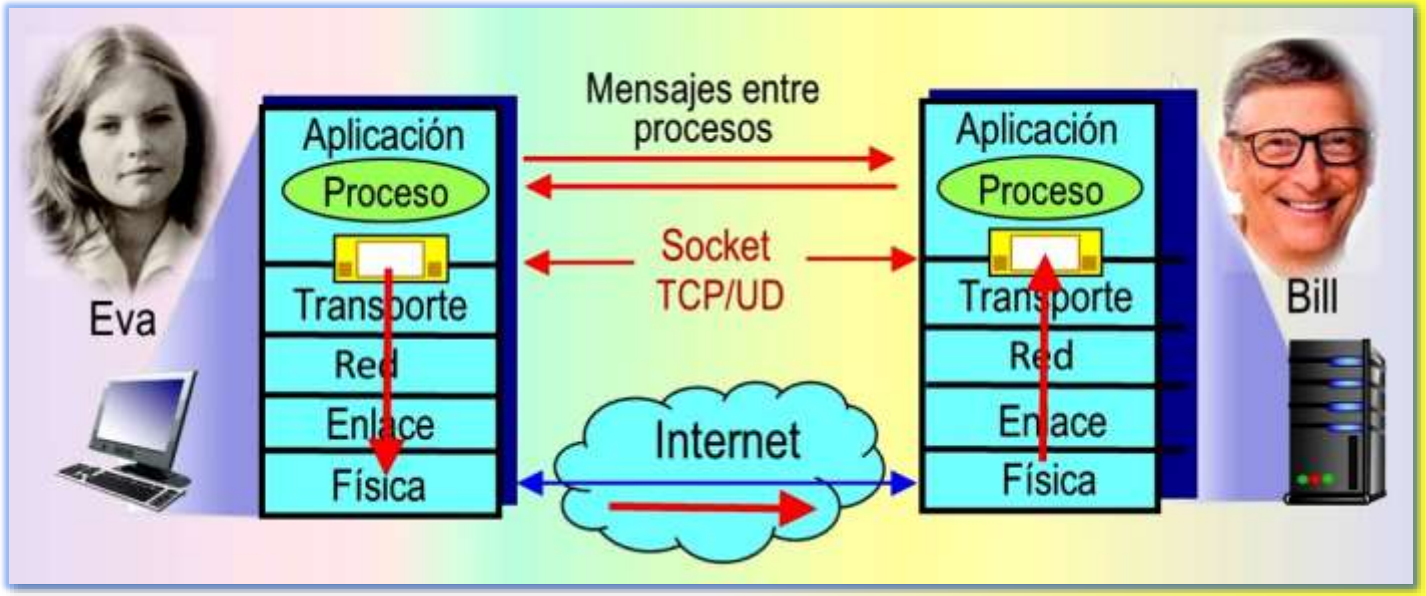
ESCENARIO DE RED WAN SEGURA

Transporte TCP seguro

(Kurose, 2017)

- **Ni TCP ni UDP** proporcionan ningún mecanismo de cifrado; los datos que el proceso emisor pasa al socket son los mismos datos que viajan a través de la red hasta el proceso de destino.

- ▶**Ejemplo 6**. Si el proceso emisor envía una contraseña en texto legible (no cifrado) a su socket, esa contraseña viajará a través de los enlaces entre el emisor y el receptor, pudiendo ser "husmeada" y descubierta en cualquiera de los enlaces intervinientes.



- **Puesto que la confidencialidad** y otras cuestiones de seguridad son críticas para muchas aplicaciones, la comunidad de Internet ha desarrollado una mejora para TCP, denominada SSL Capa de Sockets Seguros.

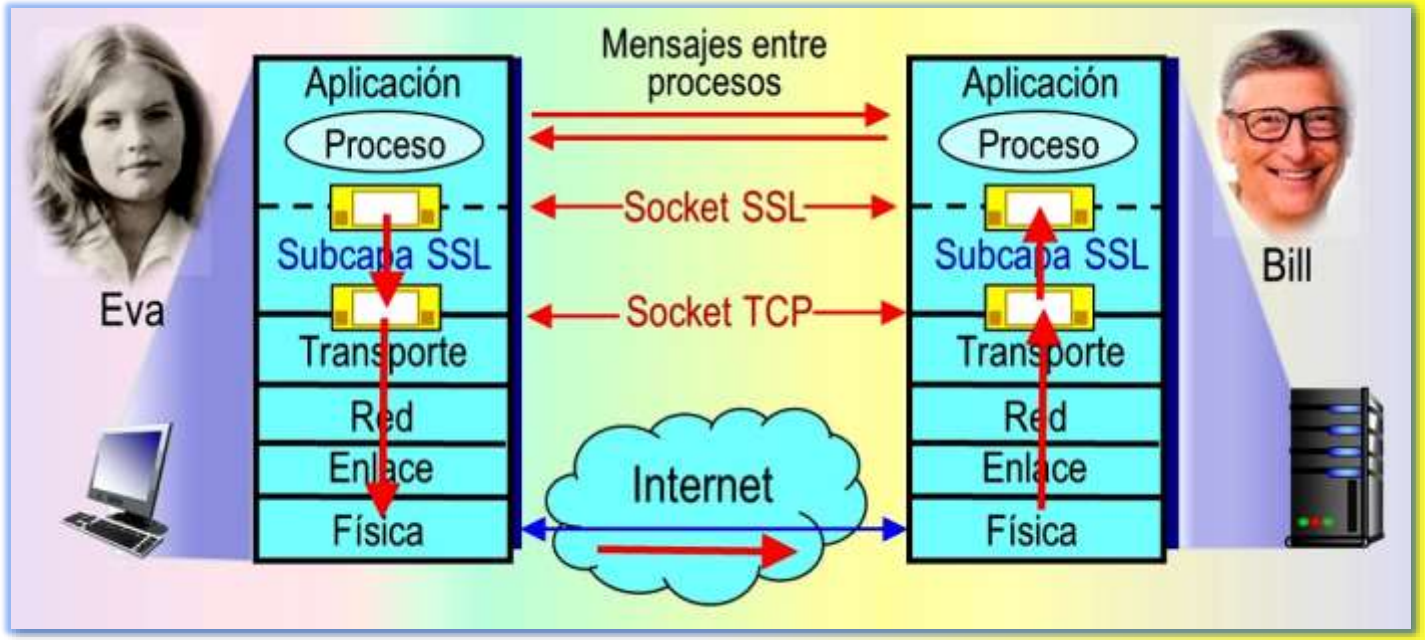
- **El TCP mejorado con SSL** no solo hace todo lo que hace el protocolo TCP tradicional, sino que también proporciona servicios críticos de seguridad proceso a proceso, entre los que se incluyen confidencialidad, integridad de los datos y autenticación del punto terminal.

Conexiones TCP seguras

ESCENARIO DE RED WAN SEGURA

El código SSL seguro

(Kurose, 2017)



- **Aunque técnicamente** SSL reside en la capa de aplicación, desde la perspectiva del desarrollador, se trata de un protocolo de la capa de transporte.
- **Se debe destacar** que SSL no es un tercer protocolo de transporte de Internet, sino que es una mejora de TCP, que se implementa en la capa de aplicación.
- **En concreto**, si una aplicación desea utilizar los servicios de SSL, tiene que incluir código SSL (existen clases y librerías optimizadas) tanto en el lado del cliente como en el del servidor de la aplicación.
  - ▶**1.** SSL tiene su propia API, Interfaz de Programación de Aplicación de Socket. Cuando una aplicación utiliza SSL; el proceso emisor pasa los datos en texto legible al socket SSL.
  - ▶**2.** A continuación, la subcapa SSL cifra los datos en el host emisor y los pasa al socket TCP.
  - ▶**3.** Los datos cifrados viajan a través de Internet hacia el socket TCP del proceso receptor.
  - ▶**4.** El socket de recepción TCP pasa los datos cifrados a la subcapa SSL, que los descifra. Por último, la subcapa SSL pasa los datos en texto legible a través de su socket SSL al proceso receptor.
- **Puede verificar** que su navegador está usando SSL viendo si el URL comienza por https: en lugar de por http:.

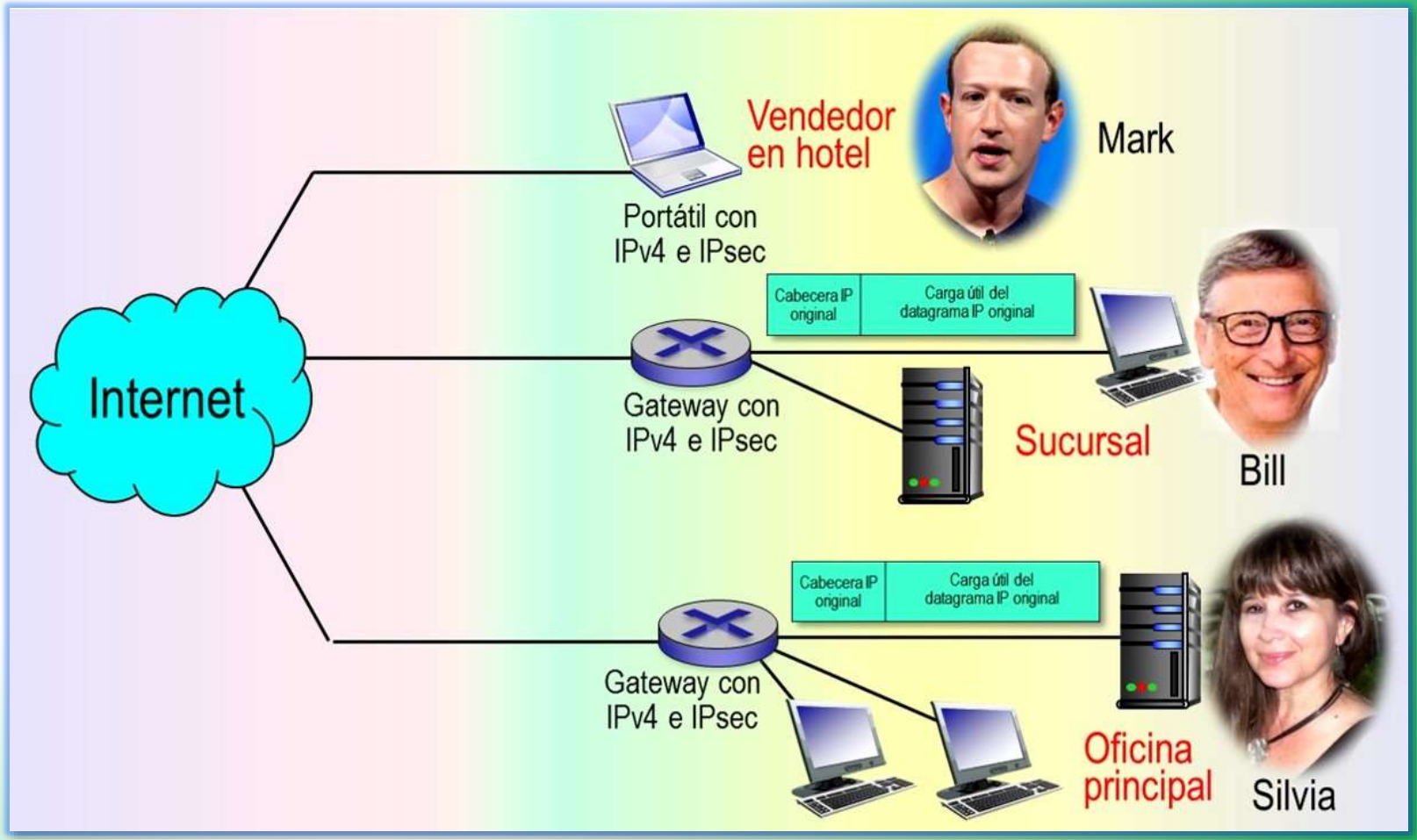
8.- VPN CON EL PROTOCOLO SEGURO IPSEC

ESCENARIO DE RED WAN SEGURA

Un ejemplo de VPN con IPsec

(Kurose, 2017)

- ▶**Ejemplo 7.** En la figura se muestra un ejemplo simple de una Red Privada Virtual (VPN). Aquí, la institución está compuesta por una oficina principal, una sucursal y una serie de vendedores itinerantes que suelen acceder a Internet desde la habitación de su hotel (solo se muestra uno de esos vendedores).
  - ✉En esta VPN, cuando dos hosts situados en la oficina principal se intercambian datagramas IP o cuando dos host de la sucursal quieren comunicarse, utilizan el protocolo simple y tradicional IPv4.

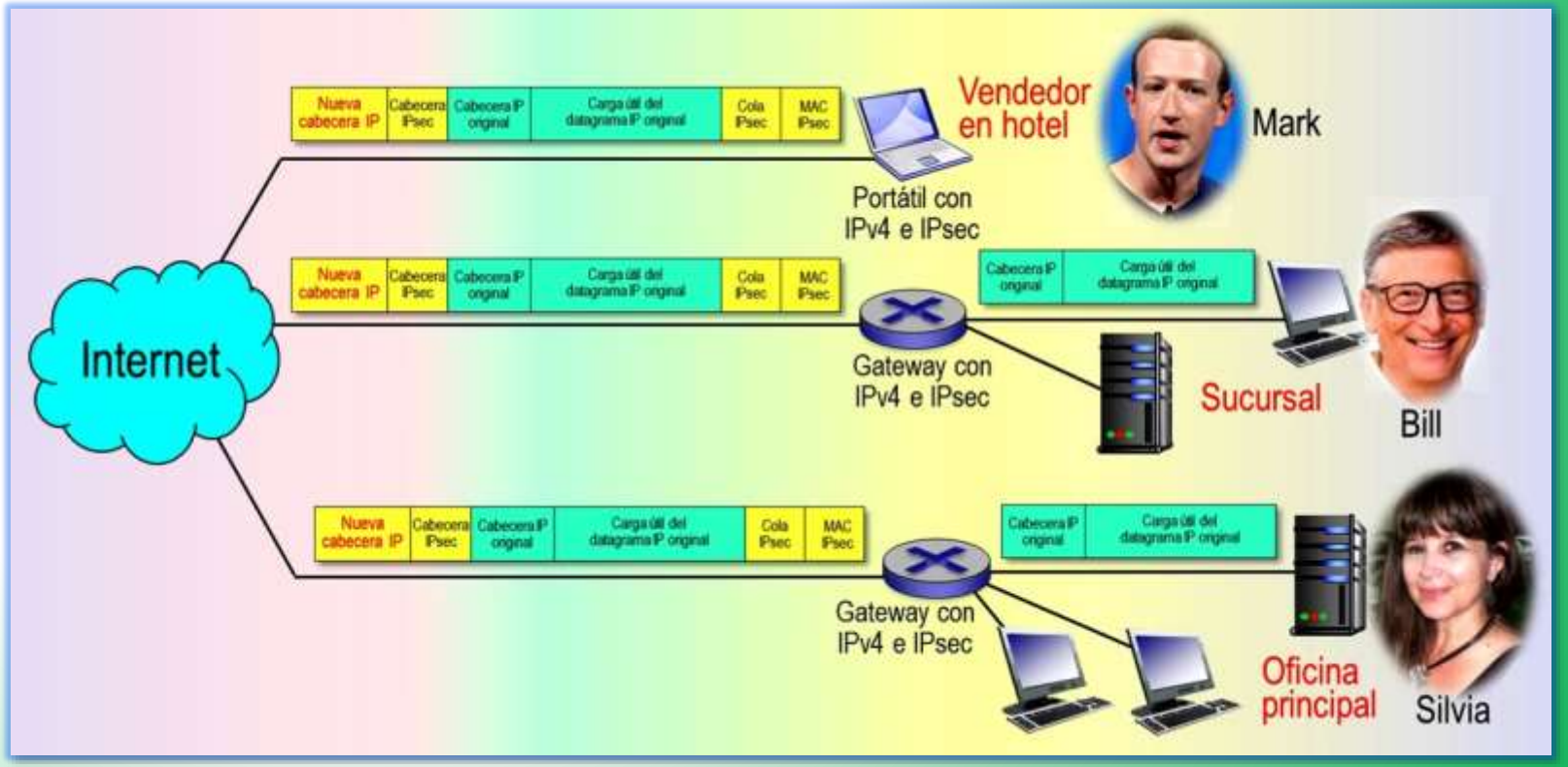


VPN con el protocolo seguro IPsec

ESCENARIO DE RED WAN SEGURA

Un ejemplo de VPN con IPsec (cont.) (Kurose, 2017)

- **Sin embargo**, cuando, por ejemplo, un host de la oficina principal (el host de Silvia) envía un datagrama IP a un vendedor (Mark) que se encuentra en un hotel, el tráfico se cifra antes de entrar a Internet.
- Este cifrado lo realiza el router gateway de la oficina principal, convirtiendo el datagrama IPv4 simple en un datagrama IPsec y luego reenvía dicho datagrama hacia Internet.
- Este datagrama IPsec tiene de hecho una nueva cabecera IPv4 tradicional, de modo que los routers de Internet procesan el datagrama como si se tratara de un datagrama IPv4 normal, para ellos el datagrama es, de hecho, como cualquier otro.



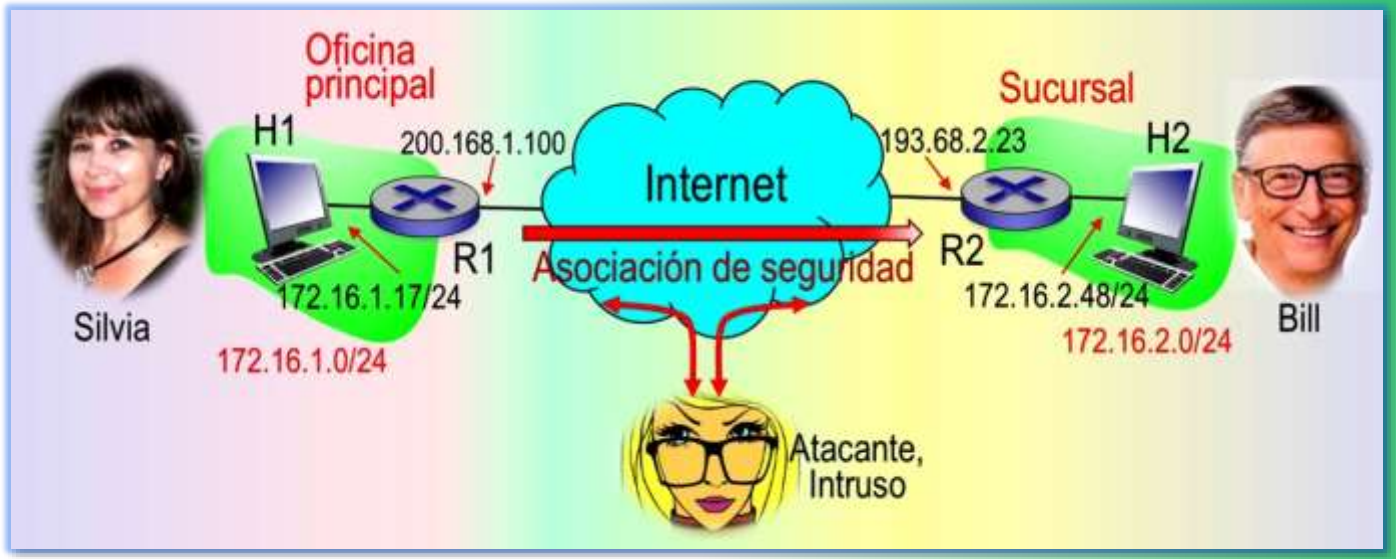
VPN con el protocolo seguro IPsec

ESCENARIO DE RED WAN SEGURA

¿Qué son las asociaciones de seguridad?

(Kurose, 2017)

- **Los datagramas IPsec** se intercambian entre parejas, como por ejemplo entre dos hosts, dos routers, o entre un host y un router.
- ▶**Ejemplo 8**. Antes de enviar datagramas IPsec, por ejemplo, desde el router de origen R1 al de destino R2, ambas crean una conexión lógica en la capa de red. Esta conexión lógica se denomina asociación de seguridad.
  - ⊠Una asociación de seguridad es una conexión lógica de tipo simple, es decir, una conexión unidireccional desde el origen al destino.
  - ⊠Si ambos routers desean enviarse datagramas seguros entre sí, entonces será necesario establecer una asociación de seguridad en cada dirección, las cuales protegerán a los datos frente a atacantes o intrusos.



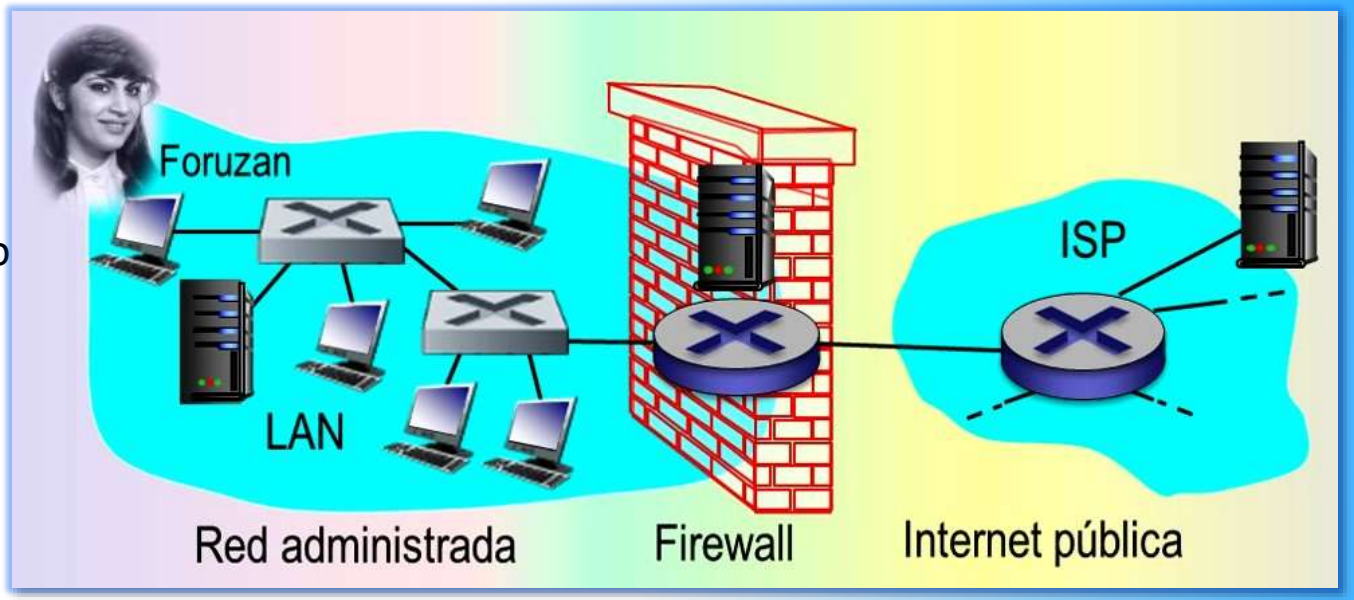
- ▶**Ejemplo 9.** Considere una VPN institucional. Esta institución consta de una oficina principal, una sucursal y un cierto número *n* de vendedores itinerantes. Suponga, que existe tráfico IPsec bidireccional entre la oficina principal y la sucursal y entre la oficina principal y los vendedores. En esta VPN, ¿cuántas asociaciones de seguridad existirán?
  - ⊠Hay dos asociaciones entre el router gateway de la oficina principal y el gateway de la sucursal (una en cada dirección).
  - ⊠Para la PC portátil de cada vendedor tambien hay dos asociaciones entre el router gateway de la oficina principal y la portátil.

ESCENARIO DE RED WAN SEGURA

¿Qué son los firewalls?

(Kurose, 2017)

- **Los firewall** son una combinación de hardware y software que aísla la red interna de la organización de Internet, permitiendo pasar a algunos paquetes y bloqueando a otros.
- **Permiten** a un administrador de red controlar el acceso desde el mundo exterior a los recursos de la red administrada.
- **Un administrador de red** configura el firewall con base en las políticas de la organización, la cual toma en cuenta la productividad del usuario y el uso de ancho de banda, así como los problemas de seguridad de una organización.



- **Cisco y Ckeck Point** son dos de las empresas líderes actuales de distribución de firewalls.
- **Un firewall** también puede crearse fácilmente a partir de una máquina Linux utilizando *iptables* (software de dominio público, que se suministra habitualmente con Linux).
- **Una organización** dispone normalmente de un router gateway que conecta su red LAN con su ISP (y por tanto con la internet publica). En este router se implementan frecuentemente los firewalls. Todo el tráfico que sale y entra de la red LAN pasa a través de este router y es en este router donde tiene lugar el filtrado de paquetes.

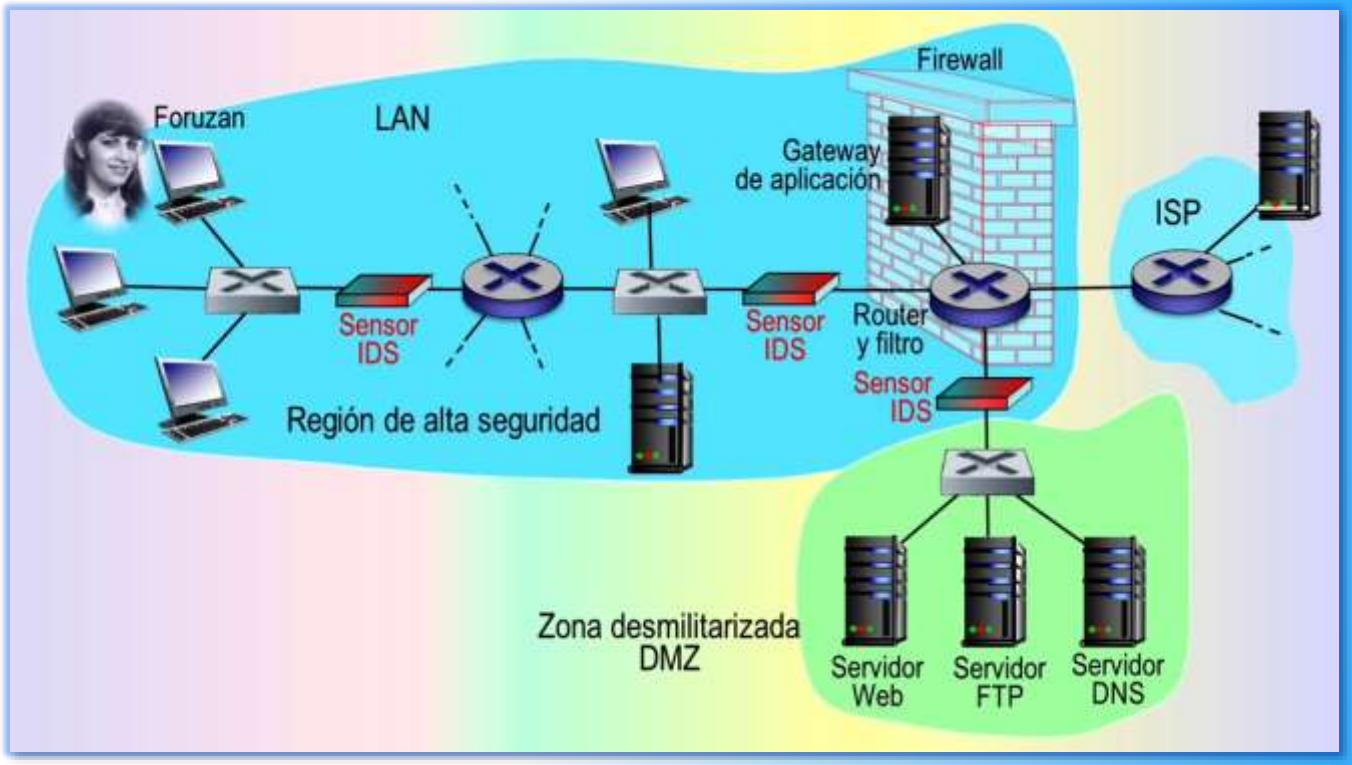
Seguridad operacional: firewalls y sensores IDS

ESCENARIO DE RED WAN SEGURA

Sistemas de detección de intrusiones IDS

(Kurose, 2017)

- **Los sistemas IDS** son dispositivos que llevan a cabo una inspección profunda de los paquetes de datos, detectan paquetes sospechosos e impiden que entren a la red de la organización para efectuar una amplia gama de ataques.
- **Actualmente**, miles de organizaciones utilizan sistemas IDS propietarios, comercializados por Cisco, Check Point principalmente. Pero muchos otros IDS son sistemas de dominio público, como el popular sistemas de IDS Snort.

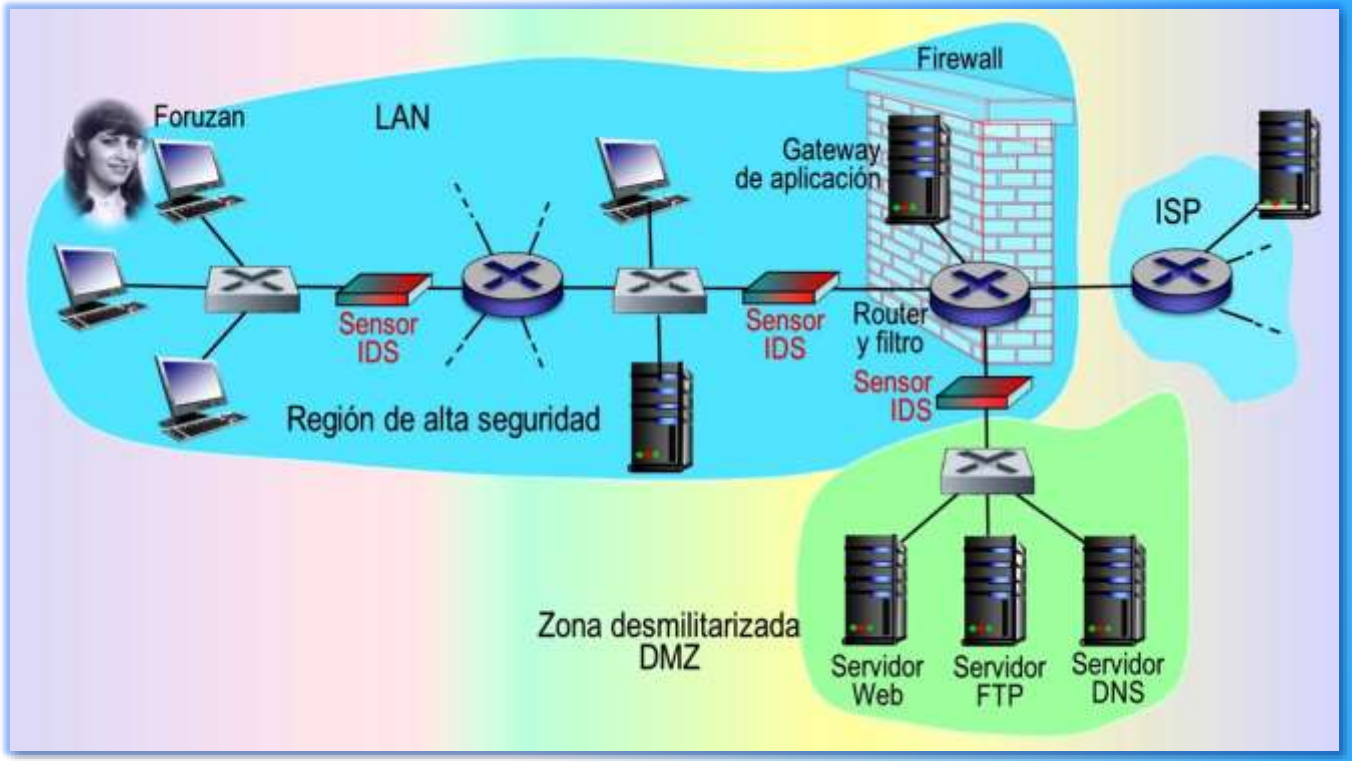


- **Una organización** puede dividir su red en dos regiones e implementar uno o más sensores IDS, a saber:
  - ▶Una región de alta seguridad, protegida por un filtro de paquetes y un gateway de aplicación y monitoreada por sensores IDS.
  - ▶Una región de menor seguridad denominada zona desmilitarizada (DMZ) que está protegida solo por el filtro de paquetes, aunque también está monitoreada mediante sensores IDS.
    - ✉La DMZ incluye los servidores de la organización que necesitan comunicarse con el mundo exterior, como su servidor web público y su servidor DNS.

Seguridad operacional: firewalls y sensores IDS

ESCENARIO DE RED WAN SEGURA

Sistemas de detección de intrusiones IDS (cont.)



Referencias bibliográficas

ESCENARIO DE RED WAN SEGURA

FIN

Referencias bibliográficas

- CISCO (2015). *CCNA Routing and Switching. Introduction to Networks*. CISCO.
- CISCO (2016). *Introducción a las redes.* Madrid: Pearson Education, S.A.
- Forouzan, B. A. (2020). *Transmisión de datos y redes de comunicaciones.* Madrid: McGraw-Hill.
- Huawei Technologies (2020). *Basics of data communication networks*. Huawei.
- Kurose, J. Keith, R. (2017). *Redes de computadoras: un enfoque descendente*. Madrid: Pearson Education, S.A.

Tema 2 de:

REDES WAN

Edison Coimbra G.