

INFOGRAFIA

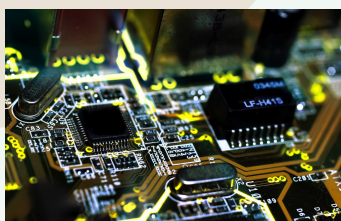
SEBASTIAN RODRIGUEZ ARCE

SALA 1:

Cuando estas navegando en línea y aparece el mensaje de "No hay internet" no es que no hay internet, ese mensaje significa que tu perdiste la conexión con el, la función de la red cambio de una red únicamente de datos a un sistema que permite conectar personas, información y dispositivos

Conforme las redes han ido avanzando hemos aprendido que hay 4 características básicas que los arquitectos de redes tienen que abordar:

- 1=Tolerancia a fallas
- 2=Escalabilidad
- 3=Calidad de servicio
- 4=Seguridad



SALA 2:

La calidad de servicio se está volviendo cada vez más importante para las redes, ya que, las nuevas aplicaciones como transmisiones de voz o de video generan grandes expectativas.

La congestión a la hora de navegar en la red se produce cuando la demanda de ancho de banda (cantidad de bits por segundo) excede la cantidad disponible. Cuando el volumen de tráfico es mayor de lo que se puede transportar, los dispositivos colocan los paquetes en cola hasta que haya recursos disponibles para transmitirlos

SALA 4:

Asegurar la infraestructura de la red incluye asegurar físicamente los dispositivos que proporcionan conectividad de red, sin embargo, los administradores de red también protegen la información guardada en los dispositivos conectados a la red.

Si queremos alcanzar los objetivos de seguridad de la red hay tres requisitos principales:

- 1-Confidencialidad: Esto se refiere a que solo los destinatarios que sean deseados puedan acceder a los datos
- 2-Integridad: Tener la seguridad de que la información no va a ser alterada
- 3-Disponibilidad: Tener la seguridad de acceder a los datos para los usuarios autorizados

SALA 3:

BYOD da la posibilidad a los usuarios de usar herramientas para acceder a la información y comunicarse a través de un campus, con el crecimiento de los dispositivos de consumo, las personas pueden tener dispositivos avanzados de redes para uso personal

BYOD Significa que se puede hacer uso de cualquier dispositivo de cualquier persona en cualquier lugar



SALA 5:

La nube nos permite hacer copias de seguridad de una unidad en servidores por medio del de Internet, se puede acceder a aplicaciones como procesamiento de texto y edición de fotos usando la.

La nube es posible gracias a los centros de datos, estos son instalaciones utilizadas para alojar componentes asociados, por lo general el mantenimiento de los centros de datos son muy costosos, por esta razón solo las grandes empresas utilizan centros de datos privados para alojar sus datos.

Por motivos principalmente de seguridad los proveedores de la nube suelen almacenar los datos en centros de datos distribuidos en diferentes ubicaciones, existen 4 tipos principales de nubes. Nubes públicas, Nubes privadas, Nubes híbridas y Nubes comunitarias

SALA 6:

Otra faceta muy importante de las redes que es crítica para el esfuerzo de comunicación y colaboración es el video el cual se usa para comunicaciones, colaboración y entretenimiento, las video llamadas se realizan desde y hacia cualquier persona con conexión a Internet, La videoconferencia es una herramienta poderosa para comunicarse con otros, tanto local como globalmente. A medida que las organizaciones se extienden más allá de los límites geográficos

SALA 7:

La tecnología inteligente en el hogar se puede ver en los electrodomésticos todos los días, como puede ser dispositivos como Alexa o bombillos inteligentes, todo esto controlado desde la comodidad de su smartphone



SALA 8:

La seguridad de la red, como anteriormente fue dicho, es una parte integral de la red informática, independientemente si la red está en un lugar con una sola conexión a Internet, asegurar la red implica protocolos, técnicas y herramientas para proteger los datos y mitigar las amenazas como lo son:

Virus gusanos y caballos de Troya: Estos contienen un software malicioso o código que se ejecuta.

Spyware: Estos son un tipo de software que se instalan en el dispositivo de un usuario y recopila en secreto información sobre el usuario

Ataques por denegación: Estos ataques ralentizan o bloquean las aplicaciones y procesos en un dispositivo de red

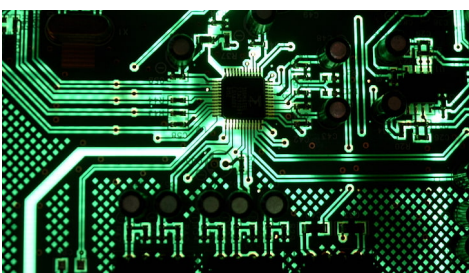
Robo de identidad: Este ataque roba las credenciales de inicio de sesión de un usuario para acceder a sus datos privados

SALA 9:

Como existen softwares que nos perjudican, tambien existen algunos que nos ayudan a evitar ese tipo de acciones, como por ejemplo lo son:

Antivirus y antispyware: Estas son aplicaciones que ayudan a proteger los dispositivos finales para que no se infecten con software malicioso

Filtrado de firewall: Este bloquea el acceso no autorizado dentro y fuera de la red, esto puede incluir un sistema de firewall ejecutado en un hostque se agrega para impedir el ingresado no autorizado a un servicio de filtrado en el router domestico



SALA 10:

Los requisitos de seguridad de la red deben tener en cuenta el entorno, así como las diversas aplicaciones y los requisitos informáticos., tanto commo el entorno doméstico como el empresarial deben poder proteger sus datos y tambien permitir la calidad de servicio que los usuarios esperan de cada tecnología, la solución de seguridad implementada debe poder adaptarse a las crecientes tendencias de red, estas deberian de cambiarse con frecuencia para mejorar la seguridad